

NOTA INFORMATIVA EN RELACIÓN CON LA PUBLICACIÓN DE LOS TEMARIOS DE LOS PROCESOS SELECTIVOS CONVOCADOS POR LA XUNTA DE GALICIA EN EL DIARIO OFICIAL DE GALICIA Nº 142 DE 26 /07/11

El Diario Oficial de Galicia nº 142, de 26 de julio de 2011, publica distintas órdenes de la Consellería de Facenda por las que se convocan diferentes procesos selectivos para el ingreso en la Administración autonómica de Galicia.

Cumpliendo con el compromiso adquirido, la EGAP, continúa con la publicación de los temarios correspondientes a los distintos procesos selectivos convocados formalmente.

Teniendo en cuenta, por una parte, el volumen y complejidad en la elaboración de un material didáctico que sirva de referencia básica y, por otra, el interés de la EGAP para que los posibles usuarios dispongan a la mayor brevedad posible de dicho material, la publicación del mismo en la página web de la Escuela (<http://egap.xunta.es>), se irá produciendo de la siguiente manera:

- 1) **Legislación**, actualizada y consolidada a la fecha de publicación en el DOG del nombramiento del tribunal del proceso (Base II.1 de la convocatoria¹), correspondiente a los procesos selectivos para el ingreso en el cuerpo superior de la Administración de la Xunta de Galicia, subgrupo A1; cuerpo de gestión de la Administración de la Xunta de Galicia, subgrupo A2; cuerpo superior de la Administración de la Xunta de Galicia, subgrupo A1, escala de sistemas y tecnología de la información; cuerpo de gestión de la Administración de la Xunta de Galicia, subgrupo A2, escala de gestión y sistemas de información y cuerpo auxiliar de la Xunta de Galicia, subgrupo C2.

La fecha prevista para dicha publicación es de 5 de agosto de 2011.

- 2) **Temarios específicos**, se irán publicando en la página web de la Escuela, a medida que los procesos de elaboración y revisión vayan concluyendo.

Sin perjuicio de su publicación en las dos lenguas oficiales y a fin de facilitar a la mayor brevedad posible este material a los usuarios, los temas se irán publicando en la web en el idioma originalmente utilizado por cada uno de los autores.

Para mayor información se pueden poner en contacto con el servicio de Estudios y Publicaciones a través del correo electrónico temarios.egap@xunta.es, y teléfono 881 997 251.

La Escuela reitera que los temarios por ella facilitados no tienen carácter oficial, por lo que en ningún caso vincularán a los opositores o a los tribunales; sino que se trata de instrumentos complementarios que servirán de apoyo y ayuda como textos de referencia pero nunca de forma exclusiva y excluyente.

Santiago de Compostela, 4 de agosto de 2011

¹ II. Proceso selectivo.

II.1. Procedimiento de oposición.

(...) Se tendrán en cuenta las normas de derecho positivo relacionadas con el contenido del programa que en el momento de publicación en el DOG del nombramiento del tribunal del proceso cuenten con publicación oficial en el boletín o diario correspondiente.

**1. GOBERNANZA DE LAS TIC.
PLANIFICACIÓN, DIRECCIÓN Y
CONTROL DE LAS TIC. COBIT
(«CONTROL OBJECTIVES FOR
INFORMATION AND RELATED
TECHNOLOGY»), OBJETIVOS
DE CONTROL Y MÉTRICAS.
PROPUESTAS DE PROYECTOS
(CASOS DE NEGOCIO O
«BUSINESS CASE»), ANÁLISIS
DE COSTES/ BENEFICIOS,
ANÁLISES DE RIESGOS,
FACTORES CRÍTICOS DE
ÉXITO. VALIT.**

Tema 1. Gobernanza de las TIC. Planificación, dirección y control de las TIC. CoBIT («Control Objectives for Information and Related Technology»), objetivos de control y métricas. Propuestas de proyectos (casos de negocio o «business case»), análisis de costes/beneficios, análisis de riesgos, factores críticos de éxito. ValIT.

INDICE

- 1.1 Gobernanza de las TIC. Planificación, dirección y control de las TIC.
- 1.2 CoBIT («Control Objectives for Information and related Technology»), objetivos de control y métricas.
 - 1.2.1 Marco de trabajo COBIT
 - 1.2.1.1 Orientado al negocio
 - 1.2.1.2 Orientado a procesos
 - 1.2.1.3 Basado en controles
 - 1.2.1.4 Impulsado por la medición
 - 1.2.2 Modelos de madurez
 - 1.2.3 Medición del desempeño
- 1.3 Propuestas de proyectos (casos de negocio o “business case”), análisis de costos/beneficios, análisis de riesgos, factores críticos de éxito. ValIT.
 - 1.3.1 Introducción
 - 1.3.1.1 Objetivo de ValIT
 - 1.3.1.2 La necesidad de ValIT
 - 1.3.1.3 Una nueva perspectiva
 - 1.3.2 El marco ValIT
 - 1.3.2.1 Principios de ValIT
 - 1.3.2.2 Procesos de ValIT
 - 1.3.3 ValIT. El caso de negocio
 - 1.3.3.1 Introducción: La importancia del caso de negocio
 - 1.3.3.2 Estructura del caso de negocio

1.1 GOBERNANZA DE LAS TIC. PLANIFICACIÓN, DIRECCIÓN Y CONTROL DE LAS TIC.

Gobernanza de las TIC es la alineación de las Tecnologías de la información y la comunicación (TIC) con la estrategia del negocio. Hereda las metas y la estrategia a todos los departamentos de la empresa, y provee el mejor uso de la tecnología y de sus estructuras organizacionales para alcanzarlas.

Para muchas empresas, la información y la tecnología que las soportan representan sus más valiosos activos, aunque con frecuencia son poco entendidos. Las empresas exitosas reconocen los beneficios de la tecnología de información y la utilizan para impulsar el valor de sus interesados (stakeholders). Estas empresas también entienden y administran los riesgos asociados, tales como el aumento en requerimientos regulatorios, así como la dependencia crítica de muchos procesos de negocio en TI.

La necesidad del aseguramiento del valor de TI, la administración de los riesgos asociados a TI, así como el incremento de requerimientos para controlar la información, se entienden ahora como elementos clave del Gobierno Corporativo. El valor, el riesgo y el control constituyen la esencia del gobierno de TI.

El gobierno de TI es responsabilidad de los ejecutivos, del consejo de directores y consta de liderazgo, estructuras y procesos organizacionales que garantizan que TI en la empresa sostiene y extiende las estrategias y objetivos organizacionales. Más aún, el gobierno de TI integra e institucionaliza las buenas prácticas para garantizar que TI en la empresa soporta los objetivos del negocio. De esta manera, el gobierno de TI facilita que la empresa aproveche al máximo su información, maximizando así los

beneficios, capitalizando las oportunidades y ganando ventajas competitivas.

Las organizaciones deben satisfacer la calidad, los requerimientos fiduciarios y de seguridad de su información, así como de todos sus activos. La dirección también debe optimizar el uso de los recursos disponibles de TI, incluyendo aplicaciones, información, infraestructura y personas. Para descargar estas responsabilidades, así como para lograr sus objetivos, la dirección debe entender el estatus de su arquitectura empresarial para TI y decidir qué tipo de gobierno y de control debe aplicar.

1.2 CoBIT («CONTROL OBJECTIVES FOR INFORMATION AND RELATED TECHNOLOGY»), OBJETIVOS DE CONTROL Y MÉTRICAS.

Para que TI tenga éxito en satisfacer los requerimientos del negocio, la dirección debe implementar un sistema de control interno o un marco de trabajo. El marco de trabajo de control COBIT contribuye a estas necesidades de la siguiente manera:

- Estableciendo un vínculo con los requerimientos del negocio
- Organizando las actividades de TI en un modelo de procesos generalmente aceptado
- Identificando los principales recursos de TI a ser utilizados
- Definiendo los objetivos de control gerenciales a ser considerados

La orientación al negocio que enfoca COBIT consiste en alinear las metas de negocio con las metas de TI, brindando métricas y modelos de madurez para medir sus logros, e identificando las responsabilidades asociadas de los dueños de los procesos de negocio y de TI.

El enfoque hacia procesos de COBIT se ilustra con un modelo de procesos, el cual subdivide TI en 34 procesos de acuerdo a las áreas de responsabilidad de planear, construir, ejecutar y monitorear, ofreciendo una visión de punta a punta de la TI. Los conceptos de arquitectura empresarial ayudan a identificar aquellos recursos esenciales para el éxito de los procesos, es decir, aplicaciones, información, infraestructura y personas.

En resumen, para proporcionar la información que la empresa necesita para lograr sus objetivos, los recursos de TI deben ser administrados por un conjunto de procesos agrupados de forma natural.

Pero, ¿cómo puede la empresa poner bajo control TI de tal manera que genere la información que la empresa necesita? ¿Cómo puede administrar los riesgos y asegurar los recursos de TI de los cuales depende tanto? ¿Cómo puede la empresa asegurar que TI logre sus objetivos y soporte los del negocio? Primero, la dirección requiere objetivos de control que definan la meta final de implementar políticas, procedimientos, prácticas y estructuras organizacionales diseñadas para brindar un aseguramiento razonable de que:

- Se alcancen los objetivos del negocio.
- Se prevengan o se detecten y corrijan los eventos no deseados.

En segundo lugar, en los complejos ambientes de hoy en día, la dirección busca continuamente información oportuna y condensada, para tomar decisiones difíciles respecto a riesgos y controles, de manera rápida y exitosa. ¿Qué se debe medir y cómo? Las empresas requieren una medición objetiva de dónde se encuentran y dónde se requieren mejoras, y deben implementar una caja de herramientas gerenciales para monitorear esta mejora.

Una respuesta a los requerimientos de determinar y monitorear el nivel apropiado de control y desempeño de TI son las definiciones específicas de COBIT de los siguientes conceptos:

- Benchmarking de la capacidad de los procesos de TI, expresada como modelos de madurez, derivados del Modelo de Madurez de la Capacidad del Instituto de Ingeniería de Software
- Metas y métricas de los procesos de TI para definir y medir sus resultados y su desempeño, basados en los principios de Balanced Scorecard de Negocio de Robert Kaplan y David Norton
- Metas de actividades para controlar estos procesos, con base en los objetivos de control detallados de COBIT

La evaluación de la capacidad de los procesos basada en los modelos de madurez de COBIT es una parte clave de la implementación del gobierno de TI.

Después de identificar los procesos y controles críticos de TI, el modelo de madurez permite identificar y demostrar a la dirección las brechas en la capacidad. Entonces se pueden crear planes de acción para llevar estos procesos hasta el nivel objetivo de capacidad deseado.

COBIT da soporte al gobierno de TI al brindar un marco de trabajo que garantiza que:

- TI está alineada con el negocio
- TI habilita al negocio y maximiza los beneficios
- Los recursos de TI se usan de manera responsable
- Los riesgos de TI se administran apropiadamente

La medición del desempeño es esencial para el gobierno de TI. COBIT le da soporte e incluye el establecimiento y el monitoreo de objetivos que

se puedan medir, referentes a lo que los procesos de TI requieren generar (resultado del proceso) y cómo lo generan (capacidad y desempeño del proceso). Muchos estudios han identificado que la falta de transparencia en los costos, valor y riesgos de TI, es uno de los más importantes impulsores para el gobierno de TI. Mientras las otras áreas consideradas contribuyen, la transparencia se logra de forma principal por medio de la medición del desempeño.

Estas áreas de enfoque de gobierno de TI describen los tópicos en los que la dirección ejecutiva requiere poner atención para gobernar a TI en sus empresas. La dirección operacional usa procesos para organizar y administrar las actividades cotidianas de TI.

COBIT brinda un modelo de procesos genéricos que representa todos los procesos que normalmente se encuentran en las funciones de TI, ofreciendo un modelo de referencia común entendible para los gerentes operativos de TI y del negocio. Se establecieron equivalencias entre los modelos de procesos COBIT y las áreas de enfoque del gobierno de TI, ofreciendo así un puente entre lo que los gerentes operativos deben realizar y lo que los ejecutivos desean gobernar.

Para lograr un gobierno efectivo, los ejecutivos esperan que los controles a ser implementados por los gerentes operativos se encuentren dentro de un marco de control definido para todo los procesos de TI. Los objetivos de control de TI de COBIT están organizados por proceso de TI; por lo tanto, el marco de trabajo brinda una alineación clara entre los requerimientos de gobierno de TI, los procesos de TI y los controles de TI.

COBIT se enfoca en qué se requiere para lograr una administración y un control adecuado de TI, y se posiciona en un nivel alto. COBIT ha sido alineado y armonizado con otros estándares y mejores prácticas más detallados de TI. COBIT actúa como un integrador de todos estos

materiales guía, resumiendo los objetivos clave bajo un mismo marco de trabajo integral que también se alinea con los requerimientos de gobierno y de negocios.

COSO (y marcos de trabajo compatibles similares) es generalmente aceptado como el marco de trabajo de control interno para las empresas. COBIT es el marco de trabajo de control interno generalmente aceptado para TI. Los productos COBIT se han organizado en tres niveles diseñados para dar soporte a:

- Administración y consejos ejecutivos
- Administración del negocio y de TI
- Profesionales en Gobierno, aseguramiento, control y seguridad.

COBIT es un marco de referencia y un juego de herramientas de soporte que permiten a la gerencia cerrar la brecha con respecto a los requerimientos de control, temas técnicos y riesgos de negocio, y comunicar ese nivel de control a los Interesados.

COBIT constantemente se actualiza y armoniza con otros estándares. Por lo tanto, COBIT se ha convertido en el integrador de las mejores prácticas de TI y el marco de referencia general para el gobierno de TI que ayuda a comprender y administrar los riesgos y beneficios asociados con TI.

La estructura de procesos de COBIT y su enfoque de alto nivel orientado al negocio brindan una visión completa de TI y de las decisiones a tomar acerca de la misma.

Los beneficios de implementar COBIT como marco de referencia de gobierno sobre TI incluyen:



- Mejor alineación, con base en su enfoque de negocios
- Una visión, entendible para la gerencia, de lo que hace TI
- Propiedad y responsabilidades claras, con base en su orientación a procesos
- Aceptación general de terceros y reguladores
- Entendimiento compartido entre todos los Interesados, con base en un lenguaje común
- Cumplimiento de los requerimientos COSO para el ambiente de control de TI

1.2.1 MARCO DE TRABAJO COBIT

El marco de trabajo COBIT se creó con las características principales de ser orientado a negocios, orientado a procesos, basado en controles e impulsado por mediciones.

1.2.1.1 ORIENTADO AL NEGOCIO

La orientación a negocios es el tema principal de COBIT. Está diseñado para ser utilizado no sólo por proveedores de servicios, usuarios y auditores de TI, sino también y principalmente, como guía integral para la gerencia y para los dueños de los procesos de negocio.

El marco de trabajo COBIT se basa en el siguiente principio: Para proporcionar la información que la empresa requiere para lograr sus objetivos, la empresa necesita invertir en, y administrar y controlar los recursos de TI usando un conjunto estructurado de procesos que provean los servicios que entregan la información empresarial requerida.

1.2.1.2 ORIENTADO A PROCESOS

COBIT define las actividades de TI en un modelo genérico de procesos organizado en cuatro dominios. Estos dominios son Planear y Organizar, Adquirir e Implementar, Entregar y Dar Soporte y Monitorear y Evaluar. Los dominios se equiparan a las áreas tradicionales de TI de planear, construir, ejecutar y monitorear. El marco de trabajo de COBIT proporciona un modelo de procesos de referencia y un lenguaje común para que todos en la empresa visualicen y administren las actividades de TI. La incorporación de un modelo operativo y un lenguaje común para todas las partes de un negocio involucradas en TI es uno de los pasos iniciales más importantes hacia un buen gobierno. También brinda un marco de trabajo para la medición y monitoreo del desempeño de TI, comunicándose con los proveedores de servicios e integrando las mejores prácticas de administración. Un modelo de procesos fomenta la propiedad de los procesos, permitiendo que se definan las responsabilidades.

PLANEAR Y ORGANIZAR (PO)

Este dominio cubre las estrategias y las tácticas, y tiene que ver con identificar la manera en que TI puede contribuir de la mejor manera al logro de los objetivos del negocio. Además, la realización de la visión estratégica requiere ser planeada, comunicada y administrada desde diferentes perspectivas. Finalmente, se debe implementar una estructura organizacional y una estructura tecnológica apropiada. Este dominio cubre los siguientes cuestionamientos típicos de la gerencia:

- ¿Están alineadas las estrategias de TI y del negocio?
- ¿La empresa está alcanzando un uso óptimo de sus recursos?
- ¿Entienden todas las personas dentro de la organización los objetivos de TI?
- ¿Se entienden y administran los riesgos de TI?
- ¿Es apropiada la calidad de los sistemas de TI para las necesidades del negocio?

ADQUIRIR E IMPLEMENTAR (AI)

Para llevar a cabo la estrategia de TI, las soluciones de TI necesitan ser identificadas, desarrolladas o adquiridas así como implementadas e integradas en los procesos del negocio. Este dominio cubre los siguientes cuestionamientos de la gerencia:

- ¿Es probable que los nuevos proyectos generen soluciones que satisfagan las necesidades del negocio?
- ¿Es probable que los nuevos proyectos sean entregados a tiempo y dentro del presupuesto?
- ¿Trabajarán adecuadamente los nuevos sistemas una vez sean implementados?
- ¿Los cambios no afectarán a las operaciones actuales del negocio?

ENTREGAR Y DAR SOPORTE (DS)

Este dominio cubre la entrega en sí de los servicios requeridos, lo que incluye la prestación del servicio, la administración de la seguridad y de la continuidad, el soporte del servicio a los usuarios, la administración de los datos y de las instalaciones operativas.

Por lo general cubre las siguientes preguntas de la gerencia:

- ¿Se están entregando los servicios de TI de acuerdo con las prioridades del negocio?
- ¿Están optimizados los costos de TI?
- ¿Es capaz la fuerza de trabajo de utilizar los sistemas de TI de manera productiva y segura?
- ¿Están implantadas de forma adecuada la confidencialidad, la integridad y la disponibilidad?

MONITOREAR Y EVALUAR (ME)

Todos los procesos de TI deben evaluarse de forma regular en el tiempo en cuanto a su calidad y cumplimiento de los requerimientos de control. Este dominio abarca la administración del desempeño, el

monitoreo del control interno, el cumplimiento regulatorio y la aplicación del gobierno. Por lo general abarca las siguientes preguntas de la gerencia:

- ¿Se mide el desempeño de TI para detectar los problemas antes de que sea demasiado tarde?
- ¿La Gerencia garantiza que los controles internos son efectivos y eficientes?
- ¿Puede vincularse el desempeño de lo que TI ha realizado con las metas del negocio?
- ¿Se miden y reportan los riesgos, el control, el cumplimiento y el desempeño?

A lo largo de estos cuatro dominios, COBIT ha identificado 34 procesos de TI generalmente usados. Mientras la mayoría de las empresas ha definido las responsabilidades de planear, construir, ejecutar y monitorear para TI, y la mayoría tienen los mismos procesos clave, pocas tienen la misma estructura de procesos o le aplicaran todos los 34 procesos de COBIT. COBIT proporciona una lista completa de procesos que puede ser utilizada para verificar que se completan las actividades y responsabilidades; sin embargo, no es necesario que apliquen todas, y, aun más, se pueden combinar como se necesite por cada empresa.

Para cada uno de estos 34 procesos tiene un enlace a las metas de negocio y TI que soporta. Información de cómo se pueden medir las metas, también se proporcionan cuáles son sus actividades clave y entregables principales, y quién es el responsable de ellas.

1.2.1.3 BASADO EN CONTROLES

COBIT define objetivos de control para los 34 procesos, así como para el proceso general y los controles de aplicación.

Control se define como las políticas, procedimientos, prácticas y estructuras organizacionales diseñadas para brindar una seguridad razonable de que los objetivos de negocio se alcanzarán, y los eventos no deseados serán prevenidos o detectados y corregidos.

La gerencia de operaciones usa los procesos para organizar y administrar las actividades de TI en curso. COBIT brinda un modelo genérico de procesos que representa todos los procesos que normalmente se encuentran en las funciones de TI, proporcionando un modelo de referencia general y entendible para la gerencia de operaciones de TI y para la gerencia de negocios. Para lograr un gobierno efectivo, los gerentes de operaciones deben implementar los controles necesarios dentro de un marco de control definido para todos los procesos TI. Ya que los objetivos de control de TI de COBIT están organizados por procesos de TI, el marco de trabajo brinda vínculos claros entre los requerimientos de gobierno de TI, los procesos de TI y los controles de TI.

Cada uno de los procesos de TI de COBIT tiene un objetivo de control de alto nivel y varios objetivos de control detallados. Como un todo, representan las características de un proceso bien administrado.

Los objetivos de control detallados se identifican por dos caracteres que representan el dominio (PO, AI, DS y ME) más un número de proceso y un número de objetivo de control. Además de los objetivos de control detallados, cada proceso COBIT tiene requerimientos de control genéricos que se identifican con PCn, que significa Control de Proceso número. Se deben tomar como un todo junto con los objetivos de control del proceso para tener una visión completa de los requerimientos de control.

PC1 Metas y Objetivos del Proceso

Definir y comunicar procesos, metas y objetivos específicos, medibles, accionables, reales, orientados a resultado y en tiempo (SMARRT

) para la ejecución efectiva de cada proceso de TI, asegurando que están enlazados a las metas de negocio y se soportan por métricas adecuadas.

PC2 Propiedad del Proceso

Asignar un dueño para cada proceso de TI, y definir claramente los roles y responsabilidades del dueño del proceso. Incluye, por ejemplo, responsabilidad del diseño del proceso, interacción con otros procesos, rendición de cuentas de los resultados finales, medición del desempeño del proceso y la identificación de mejora de las oportunidades.

PC3 Proceso Repetible

Diseñar y establecer cada proceso clave de TI de tal manera que sea repetible y consecuentemente produzca los resultados esperados. Proveer una secuencia lógica pero flexible y escalable de actividades que lleve a los resultados deseados y que sea lo suficientemente ágil para manejar las excepciones y emergencias. Usar procesos consistentes, cuando sea posible, y ajustarlos sólo cuando no se pueda evitar.

PC4 Roles y Responsabilidades

Definir las actividades clave y entregables finales del proceso. Asignar y comunicar roles y responsabilidades no ambiguas para la ejecución efectiva y eficiente de las actividades clave y su documentación, así como la rendición de cuentas para los entregables finales del proceso.

PC5 Políticas, Planes y Procedimientos

Definir y comunicar cómo todas las políticas, planes y procedimientos que dirigen los procesos de TI están documentados, revisados, mantenidos, aprobados, almacenados, comunicados y usados para el entrenamiento. Asignar responsabilidades para cada una de estas actividades y, en momentos oportunos, revisar si se ejecutan correctamente. Asegurar que las políticas, planes y procedimientos son accesibles, correctos, entendidos y actualizados

PC6 Desempeño del Proceso

Identificar un conjunto de métricas que proporcionen visión de las salidas y el desempeño del proceso. Establecer objetivos que se reflejen en las metas del proceso y los indicadores de desempeño de tal manera que permitan el logro de las metas de los procesos.

1.2.1.4 IMPULSADO POR LA MEDICIÓN

Una necesidad básica de toda empresa es entender el estado de sus propios sistemas de TI y decidir qué nivel de administración y control debe proporcionar. Para decidir el nivel correcto, la gerencia debe preguntarse: ¿Hasta dónde debemos ir?, y ¿está el costo justificado por el beneficio?

La obtención de una visión objetiva del nivel de desempeño propio de una empresa no es sencilla. ¿Qué se debe medir y cómo? Las empresas deben medir dónde se encuentran y dónde se requieren mejoras, e implementar un juego de herramientas gerenciales para monitorear esta mejora. COBIT atiende estos temas a través de:

- Modelos de madurez que facilitan la evaluación por medio de benchmarking y la identificación de las mejoras necesarias en la capacidad
- Metas y mediciones de desempeño para los procesos de TI, que demuestran cómo los procesos satisfacen las necesidades del negocio y de TI, y cómo se usan para medir el desempeño de los procesos internos basados en los principios de un marcador de puntuación balanceado (balanced scorecard)
- Metas de actividades para facilitar el desempeño efectivo de los procesos

1.2.2 MODELOS DE MADUREZ



Cada vez con más frecuencia se les pide a los directivos de empresas corporativas y públicas que consideren cómo de bien se está administrando TI. Como respuesta a esto, se debe desarrollar un plan de negocio para mejorar y alcanzar el nivel apropiado de administración y control sobre la infraestructura de información. Aunque pocos argumentarían que esto no es algo bueno, se debe considerar el equilibrio del costo/beneficio y estas preguntas relacionadas:

- ¿Qué está haciendo nuestra competencia en la industria, y cómo estamos posicionados en relación a ellos?
- ¿Cuáles son las mejores prácticas aceptables en la industria, y cómo estamos posicionados con respecto a estas prácticas?
- En base a estas comparaciones, ¿se puede decir que estamos haciendo lo suficiente?
- ¿Cómo identificamos lo que se requiere hacer para alcanzar un nivel adecuado de administración y control sobre nuestros procesos de TI?

Puede resultar difícil proporcionar respuestas significativas a estas preguntas. La gerencia de TI está buscando constantemente herramientas de evaluación para benchmarking y herramientas de auto-evaluación como respuesta a la necesidad de saber qué hacer de manera eficiente. Comenzando con los procesos y los objetivos de control de alto nivel de COBIT, el dueño del proceso se debe poder evaluar de forma progresiva contra los objetivos de control. Esto responde a tres necesidades:

1. Una medición relativa de dónde se encuentra la empresa
2. Una manera de decidir hacia dónde ir de forma eficiente
3. Una herramienta para medir el avance contra la meta

El modelo de madurez para la administración y el control de los procesos de TI se basa en un método de evaluación de la organización, de tal forma que se pueda evaluar a sí misma desde un nivel de no-existente



(0) hasta un nivel de optimizado (5). Este enfoque se deriva del modelo de madurez que el Software Engineering Institute definió para la madurez de la capacidad del desarrollo de software. Cualquiera que sea el modelo, las escalas no deben ser demasiado granulares, ya que eso haría que el sistema fuera difícil de usar y sugeriría una precisión que no es justificable debido a que en general, el fin es identificar dónde se encuentran los problemas y cómo fijar prioridades para las mejoras. El propósito no es evaluar el nivel de adherencia a los objetivos de control.

Los niveles de madurez están diseñados como perfiles de procesos de TI que una empresa reconocería como descripciones de estados posibles actuales y futuros. No están diseñados para ser usados como un modelo limitante, donde no se puede pasar al siguiente nivel superior sin haber cumplido todas las condiciones del nivel inferior. Con los modelos de madurez de COBIT, a diferencia de la aproximación del CMM original de SEI, no hay intención de medir los niveles de forma precisa o probar a certificar que un nivel se ha conseguido con exactitud. Una evaluación de la madurez de COBIT resultara en un perfil donde las condiciones relevantes a diferentes niveles de madurez se han conseguido.

1.2.3 MEDICIÓN DEL DESEMPEÑO

Las métricas y las metas se definen en COBIT a tres niveles:

- Las metas y métricas de TI que definen lo que el negocio espera de TI (lo que el negocio usaría para medir a TI)
- Metas y métricas de procesos que definen lo que el proceso de TI debe generar para dar soporte a los objetivos de TI (cómo sería medido el dueño del proceso de TI)
- Métricas de desempeño de los procesos (miden qué tan bien se desempeña el proceso para indicar si es probable alcanzar las metas).

1.3 PROPUESTAS DE PROYECTOS (CASOS DE NEGOCIO O «BUSINESS CASE»), ANÁLISIS DE COSTOS/BENEFICIOS, ANÁLISIS DE RIESGOS, FACTORES CRÍTICOS DE ÉXITO. VALIT.

1.3.1 INTRODUCCIÓN

1.3.1.1 OBJETIVO DE VAL IT

La iniciativa Val IT, en la que se incluyen investigaciones, publicaciones y servicios de soporte, tiene como objetivo ayudar a la gerencia a garantizar que las organizaciones logren un valor óptimo de las inversiones de negocio posibilitadas por TI a un coste económico, y con un nivel conocido y aceptable de riesgo. Val IT proporciona guías, procesos y prácticas de soporte para ayudar al consejo y a la dirección ejecutiva a comprender y desempeñar sus roles relacionados con dichas inversiones. Aunque es aplicable a todas las decisiones inversoras, Val IT está dirigido principalmente a las inversiones de negocio posibilitadas por TI: inversiones de negocio importantes en el mantenimiento, crecimiento o transformación del negocio con un componente crítico de TI, donde TI es un medio para conseguir un fin, siendo el fin el de contribuir al proceso de creación de valor en la empresa. En concreto, Val IT se centra en la decisión de invertir (¿estamos haciendo lo correcto?) y en la realización de beneficios (¿estamos obteniendo beneficios?). COBIT, el estándar generalmente aceptado a nivel internacional para el control sobre TI, se centra específicamente en la ejecución (¿lo estamos haciendo correctamente, y lo estamos logrando bien?).

La aplicación eficaz de los principios, procesos y prácticas contenidas en Val IT permitirá a las organizaciones:



- Aumentar el conocimiento y transparencia de los costes, riesgos y beneficios, dando como resultado unas decisiones de gestión mucho mejor informadas
- Aumentar la probabilidad de seleccionar inversiones que tienen el potencial de generar la mayor rentabilidad
- Aumentar la probabilidad de éxito al ejecutar las inversiones elegidas de modo que logren o sobrepasen su rentabilidad potencial
- Reducir costes no haciendo cosas que no deben hacerse y tomando rápidamente medidas correctivas o terminando inversiones que no están cumpliendo su potencial esperado
- Reducir el riesgo de fracaso, especialmente el fracaso de alto impacto
- Reducir sorpresas en relación con el coste y entrega de TI, y de esa forma aumentar el valor del negocio, reducir costes innecesarios y aumentar el nivel global de confianza en TI

1.3.1.2 LA NECESIDAD DE VAL IT

El nivel de inversión en TI es significativo y sigue aumentando. Son pocas las organizaciones que hoy en día podrían funcionar durante mucho tiempo sin su infraestructura de TI. Sin embargo, aunque hay muchos ejemplos de organizaciones que generan valor invirtiendo en TI, al mismo tiempo hay muchos ejecutivos que se preguntan si el valor de negocio realizado es proporcional al nivel de inversión. Por lo tanto, no sorprende que exista cada vez más demanda por parte de los consejos y dirección ejecutiva de unas guías generalmente aceptadas en torno a la toma de decisiones inversoras y la realización de beneficios. Las inversiones de negocio posibilitadas por TI, cuando se gestionan bien dentro de un marco de gobierno efectivo, suponen para las organizaciones unas oportunidades importantes para crear valor. Muchas organizaciones prósperas han creado valor seleccionando las inversiones oportunas y gestionándolas con éxito desde el concepto, pasando por la implementación hasta la realización del valor esperado. Sin un gobierno efectivo y una buena gestión, las

inversiones de negocio posibilitadas por TI generan una oportunidad igualmente importante para destruir valor. El mensaje es claro. Las inversiones de negocio posibilitadas por TI pueden reportar enormes beneficios.

1.3.1.3 UNA NUEVA PERSPECTIVA

Una lección fundamental a aprender de las experiencias citadas y de muchas otras es que la inversión en TI ya no se trata de implementar soluciones de TI, sino que se trata de implementar el cambio posibilitado por TI. El valor de negocio lo genera lo que hacen las organizaciones con TI y no la tecnología en sí. Esto implica mayor complejidad y mayor riesgo que en el pasado. Las prácticas de gestión que tradicionalmente se han aplicado ya no son suficientes. Existe un claro incentivo para la dirección, para que garantice el establecimiento de los procesos adecuados de gobierno y gestión para optimizar la creación de valor. Un componente esencial del gobierno de la empresa es garantizar la obtención de valor de las inversiones posibilitadas por TI. Implica una selección acertada de las inversiones y su gestión como activo o servicio durante todo su ciclo de vida. En COBIT, se establece un marco global para la gestión y entrega de servicios de alta calidad basados en la tecnología de información. Se fijan mejores prácticas para los medios de contribuir al proceso de creación de valor. En Val IT ahora se añaden las mejores prácticas para el fin, proporcionando así los medios para medir, monitorizar y optimizar de forma inequívoca el rendimiento, tanto financiero como no financiero, de la inversión en TI. Está comprobado que la aplicación inteligente de procesos, según están definidos en COBIT y Val IT, puede ayudar a las empresas a mejorar de forma significativa el rendimiento de sus inversiones. No es suficiente, sin embargo, tener simplemente los procesos establecidos. Existen pruebas empíricas de que el impacto más importante en la creación de valor, en lo que se refiere a la rentabilidad accionarial total, la eficiencia del capital o las rentas de activos, lo produce la creciente madurez del proceso, según está definida en el Modelo de Madurez de Capacidades



(CMM), en combinación con economías de escala y alcance. Estas conclusiones las corrobora un reciente estudio donde se comprobó que las inversiones en TI tienen poco impacto a menos que vayan acompañadas de prácticas de gestión de alta calidad, y que aquellas compañías que combinan buenas prácticas de gestión con inversiones en TI son las que mejores resultados obtienen.

Val IT complementa a COBIT desde el punto de vista financiero y de negocio, y ayudará a todos aquellos con un interés en la entrega de valor a partir de TI. Es relevante para todos los niveles de dirección a todo lo ancho del negocio y TI, desde el CEO y el consejo hasta todos aquellos involucrados directamente en los procesos de selección, aprovisionamiento, desarrollo, implementación, despliegue y realización de beneficios. Val IT contiene guías esenciales para todos.

1.3.2 EL MARCO VALIT

1.3.2.1 PRINCIPIOS DE VAL IT

Los principios de Val IT son:

- Las inversiones posibilitadas por TI se gestionarán como cartera de inversiones.
- Las inversiones posibilitadas por TI incluirán el alcance total de actividades que son necesarias para lograr el valor de negocio.
- Las inversiones posibilitadas por TI se gestionarán a lo largo de su ciclo de vida económico completo.
- En las prácticas de entrega de valor, se reconocerá que existen distintas categorías de inversión cuya evaluación y gestión será diferente.
- En las prácticas de entrega de valor, se definirán y monitorizarán las métricas claves y se responderá rápidamente a cualquier cambio o desviación.



- Las prácticas de entrega de valor implicarán a todos los socios y se asignará la responsabilidad correspondiente para la entrega de capacidades y la realización de beneficios del negocio.
- Se hará un monitoreo, evaluación y mejora continua de las prácticas de entrega de valor.

1.3.2.2 PROCESOS DE VAL IT

Para obtener la rentabilidad de la inversión, los socios de las inversiones posibilitadas por TI deberán aplicar los principios de Val IT a los siguientes procesos:

•Gobierno de Valor (VG) El gobierno de valor tiene como objetivo optimizar el valor de las inversiones posibilitadas por TI de una organización:

- Estableciendo el marco de gobierno, monitoreo y control
- Marcando la dirección estratégica para las inversiones
- Definiendo las características de la cartera de inversiones

•Gestión de Cartera (PM) La gestión de cartera tiene como objetivo asegurar que la cartera global de inversiones posibilitadas por TI de una organización esté alineada con los objetivos estratégicos de la misma mediante:

- El establecimiento y gestión de perfiles de recursos
- La definición de umbrales para la inversión
- La evaluación, priorización y selección, aplazamiento o rechazo de nuevas inversiones
- La gestión de la cartera global
- El monitoreo e informes sobre el rendimiento de la cartera

•Gestión de Inversiones (IM) La gestión de inversiones tiene como objetivo asegurar que los programas individuales de inversiones posibilitadas por TI entreguen un valor óptimo a un coste económico y con un nivel conocido y aceptable de riesgo, mediante:

- La identificación de necesidades de negocio
- Un claro entendimiento de los programas de inversión candidatos
- El análisis de las alternativas
- La definición del programa y la documentación de un caso de negocio detallado, incluyendo detalles de los beneficios
- La asignación clara de responsabilidad y propiedad
- La gestión del programa durante todo su ciclo de vida económico
- El monitoreo e informes sobre el rendimiento del programa

Esta publicación tiene como enfoque un elemento clave del proceso de gestión de inversiones: el caso de negocio. Las semillas del éxito o fracaso se siembran en el caso de negocio. Sin embargo, las organizaciones en general no son muy hábiles en el desarrollo y documentación de casos de negocio completos y comparables. El caso de negocio contiene un conjunto de opiniones y suposiciones sobre cómo se puede crear valor. Para garantizar la consecución de los resultados esperados, es necesario que dichas opiniones y suposiciones estén bien probadas. Unos indicadores cualitativos y cuantitativos permiten la validación del caso de negocio y dan ideas para las decisiones inversoras en el futuro. Aquí es donde empieza todo. En Val IT, se facilitan guías para maximizar la calidad de los casos de negocio, poniendo especial énfasis en la definición de indicadores claves, tanto financieros (valor neto actual, tasa interna de rentabilidad y período de recuperación) como no financieros, y en la evaluación y valoración global del riesgo de pérdidas.

El caso de negocio no es un documento puntual y estático, sino una herramienta operativa que hay que actualizar continuamente para reflejar la realidad actual y para dar soporte al proceso de gestión de cartera.

1.3.3 VAL IT. EL CASO DE NEGOCIO

1.3.3.1 INTRODUCCIÓN: LA IMPORTANCIA DEL CASO DE NEGOCIO

El caso de negocio – desestimado con demasiada frecuencia como obstáculo burocrático que hay que superar con el mínimo esfuerzo posible – es una de las herramientas más valiosas disponibles para la dirección, para guiarle en la creación de valor de negocio. La experiencia ha demostrado que la calidad del caso de negocio y de los procesos implicados en su creación y uso durante todo el ciclo de vida económico de una inversión, tiene un impacto enorme en la creación de valor. Los casos de negocio se basan en las expectativas de los sucesos futuros y tienen que dar respuesta a los “Cuatro Interrogatorios”

- ¿Estamos haciendo lo correcto? ¿Qué se propone y para qué resultado de negocio, y cómo contribuyen los proyectos dentro del programa?
- ¿Lo estamos haciendo correctamente? ¿Cómo se va a hacer, y qué se está haciendo para asegurar su encaje con otras capacidades actuales o futuras?
- ¿Lo estamos logrando bien? ¿Qué plan tenemos para hacer el trabajo, y qué será necesario en cuanto a recursos y financiación?
- ¿Estamos obteniendo los beneficios? ¿Cómo se van a entregar los beneficios? ¿Cuál es el valor del programa?

El proceso de desarrollo del caso de negocio debe ser propiedad del promotor del negocio e involucrar a todos los socios claves en el desarrollo y documentación de un conocimiento completo y compartido de los resultados de negocio esperados (resultados tanto intermedios como finales) de una inversión. Debe describir cómo se van a medir los

resultados del negocio, así como el pleno alcance de las iniciativas necesarias para lograr los resultados esperados. Entre estas iniciativas, se debe incluir cualquier cambio necesario en la naturaleza del negocio de la empresa, los procesos de negocio, las habilidades y competencias personales, la tecnología impulsora y la estructura organizacional. En el caso de negocio, se identifica la naturaleza de la contribución de cada iniciativa, cómo se va a medir dicha contribución, y todas las suposiciones claves. En el caso de negocio, se deben establecer también las métricas o indicadores similares para el monitoreo de la validez de dichas suposiciones. También es necesario identificar y documentar los riesgos principales, tanto para la realización con éxito de las iniciativas individuales como para la consecución de los resultados deseados, junto con las acciones de mitigación. La decisión de proceder o no con una inversión posibilitada por TI se toma primero a nivel de programa individual por parte del promotor del negocio, determinando si el caso de negocio es lo suficientemente sólido para su evaluación a nivel de cartera. A nivel de cartera, se valora el valor relativo del programa frente a otros programas activos y candidatos. Para facilitar este proceso, debe haber un método establecido para llegar a un valor normalizado, o a un conjunto de beneficios de alineación, financieros y no financieros, y puntuaciones de riesgo para los casos de negocio individuales.

Con frecuencia, la reacción al planteamiento de los casos de negocio en este contexto es que se están complicando demasiado las cosas. Es importante distinguir entre los procesos de reflexión que se deben seguir a la hora de emprender una inversión importante posibilitada por TI, y el nivel de rigor y detalle necesario para dar soporte y documentar dicha reflexión. En el marco de Val IT, se introduce el concepto de categorías de inversión con distintos niveles de complejidad y grados de libertad a la hora de asignar fondos. La categoría de la inversión, sus dimensiones, el impacto de su fracaso y su posición en el ciclo de vida económico, todos

son factores que permiten determinar a qué partes del caso de negocio hay que prestar mayor atención y qué nivel de detalle es necesario.

1.3.3.2 ESTRUCTURA DEL CASO DE NEGOCIO

El desarrollo del caso de negocio consiste en ocho pasos:

Paso 1 - Elaboración de la Hoja de Datos

La hoja de datos del caso de negocio contiene todos los datos necesarios para el análisis de la alineación estratégica, los beneficios financieros y no financieros, y los riesgos del programa. Para cada partida, a efectos de las etapas de elaboración, implementación, operación y retiro, se recogen los datos de los escenarios de caso mejor / caso peor, según corresponda, para la inversión posibilitada por TI.

Paso 2 - Análisis de Alineación

Casi siempre habrá más oportunidades de inversión en una organización que recursos para asumirlas. El análisis de alineación constituye un método para garantizar la utilización efectiva y eficiente de recursos escasos

Paso 3 - Análisis Financiero Basado en el Incremento de 'Cash Flows' Descontados

Un objetivo clave de la elaboración de un caso de negocio es el de expresar los beneficios en términos financieros, y se debe intentar en la medida de lo razonablemente posible. Se puede soportar el ejercicio en técnicas avanzadas tales como la valoración del valor real de la opción, así como en investigaciones empíricas con datos de valoración obtenidas de otras inversiones posibilitadas por TI.

Paso 4 - Análisis de Beneficios no Financieros

Aunque un objetivo clave de la elaboración de un caso de negocio es el de expresar los beneficios en términos financieros y se debe intentar en la medida de lo razonablemente posible, no se debe pasar por alto los beneficios no financieros. De hecho, en el sector público y en organizaciones sin ánimo de lucro, muchos de los resultados de negocio deseados son de carácter no financiero.

Paso 5 - Análisis de Riesgo

Los programas no son iguales en lo que se refiere a la probabilidad de que entreguen el valor de negocio esperado o la probabilidad de que cumplan con los objetivos de coste y plazo. Dos programas con el mismo nivel de alineación estratégica y valor financiero previsto pueden tener características de riesgo muy diferentes.

Paso 6 - Optimización del Riesgo y Rendimiento

La decisión de proceder o no con una inversión posibilitada por TI la toma primero el promotor del negocio a nivel de programa individual, determinando si el caso de negocio es lo suficientemente sólido para su valoración a nivel de cartera. A nivel de cartera, se contrasta el valor relativo del programa con los programas activos y candidatos. Para facilitar este proceso, debe de haber un proceso establecido para llegar a un valor normalizado, o a un conjunto de puntuaciones normalizadas de alineación global, de beneficios financieros y no financieros y de riesgo para los casos de negocio individuales.

Paso 7 - Documentar el Caso de Negocio

La categoría de la inversión, sus dimensiones, el impacto de su fracaso y su posición en el ciclo de vida económico, son factores que permiten determinar los componentes del caso de negocio a los que hay que prestar mayor atención, así como el nivel de detalle necesario.

Paso 8 - Mantener el Caso de Negocio

Un caso de negocio no es más que una fotografía en un momento dado. No debe ser creado y revisado solo una vez para determinar si proceder o no con una inversión para luego ignorarlo o, en el mejor de los casos, volver a considerarlo en la revisión post-implementación. Es una herramienta operacional que debe ser actualizada continuamente durante todo el ciclo de vida económico de una inversión y aprovechada para dar soporte a la implementación y ejecución de un programa, incluyendo la realización de beneficios.



Bibliografía

Sitios web:

<http://www.isaca.org> Information Systems and Control Association

<http://www.isaca.org/cobit>

<http://www.isaca.org/valit>

<http://www.isaca.org/riskit>

<http://www.itgi.org> IT Governance Institute

Autor:

Ramón Seoane Freijido

Director de Sistemas de Información Molduras del Noroeste

Colegiado del CPEIG



2. GESTIÓN ESTRATÉGICA DE LAS TIC. HERRAMIENTAS DE PLANIFICACIÓN Y CONTROL: CUADROS DE MANDO INTEGRAL («BALANCED SCORECARDS»), MAPAS ESTRATÉGICOS, GESTIÓN DE CONOCIMIENTOS E INNOVACIÓN.

Tema 2. Gestión estratégica de las TIC. Herramientas de planificación y control: cuadros de mando integral (“balanced scorecards”), mapas estratégicos, gestión del conocimiento e innovación.

INDICE

2.1 Herramientas de planificación y control: cuadros de mando integral (“balanced scorecards”)

2.1.1 Perspectivas del cuadro de mando integral

2.1.2 Diseño del cuadro de mando integral

2.1.2.1 Análisis de la situación actual

2.1.2.2 Desarrollo de la estrategia general del negocio

2.1.2.3 Descomposición en objetivos

2.1.2.4 Creación del mapa estratégico de la organización

2.1.2.5 Definición de las métricas de performance

2.1.2.6 Identificación y diseño de nuevas iniciativas

2.1.3 Implementación del cuadro de mando integral

2.2 Mapas estratégicos

2.2.1 Plan estratégico

2.3 Gestión del conocimiento e innovación

2.3.1 El conocimiento y su gestión

2.3.2 La Creatividad

2.3.3 La innovación

2.3.3.1 Tipos de innovación

2.3.3.2 Gestión de la innovación

2.1 HERRAMIENTAS DE PLANIFICACIÓN Y CONTROL: CUADROS DE MANDO INTEGRAL (“BALANCED SCORECARDS”)

El Cuadro de Mando Integral es una herramienta de Gestión Estratégica cuya implementación puede ayudar a una empresa a clarificar

sus objetivos a largo plazo, comunicarlos a toda la empresa y traducirlos en acciones concretas.

2.1.1 PERSPECTIVAS DEL CUADRO DE MANDO INTEGRAL

El Cuadro de Mando Integral, o Balance ScoreCard (BSC), desarrollado por Kaplan y Norton, permite transmitir las estrategias definidas por una organización de una manera clara y eficiente a todos los integrantes de la misma, y a la vez, poder traducir dichas estrategias en objetivos, indicadores y acciones concretas.

Las estrategias definidas por las máximas autoridades de la empresa se basan en muchos factores, como el análisis de la posición de la empresa en el mercado, los recursos con los que cuenta, los objetivos a corto y largo plazo y la visión de futuro basado en la intuición del empresario.

El Cuadro de Mando Integral plantea que primero se deben definir las estrategias, es decir, a dónde se quiere llegar y cómo se va a medir el éxito de las mismas. Luego se plantean los objetivos intermedios y, por último, cómo se van a alcanzar.

Estas definiciones quedan claras para todos los integrantes de la organización, como si formaran parte de un gran equipo, y es una forma de saber si sus acciones para lograr dichos objetivos son correctas o no. Todas las empresas tienen sistemas para verificar la marcha de sus actividades.

Más o menos automatizados, todas tienen sus medios, compuestos por reportes de ventas, de producción, balances contables, etc. Este conjunto de informes y reportes se llama “Sistemas de Medición de Performance”.

El valor agregado del Cuadro de Mando Integral es que los sistemas de medición de performance están asociados de forma coherente a la estrategia general definida por la dirección de la empresa. En este caso, primero se plantea hacia dónde se dirige la empresa, y luego qué se debe controlar para saber si la marcha es la correcta, para lo cual se implementan los sistemas de información.

La visión y la estrategia general de la empresa se ordenan mediante el Cuadro de Mando Integral alrededor de cuatro perspectivas básicas: finanzas, clientes, procesos internos, y aprendizaje y crecimiento:

- La perspectiva finanzas se enfoca en producir mejores ganancias para los accionistas o dueños de las organizaciones. Cuando se trata de una organización sin fines de lucro, esta perspectiva se ve como el objetivo de maximizar la utilización del presupuesto. Todo el esfuerzo de aplicar un programa de Cuadro de Mando Integral va dirigido a mejorar este aspecto, a través de mejoras en la gestión del resto de las perspectivas.

- La perspectiva clientes incluye aquellos objetivos estratégicos que tienen en cuenta la satisfacción del cliente. Un cliente más satisfecho consumirá más nuestros servicios o productos, mejorará nuestra imagen y nos posicionará mejor ante nuestra competencia. Por tanto, una mejora en este aspecto repercutirá directamente en las ganancias de nuestra empresa, es decir, en la perspectiva financiera.

- La perspectiva procesos internos se refiere a que para mejorar la satisfacción del cliente, o para mejorar la utilización de nuestros recursos, vía reducción de costos, o gastos, seguramente se deben mejorar los procesos internos en cuanto a la cadena de valor. Cualquier mejora en este aspecto tiene un impacto en las perspectivas de clientes y finanzas.

- La perspectiva de aprendizaje y crecimiento incluye aquellos aspectos relacionados con los recursos humanos necesarios para poder implementar las mejoras en el resto de las perspectivas. Suele mostrarse como la base del resto de las estrategias, tanto en los aspectos operativos, para poder cumplir con las metas de mejora en los procesos internos, como en la satisfacción de los empleados, condición necesaria para mejorar la atención a los clientes.

La combinación de las cuatro perspectivas en un sistema integrado compondrán el Cuadro de Mando Integral. Vamos a ver un ejemplo de aplicación de las perspectivas de un Cuadro de Mando Integral: Supongamos una entidad con sucursales con atención a clientes, en la que queremos reducir el tiempo promedio de permanencia en el local de 20 a 10 minutos. La estrategia es mejorar la atención a los clientes, y el objetivo es la reducción de tiempo. En cuanto a la perspectiva financiera, las mejoras van dirigidas a que la mejor atención provoque que más clientes quieran utilizar nuestros servicios. Por tanto, obtendremos mejores resultados financieros.

La mejora en la calidad de atención, relacionada con la perspectiva clientes, implicará una mayor satisfacción en los mismos. La mejora en los procesos necesarios para poder atender más rápido, ya sea por la disminución de pasos en la cadena de procesos que no agregan valor, o cambios en la logística de Atención, está relacionado con la perspectiva de procesos internos.

Todas las acciones necesarias para realizar estos cambios están relacionadas entre sí, y unas no pueden ser desarrolladas sin la colaboración de las otras. Asimismo, no se puede implementar un programa de mejoras sin considerar los riesgos que pueden aparecer si se da más importancia a una perspectiva que a otra.

Concluyendo, el Cuadro de Mando Integral sirve para comunicar la visión y la estrategia de la organización, transformándola en acciones concretas.

2.1.2 DISEÑO DEL CUADRO DE MANDO INTEGRAL

El Cuadro de Mando Integral no es sólo el sistema informático que brinda una serie de medidas a controlar, sino que implica un cambio en el management estratégico de toda la organización y, por tanto, debe ser impulsado por la más alta Dirección.

Un programa de Cuadro de Mando Integral no tiene fecha de terminación definida y todas las personas de la empresa deben participar del mismo. No hay diferencias con otras iniciativas estratégicas de mejoras de performance o calidad.

La siguiente es la enumeración de las etapas a seguir en el diseño del Cuadro de Mando Integral:

1. Análisis de la situación actual.
2. Desarrollo de la estrategia general de negocio.
3. Descomposición en objetivos.
4. Creación del mapa estratégico de la organización.
5. Definición de las métricas de performance.
6. Identificación y diseño de nuevas iniciativas.

2.1.2.1 ANÁLISIS DE LA SITUACIÓN ACTUAL

Es la etapa inicial del programa, que implica ver dónde está ubicada la empresa y dónde se quiere llegar. Suele incluir un análisis DAFO (Debilidades, Amenazas Fortalezas y Oportunidades), un análisis de mercado, un análisis económico-financiero de los últimos 6 meses y un análisis de capacidad operativa, que indique los recursos materiales, de

infraestructura y humanos con los que cuenta la empresa. Este análisis será la base del compromiso de inicio y de la definición de la misión y visión de la organización.

La misión de la organización es el propósito de la misma, es decir, la razón de ser de la empresa. La visión es el objetivo hacia dónde apuntan todas las acciones que se desarrollarán, es decir, a dónde se quiere llegar.

2.1.2.2 DESARROLLO DE LA ESTRATEGIA GENERAL DE NEGOCIO

Una vez definidas la misión y la visión de la organización, hay que definir la estrategia general de negocio, es decir, los objetivos a largo plazo, entre 3 y 5 años. La estrategia consiste en definir de qué forma se va a alcanzar la visión. Un ejemplo de estrategia puede ser: desarrollar nuevos productos.

Al mismo tiempo que se plantean las estrategias u objetivos a largo plazo, deben establecerse metas numéricas para esos objetivos, metas que suelen expresarse en términos de porcentaje.

Pueden utilizarse muchas herramientas, entre ellas la matriz DAFO de estrategias combinadas.

En ella se parte de un análisis DAFO convencional, donde se identifican Fortalezas, Oportunidades, Debilidades y Amenazas, y luego por cada cruce de características, se elaboran las estrategias que aprovechan las oportunidades de mejora que blindan dichos cruces.

2.1.2.3 DESCOMPOSICIÓN EN OBJETIVOS

Una vez definida la estrategia global, hay que definir los objetivos más detallados y a corto plazo. Estos objetivos deben estar distribuidos en

las cuatro perspectivas: finanzas, clientes, procesos internos, y aprendizaje y crecimiento. Para cada una de las perspectivas existen ciertos objetivos comunes a la mayoría de empresas, y otros más específicos, que dependen de la situación de la empresa y del giro de negocio específico de la misma.

En cuanto a los temas estratégicos para la perspectiva finanzas, hay que tratar de mejorar el valor financiero de las acciones de la empresa y del Retorno de la Inversión (ROI). Esto los conseguiremos mediante el crecimiento de las ganancias y del mix de productos, el incremento de la productividad y la reducción de costos, y mejoras en la utilización de los archivos y la estrategia de inversión.

En cuanto a los temas estratégicos para la perspectiva clientes, cabe resaltar que, mejorando las variables relacionadas con los clientes, mejorarán nuestras ganancias financieras, al ser los clientes nuestra principal fuente de ingresos. Respecto a la relación de nuestra empresa con los clientes y con el mercado, hay que tener en cuenta los siguientes aspectos: participación de mercado, retención de clientes, adquisición de clientes, satisfacción del cliente y rentabilidad del cliente. Además, hay que tener en cuenta algunas características relacionadas con lo que pensamos que el cliente valora de nuestra empresa, y que llamaremos “proposiciones de valor”. Se trata de los atributos del producto o servicio, la relación con el cliente y la imagen y reputación de la empresa.

Las estrategias relacionadas con la perspectiva de procesos internos se definen en función de la cadena de valor del producto. La cadena de valor de los procesos internos de una empresa está relacionada con el ciclo de vida del producto y se descompone en tres etapas: procesos de innovación, procesos operativos y procesos de servicio post-venta. Estos procesos abarcan desde que se detecta la necesidad del cliente hasta que las necesidades del cliente quedan satisfechas.

En los procesos de innovación, las estrategias van dirigidas a la forma en que la organización maneja los costos y las inversiones en investigación básica, investigación aplicada, desarrollo del producto y marketing. En los procesos operativos, se trata de mejorar las tareas que van desde producir, fabricar un producto o estandarización en la metodología para prestar un servicio, hasta la distribución o entrega de los servicios. En los procesos posventa se centran en los servicios y productos que se ofrezcan al cliente tras la venta, tales como garantías, políticas de devolución, etc.

En cuanto a los temas estratégicos para la perspectiva de aprendizaje y crecimiento, si queremos implementar cambios en la manera de hacer las cosas, nuestro personal debería estar motivado para realizar los cambios y capacitado para ejecutar las tareas de forma apropiada. Además, hay que contar con los recursos materiales necesarios para efectuar las tareas indicadas. Dichos recursos incluyen, por ejemplo, los sistemas informáticos adecuados, las herramientas, los uniformes, etcétera. No podemos pretender clientes satisfechos si primero no tenemos empleados satisfechos.

2.1.2.4 CREACIÓN DEL MAPA ESTRATÉGICO DE LA ORGANIZACIÓN

Una vez definidos los objetivos y las estrategias a largo plazo, dentro de cada una de las perspectivas, hay que analizar cómo cada uno de esos objetivos va encadenándose y afectándose entre sí. Al tomar una decisión en uno de los aspectos, esa decisión va afectando al resto de las dimensiones en un efecto cascada. Para la creación del mapa estratégico hay que ir relacionando los objetivos, utilizando conexiones lógicas (si... entonces) en las perspectivas correspondientes a cada uno de ellos. Dichas relaciones se utilizarán para determinar los indicadores y métricas que informarán cuando una estrategia ha tenido éxito o no.

2.1.2.5 DEFINICIÓN DE LAS MÉTRICAS DE PERFORMANCE

Tras crear el mapa estratégico, donde podremos observar cómo se relacionan cada uno de los objetivos, hay que analizar cuáles serán las métricas o indicadores clave, que permitirán conocer en qué medida se está alcanzando cada objetivo.

El proceso de definir estas medidas es iterativo, es decir, por cada una de las relaciones y objetivos se hace un listado, que luego se va refinando hasta quedarse con las más significativas. También se puede determinar primero las cinco más importantes y luego ampliarlas.

Se recomienda no sobrepasar las 25 medidas que, además, deben estructurarse en indicadores causa (porque afectan a otro objetivo con el que están relacionados) e indicadores efecto (que miden la consecución de un objetivo). Las medidas deben estar bien definidas, que el valor obtenido sea siempre el mismo, sin importar quién realiza la medición, y que sean correctamente entendidas en el marco de nuestra estrategia.

2.1.2.6 IDENTIFICACIÓN Y DISEÑO DE NUEVAS INICIATIVAS

Es el último paso en el diseño del Cuadro de Mando Integral y consiste en definir cuáles van a ser las iniciativas y actividades a desarrollar para poder implementar nuestra estrategia. Cada una de las iniciativas estará unida a un conjunto de métricas o medidas que permitirán conocer su evolución. Dichas iniciativas deben ser comprendidas como un medio para alcanzar los objetivos estratégicos y no un fin en sí mismas.

2.1.3 IMPLEMENTACIÓN DEL CUADRO DE MANDO INTEGRAL

Una vez definido el Cuadro de Mando Integral, hay muchas opciones para implementarlo en la práctica como una herramienta efectiva. La mejor solución depende de cada empresa en particular, y no existe una regla general. La mayoría de empresas pueden crear su Cuadro de Mando Integral utilizando las herramientas de automatización de oficina disponibles.

Recordemos que el Cuadro de Mando Integral debe:

- Ayudarnos en la definición de estrategias, objetivos, medidas, metas y acciones.
- Facilitarnos la comunicación de la dirección estratégica y ayudar a transmitir lo que debe hacer cada integrante de la organización para que sus acciones individuales favorezcan el cumplimiento de los objetivos.
- Permitirnos comparar la evolución de las metas y su cumplimiento.
- Ser simple de entender y fácil de manejar para el usuario final y fácil de mantener para los administradores.

Si las herramientas no están integradas en un solo sistema informático, todo lo anterior será difícil de cumplir y, por tanto, el Cuadro de Mando Integral fracasará.

Entre los factores de riesgo que pueden poner en peligro el éxito de un programa de Cuadro de Mando Integral, se encuentran:

- Falta de compromiso de la Dirección: si la Dirección no se involucra al inicio del proceso y delega la responsabilidad en gerentes o mandos medios, se generará una falta de autoridad en el líder del proyecto.
- Falta de continuidad: el Cuadro de Mando Integral debe ser un programa de largo plazo, realizando los ajustes periódicos necesarios.



- Sistema de comunicación deficiente: la información debe fluir en ambos sentidos (proporcionar la información para el Cuadro de Mando Integral y distribuir los resultados a todas las áreas) para que las personas vean los beneficios y no lo tomen como un intento de controlar sus actividades, en lugar de una herramienta para el crecimiento de toda la organización.
- Definiciones débiles: si al definir los indicadores no se unifica el lenguaje y se hace una especificación dura, que no dé posibilidad a dobles interpretaciones, cada persona hará su propia interpretación y ello generará controversias, con lo que el programa perderá confiabilidad.
- Problemas en la escalabilidad: cuando la empresa tiene cierta envergadura, se implementa el Cuadro de Mando Integral en ciertas unidades de negocio, escogidas por su importancia, y luego se extiende a toda la organización. En este caso, el Cuadro de Mando Integral se compone de varios cuadros para cada unidad de negocio. A medida que se vayan agregando más áreas al Cuadro de Mando Integral, será más complicado mantener la integridad de la información y su actualización.

En la misma medida, se agregarán potenciales usuarios, y si no tenemos un sistema que permita la conexión de muchos usuarios, aparecerán problemas de performance, o inconvenientes en la distribución (si no es un solo sistema integrado). Si implementamos un sistema informático que contemple todas las etapas en la explotación del Cuadro de Mando Integral, estos factores de riesgo mencionados pueden desaparecer, ayudando al éxito del programa.

Existen una serie de estándares acerca de qué debe poseer un sistema para poder implementar un Cuadro de Mando Integral, elaborados por la Balanced Scorecard Collaborative Inc, una organización fundada por los creadores de este concepto (Kaplan y Norton). Los requerimientos

funcionales básicos especificados en el estándar se dividen en cuatro secciones: diseño del Cuadro de Mando Integral; capacitación estratégica y comunicación; explotación del negocio; y feedback y aprendizaje.

- Diseño del Cuadro de Mando Integral: la aplicación debe permitir el desarrollo de todas las etapas del diseño del Cuadro de Mando Integral.
- Capacitación estratégica y comunicación: uno de los objetivos del Cuadro de Mando Integral es facilitar la comprensión de las estrategias de la compañía mediante la comunicación y la capacitación, por lo que se debe mantener la documentación de las definiciones de objetivos, medidas, metas e iniciativas alineadas con las estrategias.
- Explotación del negocio: las iniciativas o programas de acción son la aplicación concreta para cumplir las metas planteadas, y por tanto los objetivos estratégicos. Una herramienta que cumpla los estándares del Cuadro de Mando Integral debe permitir relacionar las iniciativas con los objetivos estratégicos.
- Feedback y aprendizaje: una herramienta de Cuadro de Mando Integral efectiva debe facilitar el análisis de las medidas a controlar, mediante una interfaz que muestre tanto valores numéricos como indicadores gráficos.

Existen otros factores que debemos tener en cuenta a la hora de elegir el software a adquirir o decidirnos a desarrollar nuestro propio software. Entre estos factores se incluye:

- Envergadura de la empresa: determina la cantidad de posibles usuarios del sistema, el nivel de automatización y los recursos económicos de los que dispone. Una empresa pequeña es probable que no necesite un gran desarrollo informático, lo que no significa

que no se pueda construir un Cuadro de Mando Integral utilizando plantillas de cálculo y bases de datos relacionales pequeñas.

- Alcance de las capacidades funcionales e integración con otros sistemas: si analizamos los estándares para el Cuadro de Mando Integral, vemos que en cuanto a las capacidades de análisis, sólo mencionan la habilidad de mostrar la evolución de los indicadores. Sin embargo, no mencionan las capacidades de drill-down y drill-up por diferentes dimensiones, como tampoco acerca de la integración con otros sistemas, como tableros de control o data warehouse. Si éstos existen y son fuente de datos, es posible que los usuarios quieran poder extender sus análisis estratégicos a análisis tácticos, mediante la navegación por el detalle de la información.

La implementación o automatización del Cuadro de Mando Integral debe afrontarse como un proyecto más de sistemas. Como tal, es conveniente aplicar alguna metodología de ingeniería de software que permita:

- Determinar el alcance y objetivos.
- Analizar la factibilidad y alternativas de solución.
- Estimar correctamente la duración del proyecto.
- Facilitar el mantenimiento y los cambios en la definición.
- Permitir la reutilización y conjunción entre el resto de sistemas.
- Mejorar la calidad, reducir costos y mejorar el aprovechamiento de recursos.

Una de las alternativas posibles es utilizar Métrica III (metodología impulsada por el Ministerio de Administraciones Públicas), que se basa en las teorías más modernas de Ingeniería de Software moderno. Sus etapas son:

- Planificación (PSI)

- Desarrollo, que incluye:
 - Estudio de la viabilidad (EVS)
 - Análisis (ASI)
 - Diseño (DSI)
 - Construcción (CSI)
 - Implantación y aceptación (IAS)
- Mantenimiento (MSI)

2.2 MAPAS ESTRATÉGICOS

El mapa estratégico es el primer paso para la implementación de la metodología de Balanced Scorecard. ¿Qué es y para qué sirve?

El primer paso del Balanced Scorecard es la construcción del mapa estratégico, una herramienta que debe servir como guía en momentos de incertidumbre. El mapa se construye en función de lo que la organización piensa hoy con respecto al futuro. Esta representación gráfica permite ir aprendiendo sobre los cambios a medida que se generan, especialmente en situaciones donde no existen certezas.

Los mapas estratégicos son una representación visual de la estrategia de una organización y demuestran claramente por qué una imagen es más poderosa que mil palabras (o incluso más poderosa que 25 indicadores de desempeño).

Estos mapas se diseñan bajo una arquitectura específica de causa y efecto, y sirven para ilustrar cómo interactúan las cuatro perspectivas del Balanced Scorecard.

1) Los resultados financieros se consiguen únicamente si los clientes están satisfechos. Es decir, la perspectiva financiera depende de cómo se construya la perspectiva del cliente.

2) La propuesta de valor para el cliente describe el método para generar ventas y consumidores fieles. Así, se encuentra íntimamente ligada con la perspectiva de los procesos necesarios para que los clientes queden satisfechos.

3) Los procesos internos constituyen el engranaje que lleva a la práctica la propuesta de valor para el cliente. Sin embargo, sin el respaldo de los activos intangibles es imposible que funcionen eficazmente.

4) Si la perspectiva de aprendizaje y crecimiento no identifica claramente qué tareas (capital humano), qué tecnología (capital de la información) y qué entorno (cultura organizacional) se necesitan para apoyar los procesos, la creación de valor no se producirá. Por lo tanto, en última instancia, tampoco se cumplirán los objetivos financieros.

En este contexto, alinear los objetivos de estas cuatro perspectivas es la clave de la creación de valor y de una estrategia focalizada e internamente consistente. Una vez creados, los mapas estratégicos son excelentes herramientas de comunicación, ya que permiten que todos los empleados comprendan la estrategia y la traduzcan en acciones específicas para contribuir al éxito de la empresa.

El mapa estratégico del BSC proporciona un marco para ilustrar de qué modo la estrategia vincula los activos intangibles con los procesos de creación de valor. Veamos con mayor detalle los elementos de cada una de las perspectivas:

La perspectiva financiera describe los resultados tangibles de la estrategia en términos financieros. Los indicadores clave para evaluar el éxito o fracaso de la estrategia son la rentabilidad de la inversión (ROI), el valor para los accionistas, el crecimiento de los ingresos y el costo por unidad.

La perspectiva del cliente, por su parte, define la propuesta de valor para los "clientes target". Si los clientes valoran la calidad constante y la entrega puntual, entonces, las habilidades, los sistemas y los procesos de desarrollo de nuevos productos y servicios de gran funcionalidad adquieren gran valor. La alineación de acciones y capacidades con la propuesta de valor para el cliente es el núcleo de la ejecución de la estrategia.

La perspectiva de procesos internos identifica los pocos procesos críticos que se espera tengan el mayor impacto sobre la estrategia. Por ejemplo, una organización puede aumentar sus inversiones en I + D y reestructurar sus procesos de desarrollo para obtener productos innovadores y de alto desempeño. Otra empresa, con la idea de ofrecer la misma propuesta de valor, podría desarrollar nuevos productos a través de alianzas estratégicas con otros fabricantes.

La perspectiva de aprendizaje y crecimiento identifica los activos intangibles más importantes para la estrategia. Los objetivos de esta perspectiva se centran en las tareas, los sistemas y el tipo de ambiente requeridos para apoyar los procesos internos de creación de valor. Estos activos deben estar agrupados y alineados con los procesos internos críticos.

En síntesis, el mapa estratégico proporciona el marco visual para integrar todos los objetivos de la empresa. La comprensión de los procesos críticos como gestión de operaciones, innovación y relaciones sociales, promueve el logro de las metas de productividad.

Por último, el mapa identifica las capacidades específicas relacionadas con los activos intangibles de la organización (capital humano, de información y organizacional) para obtener un desempeño excepcional

2.2.1 PLAN ESTRATÉGICO

El plan estratégico es una actividad administrativa que tiene como objetivo conducir el rumbo de la organización para conseguir su sostenibilidad, produciendo respuestas consistentes a las tres cuestiones fundamentales: ¿Dónde estamos? ¿Adónde queremos llegar? ¿Cómo vamos a hacer para alcanzarlo? Es un proceso de dirección que gestiona, respecto a la formulación de objetivos, la selección de programas de acción y su ejecución, llevando el seguimiento de las condiciones internas y externas a la empresa y la evolución esperada.

También considera premisas básicas que la empresa debe respetar para que todo el proceso tenga coherencia y sea sustentable.

El establecimiento de un plan estratégico envuelve seis actividades:

- definición de la misión corporativa
- análisis de la situación
- formulación de objetivos
- formulación de estrategias
- implementación
- seguimiento, aprendizaje y control.

Es cada vez mayor el número de empresas en el escenario global que, ante la complejidad del escenario empresarial y de las turbulencias e

incertidumbres, están recogiendo modelos de gestión para que las auxilien en el desempeño y perfeccionamiento del proceso de dirección.

La elaboración de un Plan Estratégico engloba varios tópicos fundamentales:

- Misión: razón de ser de la organización. Expresa las necesidades a las que atiende, de que grupos de personas y con qué competencias básicas.
- Visión: definición de dónde y cómo la organización deberá estar en el futuro – en un horizonte medio de tiempo de 5 años.
- Políticas: guías (con carácter de permanencia) para la toma de decisiones sobre aspectos importantes de la organización.
- Objetivos: resultados parciales – horizonte de 1 año – en dirección a lo propuesto por la visión de futuro
- Estrategias: vías/caminos escogidos para la realización de la visión.
- Plan de acción: conjunto de programas y proyectos propuestos para el cumplimiento de la misión y en dirección a la visión de futuro

2.3 GESTIÓN DEL CONOCIMIENTO E INNOVACIÓN.

Actualmente estamos confrontados con un nuevo paradigma donde el conocimiento se está convirtiendo en el principal activo de una empresa. La llamada sociedad del conocimiento, en la cual estamos viviendo, exige un esfuerzo orientado al mejor y total aprovechamiento del capital intelectual, entendido este como la suma resultante del conocimiento de los integrantes de una empresa.

La valoración de los activos intangibles es una característica de la sociedad del conocimiento, la misma que hasta presenta un desafío a las prácticas contables; así si tenemos dos empresas “A” y “B” con las mismas instalaciones, las mismas maquinaria, la misma tecnología y el mismo capital, en un balance patrimonial no aparecería diferencia alguna. Sin embargo, si en la empresa “A” los trabajadores son altamente especializados, con una capacitación continua, participación, sinergia y pensamiento sistémico, mientras que en la empresa “B” no encontramos tales características en los recursos humanos, entonces es evidente que la empresa “A” sería más valorada en el mercado de acciones, por ejemplo, porque es en ella donde existe mayor integración y mejor utilización del conocimiento. Y más aún la empresa “A” estará más preparada para innovar y por consiguiente competir en una economía cada vez más globalizada.

La sociedad del conocimiento es la tercera fase productiva por la que atraviesa la sociedad. La primera fase, que fue muy larga, estaba basada en la producción rural y artesanal; después de un tiempo hubo un pasaje de la sociedad rural a la sociedad industrial. La sociedad industrial se basaba en la producción en serie; el centro productivo era la fábrica y la filosofía que la orientaba era la del predominio de la razón sobre el sentimiento; la sociedad industrial fue optimizada y organizada por Taylor, mediante la producción científica, donde separaba el trabajo intelectual del operacional para evitar el desperdicio de tiempo, y donde esto fue perfeccionado por la ingeniería de métodos y movimientos; en la sociedad industrial existía una orientación hacia el producto que después es ofrecido al mercado que lo aceptará.

La actual tercera fase productiva, o sea la sociedad del conocimiento, se caracteriza por la importancia dada al conocimiento, la predominancia de los trabajadores intelectuales y donde el trabajo repetitivo es delegado a las máquinas, robots y/o computadoras.

Entonces el trabajador tiene más tiempo para pensar, sentir, emocionarse, ser creativo e innovar. En la sociedad del conocimiento las empresas están orientadas al mercado buscando identificar las señales del mismo y para esto hacen uso de la inteligencia competitiva.

Una empresa en la sociedad del conocimiento se enfrenta a los siguientes desafíos:

- La desestructuración del tiempo y del espacio, donde deja de ser importante la permanencia del trabajador durante 8 horas en el espacio físico de la empresa; pasa a ser importante el resultado creativo que el trabajador puede aportar desde su casa mediante el teletrabajo, o sea el trabajo trasciende los límites de la fábrica porque la respuesta creativa aparece en cualquier momento y en cualquier lugar.

- La calidad de vida, que es condición “sine qua non” de la creatividad; el trabajador para identificarse con los objetivos de la empresa tiene que tener una calidad de vida que le permita poder dar lo mejor de su producción intelectual al equipo del cual forma parte.

- La valoración de los activos intangibles y la gestión del conocimiento.

2.3.1 EL CONOCIMIENTO Y SU GESTIÓN.

Una gestión del conocimiento va a llevar a preguntarnos cuál es el conocimiento disponible en la empresa y cuál es el conocimiento que necesitamos. Entonces comenzamos con la identificación del conocimiento disponible dentro de la organización.

El conocimiento disponible en el interior de la organización así como la capacidad de incrementarlo es el activo intangible de tal organización. Este conocimiento disponible va a ser el conocimiento acumulado, va a estar en la forma de las prácticas compartidas en la empresa, en la forma de productos y procesos desarrollados por la empresa, en el conocimiento del mercado y de sus clientes, en la forma cómo la empresa interactúa con otras organizaciones, en el conocimiento tácito de los trabajadores de la empresa. Es importante, en esta fase, diferenciar el conocimiento tácito del conocimiento explícito.

El conocimiento tácito es aquel fruto de la experiencia y adquirido en forma práctica, en tanto que el conocimiento explícito es aquel conocimiento ya codificado disponible para su captación y/o transmisión en manuales o textos. Para intercambiar ese conocimiento es necesario ver formas de gerenciar y optimizar tal proceso.

El conocimiento tiene un carácter acumulativo, es decir lo que una empresa hará en el futuro es determinado, de alguna forma, por lo que la empresa hizo en el pasado, o sea la capacidad tecnológica no surge de la noche a la mañana.

Para conservar y disponer los conocimientos de una organización se hace necesario contar con formas versátiles de almacenamiento del conocimiento, en manuales de procedimientos, en un proyecto de gestión del conocimiento e inteligencia competitiva, y mediante la gestión estratégica de un sistema de información.

Es decir, se hace necesario tener una memoria organizada de la empresa para no perder ni el conocimiento tácito ni el explícito que la empresa fue acumulando en el transcurso de los años.

2.3.2 LA CREATIVIDAD.

Además del conocimiento, que está estrechamente ligado al razonamiento lógico, al pensamiento cartesiano, tenemos la creatividad, la cual, en contrapartida, se encuentra más cercana a lo que sería la intuición, la imaginación y la subjetividad.

Entendemos la creatividad como la adaptación al cambio resultado de un problema desafiador. En una época en que el cambio y la incertidumbre son las constantes, la respuesta creativa significará la evolución de los productos, procesos y servicios.

2.3.3 LA INNOVACIÓN.

¿Qué es la Innovación?

Podemos definir la innovación como "el proceso en el cual a partir de una idea, invención o reconocimiento de una necesidad se desarrolla un producto, técnica o servicio útil hasta que sea comercialmente aceptado". De acuerdo con este concepto, innovar no es más que el proceso de desarrollar algo nuevo o que no se conoce a partir del estudio metódico de una necesidad, ya sea personal, grupal u organizacional, para lograr una meta económica. Esto quiere decir que la innovación genera ideas que pueden venderse en un mercado específico.

Para innovar es necesario un amplio conocimiento de una necesidad; no todas las ideas innovadoras tienen éxito, por tanto es necesario jugar con todas las herramientas necesarias para que la innovación no solo sorprenda sino que también funcione.

Para que acontezca la innovación en la empresa serían necesarios los dos ingredientes anteriormente vistos, esto es: el conocimiento y la

creatividad. De esta forma podríamos establecer la siguiente ecuación que nos ayudaría a presentar el concepto:

$$\text{CONOCIMIENTO} + \text{CREATIVIDAD} = \text{INOVACION} ==> \text{COMPETITIVIDAD}$$

¿Por qué es importante la innovación?

Innovación y competitividad van de la mano, pero no necesariamente la una existe sin la otra. Se puede ser competitivo sin ser innovador con sólo mantener sistemas de mejora continua, pero los procesos de mejora no llegan a ser suficientes cuando el mercado se encuentra saturado, cuando la demanda es alta y cuando existen necesidades que los productos o servicios existentes no logran solventar.

En este punto, la innovación se convierte en un proceso fundamental para alcanzar la competitividad, debido a que los esfuerzos por mejorar han alcanzado su límite y ya no son suficientes para seguir adelante.

Pero hay que entender que la innovación, por sí sola, no garantiza necesariamente que se alcance la competitividad. Se deben establecer metodologías y estrategias definidas para poder innovar. Será fundamental realizar un estudio metódico de los factores que intervienen en el proceso para la innovación y de las oportunidades existentes en los diferentes escenarios.

2.3.3.1 TIPOS DE INNOVACIÓN

Según su aplicación:

- Innovación de PRODUCTO: Comercialización de un producto tecnológicamente distinto o mejorado; la innovación se da cuando las características de un producto cambian.

- **Innovación de PROCESO:** Ocurre cuando hay un cambio significativo en la tecnología de producción de un producto o servicio; también ocurre cuando se producen cambios significativos en el sistema de dirección y/o métodos de organización; reingeniería de procesos, planificación estratégica, control de calidad, etc.

Según su grado de originalidad:

- **Innovación RADICAL:** aplicaciones nuevas de una tecnología o combinación original de nuevas tecnologías.

- **Innovación INCREMENTAL:** mejoras que se realizan sobre un producto, servicio o método existente.

2.3.3.2 GESTIÓN DE LA INNOVACIÓN

Tradicionalmente se considera que la innovación es el resultado de una idea feliz que sólo la pueden generar empresas con grandes presupuestos de I+D, que para innovar se ha de ser un creativo... Sin negar parte de razón a estos argumentos, la realidad es que la mayor parte de las innovaciones que conocemos son el resultado de un trabajo sistemático de búsqueda de ideas-oportunidades y su transformación en realidades; parafraseando a Peter Drucker: “Hay innovaciones que surgen de un instante de genialidad, pero la mayoría de éstas, especialmente las de más éxito, son el resultado de la búsqueda consciente y deliberada de oportunidades.”

Por tanto, en un entorno como el actual, en el que la innovación es un factor clave de supervivencia, el reto de toda empresa es innovar de forma sistemática, haciendo que ésta sea una actividad más, en definitiva gestionando la innovación a través de un proceso específico, el denominado proceso de innovación.

La innovación sistemática será el resultado de una correcta gestión de este proceso y de una adecuada utilización de metodologías y técnicas.

La capacidad innovadora de la empresa dependerá de la forma en que organicemos y gestionemos el proceso de innovación, el cual está constituido por cuatro etapas principales:

1. Generar ideas. Deberemos convertirnos en una organización observadora, capaz de mirar a su alrededor, detectar los cambios que se están produciendo y descubrir la manera de aprovecharlos.
2. Seleccionar. Deberemos disponer de sistemas para evaluar la viabilidad de las ideas que generemos, para así seleccionar y ejecutar aquellas con mayores posibilidades de éxito.
3. Desarrollar. Deberemos disponer de personas capaces de ejecutar los proyectos de innovación de forma efectiva, utilizando metodologías de gestión adecuadas.
4. Medir. Si no nos medimos no sabremos si lo estamos haciendo bien, por tanto deberemos medir tanto el éxito como el fracaso de las innovaciones generadas.

Bibliografía:

Kaplan, Robert S. and David P. Norton, *The Balanced Scorecard: Translating Strategy into Action*, Boston, MA: Harvard Business School Press, 1996.

Kaplan, Robert S. and David P. Norton, *The Strategy-focused organization*, Boston, MA: Harvard Business School Press, 2000.

Paul R. Niven, *El Cuadro de Mando Integral*, Barcelona 2003, Gestión 2000

Del Moral, Anselmo, Pazos, Juan, Rodriguez, Esteban, Rodriguez-Patón, Alfonso y Suarez, Sonia; *Gestión del conocimiento*; International Thomson Editores; Madrid; 2007.

Drucker, P. F. "*The Discipline of Innovation*". Harvard Business School Publishing, 2002

Autor:

Ramón Seoane Freijido

Director de Sistemas de Información Molduras del Noroeste

Colegiado del CPEIG

**3. DIRECCIÓN Y GESTIÓN DE
PROYECTOS. GESTIÓN DE LA
INTEGRACIÓN. EL PLAN
GENERAL DEL PROYECTO.
GESTIÓN DEL ALCANCE.
GESTIÓN DEL COSTE.
PRESUPUESTOS. GESTIÓN DEL
TIEMPO. TÉCNICAS DE
PLANIFICACIÓN. GESTIÓN DE LA
CALIDAD. PLAN DE CALIDAD.
GESTIÓN DE RRHH.
CAPACIDADES DEL JEFE DE
PROYECTO. GESTIÓN DE LAS
COMUNICACIONES. GESTIÓN DEL
RIESGO. CONTINGENCIAS.
GESTIÓN DE LA
SUBCONTRATACIÓN Y
ADQUISICIONES.**

Tema 3. Dirección y gestión de proyectos. Gestión de la integración. El plan general del proyecto. Gestión del alcance. Gestión del costo. Presupuestos. Gestión del tiempo. Técnicas de planificación. Gestión de la calidad. Plan de calidad. Gestión de RRHH. Capacidades del jefe de proyecto. Gestión de las comunicaciones. Gestión del riesgo. Contingencias. Gestión de la subcontratación y adquisiciones.

INDICE

- 3.1 Dirección y gestión de proyectos
 - 3.1.1 Introducción
 - 3.1.2 Project Management Institute (PMI®)
 - 3.1.3 El Project Management Body of Knowledge (PMBOK®)
 - 3.1.3.1 Introducción
 - 3.1.3.2 Relación del PMBOK® con la dirección de las TIC
 - 3.1.3.3 Estructura del PMBOK®
- 3.2 Gestión de la integración del proyecto
 - 3.2.1 El plan general del proyecto
- 3.3 Gestión del alcance del proyecto
- 3.4 Gestión del tiempo del proyecto
 - 3.4.1 Técnicas de planificación
- 3.5 Gestión de los costos del proyecto
 - 3.5.1 Presupuestos
- 3.6 Gestión de la calidad del proyecto
 - 3.6.1 Plan de calidad
- 3.7 Gestión de los recursos humanos del proyecto
 - 3.7.1 Capacidades del jefe de proyecto.
- 3.8 Gestión de las comunicaciones del proyecto
- 3.9 Gestión de los riesgos del proyecto
 - 3.9.1 Contingencias
- 3.10 Gestión de las adquisiciones del proyecto

3.1 DIRECCIÓN Y GESTIÓN DE PROYECTOS

3.1.1 INTRODUCCIÓN

Un proyecto es una actividad temporal diseñada para producir un único producto, servicio o resultado. Un proyecto tiene un comienzo y un final, así como un alcance y recursos definidos.

Un proyecto es único en el sentido de que no es una operación repetitiva, sino un conjunto específico de operaciones diseñadas para lograr un objetivo. El equipo de proyecto incluye gente que normalmente no trabaja junta, y en muchos casos pertenecen a distintas organizaciones y países.

El desarrollo de software, la construcción de un puente o edificio, el esfuerzo de reconstrucción después de una catástrofe natural, todo son proyectos, y deben ser gestionados de forma experta para ser completados a tiempo, según lo presupuestado, y con la calidad exigida por las organizaciones.

La gestión de proyectos es la aplicación de conocimientos, habilidades y técnicas para ejecutar los proyectos de forma eficaz y eficiente. Es algo estratégico para las organizaciones, capacitándolas para alinear los resultados del proyecto a los objetivos del negocio - y por ello siendo más competitivas en sus mercados - .

3.1.2 PROJECT MANAGEMENT INSTITUTE (PMI®)

PMI es una de las asociaciones profesionales más grandes del mundo, con medio millón de miembros en más de 185 países. Es una organización sin ánimo de lucro que intenta mejorar la profesión de la gestión de proyectos por medio de estándares y certificaciones reconocidas

globalmente, comunidades colaborativas, un extenso programa de investigación, y oportunidades de desarrollo profesional.

Antecedentes

PMI Internacional se fundó en 1969 con socios voluntarios. Durante los años setenta PMI se desarrolló principalmente en el campo de la ingeniería, mientras el mundo de los negocios desarrollaba sus proyectos a través de especialistas de la misma empresa y formaban grupos de trabajo llamados “Task Force”. En los años ochenta, el mundo de los negocios comenzó gradualmente a dirigir sus esfuerzos por proyectos.

Durante este tiempo el PMI, a través del comité de estándares y colaboradores (entre ellos empresas, universidades, asociaciones de profesionales, especialistas y consultores en proyectos) realizó el estudio, evaluación y revisión de los estándares generalmente aceptados a nivel internacional, dando como resultado los estándares que representan el cuerpo de conocimientos de la Dirección de Proyectos, cuyo título original es “Project Management Body of Knowledge” (PMBOK). En 1987 se publicó su primera edición.

Estándares

Desde 1987, el PMI se ha encargado de investigar, recopilar y publicar las buenas prácticas generalmente aceptadas para la mayoría de los proyectos. Desde entonces, ha publicado 14 libros de estándares. Uno de ellos, el PMBOK, tiene en circulación más de 2.000.000 de ejemplares. Se tiene acceso a estos estándares como socio del PMI®.

Misión

La misión del PMI es servir a su comunidad de asociados y profesionales interesados, desarrollando el arte de dirigir y llevar a la práctica la Dirección de Proyectos como disciplina profesional.

Objetivos

Los principales objetivos del PMI son:

- Promover la dirección de proyectos.
- Compartir la experiencia internacional a través del desarrollo de profesionales.
- Desarrollar calidad en los recursos humanos para la dirección de proyectos.
- Compartir los conocimientos generalmente aceptados que dan reconocimiento a la profesión.
- Consolidar estándares internacionales
- Certificación de profesionales en proyectos reconocidos a nivel mundial.

3.1.3 EL PROJECT MANAGEMENT BODY OF KNOWLEDGE (PMBOK)

3.1.3.1 INTRODUCCIÓN

El Project Management Body of Knowledge (PMBOK) es un término que describe la suma de los conocimientos involucrados en la profesión de la administración de proyectos.

El conocimiento y las prácticas descritas en el PMBOK son aplicables a la mayoría de los proyectos. Sin embargo, el equipo administrador del proyecto es siempre el responsable de determinar lo que es apropiado para cada proyecto.

PMBOK provee la terminología común de la administración de proyectos.

PMBOK describe los métodos y prácticas que deben tenerse en consideración desde que se inicia un proyecto hasta su finalización. La aplicación de éstas prácticas permitirá llevar una buena gestión del

proyecto y mantener un mayor control, permitiendo al Project Manager y a su equipo realizar proyectos de manera eficaz y eficiente (en alcance, tiempo, coste), así como asegurar la calidad y transparencia a lo largo de toda la vida del proyecto

La guía del PMBOK es integrada mediante un proceso de desarrollo de normas por consenso voluntario. Este proceso reúne a voluntarios y/o trata de obtener las opiniones de personas que tienen interés en el tema cubierto por esta publicación. Aunque PMI administra el proceso y establece reglas para promover la equidad en el desarrollo del consenso, no redacta el documento y no prueba, ni evalúa, ni verifica de manera independiente la exactitud o integridad de ninguna información ni la solidez de ningún juicio contenido en ella.

Finalidad del PMBOK

La finalidad principal del PMBOK es identificar, concentrar y publicar las mejores prácticas generalmente aceptadas en la Dirección de Proyectos.

Generalmente aceptadas se refiere a que los conocimientos y las prácticas descritos son aplicables a la mayoría de los proyectos, la mayor parte del tiempo, y que existe un amplio consenso sobre su valor y utilidad.

Mejores prácticas se refiere a que existe un acuerdo general en que la correcta aplicación de estas habilidades, herramientas y técnicas puede aumentar las posibilidades de éxito de una amplia variedad de proyectos diferentes.

¿Cómo se organiza el PMBOK?

La base del PMBOK son los procesos, los cuales se clasifican por grupos y áreas de conocimiento:

- Grupos de Procesos: modo lógico de agrupar los procesos de dirección de proyectos, necesarios para cualquier proyecto, con dependencias entre ellos, y que se llevan a cabo en la misma secuencia siempre. Son los siguientes: Iniciación, Planificación, Ejecución, Seguimiento y Control y Cierre
- Áreas de Conocimiento: categoría que agrupa elementos en común. Son 9 en total: Integración, Alcance, Tiempo, Coste, Calidad, Comunicaciones, Recursos Humanos, Riesgo y Adquisiciones

¿A quién está dirigido el PMBOK?

Los conocimientos contenidos en el PMBOK proporcionan una referencia internacional para cualquiera que esté interesado en la profesión de la Dirección de Proyectos. Entre ellos se pueden mencionar: Altos ejecutivos, Gerentes de programa y gerentes de directores de proyectos, Directores del proyecto y otros miembros del equipo del proyecto, Miembros de una oficina de gestión de proyectos, Clientes y otros interesados, Consultores Formadores, Empresas , etc.

Fortalezas de PMBOK

- ✓ La guía de PMBOK es un marco y un estándar.
- ✓ Está orientada a procesos.
- ✓ Indica el conocimiento necesario para manejar el ciclo vital de cualquier proyecto, programa y portafolio a través de sus procesos.
- ✓ Define para cada proceso sus entradas, herramientas, técnicas y reportes necesarios.
- ✓ Define un cuerpo de conocimiento en el que cualquier industria pueda construir las mejores prácticas específicas para su área de aplicación

Limitaciones de PMBOK

- ✓ Complejo para los pequeños proyectos
- ✓ Tiene que ser adaptado a la industria del área de aplicación, tamaño y alcance del proyecto, el tiempo y el presupuesto y las exigencias de calidad.

¿Qué necesidades satisface PMBOK?

Por lo que respecta a las TI, PMBOK aporta principalmente elementos para satisfacer las necesidades de administración de proyectos de TI.

Los proyectos son una forma de organizar las actividades que no pueden ser tratadas dentro de los límites operativos de la organización. Así mismo, los proyectos se utilizan para lograr los objetivos definidos en el plan estratégico de la empresa, independientemente si el proyecto es administrado por la propia organización, o si corresponde a un proveedor de servicios externo.

Por lo anterior, las mejores prácticas integradas en PMBOK ayudan al departamento de TI a lograr los resultados esperados de los proyectos informáticos de forma más efectiva, garantizando que éstos sirven como inductores para la consecución de los objetivos definidos en el plan estratégico.

3.1.3.2 RELACIÓN DEL PMBOK CON LA DIRECCIÓN DE LAS TIC

En los siguientes apartados se analiza la relación del PMBOK con las diversas normas, modelos, marcos, prácticas, etc. que se pueden aplicar al ámbito de la dirección de las TIC.

BSC (Balanced Scorecard)

Contempla un sistema de administración del desempeño que permite a las empresas conducir su estrategia acorde a lo planeado mediante el monitoreo continuo, complementando los indicadores financieros tradicionales con criterios de medición de desempeño orientados a: “Clientes”, “Procesos Internos” y “Aprendizaje y Crecimiento”. Las mejores prácticas definidas en PMBOK sirven como referencia para la administración de los proyectos que sustentan la consecución de la estrategia de la empresa, la cual puede ser definida e implementada mediante Balanced Scorecard.

COBIT (Control Objectives for Information and Related Technology)

Es un compendio de objetivos de control para la Tecnología de Información que incluye herramientas de soporte que permiten a la administración cubrir la brecha entre los requerimientos de control, los aspectos tecnológicos y los riesgos de negocio.

Las mejores prácticas definidas en PMBOK están relacionadas con los objetivos de control “Administrar las Inversiones de TI”, “Administrar la Calidad”, “Evaluar y Administrar los Riesgos de TI”, “Administrar los Proyectos de TI” y “Aprovisionamiento de los Recursos de TI” definidos en COBIT.

IT Governance

Es un conjunto de mecanismos utilizados por la administración de una organización para dirigir y controlar su desarrollo tecnológico, asegurando que las metas del negocio sean alcanzadas de forma efectiva mediante la detección y control de los riesgos asociados. IT Governance puede tomar como referencia las áreas de conocimiento definidas en PMBOK para determinar las habilidades y conocimientos necesarios para la administración efectiva de los proyectos dentro de un ambiente de TI.

CMMI (Capability Maturity Model Integration)

Es un modelo de mejora de procesos de construcción de software que puede tomar como referencia PMBOK para administrar los proyectos orientados a mejorar la capacidad y madurez de los procesos involucrados en la construcción de software.

ITIL (Information Technology Infrastructure Library)

Es el marco de referencia para la Gestión de Servicios de TI más aceptado y utilizado en el mundo. Proporciona un conjunto de mejores prácticas en materia de administración de TI extraídas de organismos del sector público y privado que están a la vanguardia tecnológica a nivel internacional.

ISO 9000

Es el estándar para establecer sistemas de gestión de calidad más reconocido y adoptado en el mundo, debido a los beneficios que brinda el uso de sus normas definidas para establecer, documentar, controlar, medir y mejorar los procesos y productos dentro de la organización.

3.1.3.3 ESTRUCTURA DEL PMBOK

La Guía del PMBOK está dividida en tres secciones:

Sección I. Marco Conceptual de la Dirección de Proyectos: proporciona una estructura básica para entender la Dirección de Proyectos.

Se definen los términos clave y proporciona una descripción general del resto de la Guía del PMBOK. También se describe el Ciclo de Vida del Proyecto y la Organización.

Sección II. Norma para la Dirección de Proyectos aplicable a un proyecto: especifica todos los procesos de Dirección de Proyectos que usa el equipo del proyecto para gestionar el mismo.

Se describen los cinco Grupos de Procesos de Dirección de Proyectos aplicables a cualquier proyecto y los procesos de Dirección de Proyectos que componen tales grupos.

Un grupo de procesos es un modo lógico de agrupar los procesos de dirección de proyectos, necesarios para cualquier proyecto, con dependencias entre ellos, y que se llevan a cabo en la misma secuencia siempre. Son los siguientes:

Procesos de inicio: procesos mediante los cuales se lleva a cabo la autorización formal para comenzar un proyecto.

Procesos de Planificación: procesos que deberán refinar los objetivos planteados durante el grupo de procesos de Inicio y planificar el curso de acción requerido para lograr los objetivos y el alcance pretendido del proyecto.

Procesos de Ejecución: procesos que se despliegan para completar el trabajo definido en el grupo de procesos de Planificación con objeto de cumplir los requisitos del proyecto.

Procesos de Control: procesos realizados para medir y supervisar regularmente el avance del proyecto, de manera que se puedan identificar las variaciones respecto a la planificación y adoptar, cuando sea necesario, las acciones correctivas, preventivas y de control de cambios para cumplir con los objetivos del proyecto.

Procesos de Cierre: procesos requeridos para cerrar formalmente un proyecto y que aseguran que las experiencias adquiridas durante el proyecto queden registradas y a disposición de futuros usos.

Sección III: Áreas de Conocimiento de la Dirección de Proyectos: organiza los 42 procesos de Dirección de Proyectos en nueve Áreas de Conocimiento. La introducción de la Sección III describe la leyenda de los

diagramas de flujo de procesos que se usan en cada capítulo de Área de Conocimiento y en la introducción de todas las Áreas de conocimiento.

Un equipo de proyectos funciona en 9 áreas de conocimiento con un número de procesos básicos según el resumen que presentamos a continuación:

- **Integración.** Desarrollo de la carta del proyecto, la declaración del alcance y el plan. Dirección, supervisión y control del proyecto.
- **Alcance.** Planificación, definición, creación, verificación y control de la estructura de desglose de trabajo (EDT).
- **Tiempo.** Definición, secuenciación, estimación de recursos necesarios y de la duración, desarrollo y control del cronograma.
- **Costo.** Planificación de recursos, costos estimados, presupuesto y control.
- **Calidad.** Planificación de la calidad, aseguramiento de calidad y control de calidad.
- **Recursos Humanos.** Planificación, contratación, desarrollo y administración de los Recursos Humanos.
- **Comunicaciones.** Planificación de comunicaciones, distribución de la información, difusión del desempeño, Gestión de *stakeholders* (*interesados*).
- **Riesgos.** Planificación e identificación de riesgos, Análisis de riesgos (cualitativa y cuantitativa), planificación de la respuesta ante riesgos (acción), y supervisión y control del riesgo.
- **Adquisiciones.** Plan de contrataciones y adquisiciones, selección e incentivos de los vendedores, administración y cierre de contratos

En los siguientes apartados se comenta cada una de dichas áreas de conocimiento, describiendo cada uno de los procesos que las componen.

3.1 GESTIÓN DE LA INTEGRACIÓN DEL PROYECTO

Describe los procesos y actividades que forman parte de los diversos elementos de la Dirección de Proyectos, que se identifican, definen, combinan, unen y coordinan dentro de los Grupos de Procesos de Dirección de Proyectos. Se compone de los procesos:

- Desarrollar el **Acta de Constitución del Proyecto**: Se autoriza formalmente el proyecto o una fase del mismo, documentándose los requisitos iniciales que satisfagan las necesidades y expectativas de los interesados.
- Desarrollar el **Plan para la Dirección del Proyecto**: Se documentan las acciones necesarias para definir, preparar, integrar y coordinar todos los planes subsidiarios.
- **Dirigir y Gestionar** la Ejecución del Proyecto: Se lleva a cabo el trabajo definido en el plan para la dirección del proyecto para así cumplir con los objetivos del mismo.
- **Monitorear y Controlar** el Trabajo del Proyecto: Se monitorea, revisa y regula el avance para ver las posibles desviaciones respecto a las líneas base definidas en el plan para la dirección del proyecto.
- Realizar el **Control Integrado de Cambios**: Se revisan todas las solicitudes de cambio, además de aprobar y gestionar los cambios.
- **Cerrar** el Proyecto o una Fase: Se finalizan todas las actividades, dando por completado formalmente el proyecto o una fase del mismo.

3.2.1 EL PLAN GENERAL DEL PROYECTO

Desarrollar el Plan para la Dirección del Proyecto es el proceso que consiste en documentar todas las acciones necesarias para definir, preparar, integrar y coordinar todos los planes subsidiarios. El plan para la dirección del proyecto define el modo en que el proyecto se ejecuta, se monitorea, se controla y se cierra. En función del área de aplicación y de la

complejidad del proyecto, el contenido del plan para la dirección del proyecto podrá variar. El plan para la dirección del proyecto se desarrolla a través de una serie de procesos integrados hasta llegar al cierre del proyecto.

Este proceso da lugar a un plan para la dirección del proyecto que se elabora de forma gradual por medio de actualizaciones, y se controla y se aprueba a través del proceso Realizar el Control Integrado de Cambios

3.3 GESTIÓN DEL ALCANCE DEL PROYECTO

Describe los procesos necesarios para asegurarse que el proyecto incluya todo el trabajo requerido para completarse satisfactoriamente. Se compone de los procesos:

- **Recopilar Requisitos:** Se documentan las necesidades de los interesados para convertirlas en requisitos del proyecto.
- **Definir** el Alcance: Se desarrolla el enunciado del alcance detallado, el qué.
- Crear la **Estructura de Desglose del trabajo** o EDT: Descomponer el proyecto en partes más pequeñas.
- **Verificar** el Alcance: Conseguir la aceptación formal del alcance por parte del cliente o patrocinador.
- **Controlar** el Alcance: Gestionar los cambios en el alcance.

En el contexto del proyecto, el término alcance puede referirse a:

- **Alcance del producto:** Las características y funciones que definen un producto, servicio o resultado.
- **Alcance del proyecto:** El trabajo que debe realizarse para entregar un producto, servicio o resultado con las características y funciones especificadas.

3.4 GESTIÓN DEL TIEMPO DEL PROYECTO

Describe los procesos relativos a la puntualidad en la conclusión del proyecto. Se compone de los procesos:

- **Definir** las Actividades: Se identifica cada una de las actividades que se deben realizar para lograr un proyecto exitoso.
- **Secuenciar** las Actividades: Se analiza qué tipo de dependencias existe entre las distintas actividades.
- Estimar los **Recursos** de las Actividades: Se determina cuáles son los recursos necesarios y disponibles para llevar a cabo cada actividad.
- Estimar la **Duración** de las Actividades: Se estima el tiempo necesario para completar las actividades.
- Desarrollar el **Cronograma**: Se analiza la integración existente entre la secuencia, los recursos necesarios, las restricciones y la duración de cada actividad.
- **Controlar el Cronograma**: Se administran los cambios en el cronograma

3.4.1 TÉCNICAS DE PLANIFICACIÓN

Método de la Ruta Crítica: El método de la ruta crítica calcula las fechas teóricas de inicio y finalización tempranas y tardías para cada una de las actividades, sin tener en cuenta las limitaciones de recursos, realizando un análisis que recorre hacia adelante y hacia atrás la red del cronograma.

Método de la Cadena Crítica: Consiste en modificar el cronograma del proyecto teniendo en cuenta la restricción de recursos.

Nivelación de recursos: Se modifica la programación del proyecto para mejorar la eficiencia en cuanto a asignación de recursos.

Análisis “que pasa si”: Se realizan simulaciones de cómo cambiaría el cronograma del proyecto si cambiásemos alguna de las variables que lo afectan

Aplicación de Adelantos y Retrasos: Los adelantos y retrasos son una técnica de refinamiento que se aplica durante el análisis de la red para desarrollar un cronograma viable.

Compresión del cronograma: Consiste en acortar el cronograma del proyecto sin modificar el alcance. Dos de las técnicas más utilizadas son:

- Compresión (Intensificación o Crashing): se agregan más recursos al proyecto para acortar la duración. Por lo general, esta técnica implicará mayores costos.
- Ejecución rápida (fast-tracking): se realizan actividades en paralelo para acelerar el proyecto, agregando riesgos al mismo.

3.5 GESTIÓN DE LOS COSTOS DEL PROYECTO

Describe los procesos involucrados en la planificación, estimación, presupuesto y control de costes de forma que el proyecto se complete dentro del presupuesto aprobado. Se compone de los procesos:

- **Estimar** los Costos: Se calculan los costos de cada recurso para completar las actividades del proyecto.
- Determinar el **Presupuesto:** Se suman los costos de todas las actividades del proyecto a través del tiempo.
- **Controlar** los Costos: Se influye sobre las variaciones de costos y se administran los cambios del presupuesto

Existen diversos tipos de costos, a continuación mencionaremos los principales.

- **Costos variables:** dependen del volumen de producción.
- **Costos fijos:** no cambian con el volumen de producción.
- **Costos directos:** se pueden atribuir directamente al proyecto.
- **Costos indirectos:** benefician a varios proyectos y generalmente no se puede identificar con exactitud la proporción que corresponde a cada uno
- **Costo de oportunidad:** el costo de oportunidad de un recurso es su mejor alternativa dejada de lado.
- **Costos hundidos o enterrados:** costos que ya fueron devengados y no cambiarán con la decisión de hacer o no hacer el proyecto

3.5.1 PRESUPUESTOS

Para realizar los presupuestos se cuenta con las siguientes herramientas y técnicas:

Suma de Costos

Las estimaciones de costos se suman por paquetes de trabajo, de acuerdo con la EDT; a continuación se van sumando los niveles superiores de componentes de la EDT, tales como las cuentas de control, y finalmente el proyecto completo.

Análisis de Reserva

El análisis de reserva del presupuesto puede establecer tanto las reservas para contingencias como las de gestión del proyecto. Las reservas para contingencias son asignaciones para aquellos cambios que no han sido planificados previamente, pero que son potencialmente necesarios. Las reservas de gestión son presupuestos reservados para cambios no planificados al alcance y al costo del proyecto. Las reservas no forman parte de la línea base de costo, pero pueden incluirse en el presupuesto total del proyecto.

Juicio de Expertos

Es aquel que se obtiene en base a la experiencia en un área de aplicación, un área de conocimiento, una disciplina, una industria, etc., según resulte apropiado para la actividad que se está desarrollando, y que debe utilizarse para determinar el presupuesto. El juicio de expertos puede provenir de diversas fuentes, entre otras:

- otras unidades dentro de la organización ejecutante
- consultores
- interesados, incluyendo clientes
- asociaciones profesionales y técnicas
- grupos industriales

Relaciones Históricas

Cualquier relación histórica que dé como resultado estimaciones paramétricas o análogas implica el uso de características (parámetros) del proyecto para desarrollar modelos matemáticos que permitan predecir los costos totales del proyecto. Estos modelos pueden ser simples (p.ej., construir una vivienda costará una cierta cantidad por metro cuadrado de espacio útil) o complejas (p.ej., un modelo de costo de desarrollo de software utiliza varios factores de ajuste separados, con múltiples criterios por cada uno de esos factores).

3.6 GESTIÓN DE LA CALIDAD DEL PROYECTO

Describe los procesos necesarios para asegurarse de que el proyecto cumpla con los objetivos para los cuales ha sido emprendido. Se compone de los procesos:

- **Planificar la Calidad:** Se establece qué normas son relevantes y cómo se van a satisfacer.
- **Asegurar la Calidad:** Se utilizan los procesos necesarios para cumplir con los requisitos del proyecto. Dicho de otro modo, se asegura que se estén utilizando los planes para la gestión de calidad.

- **Controlar la Calidad:** Se supervisa que el proyecto esté dentro de los límites pre-establecidos.

En todo proyecto es sumamente importante dedicar tiempo a la gestión de calidad para:

- Prevenir errores y defectos
- Evitar realizar de nuevo el trabajo, lo que implica ahorrar tiempo y dinero
- Tener un cliente satisfecho

La gestión de la calidad implica que el proyecto satisfaga las necesidades por las cuales se emprendió. Para ello será necesario lo siguiente:

- Convertir las necesidades y expectativas de los interesados en requisitos del proyecto
- Lograr la satisfacción del cliente cuando el proyecto produzca lo planificado y el producto cubra las necesidades reales
- Realizar acciones de prevención sobre la inspección
- Buscar de forma permanente la perfección: mejora continua

La gestión moderna de la calidad complementa la dirección de proyectos. Ambas disciplinas reconocen la importancia de:

- **La satisfacción del cliente.** Entender, evaluar, definir y gestionar las expectativas, de modo que se cumplan los requisitos del cliente.
- **La prevención antes que la inspección.** Uno de los preceptos fundamentales de la gestión moderna de la calidad establece que la calidad se planifica, se diseña y se integra (y no se inspecciona).

- **La mejora continua.** El ciclo planificar-hacer-revisar-actuar es la base para la mejora de la calidad, según la definición de Shewhart, modificada por Deming.
- **La responsabilidad de la dirección.** El éxito requiere la participación de todos los miembros del equipo del proyecto, pero proporcionar los recursos necesarios para lograr dicho éxito sigue siendo responsabilidad de la dirección.

3.6.1 PLAN DE CALIDAD

El plan de gestión de calidad describe cómo el equipo de dirección del proyecto implementará la política de calidad de la organización ejecutante. Es un componente o un plan subsidiario del plan para la dirección del proyecto. El plan de gestión de calidad proporciona entradas al plan general para la dirección del proyecto y comprende: el control de calidad, el aseguramiento de la calidad y métodos de mejora continua de los procesos del proyecto.

El plan de gestión de calidad puede ser redactado de modo formal o informal, muy detallado o formulado de manera general. El formato y el grado de detalle se determinan según los requisitos del proyecto. El plan de gestión de calidad debe revisarse en las etapas iniciales del proyecto, para asegurarse que las decisiones estén basadas en informaciones precisas. Los beneficios de esta revisión pueden incluir la reducción del costo y sobrecostos en el cronograma ocasionados por el reproceso.

3.7 GESTIÓN DE LOS RECURSOS HUMANOS DEL PROYECTO

La Gestión de los Recursos Humanos del Proyecto incluye los procesos que organizan, gestionan y conducen el equipo del proyecto. El equipo del proyecto está conformado por aquellas personas a las que se les

han asignado roles y responsabilidades para completar el proyecto. Se compone de los procesos:

- Desarrollar el **Plan de Recursos Humanos**: Se definen los roles, responsabilidades y habilidades de los miembros del equipo, así como las relaciones de comunicación.
- **Adquirir** el equipo: Se obtienen los recursos humanos necesarios para llevar a cabo las actividades del proyecto.
- **Desarrollar** el equipo: Se mejoran las competencias y las habilidades de interacción entre los miembros del equipo.
- **Gestionar** el equipo: Se monitorea el desempeño individual y de grupo de cada persona y se resuelven los conflictos que suelen ocurrir entre los miembros del equipo.

3.7.1 CAPACIDADES DEL JEFE DE PROYECTO

Los directores de proyecto usan una combinación de habilidades técnicas, humanas y conceptuales para analizar las situaciones e interactuar de manera apropiada con los miembros del equipo. Mediante dichas habilidades, los directores de proyecto podrán sacar provecho de los puntos fuertes de los miembros del equipo.

Algunas de las habilidades interpersonales usadas con mayor frecuencia por los directores del proyecto se describen brevemente a continuación.

Liderazgo. Los proyectos exitosos requieren fuertes habilidades de liderazgo. El liderazgo es importante en todas las fases del ciclo de vida del proyecto. Es fundamental comunicar la visión e inspirar al equipo del proyecto a fin de lograr un alto desempeño.

Existen distintos estilos de **liderazgo** como por ejemplo:

- Directivo: decir qué hay que hacer

- Consultivo (Coaching): dar instrucciones
- Participativo (Supporting): ofrecer asistencia
- Delegativo (Empowerment): el empleado decide por sí solo
- Facilitador: coordina a los demás
- Autocrático: tomar decisiones sin consultar
- Consenso: resolución de problemas grupales

Influencia. Dado que a menudo la autoridad directa de los directores del proyecto sobre los miembros de su equipo es escasa o nula en una organización de tipo matricial, su capacidad de influir en los interesados resulta vital para el éxito del proyecto. Entre las habilidades clave de influencia se encuentran:

- Tener la habilidad para persuadir y expresar con claridad los puntos de vista y las posiciones asumidas.
- Contar con gran habilidad para escuchar de manera activa y eficaz.
- Tener en cuenta las diversas perspectivas en cualquier situación.
- Recopilar información relevante y crítica a fin de abordar los asuntos importantes y lograr acuerdos.

Toma de decisiones eficaz. Esto implica tener la habilidad de negociar e influir sobre la organización y el equipo de dirección del proyecto. Algunas pautas en materia de toma de decisiones incluyen:

- centrarse en los objetivos perseguidos
- seguir un proceso de toma de decisiones
- desarrollar las cualidades personales de los miembros del equipo
- fomentar la creatividad del equipo
- gestionar las oportunidades y los riesgos

3.8 GESTIÓN DE LAS COMUNICACIONES DEL PROYECTO

Describe los procesos relacionados con la generación, distribución, almacenamiento y destino final de la información del proyecto en tiempo y forma. Se compone de los procesos:

- **Identificar** a los Interesados: Se identifica a todas las personas u organizaciones que de alguna manera se verán afectadas por el proyecto.
- **Planificar** las Comunicaciones: Se determinan cuáles serán las necesidades de información del proyecto.
- **Distribuir** la Información: Se coloca la información a disposición de los interesados.
- **Gestionar las Expectativas** de los Interesados: Se satisfacen los requisitos de los interesados y se resuelven los conflictos entre los recursos humanos.
- **Informar** el Desempeño: Se comunica el estado de avance del proyecto.

En el momento de distribuir la información hay que tener en cuenta las distintas dimensiones de la comunicación:

- Interna: entre las personas que forman parte del proyecto
- Externa: hacia los interesados externos del proyecto
- Vertical: entre jefe-empleado y viceversa
- Horizontal: entre colegas del proyecto
- Escrita formal: planes, solicitud, etc.
- Escrita informal: memos, e-mails, notas
- Oral formal: presentaciones
- Oral informal: reuniones, conversaciones

La mayoría de las habilidades de comunicación son comunes a la dirección en general y a la dirección de proyectos. Entre estas habilidades, se incluye:

- escuchar de manera activa y eficaz
- formular preguntas, sondear ideas y situaciones para garantizar una mejor comprensión
- educar para aumentar el conocimiento del equipo a fin de que sea más eficaz
- investigar para identificar o confirmar la información
- identificar y gestionar expectativas
- persuadir a una persona u organización para llevar a cabo una acción
- negociar a fin de lograr acuerdos entre partes que resulten mutuamente aceptables
- resolver conflictos para prevenir impactos negativos

3.9 GESTIÓN DE LOS RIESGOS DEL PROYECTO

No se debería comenzar con la ejecución del proyecto sin un análisis de riesgo. La planificación de los riesgos es un área integradora del resto de las áreas del conocimiento. Por ejemplo, no podemos afirmar que tenemos un cronograma y presupuesto realista si todavía no hemos finalizado el análisis de riesgo. Con el análisis de riesgo se determinarán las reservas para contingencia de plazos y costos que deben incluirse en el plan para la dirección del proyecto. Se compone de los procesos:

- **Planificar** la Gestión de Riesgos: Se definen las actividades de gestión de los riesgos para un proyecto.
- **Identificar** los Riesgos: Una vez realizado el plan de gestión de riesgos, es necesario comenzar con la identificación de los eventos con riesgo que, si ocurriesen, afectarían el resultado del proyecto ya sea para bien o para mal.

- Realizar el **Análisis Cualitativo de Riesgos**: Se priorizan los riesgos para realizar otros análisis o acciones posteriores, evaluando y combinando la probabilidad de ocurrencia y el impacto de dichos riesgos. Para ello se pueden usar las siguientes herramientas y técnicas:
 - **Evaluación de probabilidad e impacto**: se estima cuál es la probabilidad de ocurrencia y el impacto de cada riesgo identificado.
 - **Matriz de probabilidad e impacto**: tabla de doble entrada donde se combina la probabilidad y el impacto para poder hacer una priorización de los riesgos.
 - **Categorización de los riesgos**: se agrupan los riesgos por causas comunes
- Realizar el **Análisis Cuantitativo de Riesgos**: Se analiza numéricamente el efecto de los riesgos identificados sobre los objetivos generales del proyecto. Para ello se pueden usar las siguientes herramientas y técnicas:
 - **Distribuciones de probabilidad**: uniforme, triangular, beta, normal, log normal, poisson, F, Chi-cuadrada, etc.
 - **Valor monetario esperado**: se obtiene de multiplicar la probabilidad de ocurrencia por el impacto en valor monetario
 - **Árbol de decisión**: diagrama que describe las implicaciones de elegir una u otra alternativa entre todas las disponibles.
- **Planificar la Respuesta** a los Riesgos: Se desarrollan las acciones para mejorar las oportunidades y reducir las amenazas a los objetivos del proyecto. Para los **riesgos negativos** se suelen utilizar las siguientes estrategias o herramientas: evitar, transferir, mitigar o aceptar. Por su parte, para los **riesgos positivos** se suelen utilizar las siguientes estrategias o herramientas: explotar, compartir, mejorar, aceptar.

- **Monitorear y Controlar** los Riesgos: Se implementan planes de respuesta a los riesgos, se rastrean los riesgos identificados, se monitorean los riesgos residuales, se identifican nuevos riesgos y se evalúa la efectividad del proceso contra riesgos a través del proyecto.

3.9.1 CONTINGENCIAS

Algunas estrategias están diseñadas para ser usadas únicamente si se presentan determinados eventos. Para algunos riesgos, resulta apropiado para el equipo del proyecto elaborar un plan de respuesta que sólo se ejecutará bajo determinadas condiciones predefinidas, si se cree que habrá suficientes señales de advertencia para implementar el plan. Los eventos que disparan la respuesta para contingencias, tales como no cumplir con hitos intermedios u obtener una prioridad más alta con un proveedor, deben definirse y rastrearse.

Reservas para contingencias

Para aquellos riesgos conocidos, identificados y cuantificados, se puede estimar una reserva monetaria para contingencias, que no forma parte de la línea base de costo del proyecto. Por su parte, los riesgos desconocidos no se pueden gestionar de manera proactiva y podrían considerarse asignando una reserva de gestión general al proyecto, que no forma parte de la línea base de costo, pero sí se incluye en el presupuesto total del proyecto

3.10 GESTIÓN DE LAS ADQUISICIONES DEL PROYECTO

Describe los procesos para comprar o adquirir productos, servicios o resultados, así como para contratar procesos de dirección. Se compone de los procesos:

- **Planificar** las Adquisiciones: Se documentan las decisiones de compra para el proyecto, especificando cómo hacerlo e identificando a los posibles vendedores.
- **Efectuar** las Adquisiciones: Se obtienen las respuestas de los vendedores, seleccionando los más ventajosos para el proyecto y adjudicando los contratos.
- **Administrar** las Adquisiciones: Se gestionan las relaciones de adquisiciones, se monitoriza la ejecución de los contratos, y se efectúan cambios y correcciones según sea necesario.
- **Cerrar** las Adquisiciones: Se completa cada adquisición para el proyecto.

Los procesos de Gestión de las Adquisiciones del Proyecto implican la realización de contratos, que son documentos legales que se establecen entre un comprador y un vendedor. Dicho documento representa un acuerdo vinculante para las partes en virtud del cual el vendedor está obligado a proveer los productos, servicios o resultados especificados, y el comprador debe proporcionar dinero o cualquier otra contraprestación válida. Un contrato de adquisición incluye términos y condiciones, y puede incorporar otros aspectos especificados por el comprador para establecer lo que el vendedor debe realizar o proporcionar. Es responsabilidad del equipo de dirección del proyecto asegurar que todas las adquisiciones cumplen las necesidades del proyecto, a la vez que se respetan las políticas de la organización en cuanto a adquisiciones se refiere.

Bibliografía:

Guía de los fundamentos para la dirección de proyectos (Guía del PMBOK)
4ª Edición.

Sitios web:

<http://www.pmi.org> Project Management Institute®

Autor:

Ramón Seoane Freijido

Director de Sistemas de Información Molduras del Noroeste

Colegiado del CPEIG



4. SISTEMAS DE GESTIÓN DE CALIDAD. NORMALIZACIÓN Y CERTIFICACIÓN. EFQM. SERIE ISO 9000.

Tema 4. Sistemas de Gestión de Calidad. Normalización y certificación. EFQM. Serie ISO 9000.

INDICE

4.1 Normalización y certificación

4.1.1 Normalización. Conceptos básicos

4.1.2 Certificación. Pasos

4.2 EFQM. Modelo EFQM de excelencia

4.2.1 Introducción al modelo

4.2.2 ¿Qué es la EFQM?

4.2.3 Historia de la EFQM

4.2.4 ¿Qué es el modelo EFQM?

4.2.5 ¿Para qué sirve el modelo EFQM?

4.2.6 Composición del modelo EFQM

4.2.7 Ventajas de adoptar el modelo EFQM

4.2.8 Cambios que origina la excelencia en gestión

4.3 Serie ISO 9000

4.3.1 Introducción

4.3.2 La familia de normas ISO 9000

4.3.3 Principios de gestión

4.3.4 Versiones específicas de la norma ISO 9000

4.3.5 Costos y beneficios de establecer un sistema de gestión de la calidad

4.3.6 Implementación de un sistema de gestión de la calidad

4.1 NORMALIZACIÓN Y CERTIFICACIÓN.

4.1.1 NORMALIZACIÓN. CONCEPTOS BÁSICOS.

¿Qué se entiende por normalización?

La normalización es una actividad colectiva encaminada a establecer soluciones a situaciones repetitivas.

En particular, esta actividad consiste en la elaboración, difusión y aplicación de normas.

La normalización ofrece importantes beneficios, como consecuencia de adaptar los productos, procesos y servicios a los fines a los que se destinan, proteger la salud y el medio ambiente, prevenir los obstáculos al comercio y facilitar la cooperación tecnológica.

¿Qué es una norma?

Las normas son documentos técnicos con las siguientes características:

- Contienen especificaciones técnicas de aplicación voluntaria.
- Son elaborados por consenso de las partes interesadas:
- Están basados en los resultados de la experiencia y el desarrollo tecnológico.
- Son aprobados por un Organismo Nacional/Regional/Internacional de Normalización reconocido.
- Están disponibles al público.

Las normas ofrecen un lenguaje común de comunicación entre las empresas, la Administración y los usuarios y consumidores, establecen un equilibrio socioeconómico entre los distintos agentes que participan en las transacciones comerciales, base de cualquier economía de mercado, y son un patrón necesario de confianza entre cliente y proveedor.

¿Qué ventajas ofrece la normalización?

a) Para los consumidores:

- Establece niveles de calidad y seguridad de los productos y servicios.
 - Informa de las características del producto.
 - Facilita la comparación entre diferentes ofertas.
- b) Para los fabricantes:
- Racionaliza variedades y tipos de productos.
 - Disminuye el volumen de existencias en almacén y los costes de producción.
 - Mejora la gestión y el diseño.
 - Agiliza el tratamiento de los pedidos.
 - Facilita la comercialización de los productos y su exportación.
 - Simplifica la gestión de compras.
- c) Para la Administración:
- Simplifica la elaboración de textos legales.
 - Establece políticas de calidad, medioambientales y de seguridad.
 - Ayuda al desarrollo económico.
 - Agiliza el comercio.

¿Qué se puede normalizar?

El campo de actividad de las normas es tan amplio como la propia diversidad de productos o servicios, incluidos sus procesos de elaboración.

Así, se normalizan los Materiales (plásticos, acero, papel, etc.), los Elementos y Productos (tornillos, televisores, herramientas, tuberías, etc.), las Máquinas y Conjuntos (motores, ascensores, electrodomésticos, etc.), Métodos de Ensayo, Temas Generales (medio ambiente, calidad del agua, reglas de seguridad, estadística, unidades de medida, etc.), Gestión y Aseguramiento de la Calidad, Gestión Medioambiental (gestión, auditoría, análisis del ciclo de vida, etc.), Gestión de prevención de riesgos en el trabajo (gestión y auditoría), etc.

¿Qué clases de normas existen?

Los documentos normativos pueden ser de diferentes tipos dependiendo del organismo que los haya elaborado.

En la clasificación tradicional de normas se distingue entre:

- Normas nacionales. Son elaboradas, sometidas a un período de información pública y sancionadas por un organismo reconocido legalmente para desarrollar actividades de normalización en un ámbito nacional. En España estas normas son las normas UNE, aprobadas por AENOR, que es el organismo reconocido por la Administración Pública española para desarrollar las actividades de normalización en nuestro país (Real Decreto 2000/1995).
- Normas regionales. Son elaboradas en el marco de un organismo de normalización regional, normalmente de ámbito continental, que agrupa a un determinado número de Organismos Nacionales de Normalización. Las más conocidas, aunque no las únicas, son las normas europeas elaboradas por los Organismos Europeos de Normalización (CEN, CENELEC, ETSI), y preparadas con la participación de representantes acreditados de todos los países miembros. AENOR es el organismo nacional de normalización español miembro de CEN y CENELEC y, por lo tanto, la organización a través de la cual se canalizan los intereses y la participación de los agentes socioeconómicos de nuestro país en la normalización europea.
- Normas internacionales. Tienen características similares a las normas regionales en cuanto a su elaboración, pero se distinguen de ellas en que su ámbito es mundial. Las más representativas por su campo de actividad son las normas CEI/IEC (Comité Electrotécnico Internacional) para el área eléctrica, las UIT/ITU (Unión Internacional de Telecomunicaciones) para el sector de las telecomunicaciones y las normas ISO (Organización Internacional de Normalización) para el resto. AENOR es el organismo nacional de normalización español miembro de ISO y CEI y, por lo tanto, la

organización a través de la cual se canalizan los intereses y la participación de los agentes socioeconómicos de nuestro país en la normalización internacional.

¿Qué es una norma UNE?

Una norma UNE es una especificación técnica de aplicación repetitiva o continuada cuya observancia no es obligatoria, establecida con participación de todas las partes interesadas, que aprueba AENOR, organismo reconocido a nivel nacional e internacional por su actividad normativa (Ley 21/1992, de 16 de julio, de Industria).

¿Cómo se elabora una norma UNE?

La elaboración de una norma UNE, incluida la adopción de normas europeas, se lleva a cabo en el seno de los Comités Técnicos de Normalización (CTN) a través de las siguientes fases:

- Trabajos preliminares (recopilación de documentación, discusión sobre el contenido...) previos a la toma en consideración de una nueva iniciativa;
- Elaboración del proyecto de norma; incluye todas aquellas actividades que se desarrollan por el Comité hasta la aprobación de un documento como proyecto de norma, buscando siempre el consenso de todas las partes;
- Información pública en el BOE; anuncio de la existencia del proyecto de norma, tanto nacional como europea, para que cualquier persona, física o jurídica, pueda remitir las observaciones al mismo que estime oportunas;
- Elaboración de la propuesta de norma; una vez superada la fase anterior, y recibidas en AENOR las posibles observaciones al proyecto, el CTN

procede al estudio de las mismas y aprobación de la propuesta de norma final, para su consideración y adopción por AENOR;

- Registro, edición y difusión de la norma UNE; publicación de la norma UNE por AENOR, notificación a BOE, promoción y comercialización, a través de los servicios comerciales de AENOR.

4.1.2 CERTIFICACIÓN. PASOS.

El proceso de certificarse con base en ISO 9001, y de mantener este status una vez conseguido, se presenta en los pasos siguientes:

1. Cómo seleccionar un organismo de certificación

Las organizaciones que deseen obtener un certificado, deben presentar una solicitud al organismo de certificación de su elección. Los aspectos a considerar al seleccionar el organismo de certificación incluyen:

- Si la naturaleza de la acreditación del organismo de certificación es aceptable en el mercado al cual la organización desea exportar.
- La imagen del organismo de certificación en el mercado.
- Cotizaciones de las tarifas de certificación y auditorías, etc.

2. Preparación para la evaluación

De acuerdo con la ISO 9001, el primer requisito es definir los procesos de la organización que afectan a la calidad, de manera que el primer paso es que el auditor del organismo de certificación se reúna con la alta dirección de la organización, con el fin de que aquél obtenga una comprensión clara acerca de los procesos de la organización.

3. Auditoría

Los auditores recogen evidencia de conformidad o no conformidad mediante la observación de actividades, el examen de procedimientos/registros, observaciones de las condiciones de manejo de la

empresa, a través de entrevistas con los directores y personal involucrado de la organización, etc. La información recolectada mediante las entrevistas es verificada o ensayada por los auditores mediante la recolección de la misma información de otras fuentes, tales como observaciones físicas o mediciones realizadas en el producto y sus registros relacionados. Los auditores visitan y verifican la conformidad con el SGC en todos los departamentos y funciones dentro del alcance del SGC.

4. No conformidades

La evidencia recogida por los auditores es comparada con los criterios de la auditoría (políticas y objetivos de la compañía, manuales, procedimientos, instrucciones, contratos, reglamentaciones, etc.) y los hallazgos de las auditorías, incluidas las no conformidades, si las hay, son aclaradas y reportadas a la alta dirección al final de auditoría en el sitio, en una reunión formal con la alta dirección, llamada “Reunión de Cierre”. Las no conformidades (NC) son clasificadas por los auditores como “mayores” o “menores”. Las “observaciones” también se registran.

5. Otorgamiento del certificado ISO 9000

Con base a las recomendaciones del auditor y después de la revisión independiente de estas recomendaciones por el organismo certificador, éste expide un certificado a la organización. El certificado se expide para el alcance específico del negocio y para los productos o servicios para los cuales la organización ha implementado un SGC.

6. Auditorías de seguimiento

El certificado se otorga inicialmente por un período de tres años. Durante este tiempo, el organismo de certificación realiza auditorías de seguimiento periódicas (una o dos veces al año), en fechas acordadas mutuamente. El organismo de certificación informa previamente un plan de auditoría de tres años, en el que se indique el alcance de cada auditoría de seguimiento. Estas auditorías se planifican de manera que todos los

aspectos del SGC se auditen en un período de tres años. Después de los tres años se lleva a cabo una auditoría de re-certificación usando los pasos 2 y 5 anteriores.

4.2 EFQM. MODELO EFQM DE EXCELENCIA

4.2.1 INTRODUCCIÓN AL MODELO

El Modelo EFQM de Excelencia es un marco de trabajo no-prescriptivo que tiene nueve criterios. Los criterios que hacen referencia a un Agente Facilitador tratan sobre lo que la organización hace. Los criterios que hacen referencia a los Resultados tratan sobre lo que la organización logra. Los Resultados son consecuencia de los Agentes Facilitadores.

El Modelo, que reconoce que la Excelencia en todo lo referente a resultados y rendimiento de una organización se puede lograr de manera sostenida mediante distintos enfoques, se fundamenta en que:

"Los resultados excelentes con respecto al Rendimiento de la Organización, a los Clientes, las Personas y la Sociedad se logran mediante un Liderazgo que dirija e impulse la Política y Estrategia, las Personas de la organización, las Alianzas y Recursos, y los Procesos."

4.2.2 ¿QUÉ ES LA EFQM?

EFQM (European Foundation for Quality Management o Fundación Europea para la Gestión de la Calidad).

MISSION: Ser la fuerza que impulsa la Excelencia en las organizaciones europeas de manera sostenida.

VISION: Un mundo en el que las organizaciones europeas sobresalgan por su Excelencia

EFQM es una organización sin ánimo de lucro cuyo ámbito es Europa y su sede está en Bruselas.

EFQM es el creador y el gestor del premio a la Excelencia EEA (EFQM Excellence Award) que reconoce la Excelencia en Gestión en las organizaciones.

EFQM es la propietaria del Modelo de Excelencia EFQM y es la encargada de actualizarla con las buenas prácticas que se están llevando en las organizaciones punteras en el tema de la Excelencia en Gestión.

4.2.3 HISTORIA DE LA EFQM

1988 Fue creada la Fundación Europea para la Gestión de la Calidad (EFQM) siendo una organización sin ánimo de lucro formada por 14 organizaciones europeas (Bosch, BT, Bull, Ciba-Geigy, Dassault, Electrolux, Fiat, KLM, Nestlé, Olivetti, Philips, Renault, Sulzer y Volkswagen)

1989 Fue establecida la misión, visión y objetivos del EFQM y se comienzan los trabajos de desarrollo del Modelo Europeo de Calidad. Además, se añadieron otras 53 empresas.

1991 Nace el Modelo de Excelencia EFQM y se lanza el primer Premio Europeo de Calidad para empresas

1992 Se presenta el Premio Europeo de Calidad

1995 Se adapta el Modelo y lanza el Premio Europeo para el sector público

1996 Se simplifica el Modelo y lanza el Premio Europeo para pymes y unidades operativas

2003 Se actualiza el Modelo de Excelencia

2005 Se lanza el sistema 2005+ para la presentación de memorias y evaluación para el Premio EFQM a la Excelencia (EEA)

4.2.4 ¿QUÉ ES EL MODELO EFQM?

El Modelo EFQM de Excelencia es un instrumento práctico que ayuda a las organizaciones a establecer un sistema de gestión apropiado, midiendo en qué punto se encuentran dentro del camino hacia la

excelencia, identificando posibles carencias de la organización y definiendo acciones de mejora.

4.2.5 ¿PARA QUÉ SIRVE EL MODELO EFQM?

Es un marco que las organizaciones pueden utilizar para ayudarse a desarrollar su visión y las metas para el futuro de una manera tangible.

Es un instrumento que las organizaciones pueden utilizar para identificar y entender la naturaleza de su negocio, es decir, las relaciones entre los distintos agentes presentes en la actividad, y las relaciones causa-efecto.

Es una herramienta que permite establecer un mismo lenguaje y modo de pensar en toda la organización.

Es una herramienta de diagnóstico para determinar la salud actual de la organización, detectando puntos de mejora e implantando acciones que le ayuden a mejorar.

Es la base para la concesión del Premio EFQM a la Excelencia, esto es, un proceso de evaluación que permite a Europa reconocer a sus organizaciones mejor gestionadas y promoverlas como modelos de excelencia del que las demás organizaciones puedan aprender.

4.2.6 COMPOSICIÓN DEL MODELO EFQM

El Modelo de Excelencia EFQM es un marco no preceptivo basado en nueve criterios.

Cinco de estos son “Agentes Facilitadores” (Lo que la organización hace. Incluye 24 subcriterios) y cuatro son “Resultados” (Lo que la organización logra. Incluye 8 subcriterios). Total: 9 CRITERIOS, 32 subcriterios y 298 áreas a contemplar.

CRITERIO 1: LIDERAZGO

Cómo los líderes desarrollan y facilitan la consecución de la misión y la visión, desarrollan los valores necesarios para alcanzar el éxito a largo plazo e implantan todo ello en la organización mediante las acciones y los comportamientos adecuados, estando implicados personalmente en asegurar que el sistema de gestión de la organización se desarrolla e implanta.

Subcriterios

- 1a. Desarrollo de la misión, visión y valores por parte de los líderes, que actúan como modelo de referencia dentro de una cultura de Excelencia.
- 1b. Implicación personal de los líderes para garantizar el desarrollo, implantación y mejora continua del sistema de gestión de la organización.
- 1c. Implicación de los líderes con clientes, partners y representantes de la sociedad.
- 1d. Refuerzo por parte de los líderes de una cultura de Excelencia entre las personas de la Organización.
- 1e. Los cambios en la organización son definidos e impulsados por los líderes.

CRITERIO 2: POLÍTICA Y ESTRATEGIA

Cómo implanta la organización su misión y visión mediante una estrategia claramente centrada en todos los grupos de interés y apoyada por políticas, planes, objetivos, metas y procesos relevantes.

Subcriterios

- 2a. Las necesidades y expectativas actuales y futuras de los grupos de interés son el fundamento de la política y estrategia
- 2b. La información procedente de las actividades relacionadas con la medición del rendimiento, investigación, aprendizaje y creatividad son el fundamento de la política y estrategia
- 2c. Desarrollo, revisión y actualización de la política y estrategia

2d. Comunicación y despliegue de la política y estrategia a través de un esquema de procesos clave

CRITERIO 3: PERSONAS

Cómo gestiona, desarrolla y aprovecha la organización el conocimiento y todo el potencial de las personas que la componen, tanto a nivel individual, como de equipos o de la organización en su conjunto; y cómo planifica estas actividades en apoyo de su política y estrategia y del eficaz funcionamiento de sus procesos

Subcriterios

3a. Planificación, gestión y mejora de los recursos humanos

3b. Identificación, desarrollo y mantenimiento del conocimiento y la capacidad de las personas de la organización

3c. Implicación y asunción de responsabilidades por parte de las personas de la organización

3d. Existencia de un diálogo entre las personas de la organización

3e. Recompensa, reconocimiento y atención a las personas de la organización

CRITERIO 4: ALIANZAS Y RECURSOS

Cómo planifica y gestiona la organización sus alianzas externas y sus recursos internos en apoyo de su política y estrategia y del eficaz funcionamiento de sus procesos

Subcriterios

4a. Gestión de las alianzas externas

4b. Gestión de los recursos económicos y financieros

4c. Gestión de los edificios, equipos y materiales

4d. Gestión de la tecnología

4e. Gestión de la información y del conocimiento

CRITERIO 5: PROCESOS

Cómo diseña, gestiona y mejora la organización sus procesos para apoyar su política y estrategia y para satisfacer plenamente, generando cada vez mayor valor, a sus clientes y otros grupos de interés.

Subcriterios

5a. Diseño y gestión sistemática de los procesos

5b. Introducción de las mejoras necesarias en los procesos mediante la innovación, a fin de satisfacer plenamente a clientes y otros grupos de interés, generando cada vez mayor valor

5c. Diseño y desarrollo de los productos y servicios basándose en las necesidades y expectativas de los clientes

5d. Producción, distribución y servicio de atención, de los productos y servicios

5e. Gestión y mejora de las relaciones con los clientes

CRITERIO 6: RESULTADOS EN LOS CLIENTES

Qué logros está alcanzando la organización en relación con sus clientes externos.

Subcriterios

6a. Medidas de percepción

Se refieren a la percepción que tienen los clientes de la organización, y se obtienen, por ejemplo, de las encuestas a clientes, grupos focales, clasificaciones de proveedores existentes en el mercado, felicitaciones y reclamaciones.

6b. Indicadores de rendimiento

Son medidas internas que utiliza la organización para supervisar, entender, predecir y mejorar el rendimiento, así como para anticipar la percepción de sus clientes externos.

CRITERIO 7: RESULTADOS EN LAS PERSONAS

Qué logros está alcanzando la organización en relación con las personas que la integran.

Subcriterios

7a. Medidas de percepción

Se refieren a la percepción de la organización por parte de las personas que la integran, y se obtienen, por ejemplo, de encuestas, grupos focales, entrevistas y evaluaciones de rendimiento estructuradas.

7b. Indicadores de rendimiento

Son medidas internas que utiliza la organización para supervisar, entender, predecir y mejorar el rendimiento de las personas que la integran, así como para anticipar sus percepciones.

CRITERIO 8: RESULTADOS EN LA SOCIEDAD

Qué logros está alcanzando la organización en la sociedad.

Subcriterios

8a. Medidas de percepción

Se refieren a la percepción de la organización por parte de la sociedad, y se obtienen, por ejemplo, de encuestas, informes, reuniones públicas, representantes sociales y autoridades gubernativas.

8b. Indicadores de rendimiento

Son medidas internas que utiliza la organización para supervisar, entender, predecir y mejorar su rendimiento, así como para anticipar las percepciones de la sociedad.

CRITERIO 9: RESULTADOS CLAVE

Qué logros está alcanzando la organización con relación al rendimiento planificado

Subcriterios

9a. Resultados Clave del Rendimiento de la Organización

Estas medidas son los resultados clave planificados por la organización y, dependiendo del objeto y de los objetivos de la misma, pueden hacer referencia a:

- Resultados económicos y financieros
- Resultados no económicos

9b. Indicadores Clave del Rendimiento de la Organización

Son las medidas operativas que utiliza la organización para supervisar, entender, predecir y mejorar los probables resultados clave del rendimiento de la misma.

4.2.7 VENTAJAS DE ADOPTAR EL MODELO EFQM

Aumentar la competitividad de la organización:

- Siendo más rentables
- Logrando un buen clima de trabajo
- Ofreciendo una excelente calidad de servicio, teniendo en cuenta tanto los requisitos legales como las necesidades y expectativas de los clientes.

4.2.8 CAMBIOS QUE ORIGINA LA EXCELENCIA EN GESTIÓN

Concepto tradicional

- Desconocimiento del cliente
- Los empleados buscan satisfacer a los jefes
- La calidad se refiere a la producción y a las materias primas
- El departamento de calidad es el que asegura la calidad
- Existe una reticencia hacia el cambio
- La organización está dividida en departamentos
- No hay involucración entre departamentos
- La participación y la involucración no es prioritario e incluso es sancionada

- Los jefes son los que deciden
- Gestión cualitativa

Concepto Excelente

- El cliente es el que manda
- Toda la organización busca satisfacer a los clientes
- La calidad concierne a todas las personas de la organización
- Cada empleado garantiza la calidad
- El entorno es cambiante por lo tanto el cambio es natural en las empresas
- La organización está integrada y cohesionada
- Se estimula y se premia la participación y la involucración
- Los líderes delegan
- Gestión con datos, los indicadores señalan oportunidades de mejora

4.3 SERIE ISO 9000.

4.3.1 INTRODUCCIÓN.

La Norma Internacional UNE EN ISO 9001 es un método de trabajo considerado como el mejor para la mejora de la calidad y de la satisfacción del cliente. En su última revisión, ISO 9001:2008 se clarifican algunos aspectos de su anterior revisión (ISO 9001:2000), manteniendo la esencia de la misma, sin ampliar su especificación.

El Estándar ISO 9000 está basado en un modelo de gestión por procesos que desarrolla los ocho principios de la Gestión de la Calidad.

La nueva versión de la norma ISO 9001:2008 fue publicada en 2008, fruto del trabajo realizado por el Comité ISO TC/176/SC2.

La norma ISO 9001:2008 mantiene de forma general la filosofía del enfoque a procesos y los ocho principios de gestión de la calidad, a la vez que seguirá siendo genérica y aplicable a cualquier organización independientemente de su actividad, tamaño o su carácter público o privado.

Si bien los cambios abarcan prácticamente la totalidad de los apartados de la norma, éstos no suponen un impacto para los sistemas de gestión de la calidad de las organizaciones basados en la ISO 9001:2000, ya que fundamentalmente están enfocados a mejorar o enfatizar aspectos como:

- Importancia relevante del cumplimiento legal y reglamentario.
- Alineación con los elementos comunes de los sistemas ISO 14001
- Mayor coherencia con otras normas de la familia ISO 9000
- Mejora del control de los procesos subcontratados.
- Aumento de comprensión en la interpretación y entendimiento de los elementos de la norma para facilitar su uso.

4.3.2 LA FAMILIA DE NORMAS ISO 9000

ISO 9000, Quality management systems – Fundamentals and vocabulary (Sistemas de gestión de la calidad – Fundamentos y vocabulario)

Esta norma describe los conceptos de un Sistema de Gestión de la Calidad (SGC) y define los términos fundamentales usados en la familia ISO 9000. La norma también incluye los ocho principios de gestión de la calidad que se usaron para desarrollar la ISO 9001 y la ISO 9004.

ISO 9001, Quality management systems - Requirements (Sistemas de gestión de la calidad – Requisitos)

Esta norma especifica los requisitos de un SGC, con el cual una organización busca evaluar y demostrar su capacidad para suministrar productos que cumplan con los requisitos de los clientes y los

reglamentarios aplicables, y con ello aumentar la satisfacción de sus clientes.

ISO 9004, Quality management systems – Guidelines for performance improvements (Sistemas de gestión de la calidad – Directrices para la mejora del desempeño)

Esta norma proporciona orientación para la mejora continua y se puede usar para mejorar el desempeño de una organización. Mientras que la ISO 9001 busca brindar aseguramiento de la calidad a los procesos de fabricación de productos y aumentar la satisfacción de los clientes, la ISO 9004 asume una perspectiva más amplia de gestión de la calidad y brinda orientación para mejoras futuras. Las directrices para autoevaluación se han incluido en el Anexo A de la ISO 9004. Este anexo brinda un enfoque sencillo y de fácil uso para determinar el grado relativo de madurez del SGC de una organización e identificar las principales áreas de mejora.

La ISO 9000 es un punto de partida para entender las normas, ya que define los términos fundamentales usados en la “familia” ISO 9000, o en el grupo de normas relativas a gestión de la calidad. La ISO 9001 especifica los requisitos para un sistema de gestión de la calidad con el cual se pueda demostrar la capacidad de suministrar productos que cumplan los requisitos de los clientes, al igual que los requisitos aplicables; también busca incrementar la satisfacción de los clientes. La ISO 9004 le brinda orientación sobre la mejora continua de su sistema de gestión de la calidad, de manera que se cumplan las necesidades y expectativas de todas las partes interesadas. Dentro de las partes interesadas se incluyen los clientes y los usuarios finales; los directores y personal de la organización; los propietarios e inversionistas; los proveedores y socios, y la sociedad en general.

La ISO 9001 y la ISO 9004 son un “par coherente” de normas que relacionan la gestión de la calidad moderna con los procesos y actividades

de una organización, y enfatizan en la promoción de la mejora continua y el logro de la satisfacción del cliente. La ISO 9001, que se enfoca en la eficacia del sistema de gestión de la calidad para cumplir los requisitos de los clientes, se usa para certificación o para acuerdos contractuales entre proveedores y compradores. Por otra lado, la ISO 9004 no se puede usar para certificación, ya que no establece requisitos sino que proporciona orientación sobre la mejora continua del desempeño de una organización. La ISO 9001 se enfoca en la “eficacia”, es decir, en hacer lo correcto, mientras que la ISO 9004 hace énfasis tanto en la “eficacia” como en la “eficiencia”, es decir, en hacer lo correcto en la forma correcta.

4.3.3 PRINCIPIOS DE GESTIÓN

La ISO 9000 se basa en los 8 principios de gestión:

- Enfoque al cliente, que da como resultado el cumplimiento de los requisitos de los clientes y el esforzarse por excederlos.
- Liderazgo, que apunta a crear un ambiente interno en el cual las personas estén totalmente involucradas.
- Participación del personal, que es la esencia de una organización.
- Enfoque basado en procesos, que da como resultado la mejora de la eficiencia para obtener los resultados deseados.
- Enfoque de sistema para la gestión, que conduce a la mejora de la eficiencia y la eficacia por medio de la identificación, comprensión y gestión de procesos interrelacionados.
- Mejora continua, que se convierte en un objetivo permanente de la organización.
- Enfoque basado en hechos para la toma de decisiones, basado en el análisis de datos e información, y
- Relaciones mutuamente beneficiosas con el proveedor, basado en la comprensión de su interdependencia

Para el manejo de una organización la ISO 9000 estimula la adopción del enfoque basado en procesos. Para el modelo de procesos revisado en la ISO 9000 se consideran cinco áreas principales:

- Sistema de gestión de la calidad
- Responsabilidad de la alta dirección
- Gestión de recursos
- Realización del producto
- Medición, análisis y mejora

El modelo de proceso usado en las normas es completamente compatible con el bien conocido ciclo de PLANEAR, HACER, VERIFICAR, ACTUAR.

La gestión de calidad debe incluir los procesos requeridos para lograr calidad, y resaltar la interacción entre ellos. La alta gerencia debe asumir la responsabilidad por el liderazgo, compromiso y participación activa para desarrollar y mantener el sistema de calidad. La alta dirección debería suministrar los recursos adecuados, de manera que los clientes obtengan lo que se acordó mutuamente. Es necesario contar con procesos bien definidos, tanto operacionales como de soporte, para poder realizar el producto. La satisfacción de los clientes se debe medir y analizar de manera que la organización pueda mejorar continuamente.

4.3.4 VERSIONES ESPECÍFICAS DE LA NORMA ISO 9000

Las normas para “sectores específicos” son normas de gestión de la calidad destinadas a una industria específica, un producto o grupo de productos. Por ejemplo, existen normas de gestión de calidad específicas para la industria automotriz, la industria de alimentos y bebidas, la industria de las telecomunicaciones, etc.

La familia de normas ISO 9000, genérica por naturaleza, es aplicable a cualquier tipo de producto o servicio y puede ser implementada por cualquier industria. Por tanto, la ISO (Organización Internacional de

Normalización), busca limitar la proliferación de normas en el campo de la gestión de la calidad. El comité técnico ISO 176 (ISO/TC 176), responsable del desarrollo de la familia de normas ISO 9000, apoya el desarrollo de normas para sectores específicos, una vez se haya establecido que hay necesidad de ellas.

4.3.5 COSTOS Y BENEFICIOS DE ESTABLECER UN SISTEMA DE GESTIÓN DE LA CALIDAD

1. Costos...

La implementación de costos en que incurren las compañías se puede pormenorizar en costos directos e indirectos.

Los costos directos incluyen, entre otros, los siguientes:

- Contratación de formadores o consultores externos, si se requieren.
- Envío de personal para recibir formación externa.
- Adquisición de las normas nacionales e internacionales pertinentes de la familia ISO 9000, y los libros y publicaciones relacionadas, y
- Adquisición de equipos adicionales, instrumentos y otros recursos que identifique la compañía.

Los costos indirectos incluyen, entre otros, los siguientes:

- Tiempo empleado por la dirección y demás personal, para el desarrollo del sistema.
- Reorganización de los procesos, incluidas las mejoras en el manejo de la empresa, si se requieren.
- Costos de calibración externa de los equipos, con el fin de asegurar la trazabilidad de las mediciones comparado con patrones de medición trazables a patrones de medición nacionales o internacionales.
- Organización de la formación interna.
- Tiempo gastado por los auditores internos para las auditorías internas periódicas.

- Acciones correctivas, incluida la actualización de manuales y procedimientos, si se requiere.
- Gastos en digitalización de documentos, papelería y otros artículos de consumo requeridos para la preparación de manuales y documentación de procesos, etc.

Algunos factores que pueden ayudar a reducir los costos anteriores incluyen:

- Hacer que el personal de la compañía se familiarice con los requisitos del SGC.
- Contar con actividades documentadas relacionadas con el sistema, como por ejemplo instrucciones de trabajo, planes de calidad, procedimientos, etc., ya implementadas.
- La contratación de consultores únicamente para actividades específicas tales como "análisis de brechas", formación de auditores, auditorías de preevaluación, etc., y contar con personal interno para supervisar las actividades restantes.

De otra parte, hay factores que pueden significar costos de implementación mayores para la compañía. Por ejemplo, si su compañía realiza actividades en diferentes lugares, o está involucrada en el diseño y desarrollo de productos, esto puede aumentar los costos.

2. ... y beneficios de obtener una certificación con base en ISO 9000

La implementación de un sistema de gestión de calidad genera beneficios internos a la mayoría de organizaciones, al igual que oportunidades con relación al mundo exterior.

Los beneficios internos para la compañía incluyen:

- Enfoque mejorado hacia el cliente y orientación a los procesos dentro de la compañía.
- Mayor compromiso de la dirección y mejor toma de decisiones.
- Condiciones de trabajo mejoradas para los empleados.

- Aumento de motivación por parte de los empleados.
- Costo reducido de fallas internas (menores tarifas de reprocesos, rechazo, etc.) y fallas externas (menos devoluciones de los clientes, reemplazos, etc.), y último, aunque no el menos importante,
- La mejora continua del sistema de gestión de la calidad.

Se generan los siguientes beneficios externos:

- Los clientes tienen más confianza en que recibirán productos conformes a sus requisitos, lo que a su vez redunda en mayor satisfacción del cliente.
- Una mejor imagen de la compañía.
- Publicidad más agresiva, ya que los clientes pueden estar informados de los beneficios de realizar negocios con una compañía que maneja la calidad de sus productos.
- Más confianza en que los productos de la compañía cumplen los requisitos reglamentarios pertinentes.
- Mejor evidencia objetiva para defenderse contra demandas por obligación civil, si los clientes llegaran a entablar alguna.

4.3.6 IMPLEMENTACIÓN DE UN SISTEMA DE GESTIÓN DE LA CALIDAD

Un sistema de gestión de calidad con base en ISO 9000 se puede implementar en los siguientes pasos:

1. Evaluar la necesidad y metas de la organización con relación a la implementación de un SGC

La necesidad puede surgir a raíz de quejas repetidas de los clientes, devoluciones frecuentes por garantía, entregas retrasadas, altos inventarios, retrasos frecuentes en la producción, un alto nivel de reprocesos, o rechazo de productos o servicios. En esta etapa, identifique las metas que quisiera alcanzar a través de un SGC, tales como la

satisfacción de sus clientes, una mayor participación en el mercado, mejores comunicaciones y moral de la organización, una mayor eficiencia y rentabilidad, etc.

Otro objetivo de implementar un SGC puede ser la demostración de conformidad por medio de una certificación por tercera parte, que puede solicitar un cliente importante, o que se exige para poder registrarse como proveedor de grandes compañías, por ejemplo, los fabricantes de equipos originales (OEMs).

2. Obtener información acerca de la familia ISO 9000

Las personas identificadas para iniciar el desarrollo de un SGC con base en ISO 9000 necesitan entender los requisitos de la ISO 9001, conjuntamente con la ISO 9000 y la ISO 9004.

La información de soporte, como por ejemplo los principios de gestión de calidad, preguntas frecuentes (FAQ), orientación sobre el numeral 1.2 (aplicación) de la ISO 9001, orientación sobre los requisitos de documentación de la ISO 9001 y otros folletos, se encuentran disponibles en la página web de ISO: <http://www.iso.org>

3. Nombrar un consultor, si es necesario

Si dentro de la organización no se cuenta con la competencia adecuada para desarrollar un SGC, se puede contratar un consultor. Antes de hacerlo, es conveniente verificar sus conocimientos y experiencia; el conocimiento de éste acerca de los procesos de realización del producto de su organización, y su experiencia en ayudar a otras organizaciones a alcanzar sus metas establecidas, incluida la certificación.

4. Toma de conciencia y formación

Hay que despertar la conciencia acerca de los requisitos del SGC entre todo el personal que realiza actividades que afectan a la calidad. También planificar y brindar formación específica acerca de cómo desarrollar Manuales de Calidad, cómo planear un SGC, cómo identificar e

implementar procesos de mejora, y sobre cómo auditar la conformidad con el SGC.

5. Realizar el análisis de brechas (Gap analysis)

Se deben evaluar las brechas que hay entre el sistema de gestión de la calidad existente y los requisitos de ISO 9001 para el SGC, y preparar la manera de cerrar estas brechas, incluida la planificación de los recursos adicionales requeridos. El análisis de estas brechas se puede llevar a cabo mediante una autoevaluación o un consultor externo.

6. Procesos de realización del producto

Examinar el numeral 7 de la ISO 9001 relativo a "realización del producto", para determinar cómo los requisitos se aplican o no al SGC de la compañía. Los procesos cobijados por este numeral incluyen:

- Procesos relacionados con el cliente.
- Diseño y desarrollo.
- Compras.
- Producción y suministro del servicio.
- Control de dispositivos de medición y seguimiento

7. Suministrar el personal

Decidir sobre las responsabilidades de las personas que estarán involucradas en el desarrollo y documentación de su SGC, incluido el nombramiento de un representante de la dirección, quien supervisará la implementación del SGC. La creación de un Comité Director del proyecto también puede ser útil para supervisar el progreso y suministrar los recursos cuando estos se requieran.

8. Elaborar el cronograma

Preparar un plan completo para cerrar las brechas identificadas en el Paso 5 para desarrollar los procesos del SGC. En este plan incluir las actividades por realizar, los recursos requeridos, las responsabilidades y un

tiempo de finalización estimado para cada actividad. Los numerales 4.1 y 7.1 de la ISO 9001 brindan información que se debería usar al desarrollar el plan. El tiempo total requerido para cada fase (planificación, documentación, implementación y evaluación) depende de la extensión de las brechas en su SGC existente.

9. Redactar el Manual de Calidad

En el Manual de Calidad:

- Incluir cómo se aplica el SGC a los productos, procesos, instalaciones y departamentos de la organización.
- Excluir cualquier requisito que se haya decidido en el paso 6, con su respectiva justificación.
- Hacer referencia o incluir procedimientos documentados para su SGC.
- Describir la interacción entre los procesos del SGC, por ejemplo, la interacción entre los procesos de realización del producto y otros procesos de gestión, medición y mejora, y
- Redactar la política de calidad y los objetivos de calidad de la organización.

El personal involucrado en la organización debería revisar el Manual de Calidad y los procedimientos documentados, de manera que sus comentarios y sugerencias puedan ser tenidos en cuenta antes de que el Manual de Calidad y los procedimientos sean aprobados para publicación y uso. También se debería llegar a una decisión acerca de la fecha de implementación.

10. Realización de auditorías internas

Durante la fase de implementación, de aproximadamente tres a seis meses después de que se escribe la documentación, los auditores entrenados deberían llevar a cabo una o dos auditorías internas que cubran todas las actividades del SGC, y la dirección involucrada debería

emprender sin demora las acciones correctivas sobre los hallazgos de auditoría. Cuando se requiera, actualizar los manuales, los procedimientos y los objetivos. Después de cada auditoría interna, la alta dirección debería revisar la eficacia del sistema y suministrar los recursos necesarios para las acciones correctivas y mejoras.

11. Solicitud de la certificación

Una vez finalizado satisfactoriamente el Paso 10, y si la compañía decide obtener una certificación por tercera parte, se puede solicitar una certificación a un organismo de certificación acreditado.

12. Realización de evaluaciones periódicas

Después de la certificación, la organización debería realizar periódicamente auditorías internas para revisar la eficacia del SGC y ver cómo se puede “mejorar continuamente”. La organización debería evaluar periódicamente si el propósito y metas (ver el Paso 1) para los cuales se desarrolló el SGC se están logrando, incluida su mejora continua.

Bibliografía:

Sitios web:

<http://www.iso.org>

International Organization for Standardization

<http://www.aenor.es>

Asociación Española de Normalización y

Certificación

<http://www.efqm.org>

European Foundation for Quality Management

Autor:

Ramón Seoane Freijido

Director de Sistemas de Información Molduras del Noroeste

Colegiado del CPEIG

5. LA BIBLIOTECA DE INFRAESTRUCTURA TI (ITIL). SOPORTE AL SERVICIO. ENTREGA DE SERVICIOS. ISO 20.000. OBJETIVOS DE LA NORMA. MAPA Y DESCRIPCIÓN DE LOS PROCESOS.

Tema 5. La biblioteca de infraestructura TI (ITIL). Soporte al servicio. Entrega de servicios. ISO 20.000. Objetivos de la norma. Mapa y descripción de los procesos.

INDICE

5.1 La biblioteca de infraestructura TI (ITIL)

5.1.1 Introducción

5.1.2 Antecedentes

5.1.3 ¿Qué es ITIL?

5.1.3.1 Objetivos

5.1.3.2 Beneficios

5.1.3.3 Estructura

5.1.4 Libros de ITIL V3

5.1.5 Conclusiones

5.2 Soporte al servicio. Entrega de servicios.

5.2.1 Soporte al servicio

5.2.1.1 Procesos

5.2.2 Entrega de servicios

5.2.2.1 Procesos

5.3 ISO 20.000. Objetivos de la norma

5.3.1 ¿Qué es ISO 20.000?

5.3.2 Utilidades del certificado ISO 20.000

5.3.3 ISO 20.000 e ITIL

5.3.4 ¿Qué representa exactamente ser conforme a ISO 20.000?

5.4 Diseño del mapa de procesos ITIL

5.4.1 Utilidad del modelo de referencia de ITIL

5.1 LA BIBLIOTECA DE INFRAESTRUCTURA TI (ITIL)

5.1.1 INTRODUCCIÓN

En la actualidad la dependencia por las TI es un factor crítico en el desarrollo de las organizaciones. El depender de las TI solamente podrá ser vista como positiva siempre y cuando exista una manera de operar que permita aprovechar las TI y las convierta en una ventaja que aporte funcionalidad y flexibilidad institucional. Para lograr lo anteriormente dicho, es indispensable que existan estándares internacionales que orienten a las organizaciones respecto a cómo es posible organizar y estructurar de la mejor manera y a los mejores costos, todos los servicios de TI que giran en torno a la organización, además de lograr que se comuniquen los principales actores que intervienen en el desarrollo de la estrategia del negocio.

Es por ello que actualmente existen una serie de estándares o lineamientos definidos por diversas instituciones de reconocido prestigio, los cuales pretender ofrecer a las organizaciones un marco de trabajo que les permita adoptar nuevas políticas interinstitucionales para la administración organizada y estructurada de los Servicios de TI. Entre los estándares comúnmente reconocidos a nivel mundial se encuentra ISO 9000, COBIT, BS-15000, ITIL, ISO 20000, etc.

ITIL (Information Technology Infrastructure Library) considerado como un modelo que permite adoptar “mejores prácticas” en las organizaciones, es el resultado de la unión de varias librerías estandarizadas dedicadas a una práctica en particular dentro de la Gestión de Servicios de TI; ofrece herramientas que facilitan la administración y optimización de las TI en las organizaciones. Es una estrategia que puede ser aplicable en todo tipo de organizaciones pues su propósito final es implementar buenas prácticas en la prestación de servicios de TI.

5.1.2 ANTECEDENTES

El incremento en la dependencia de las Tecnologías de Información (TI), así como la adopción de estándares propios para gestionar la información, incurriendo algunas veces en la duplicidad de esfuerzos en los proyectos o en mayores costos y la calidad de los servicios TI que ofrecía el gobierno británico, conllevaron a que en el año 1980 la Central Computer and Telecommunications Agency (CCTA) desarrollara unas primeras recomendaciones que facilitarían la administración y optimización de las TI, recomendaciones que actualmente se conocen como ITIL (Information Technology Infraestructura Library). Esta iniciativa se convirtió en un marco de trabajo conformado por numerosos volúmenes, que probó su utilidad no solamente en organizaciones gubernamentales sino en todos los sectores, convirtiéndose en la base para todo tipo de empresas, grandes ó pequeñas, que tuvieran la disposición de implementar Mejores Prácticas.

Inicialmente, CCTA se enfocó a recopilar información tendiente a verificar cómo las organizaciones dirigían la administración de sus servicios, logrando analizar y filtrar los diferentes problemas que se generaban; luego, comprobaron la utilidad y los beneficios de sus recomendaciones. En la década de los 90s, muchas empresas del gobierno europeo adoptaron este marco de trabajo, convirtiéndose en una buena práctica para la administración de los servicios de TI.

En el año 2001, la CCTA y todas las actividades que estaban bajo su control pasaron a formar parte de la OGC (Office of Government Commerce), oficina del Ministerio de Hacienda Británico, convirtiéndose de esta manera en la nueva entidad propietaria de ITIL, cuya finalidad era ayudar a modernizar la provisión de TI del gobierno británico, a través del uso de buenas prácticas, logrando de esta manera el mejor valor monetario en sus relaciones comerciales. Posteriormente, la OGC publicaría nuevas versiones de librerías de buenas prácticas, escritas por expertos internacionales de diversas organizaciones del sector público y privado.

En 1991, se crea en el Reino Unido la red mundial de grupos de usuarios de las TI que ofrecen mejores prácticas y guías basadas en estándares para la Gestión de Servicios de TI; esta red es denominada itSMF (Information Technology Service Management Forum); es el único grupo dedicado exclusivamente a este tipo de gestión siendo reconocido internacionalmente.

Está presente en varios países de Europa y en algunos de América Latina, trabajando en asociación con la OGC, BSI (British Standard Institute (BSI), la Information Systems Examination Board (ISEB) y Examination Institute of the Netherlands (EXIN) y contribuyendo de esta manera a la industria de las Mejores Prácticas. Los capítulos desarrollados por itSMF, fomentan el intercambio de información y experiencias vividas, orientando a las organizaciones de TI en la implementación y mejoras en los servicios que ofrecen.

5.1.3 ¿QUÉ ES ITIL?

ITIL (Information Technology Infrastructure Library) se considera una colección de guías especializadas en temas organizacionales enfocadas a la planeación, el suministro y soporte de servicios de TI. Se reconoce como un estándar global que resume las mejores prácticas para el área de la Gerencia de Servicios de TI, enfocadas específicamente a describir qué funciones o procesos son los que se recomienda desarrollar, mas no en el cómo desarrollarlos; para este último, es responsabilidad de la organización definir las estrategias y métodos necesarios para implementarla, siempre y cuando se adapten al tamaño, a la cultura y a las necesidades internas de la organización.

ITIL ofrece un marco de trabajo para las actividades del área de TI, proporcionando una descripción de los roles, tareas, procedimientos y responsabilidades que pueden ser adaptados en organizaciones de TI cuya

finalidad sea mejorar la Gestión de sus Servicios; gracias a la cantidad de temas que cubre, se considera un elemento de referencia útil para las organizaciones, ya que permite fijar nuevos objetivos de mejora para la organización de TI, basándose en la calidad del servicio y en el desarrollo de los procesos de una manera eficaz y eficiente.

En varias ocasiones, las mejores prácticas se han considerado como procesos que cubren las actividades más importantes a tener en cuenta dentro de las organizaciones de servicios de TI, por lo que se puede afirmar que ITIL es una colección coherente de las mejores prácticas desarrolladas en la industria y no solamente puede ser adaptado al sector público sino también al privado.

Las publicaciones de ITIL describen cómo pueden ser optimizados y coordinados de una mejor manera todos aquellos procesos que han sido previamente identificados y que intervienen en la administración y operación de la infraestructura de TI, tales como el desarrollo del servicio, la gestión de la infraestructura y la provisión y soporte de los servicios; de igual manera, revelan cómo estos pueden ser formalizados dentro de una organización, brindando un marco de trabajo que facilita unificar la terminología relevante dentro de la organización y permite a las personas hablar un lenguaje común, permitiendo así definir objetivos claros e identificar los recursos y el esfuerzo necesarios para su cumplimiento.

5.1.3.1 OBJETIVOS

Específicamente ITIL se concentra en ofrecer servicios de alta calidad, dando especial importancia a las relaciones establecidas con los Clientes, para lo cual el departamento de TI debe proveer y cumplir con todos los acuerdos de servicios previamente definidos con ellos, y para lograrlo es necesario que exista una fuerte relación entre estos dos; es por esto que algunos de los objetivos de ITIL están relacionados con:



- Promover la visión de IT como proveedor de servicios.
- Generar mejoras en la calidad del suministro de los servicios de TI.
- Fomentar la reducción de costos de los servicios de TI.
- Alinear la prestación de los servicios de TI con las necesidades actuales y futuras del negocio de las organizaciones, además de mejorar la relación con los Clientes.
- Estandarizar los procesos que forman parte de la Gestión de Servicios de TI.
- Promover el uso de un lenguaje común por parte de las personas para mejorar la comunicación dentro de las organizaciones.
- Servir de base para la certificación de las personas y de las organizaciones que desean adoptar este estándar.
- Mejorar la eficiencia, aumentando la efectividad.
- Reducir los posibles riesgos que se pueden presentar.

5.1.3.2 BENEFICIOS

ITIL centra sus esfuerzos en la satisfacción de los requerimientos organizacionales con la mejor relación costo/beneficio, a través de la descripción de un enfoque sistémico y profesional de la Gerencia de Servicios de TI. Algunos de los beneficios que se consiguen con la adopción de las mejores prácticas manejadas en ITIL están relacionados directamente con el Cliente y con la organización; principalmente tienen que ver con:

- El suministro de los servicios de TI se orienta especialmente al Cliente y los acuerdos sobre la calidad del servicio mejoran la relación entre el departamento de TI y el Cliente.
- La mejora en los niveles de satisfacción de los Clientes por medio de medidas objetivas y eficacia en la disponibilidad y desempeño de la calidad de los servicios de TI.
- Implantación de estándares que permitan realizar el control, la administración y operación de los recursos de la organización.



- Los servicios ofrecidos son descritos en un lenguaje más cómodo y con mayores detalles para los Clientes.
- Se gestionan de una mejor manera la calidad, disponibilidad, fiabilidad y coste de los servicios ofrecidos en la organización.
- Mejoras en la comunicación con el departamento de TI en el momento de acordar los puntos de contacto.
- El departamento de TI genera una estructura clara, centrada en los objetivos corporativos de una manera eficaz.
- Soporte a los procesos de negocio y las actividades de los decisores de TI.
- El departamento de TI cuenta con un mayor control sobre la infraestructura y los servicios que tiene a cargo, obteniéndose una visión clara de la capacidad del departamento; además, permite administrar los cambios de una manera sencilla y fácil de manejar.
- La definición de funciones, roles y responsabilidades en el área de los servicios.
- Es posible identificar, a través de una estructura procedimental, la externalización de algunos de los elementos de los servicios de TI.
- Suministro de servicios de TI que satisfagan las necesidades del negocio de la organización.
- Incremento y mejoras en la productividad y eficiencia organizacional a través de las experiencias vividas y los conocimientos adquiridos.
- Genera un cambio cultural hacia la provisión de servicios y sustenta la introducción de un sistema de gestión de calidad.
- Establece un marco de trabajo coherente para las comunicaciones tanto internas como externas, permitiendo contar con la identificación y estandarización de los procedimientos a seguir.
- Mejoras en la satisfacción del personal de la organización reduciendo notablemente su rotación.
- Mejoras en la comunicación entre el personal de TI y sus clientes.
- Genera el intercambio de experiencias obtenidas con su adopción.

5.1.3.3 ESTRUCTURA

El marco de trabajo de ITIL está conformado por cinco (5) elementos principales, los cuales tienen directa relación entre sí, ya que el éxito de cada uno de ellos depende de su interacción y coordinación con los demás. Estos elementos son:

- The Business Perspective (La Perspectiva del Negocio)
- Managing Applications (Administración de Aplicaciones)
- Deliver IT Services (Entrega de Servicios de TI)
- Support IT Services (Soporte a los Servicios de TI)
- Manage the Infrastructure (Gestión de la Infraestructura)

Cada una de las publicaciones de ITIL se enfoca en documentar uno a uno los elementos del marco de trabajo, se realiza una descripción general de lo que se requiere para estructurar la Gestión de Servicios de TI y se definen los objetivos, las actividades, los roles, los flujos de comunicación necesarios y las entradas y salidas de cada uno de los procesos que son indispensables en una organización de TI.

Se han realizado tres publicaciones de las mejores prácticas de ITIL, la primera versión (V1) fue inicialmente desarrollada en la década de 1980, estaba conformada por diez (10) libros básicos que se enfocaban a cubrir la Gestión del Servicio, específicamente en sus dos áreas principales: (i) la entrega del servicio de TI y (ii) el soporte a dichos servicios, siendo soportados posteriormente por treinta (30) libros complementarios, que abarcaban diversos temas, desde el Cableado, hasta la Gestión de Continuidad del Negocio; debido a la cantidad de información existente, surge la segunda versión (V2), la cual empezó a ser reestructurada entre 1999 a 2001, cuando ITIL se convierte en la piedra angular para la Gestión del Servicio, reorganizándose de una manera más sencilla, donde la mayoría de la información relacionada con la entrega del servicio y el soporte de los servicios se convierte en la base del marco de trabajo y se agrupa en dos grandes volúmenes, eliminando de esta forma la duplicidad

en la información existente en la primera versión, de ahí que esta versión quedara reorganizada aproximadamente en diez (10) libros; en la tercera versión (V3) liberada en mayo de 2007, se redujeron las publicaciones a cinco (5) volúmenes articulados, los cuales principalmente se enfocan en el concepto y desarrollo del ciclo de vida del Servicio de TI. Ese ciclo se inicia con una definición de la estrategia del servicio, luego se concentra en realizar el diseño del servicio, posteriormente inicia un periodo de transición donde se busca realizar el desarrollo y la implantación del servicio, en seguida se realiza la operación del servicio y finalmente se concentra en proveer una mejora continua del servicio, la cual está relacionada permanentemente con las demás etapas del ciclo de vida.

5.1.4 LIBROS DE ITIL V3

Service Strategy

Se encarga de asegurar que la estrategia del servicio sea definida, se mantenga y se implemente; se introducen nuevos conceptos, tales como la consecución del valor, la definición del mercado y el espacio de solución; se centra en el desarrollo de prácticas que permitan la toma de decisiones, basado en la comprensión del servicio activo, las estructuras y los servicios de la economía con el objetivo final de incrementar la vida económica de los servicios; busca obtener el alineamiento entre las TI y el negocio, no como anteriormente se venía trabajando, donde solamente las TI eran las que debían adaptarse al negocio.

Algunos de los conceptos generales que se abordan en este libro tienen que ver con la definición del servicio, la estrategia del Service Management y la planificación del valor, la identificación de la dirección y del gobierno de los servicios de las TI, la correspondencia existente entre los planes de negocio y las estrategias de los servicios de TI, algunos arquetipos de servicios y tipos de proveedores de servicios, y lo más importante, qué debe formularse, implantarse y revisarse como estrategia del negocio.

Service Design

Este libro se concentra en definir cómo se diseñará el servicio identificado previamente en la estrategia, a través del desarrollo de planes que la conviertan en realidad; para el diseño de servicios de TI adecuados e innovadores, es necesario establecer e implantar políticas de TI, arquitecturas y alguna documentación pertinente. Dentro de los aspectos abordados en el nuevo proceso de Gestión de Proveedores que forma parte del diseño del servicio, se encuentran el aprovechamiento de la disponibilidad, la capacidad, la continuidad y administración del SLA, así como los conceptos de garantía del servicio y utilidad, los cuales son considerados como aspecto fundamental por los Clientes.

Otros conceptos que son trabajados en este volumen están asociados con el ciclo de vida del servicio, objetivos y elementos en el diseño de los servicios, selección de un modelo de servicios apropiado, identificación de servicios, personas, procesos, herramientas, etc., modelo de costos, un análisis de riesgos y beneficios, y la implementación del diseño del servicio.

Service Transition

Tiene como objetivo minimizar de una manera eficaz la brecha existente entre los proyectos y las operaciones; se concentra en las acciones que intervienen una vez el servicio diseñado debe ponerse en producción, enfocándose especialmente al papel que desempeña el Change Management y explicando las prácticas existentes para un correcto Release Management, de una manera amplia y con visión a largo plazo, permitiendo que se consideren todos los factores que participan, tales como mecanismos de entrega, riesgos, beneficios y facilidad en la posterior operación continua del servicio diseñado.

La transición del servicio tiene que ver con la calidad y el control de la entrega de las operaciones y proporciona modelos para apoyar la transición orientando la forma para reducir variaciones en la entrega.

Service Operation

El ciclo de vida de cualquier servicio culmina con su operación, la cual debe ser tan robusta y efectiva que permita obtener una estabilidad en la gestión del servicio en todo momento y de extremo a extremo. En este volumen se explican las actividades necesarias para garantizar operatividad en el día a día, abarca muchas de las disciplinas y conceptos definidas en la V2 de ITIL, específicamente se concentra en los libros de Service Support y Service Delivery. A través de los conocimientos que se adquieren con la prestación real del servicio, puede llegar a influir en la estrategia del servicio, el diseño, la transición y la mejora continua del servicio.

Continual Service Improvement

Este libro abarca la calidad del servicio en el contexto de mejora continua, además se centra también en ofrecer mejora continua del servicio aún cuando este se encuentre cercano a ser retirado. Uno de los mayores beneficios de este libro es que indica explícitamente las acciones que se deben realizar para la revisión y mejora de los procesos, información que en la V2 no era tan clara.

Algunos de los conceptos que contempla este libro están relacionados con los principios de la mejora continua del servicio, la implantación de la mejora de servicios, algunos elementos del negocio y de la tecnología que pueden conllevar a la mejora continua del servicio y los beneficios generados que favorecen el negocio, la organización y el aspecto financiero.

5.1.5 CONCLUSIONES

Las mejores prácticas de ITIL ofrecen un marco de trabajo que permite a las organizaciones mejorar el nivel de calidad en los servicios de TI ofrecidos, es por esto que su adopción es un paso fundamental y trascendental que debe ser tomado, ya que los beneficios que se van a obtener, no solamente en el mediano sino en el largo plazo, van a permitir que se perciba una mejora continua a nivel institucional.

La adopción de un estándar como el de ITIL implica el desarrollo disciplinado de un proceso enfocado en el ciclo de vida del servicio de TI, en el cual intervienen varios actores de la organización, tanto internos como externos y donde el aporte y contribución de cada uno de ellos con el cumplimiento de las políticas y actividades definidas para todos los procesos, favorecen de manera significativa el éxito de su implantación. La estructura de las publicaciones que han sido liberadas de esta metodología en su V3 permite a las organizaciones adaptarlo de una mejor manera, ya que ofrece las herramientas necesarias que se deben tener en cuenta durante la definición e implantación de los procesos de TI; como el objetivo central es el Ciclo de Vida de los Servicios de TI, presenta de una manera organizada y centralizada todas las actividades que deben ser consideradas durante su implantación, desde la definición de la estrategia del servicio, el diseño del servicio, el periodo de transición por el que debe pasar, la operación del servicio y hasta llegar a obtener una mejora continua del servicio.

Cada uno de los procesos que se han identificado para ITIL tienen estrecha relación entre ellos mismos y de su interacción y comunicación depende en gran parte el éxito de la implantación de las mejores prácticas; el simple hecho de que algunos de los elementos necesarios en los procesos no cumpla con los lineamientos establecidos en el estándar, incrementa las posibilidades de que la adopción se convierta en un fracaso.

Cada vez son más las organizaciones que entran a formar parte de la familia de ITIL, lo que ha ocasionado que ahora los Gerentes empiecen a

preocuparse por la identificación de la manera de cómo deben planear, implementar y administrar exitosamente estas mejores prácticas, convirtiéndose en uno de sus retos laborales y personales. También son varias las organizaciones que ya tienen implementadas exitosamente las mejores prácticas de ITIL y gracias a las experiencias que cada uno de ellos han vivido con su adopción se ha podido enriquecer este modelo, ofreciendo valiosos tips a las nuevas organizaciones que la están implementando.

5.2 SOPORTE AL SERVICIO. ENTREGA DE SERVICIOS.

La Gestión de los Servicios de TI está conformada por dos grandes áreas: Entrega del Servicio (Service Delivery) y Soporte al Servicio (Service Support). En libros independientes se trabaja todo lo relacionado con la perspectiva del negocio, la gestión de la infraestructura, la planeación que se requiere para implementar la gestión del servicio, la gestión de la seguridad y la gestión de las aplicaciones.

5.2.1 SOPORTE AL SERVICIO

Es considerado como uno de los ejes principales de la Gestión del Servicio de TI; el contenido del libro se centra en describir los procesos necesarios para mantener las operaciones funcionando en el día a día; explica cómo el Service Desk es el responsable y soporta la Gestión de Incidentes, proporcionando una base para el soporte a las solicitudes y problemas que se le pueden presentar a los usuarios en una organización. Así mismo, se encarga de explicar cómo la Gestión de Problemas necesita ser, en cierto modo, proactiva y reactiva, además de exponer los beneficios que se pueden obtener cuando se realiza un análisis efectivo de las causas fundamentales que ocasionan los problemas, ofreciendo una amplia visión en la reducción del impacto que se genera cuando existe una suspensión en el servicio a los usuarios.

En resumen, se encarga de describir la manera en que los clientes y usuarios pueden acceder a los servicios que les permitan apoyar el desarrollo de sus actividades diarias y las del negocio, así como la forma en que dichos servicios deben ser soportados; además, se centra en todos los aspectos que intervienen para garantizar que el servicio ofrecido a los usuarios sea un servicio continuo, que esté disponible y que sea de calidad.

5.2.1.1 PROCESOS

Service Desk

Es el único punto de contacto entre el cliente y los usuarios con los proveedores de servicios de TI para todo lo relacionado con el suministro de servicios de TI; también es el punto de partida encargado de informar sobre los Incidentes y la toma de solicitudes de servicio realizadas por los usuarios. Su obligación es mantener informados a los usuarios del servicio sobre los eventos, acciones y oportunidades que pueden llegar a afectar de alguna manera la disponibilidad del servicio y por consiguiente la continuidad en el suministro del servicio en el día a día. Todo lo anterior es posible a través del registro, resolución y monitoreo de problemas.

Dentro del marco de trabajo de las mejores prácticas de ITIL, el Service Desk no fue concebido como un proceso sino como una función por desarrollar dentro de la organización del servicio; algunas de las tareas a su cargo incluyen: ser el punto primario de contacto (SPOC) con los clientes y usuarios; recibir y atender todas las solicitudes, consultas e inquietudes de los clientes y usuarios relacionadas con el suministro de los servicios de TI; documentar, priorizar y realizar un seguimiento adecuado a las solicitudes de modificaciones o cambios realizadas por los usuarios; atender todos los procesos de la Gerencia de Servicios definidos por ITIL; mantener informados sobre el estado y progreso de las solicitudes a los usuarios que las realizaron; clasificar las solicitudes recibidas e iniciar su

proceso según los acuerdos del nivel de servicio (SLA) y procedimientos establecidos; cuando se requiera de un soporte de segundo nivel, deberá encargarse de realizar la coordinación del soporte y el suministro del servicio, al igual que la de los proveedores o participación de terceros; gestionar la restauración de los servicios con el mínimo impacto en el negocio, según los SLA's y prioridades del negocio establecidas; cerrar las solicitudes de servicio realizadas por los usuarios y aplicando la evaluación de satisfacción del cliente; realizar seguimiento a los SLA's definidos tomando las acciones necesarias en caso de presentarse incumplimientos; suministrar la información solicitada por la Gerencia de TI para mantener y mejorar la calidad en los servicios ofrecidos.

De acuerdo con las mejores prácticas de ITIL, el Service Desk se clasifica en tres tipos: Call Center (Centro de Llamadas), Help Desk (Mesa de Ayuda) y Service Desk (Centro de Soporte); por su parte, el Help Desk esta categorizado en: Service Desk Local, a través del cual se busca canalizar localmente todas las necesidades del negocio, tornándose práctico en varios sitios que requieren servicios de soporte, pero siendo grandes los costos en los que se puede llegar a incurrir, ya que el servicio es ofrecido en diferentes lugares, lo cual implica la definición de un estándar operacional; el Service Desk Central, busca que todos los requerimientos del servicio sean registrados en una ubicación central, minimizando costos operacionales ya que existe solamente una mesa de ayuda a nivel organizacional que atiende todos los requerimientos; y el Service Desk Virtual cuya finalidad es ofrecer el servicio en cualquier parte del mundo a través de la red, no importa su ubicación física ya que el servicio se encuentra disponible en todo momento, y su éxito se da siempre y cuando todos los usuarios de la organización cuenten con infraestructura tecnológica para poder acceder a ella. En conclusión, la implementación exitosa y ejecución del proceso de Service Desk generará mayores beneficios en la organización, representado en la satisfacción de

los clientes, minimización de costos, compromiso personal y profesionalidad.

Configuration Management

Conocida también como Gestión de la Configuración, es parte integral de todos los demás procesos de la Gestión del Servicio; tiene por objetivo controlar los activos y elementos de configuración que forman parte de la infraestructura de TI, por lo cual se encarga de todos los procesos, herramientas y técnicas necesarias para lograrlo; también es su responsabilidad proporcionar información confiable y actualizada no solamente de los elementos específicos de la infraestructura (Elementos de Configuración ó CIs) necesarios para ejecutar los procesos del negocio, sino también sobre las relaciones entre ellos mismos, asegurando la integración con las demás disciplinas de la Gestión del Servicio; permite el desarrollo de los servicios informáticos de mejor calidad de una manera viable económicamente y suministra información importante para el cálculo de los costos y la facturación de los servicios ejecutados. Las solicitudes de cambio sobre los CIs, se registran en una base de datos creada para la Gestión de la Configuración denominada Configuration Management Database (CMDB); en esta base de datos se encuentran registrados todos los datos de los CIs requeridos para la prestación del servicio, desde su descripción e interconexión, hasta un nivel de detalle que incluye la categoría, las relaciones, los atributos y los posibles estados en los cuales puede estar en determinado momento; es necesario actualizar la CMDB cada vez que se realiza un cambio en la infraestructura y dicho cambio esté relacionado con la gestión de la configuración.

Incident Management

El objetivo de este proceso es resolver cualquier incidente que genere una interrupción en la prestación del servicio, restaurándolo nuevamente de la manera más rápida y efectiva posible; este proceso no se detiene en encontrar, evaluar y analizar cuales fueron las causas que

desencadenaron la ocurrencia de dicho incidente, el cual generó una interrupción en el servicio, sino simplemente se limita a solucionarlo temporalmente y a restaurar el servicio de cualquier manera, lo que probablemente puede llegar a generar nuevas interrupciones al servicio por el mismo incidente; los incidentes se reportan sobre los CIs.

Una de las mayores contribuciones que se le atribuyen a las mejores prácticas de ITIL fue la de establecer la diferencia que existe entre los incidentes y los problemas, donde se distingue entre la restauración rápida del servicio (Incident Management) y la identificación y corrección total de la causa que ocasionó el incidente (Problem Management), pero se destaca la articulación que debe existir entre estos dos procesos, al igual que con Change Management (Gestión de Cambios) y el Service Desk; se recomienda que todas las modificaciones realizadas a los incidentes sean relacionados en la misma CMDB lo mismo que los registros de problemas, errores conocidos y cambios, pues de esta manera será más fácil identificar si la ocurrencia del incidente puede convertirse posteriormente en un problema, lo que permite analizar y buscar su solución definitiva o corrección total, además de que se evita la ocurrencia de nuevos incidentes como consecuencia de los cambios implementados. Algunas de las tareas a cargo de este proceso tienen que ver con: identificación y documentación de todos los reportes que se hayan realizado de los incidentes ocurridos, incluyendo informes e investigaciones; priorizar y categorizar los reportes de los incidentes que se han generado; proporcionar un análisis inicial del incidente ofreciendo un soporte de primer nivel; escalar, cuando sea necesario, la ejecución de soporte de segundo y tercer nivel; cuando se encuentre en riesgo el cumplimiento en los SLAs, es necesario incrementar la asignación de recursos que trabajan en la solución del incidente; resolver la situación en el menor tiempo posible, restaurando el servicio; cerrar y documentar los incidentes ocurridos; realizar seguimiento exhaustivo a cada uno de los incidentes que se presentan (monitoreo, revisión y comunicación del progreso); realizar una evaluación de los incidentes

reportados, analizarlos y generar informes sobre posibles mejoras al servicio.

Problem Management

Este proceso se dedica a identificar las causas (origen) que ocasionan los problemas que se presentan en la infraestructura de TI y su solución definitiva para evitar nuevas ocurrencias; cuando existe un incidente que se repite más de una vez, es posible que posteriormente se pueda convertir en un problema, aunque la idea es evitar que esto suceda siendo proactivos y previniendo nuevas ocurrencias cuando sea posible; de ahí que se hable de la gestión de problemas proactiva, en donde los incidentes son detectados con demasiada anterioridad de tal manera que permita tomar las acciones preventivas necesarias garantizando que el servicio permanezca disponible y no se vea afectado en ningún momento.

Como resultado de la identificación temprana de los incidentes, las acciones preventivas que se recomienda realizar se traducen en la ejecución de cambios en los CIs interactuando de esta forma con la Gestión de Cambios; este proceso también se relaciona con la Gestión de Incidentes, ya que requiere de un registro preciso y completo de todos los incidentes con el fin de identificar eficiente y eficazmente su causa y las tendencias en su ocurrencia; además, una vez se encuentre solución a un problema, los incidentes que previamente habían sido reportados y que tenían directa relación con las causas del problema podrán pasar a un estado Cerrado o Datos de Baja.

Change Management

Este proceso tiene una estrecha relación con el proceso de Configuration Management, ya que de la exactitud de los datos de los elementos de la infraestructura (CMDB) es posible garantizar que el análisis del impacto es realizado y conocido, logrando tramitar de esta manera los cambios necesarios a través de procesos y procedimientos estandarizados

y consistentes; se encarga de dirigir la aprobación para realizar cualquier cambio, así como de controlar la implementación de los cambios de la infraestructura de TI.

Dentro de sus objetivos se encuentran: realizar una valoración de los cambios y garantizar que pueden ejecutarse ocasionando el mínimo impacto en la prestación de los servicios de TI y en la infraestructura actual o nueva, y asegurar de manera simultánea la trazabilidad de los cambios; implementar los cambios autorizados y requeridos para el cumplimiento de los SLAs de manera eficiente, efectiva, económica y oportuna; minimizar los cambios, evitando que se implementen cambios no autorizados.

Release Management

Con la implementación de los cambios, se puede generar como resultado la instalación de nuevo hardware, la instalación de nuevas versiones de software ó simplemente la actualización o generación de nueva documentación; es por ello que todas estas acciones deben ser controladas y distribuidas de una manera organizada, como parte de un nuevo paquete o versión.

Este proceso está asociado con la correcta implantación de todas las versiones de los CIs requeridas para la prestación de un SLA, proporcionando un marco de trabajo para la coordinación, el control y la introducción física de un cambio; se encarga de llevar el control de todos los cambios y nuevas versiones que se han generado como resultado de la implementación de un cambio o de una nueva adquisición (ej. Nuevo software instalado en una máquina); es importante tener claridad en las relaciones que existen entre los CIs para que cuando se realice un cambio de versión se conozca con certeza qué acciones o consideraciones es necesario tener en cuenta y a qué otros CIs se está afectando, además de mantener los registros actualizados en la CMDB.

5.2.2 ENTREGA DE SERVICIOS.

Considerado otro de los ejes fundamentales de la Gestión del Servicio de TI, el Service Delivery se concentra en describir todos los aspectos que deben tenerse en cuenta para realizar una planificación y mejora continua del servicio de TI a largo plazo y en todos los procesos que intervienen para que la prestación del servicio se mantenga y se suministre de tal manera que satisfaga las necesidades actuales y futuras del negocio; algunos de los aspectos que describe están relacionados con la gestión de los niveles del servicio, los niveles de seguridad requeridos, la viabilidad financiera de los servicios, su capacidad, continuidad y disponibilidad, entre otros.

5.2.2.1 PROCESOS

Availability Management

Este proceso se encarga de garantizar que los servicios de TI puedan ser accedidos de una manera confiable y se encuentren disponibles y funcionando correctamente cada vez que los Clientes o usuarios así lo requieran, enmarcados en los SLAs que se hayan definido para la prestación del servicio.

Dentro de los objetivos definidos para este proceso se encuentra realizar el diseño de los servicios de TI con el nivel de disponibilidad requerido por el negocio, garantizar que exista una disponibilidad no solamente en los servicios de TI sino también en su infraestructura, de tal forma que cumpla con los SLAs establecidos, generar reportes de disponibilidad que demuestren la confiabilidad y mantenibilidad del sistema y minimizar la frecuencia y duración que tarda la solución de un incidente.

Capacity Management

El objetivo de este proceso es asegurar la existencia de cierta capacidad a nivel de infraestructura de TI, la cual debe encontrarse disponible constantemente para satisfacer los requerimientos del negocio a

nivel del volumen de transacciones, el tiempo de proceso, el tiempo de respuesta y ante todo contemplando su viabilidad cuantitativa y económica para no incurrir en costos desproporcionados.

Como su nombre indica, la gestión de la capacidad se concentra en verificar y garantizar que todos los servicios de TI estén soportados con la suficiente capacidad de proceso y almacenamiento y que además esté dimensionada de tal manera que no implique costos innecesarios para la organización, pero que tampoco genere insatisfacción en los Clientes o usuarios debido a la escasa calidad en la prestación del servicio.

Financial Management for IT Services

Se concentra en realizar un adecuado manejo del recurso financiero (ingresos y gastos) asociado a lo que implica la prestación de los servicios de TI, siempre enfocándose en el cumplimiento de los SLAs definidos; determina cuál es el manejo financiero asociado para cada uno de los recursos que participan en el suministro de un servicio, buscando mantener un balance permanente. Mantiene una estrecha relación con la gestión de la capacidad, la gestión de la configuración y la gestión de niveles de servicio, y a través de la información que cada uno de ellos provee, es posible determinar exactamente cuál es el costo real de un servicio.

IT Service Continuity Management

La función principal de este proceso es evitar que una grave e imprevista interrupción en el servicio atente contra la continuidad del negocio, por lo que se concentra en la preparación y planificación de las medidas que se deben tomar para recuperar el servicio en caso de que algún desastre ocurra.

Busca asegurar la disponibilidad del servicio a través de la toma de medidas preventivas que se orienten a reducir la probabilidad de fallas y en el evento de que ocurra algún fenómeno considerado como catastrófico o

desastre, el servicio pueda ser restablecido en el menor tiempo posible y con las menores pérdidas de información para la organización.

Service Level Management (SLM)

Se encarga de definir los servicios de TI ofrecidos, formalizándolos a través de Acuerdos de Niveles de Servicio (SLA) y Acuerdos de Nivel Operativo (SLO); realiza una evaluación del impacto que ocasionan los cambios sobre la calidad del servicio y los SLAs una vez estos cambios hayan sido propuestos e implementados, asegurando de esta manera que cualquier impacto negativo sobre la calidad en los servicios de TI sea relativamente bajo; también se encarga de la creación de planes y emisión de informes respecto a la calidad del servicio que se está ofreciendo.

Explica la importancia de establecer una buena relación con los Clientes y de esta manera asegurar que las necesidades de las empresas sean entendidas; es por esto que el Service Level Management se enfoca también en conocer las necesidades de los Clientes, definir correctamente los servicios que serán ofrecidos y monitorear la calidad de los servicios ofrecidos por medio de los SLAs definidos.

Algunos de los aspectos más importantes que se deben considerar en la definición de los SLAs están relacionados con la descripción del servicio y sus características de funcionamiento, con la disponibilidad del servicio, es decir, cuál es el tiempo que la organización se compromete a mantener el servicio disponible a sus Clientes, para lo cual también es indispensable que sean acordados tiempos de reacción (mínimos y máximos) en la resolución de incidentes, de ahí que los SLAs dependan de la solución de los incidentes en los tiempos acordados. Otro aspecto a tener en cuenta tiene que ver con los objetivos de disponibilidad, seguridad y continuidad del servicio, las obligaciones que recaen tanto en los Clientes como en los Proveedores y las horas críticas del negocio, entre otros.

5.3 ISO 20.000. OBJETIVOS DE LA NORMA

5.3.1 ¿QUÉ ES ISO 20.000?

ITIL muestra todo lo que se debe hacer para que los usuarios ofrezcan servicios de TI adecuados cumpliendo los procesos de su empresa. Para personas individuales es posible obtener certificaciones de ITIL pero hasta el momento no ha sido posible para una organización de TI presentar pruebas de que trabaja según las recomendaciones de ITIL.

Las normas ISO fueron concebidas para llenar este vacío. En base a ITIL las organizaciones itSMF y BSI (British Standard Institute) elaboraron una normativa que define los requisitos de la gestión de servicios a organizaciones de TI.

En la actualidad, la normativa del BSI se conoce internacionalmente como normativa ISO 20000 y une los enfoques de ITIL y COBIT. ISO 20000 abre las puertas a las organizaciones de TI para que puedan obtener por primera vez una certificación.

Aquellas organizaciones que aspiren a lograr una certificación según ISO 20000 deben cumplir los requisitos formulados en la normativa —UNE-ISO/IEC 20000, Parte 1: Especificaciones, en los que se fijan los requisitos obligatorios que debe cumplir toda organización que desee una certificación según esta normativa.

Los requisitos centrales de la normativa ISO 20000 a una organización de TI son:

- o El alineamiento de los procesos de TI según las normas de ISO 20000, que corresponden esencialmente a las recomendaciones de la Gestión del Servicio de ITIL (en especial tras la introducción de ITIL V3).



- o El uso de un método de gestión en la organización de TI según las normas ISO 9001, basado en los principios de la gestión de procesos y dirigido a una mejora continua de la calidad.

La norma contiene asimismo dos partes más con carácter recomendatorio:

- UNE-ISO/IEC 20000, Parte 1: Anexo A (Informativo) muestra la correspondencia entre la norma ISO/IEC 20000-1:2005 y la norma ISO 9001:2008.
- UNE-ISO/IEC 20000, Parte 2: Código de buenas prácticas ofrece recomendaciones sobre procesos de la Gestión de Servicios de TI para organizaciones que deseen una certificación.

5.3.2 UTILIDADES DEL CERTIFICADO ISO 20.000

Un certificado ISO 20000 demuestra que una organización de TI:

- está orientada a las necesidades de los clientes,
- está en condiciones de prestar servicios que cumplen con los objetivos de calidad fijados,
- utiliza sus recursos de forma económica.

Este certificado supone siempre una ventaja sobre la competencia. Cada vez hay más clientes que esperan una certificación ISO 20000 de su proveedor de TI, con lo cual el certificado se convierte en una condición imprescindible para ganar cuota de mercado.

Pero también para la empresa misma, trabajar según los principios de ISO 20000 (e ITIL) conlleva una serie de beneficios. La normativa tiene

como objetivo proveer a los negocios con los servicios de TI que realmente necesite y ocuparse siempre de que esto suceda de forma eficiente.

Empezar una iniciativa ISO 20000 es una buena forma de impulsar la introducción de mejores prácticas en la organización de TI y mantener a la larga la motivación para su implementación.

5.3.3 ISO 20.000 E ITIL

ISO 20000 fija requisitos a los procesos sin ocuparse de cómo deben ser conformados tales procesos de forma concreta.

Ahí es donde aparece ITIL en escena: ITIL (y más especialmente la nueva versión 3) se orienta a la normativa ISO 20000 y presenta un gran abanico de recomendaciones de mejores prácticas, lo que supone una base de partida bien fundamentada para diseñar procesos conforme a ISO 20000.

La introducción de ITIL es por lo tanto la mejor forma de prepararse para una certificación ISO 20000.

5.3.4 ¿QUÉ REPRESENTA EXACTAMENTE SER CONFORME A ISO 20000?

Obtener una certificación ISO 20000 es un proyecto laborioso. La condición más importante al iniciar un proyecto así es determinar qué objetivo se persigue. Concretamente debe responderse a la pregunta: ¿Cómo debe ser la organización de TI al final del proyecto?

La normativa deja abierta sin embargo esta cuestión, ciñéndose sólo a nombrar los requisitos sin especificar cómo deben cumplirse. Por eso no

existe una respuesta válida a la pregunta sobre lo que representa “ser conforme a ISO 20000”

Así las cosas, no es de extrañar que al empezar una iniciativa ISO 20000 se haga evidente un gran problema: No queda claro cómo debe estructurarse de forma concreta la labor de una organización de TI para cumplir los requerimientos de la normativa ISO y por lo tanto no es fácil determinar los cambios necesarios para ello.

Aquí es donde ITIL puede prestar una ayuda decisiva ya que ISO 20000 está orientada a ITIL.

Los conocimientos sobre ITIL se adquieren normalmente mediante libros o, de forma alternativa, con el Mapa de Procesos ITIL® V3 en combinación con el ITIL - ISO 20000 Bridge

5.4 DISEÑO DEL MAPA DE PROCESOS ITIL

El Mapa de Procesos ITIL® V3 es un modelo de referencia íntegro de ITIL. Contiene la descripción completa de forma gráfica de todos los procesos estándar en la Gestión de Servicios de TI según ITIL V3. El modelo de procesos muestra cómo funciona ITIL en la práctica: le ahorra trabajo a la hora de convertir en procesos implementables las múltiples normas recogidas en la bibliografía sobre ITIL.

El Mapa de Procesos ITIL® V3 ha sido creado para organizaciones de TI y proveedores de servicios de TI que

- tengan previsto introducir por primera vez, parcial o totalmente, la Gestión de Servicios de TI según ITIL V3,
- deseen revalorar los procesos ya introducidos de ITIL en base a ITIL V3
- quieran orientarse según ISO 20000 y/o
- se estén preparando para una certificación según ISO 20000.

5.4.1 UTILIDAD DEL MODELO DE REFERENCIA DE ITIL

El Mapa de Procesos ITIL® V3 está organizado para prestar el apoyo óptimo en todos los pasos de cualquier proyecto ITIL o ISO 20000, desde la primera planificación hasta una organización de TI que funcione según los principios de las mejores prácticas. Su uso ofrece ventajas decisivas:

- El tratamiento gráfico y navegable de los contenidos de ITIL facilita la comprensión de los procesos ITIL y de sus interrelaciones. Con el modelo de procesos de ITIL puede aclarar ITIL a todos los colaboradores de su organización de TI de una forma muy efectiva y económica.
- Los modelos de procesos, claramente estructurados, y las guías complementarias sirven de hilo conductor a la hora de incorporar su proyecto a la implementación de ITIL y llevarlo a cabo. En la definición y documentación de procesos se reducirá su trabajo, ya que adaptará los procesos de referencia existentes a las necesidades de su organización sin tener que empezar con una hoja en blanco.
- El Mapa de Procesos es una documentación de procesos profesional con la que la gestión de TI estará en la ventajosa situación de poder demostrar a los clientes que la organización de TI realiza su labor de forma planificada, orientada al cliente y de calidad.

Bibliografía:

Sitios web:

<http://www.itiil-officialsite.com/>

<http://www.best-management-practice.com/>

<http://iso20000enespanol.com/>

Autor:

Ramón Seoane Freijido

Director de Sistemas de Información Molduras del Noroeste

Colegiado del CPEIG

6. AUDITORÍA INFORMÁTICA. MARCO GENERAL. METODOLOGÍA. AUDITORÍA DE LOS GRANDES SISTEMAS INFORMÁTICOS. AUDITORÍA DE LA INFORMÁTICA PERSONAL Y LAS REDES DE ÁREA LOCAL.

Tema 6. Auditoría informática. Marco general. Metodología. Auditoría de los grandes sistemas informáticos. Auditoría de la informática personal y las redes de área local.

INDICE

6.1 Auditoría Informática. Marco general.

6.1.1 Introducción

6.1.2 Definiciones

6.1.3 Bases sobre las que se sustenta la auditoría informática

6.1.4 Carácter interdisciplinar de AI

6.1.5 Objetivos

6.1.6 Controles

6.1.7 Conclusiones

6.2 Metodología

6.3 Auditoría de los grandes sistemas informáticos

6.3.1 Regulación internacional sobre auditoría de sistemas de información

6.4 Auditoría de las redes de área local

6.4.1 Etapas a implementar en la auditoría de redes

6.5 Auditoría de la informática personal

6.5.1 Análisis forense

6.5.1.1 Introducción

6.5.1.2 Fases del análisis forense

6.1 AUDITORÍA INFORMÁTICA

6.1.1 INTRODUCCIÓN

Hoy en día, las tecnologías de la información están presentes en todas las áreas de las organizaciones. Esta implantación generalizada de Sistemas Informáticos (SI) se ha realizado en muchos casos sin la necesaria planificación, en parte porque los conceptos necesarios no estaban

suficientemente desarrollados. La tendencia hacia los sistemas abiertos, la interconexión global y el deseo por parte de los consumidores de independizarse de los fabricantes traen consigo la necesidad de un estudio más profundo de los SI antes de tomar decisiones. Por lo tanto, se hace necesario mejorar la planificación de futuras implementaciones, la compatibilidad entre sistemas y la organización del personal y de la empresa.

En las organizaciones modernas, tanto públicas como privadas, la misión de las tecnologías de la información es facilitar la consecución de sus objetivos estratégicos. Para ello, se invierte una considerable cantidad de recursos en personal, equipos y tecnología, además de los costos derivados de la posible organización estructural que muchas veces conlleva la introducción de estas tecnologías. Esta importante inversión debe ser constantemente justificada en términos de eficacia y eficiencia. Por tanto, el propósito a alcanzar por una organización que contrata la auditoría de cualquier parte de sus SI es asegurar que sus objetivos estratégicos son los mismos que los de la propia organización y que los sistemas prestan el apoyo adecuado a la consecución de estos objetivos, tanto en el presente como en su evolución futura.

6.1.2 DEFINICIONES

La auditoría puede definirse como el examen comprensivo y constructivo de la estructura organizativa de una empresa, de una institución, o de cualquier otra entidad y de sus métodos de control, medios de operación y empleo que dé a sus recursos humanos y materiales.

Auditoría en Informática es la revisión y evaluación de los controles, sistemas, procedimientos de informática, de los equipos de cómputo, su utilización, eficiencia y seguridad, de la organización que participa en el procesamiento de la información, a fin de que por medio del señalamiento

de cursos alternativos se logre una utilización más eficiente y segura de la información que servirá para la adecuada toma de decisiones.

6.1.3 BASES SOBRE LAS QUE SE SUSTENTA LA AUDITORÍA INFORMÁTICA

En la actualidad los temas relativos a la auditoría informática cobran cada vez más relevancia, debido a que la información se ha convertido en el activo más importante de las empresas, representando su principal ventaja estratégica, por lo que éstas invierten enormes cantidades de dinero y tiempo en la creación de sistemas de información, con el fin de obtener la mayor productividad y calidad posibles.

Entonces, de igual modo que se exige para los otros activos de la empresa, los requerimientos de calidad, controles, seguridad e información, son indispensables. La gerencia, por ende, debe establecer un sistema de control interno adecuado y tal sistema debe soportar debidamente los procesos del negocio.

Haciendo eco de estas tendencias, la Organización ISACA (Information Systems Audit and Control Association), a través de su Fundación, publicó en diciembre de 1995 el COBIT, como resultado de cuatro años de intensa investigación y del trabajo de un gran equipo de expertos internacionales. Siendo esta metodología el marco de una definición de estándares y conducta profesional para la gestión y el control de los SI, en todos sus aspectos, unificando diferentes estándares, métodos de evaluación y controles anteriores.

Adicionalmente, esta metodología aporta la orientación hacia el negocio y está diseñada no solo para ser utilizada por usuarios y auditores, sino también como una extensa guía para gestionar los procesos de negocios.

6.1.4 CARÁCTER INTERDISCIPLINAR DE AI

Auditoría Informática no es solo una prolongación de la auditoría tradicional, sino que es un aspecto importante en la seguridad y buen funcionamiento de la empresa.

Se puede considerar AI como la intersección de cuatro disciplinas: Auditoría Tradicional, Ciencias del Comportamiento, Gestión de Sistemas de Información e Informática.

Auditoría Tradicional

Proporciona conocimiento y experiencia en Técnicas de Control Interno. Es decir, aspectos sobre cómo controlar las actividades de la empresa. Un SPD tiene componentes manuales y mecanizados, que serán objeto de control.

- Los manuales están sujetos a los principios de Control Interno de la auditoría tradicional: separación de tareas, personal fiable, definición clara de responsabilidades, etc.
- Los mecanizados pueden utilizar controles “clásicos”, desde el punto de vista informático: totales de control, cuadros, balances, etc.

Otra aportación de la auditoría tradicional la constituyen las metodologías de recogida y evaluación de evidencias, aunque el aspecto más importante es que la auditoría tradicional proporciona un “saber hacer”, un “modus operandi”, para examinar los datos y procesos con mente crítica, cuestionando la capacidad de un SPD de salvaguardar los bienes, y de mantener la integridad de los datos de un modo eficaz y eficiente.

Gestión de Sistemas de Información

En los comienzos de la era informática hubo grandes fracasos al implementar Sistemas de Proceso de Datos por no disponer de técnicas y herramientas adecuadas. Por desgracia, esto a veces sigue ocurriendo en nuestros días... por no utilizarlas.

Hoy en día disponemos de mejores técnicas: Programación Estructurada, Estándares de Gestión de Proyectos, Equipos de Trabajo, Metodologías de Análisis y Desarrollo, etc.

La causa final de la existencia de estas técnicas es la de simplificar el mantenimiento de los SPD's. Todos estos avances tienen un impacto en AI porque afectan directamente a las funciones de AI.

Ciencias del comportamiento

La razón principal del fallo de los SPD's es el desconocimiento de los problemas del comportamiento organizativo en el diseño e implantación de los Sistemas de Información.

El auditor debe de conocer las condiciones que originan problemas de comportamiento y que pueden causar fallos en el Sistema. Es decir, es necesario conocer los problemas de las personas en las organizaciones.

Algunos investigadores están aplicando la Teoría de las Organizaciones al desarrollo e implantación de los Sistemas de Información. Es decir, se debe de considerar, de modo concurrente, el impacto de un SPD tanto en:

- El cumplimiento de las tareas (que se haga lo que se espera)
- El sistema técnico (que tengamos recursos técnicos para realizar las tareas)
- El sistema social (la calidad de trabajo de las personas; que haya un buen ambiente de trabajo)

Informática

La última de las disciplinas base de AI es la Informática. Los informáticos también están fuertemente involucrados en las funciones de AI.

En Ingeniería del Software se han desarrollado investigaciones sobre:

- Como desarrollar software con “cero errores”
- Como mantener la integridad global del hardware y el software: Programación Estructurada, Teoría de Fiabilidad, Teoría de Control, etc.

Y estas disciplinas se han incorporado en AI, ya que deben ser conocidas por el auditor informático. No obstante, este conocimiento tecnológico de alto nivel ocasiona beneficios y desventajas a AI, ya que:

- Permite al auditor despreocuparse acerca de la fiabilidad de algunos componentes del Sistema, ya que supone que funcionarán correctamente.
- Si hay “abuso” será muy difícil de detectar. Ya que no tiene los conocimientos necesarios para detectarlos.
- El fraude perpetrado por un programador altamente cualificado será muy difícil de detectar por un auditor que no tenga ese alto grado de conocimiento técnico.

6.1.5 OBJETIVOS

Distinguimos entre dos tipos de Auditoría en función de sus objetivos:

- Auditoría externa: que se centra en objetivos de seguridad: salvaguarda de bienes e integridad de datos, principalmente.
- Auditoría interna: que, además de en los objetivos anteriores, se centra en objetivos de gestión, es decir garantizar que las tareas se realicen en unos grados adecuados de efectividad y eficiencia.

Objetivos de salvaguarda de bienes

Consideraremos como “bienes” de un Centro de Proceso de Datos (CPD) el hardware, software, personas, datos (ficheros, bases de datos, etc.), documentación, suministros, etc. El hardware puede ser dañado por accidente o malintencionadamente; el software, al igual que los datos, puede ser robado o destruido; los suministros pueden ser usados con fines ajenos a los de la empresa, etc.

Además, estos bienes se concentran todos en un mismo sitio, el ámbito físico del CPD, por lo que deben de ser especialmente protegidos por un sistema de control interno, y su protección debe de ser un objetivo importante.

Objetivos de integridad de datos

Uno de los aspectos que debemos cuidar especialmente es la integridad de los datos, pero realizar esta tarea nos va a suponer un coste frente a los beneficios esperados al implantar unas medias de seguridad. Desde de un punto de vista puramente empresarial, estos beneficios deben superar los costes de implantación, para que sea rentable su utilización. No obstante, disposiciones legales pueden obligar a establecer controles, al margen de su rentabilidad.

Para determinar los costes y beneficios, estudiaremos dos factores que afectan al valor de un dato para la empresa:

1. El valor de la información que proporciona el dato. Este valor depende de la capacidad que ésta tenga para reducir la ambigüedad en una toma de decisiones. Es decir, los datos que influyen directamente en las tomas de decisiones serán los más importantes y deberán ser especialmente protegidos.

2. Las veces en que el dato es usado por personas que toman decisiones. Si el dato es compartido, su falta de integridad afectará a todos los usuarios, por lo que en un entorno compartido es vital mantener esta integridad.

Objetivos de efectividad del sistema

Para ver si un SPD (Sistema de Proceso de Datos) es efectivo hay que conocer las características del usuario y el tipo de decisiones que se van a tomar. No se debe evaluar de igual manera la efectividad de un SPD de una gran empresa que la de un pequeño comercio, por ejemplo.

Para saber si el sistema está trabajando correctamente, y para poder medir su efectividad, es necesario esperar a que el sistema lleve funcionando un cierto tiempo, tras el cual normalmente la gerencia solicita una auditoría para saber si el sistema alcanza los objetivos que se había planteado.

Como resultado de la auditoria se sabrá si hay que descartar el SPD, modificarlo, o si se debe de dejar como está. Téngase en cuenta que esta auditoría también se puede hacer durante la fase de Diseño del Sistema. Además, es posible que la gerencia solicite una auditoría independiente.

Objetivos de eficiencia del sistema

Un SPD eficiente es el que utiliza el mínimo de recursos (tiempo de máquina, periféricos, canales, software de sistemas, mano de obra, etc.) para alcanzar sus objetivos.

En cualquier sistema los recursos son escasos y hay que compartirlos, por lo que saber si se están utilizando los recursos de forma eficiente no siempre es fácil. Además, no se puede considerar la eficiencia de un sistema por sí solo, sino en conjunto con los demás sistemas dentro de la organización.

Suboptimización: Se produce cuando un sistema se optimiza a expensas de otros. Ejemplo: Dedicar exclusivamente un recurso a un sistema (que no lo utiliza a tiempo completo) penalizará a otros sistemas que necesiten el recurso.

La eficiencia se vuelve crítica cuando el ordenador comienza a estar escaso de recursos (escasez de capacidad de almacenamiento en discos, de memoria, de procesador, etc.), por lo que, si además los recursos son caros, hay que saber si se agotaron porque las aplicaciones son

ineficientes, porque existen cuellos de botella, o simplemente porque el crecimiento natural de las aplicaciones ha reducido dichos recursos.

6.1.6 CONTROLES

Estando en un medio informático en el que el ordenador realiza de forma automática las tareas tendremos que controlar si lo que hace es lo que realmente queremos que haga.

Los ordenadores juegan un papel muy importante al ayudarnos en el proceso de datos, por lo que hay que controlar su uso, ya que en el procesamiento de datos es uno de los puntos donde se puede producir el fraude con mayor facilidad.

Estos controles son necesarios ya que los medios abusan de la capacidad del proceso de datos, dando lugar a intercambio de datos privados entre empresas o fraudes por falta de controles en los sistemas.

Por todo ello es necesario establecer mecanismos de Control y Auditoría de Ordenadores en las organizaciones, y de este modo evitar:

- Costes por la pérdida de datos en las organizaciones

En la actualidad, los datos son recursos críticos para la continuidad de las funciones de cualquier empresa, y su importancia dependerá de lo vital que sean para la organización.

Para poder proteger estos recursos será necesario establecer una política a nivel organización, de copias de seguridad y recuperación.

- Toma de decisiones incorrecta

Los datos nos van a permitir entre otras cosas realizar tomas de decisión. Pero para que las decisiones tomadas a partir de los datos sean



correctas, tendremos que garantizar que los datos que nos son suministrados son asimismo correctos.

La importancia de la veracidad de los datos viene dada por el tipo de decisiones que se toman a partir de ellos. Por ejemplo:

- En planes estratégicos a largo plazo: Los datos que facilitan la toma de decisiones pueden ser “algo” imprecisos, puesto que el resultado es global, genérico. Se pueden utilizar “grandes números”, es decir, cantidades brutas aproximadas, sin importar el detalle.
- En cambio, en control de operaciones y en control de gestión se necesitan datos totalmente precisos.

- Abuso Informático o Abuso del Ordenador

Se podría pensar que el abuso informático constituye la causa principal de la necesidad de AI. No obstante, tras estudios intensivos se ha llegado a la conclusión de que existen otras dos causas de problemas, que son aún más importantes que el abuso informático:

- 1) Errores y omisiones que originan pérdidas: frecuentemente, son el motivo de toma de decisiones erróneas. Por ejemplo: un simple error en el inventario que indique que existen 500 unidades de un determinado producto, cuando en realidad hay 5.000, puede inducir a realizar un nuevo pedido, con el consiguiente coste de adquisición, almacenamiento o pérdidas si el producto es perecedero.
- 2) Destrucción de datos ocasionada por desastres naturales (agua, fuego, y fallos de energía)

Esto nos obliga a plantear soluciones para estas dos causas en primer lugar, antes incluso que al abuso informático.

De todos modos, no podemos dejar de establecer controles para evitar el abuso informático, dado que los costes derivados de éste suelen ser muy superiores a los producidos por el abuso “manual”, o a los derivados de las dos causas anteriormente citadas. En general, los fraudes

que se pueden realizar con los ordenadores producen más pérdidas que los que se realizan con sistemas manuales.

- Pérdida de privacidad de los datos

Desde siempre se han recogido datos de personas para su uso comercial: datos personales, médicos, de impuestos, etc. Pero desde la llegada de los ordenadores la difusión “incontrolada” de estos datos se ha convertido en un serio problema, principalmente debido a que crear, actualizar y difundir una base de datos con datos personales de posibles clientes es mucho más fácil ahora que cuando los sistemas eran manuales.

En muchos países, la privacidad de los datos es un derecho. En nuestro país, la Ley de Protección de Datos de Carácter Personal asegura la confidencialidad de los datos y protege a los propietarios de los mismos del uso ilegítimo de ellos por terceras personas.

Lo que tenemos es que garantizar que esto no ocurra, y que los datos sólo se utilizan con el propósito para el que fueron dados por su propietario, fin último de la Auditoría Informática.

6.1.7 CONCLUSIONES

Los cambios en la tecnología influyen en qué auditar y en cómo auditar, por lo que inevitablemente, la auditoría ha cambiado de manera drástica en los últimos años con el gran impacto que han generado las técnicas informáticas en la forma de procesarla.

Los procesos de negocios, que se llevan a cabo dentro de las unidades de una organización, se coordinan en función de los procesos de gestión básicos de planificación, ejecución y supervisión. El control que provee la auditoría es parte de dichos procesos y está integrado en ellos, permitiendo su funcionamiento adecuado y supervisando su

comportamiento y aplicabilidad en cada momento, con lo que constituye una herramienta útil para la gestión, pero no un sustituto de ésta.

6.2 METODOLOGÍA.

El método de trabajo del auditor pasa por las siguientes etapas:

- Alcance y Objetivos de la Auditoría Informática.
- Estudio inicial del entorno auditable.
- Determinación de los recursos necesarios para realizar la auditoría.
- Elaboración del plan y de los Programas de Trabajo.
- Actividades propiamente dichas de la auditoría.
- Confección y redacción del Informe Final.

Definición de Alcance y Objetivos

El alcance de la auditoría expresa los límites de la misma. Debe existir un acuerdo muy preciso entre auditores y clientes sobre las funciones, las materias y las organizaciones a auditar.

A los efectos de acotar el trabajo, resulta muy beneficioso para ambas partes expresar las excepciones de alcance de la auditoría, es decir cuales materias, funciones u organizaciones no van a ser auditadas. Tanto los alcances como las excepciones deben figurar al comienzo del Informe Final.

Las personas que realizan la auditoría han de conocer con la mayor exactitud posible los objetivos a los que su tarea debe llegar. Deben comprender los deseos y pretensiones del cliente, de forma que las metas fijadas puedan ser cumplidas.

Una vez definidos los objetivos (objetivos específicos), éstos se añadirán a los objetivos generales y comunes de a toda auditoría Informática: La operatividad de los Sistemas y los Controles Generales de Gestión Informática.

Estudio Inicial

Para realizar dicho estudio han de examinarse las funciones y actividades generales de la informática.

Para el equipo auditor, el conocimiento de quién ordena, quién diseña y quién ejecuta es fundamental. Para realizar esto en auditor deberá fijarse en:

A- La Organización:

1) Organigrama: El organigrama expresa la estructura oficial de la organización a auditar.

2) Departamentos: El equipo auditor describirá brevemente las funciones de cada uno de ellos.

3) Relaciones Jerárquicas y funcionales entre órganos de la Organización: El equipo auditor verificará si se cumplen las relaciones funcionales y Jerárquicas previstas por el organigrama.

B- Entorno Operacional:

1) Arquitectura y configuración de Hardware y Software: Los auditores, en su estudio inicial, deben tener en su poder la distribución e interconexión de los equipos.

El auditor recabará información escrita, en donde figuren todos los elementos físicos y lógicos de la instalación. En cuanto a Hardware

figurarán las CPUs, unidades de control local y remotas, periféricos de todo tipo, etc.

El inventario de software debe contener todos los productos lógicos del Sistema, desde el software básico hasta los programas de utilidad adquiridos o desarrollados internamente. Suele ser habitual clasificarlos en facturables y no facturables.

2) Comunicación y Redes de Comunicación: En el estudio inicial los auditores dispondrán del número, situación y características principales de las líneas, así como de los accesos a la red pública de comunicaciones. Igualmente, poseerán información de las Redes Locales de la Empresa.

3) Aplicaciones de bases de datos y ficheros: El auditor recabará información de tamaño y características de las Bases de Datos, clasificándolas en relación y jerarquías.

Estos datos proporcionan una visión aceptable de las características de la carga informática.

Determinación de recursos de la auditoría Informática

Mediante los resultados del estudio inicial realizado se procede a determinar los recursos humanos y materiales que han de emplearse en la auditoría.

Recursos materiales

Es muy importante su determinación, por cuanto la mayoría de ellos son proporcionados por el cliente.

Recursos Humanos

La cantidad de recursos depende del volumen auditable. Las características y perfiles del personal seleccionado dependen de la materia auditable.

Elaboración del Plan y de los programas de trabajo

Una vez asignados los recursos, el responsable de la auditoría y sus colaboradores establecen un plan de trabajo. Decidido éste, se procede a la programación del mismo.

El plan se elabora teniendo en cuenta, entre otros criterios, los siguientes:

a) Si la Revisión debe realizarse por áreas generales o áreas específicas. En el primer caso, la elaboración es más compleja y costosa.

b) Si la auditoría es global, de toda la Informática, o parcial. El volumen determina no solamente el número de auditores necesarios, sino las especialidades necesarias del personal.

Una vez elaborado el Plan, se procede a la Programación de Actividades.

Actividades de la Auditoría Informática

Para completar las distintas actividades propias de la auditoría informática, el auditor puede hacer uso de las siguientes técnicas y herramientas:

Técnicas de Trabajo:

- Análisis de la información recabada del auditado.
- Análisis de la información propia.
- Entrevistas.
- Simulación.
- Muestreos.

Herramientas:

- Cuestionario general inicial.
- Cuestionario Checklist.
- Estándares.
- Monitores.
- Simuladores (Generadores de datos).
- Paquetes de auditoría (Generadores de Programas).
- Matrices de riesgo.

Informe Final

La función de la auditoría se materializa exclusivamente por escrito. Por lo tanto la elaboración final es el exponente de su calidad.

Resulta evidente la necesidad de redactar borradores e informes parciales previos al informe final, que son elementos de contraste entre opinión entre auditor y auditado y que pueden descubrir fallos de apreciación en el auditor.

6.3 AUDITORÍA DE LOS GRANDES SISTEMAS INFORMÁTICOS

La auditoría de los S.I. deberá comprender no sólo la evaluación de los equipos de cómputo, de un sistema o procedimiento específico, sino que además habrá de evaluar los sistemas de información en general desde sus entradas, procedimientos, controles, archivos, seguridad y obtención de información.

La auditoría de los S.I. es de vital importancia para el buen desempeño de los sistemas de información, ya que proporciona los controles necesarios para que los sistemas sean confiables y con un buen nivel de seguridad. Además debe evaluar todo (informática, organización de centros de información, hardware y software).

Para hacer una adecuada planificación de la auditoría de los S.I., hay que seguir una serie de pasos previos que permitirán dimensionar el tamaño y características del organismo a auditar, sus sistemas, organización y equipo.

6.3.1 REGULACIÓN INTERNACIONAL SOBRE AUDITORÍA DE SISTEMAS DE INFORMACIÓN

En materia de Auditoría de Sistemas de Información existen varias metodologías desde el enfoque de control a nivel internacional. Algunas de las más importantes para los profesionales de la auditoría son:

A) ISACA-COBIT

The Information Systems Audit and Control Foundation, ISACA (<http://www.isaca.org>). Es la asociación líder en Auditoría de Sistemas, con 23.000 miembros en 100 países.

ISACA propone la metodología COBIT ® (Control Objectives for Information and related Technology). Es un documento realizado en el año de 1996 y revisado posteriormente, dirigido a auditores, administradores y usuarios de sistemas de información, que tiene como objetivos de control la efectividad y la eficiencia de las operaciones; confidencialidad e integridad de la información financiera y el cumplimiento de las leyes y regulaciones.

B) COSO

The Committee of Sponsoring Organizations of the Treadway Commission's Internal Control - Integrated Framework (COSO). Publicado en 1992 hace recomendaciones a los contables de gestión de cómo evaluar, informar e implementar sistemas de control, teniendo como objetivo de control la efectividad y eficiencia de las operaciones, la información financiera y el cumplimiento de las regulaciones que explica en

los componentes del ambiente de control, valoración de riesgos, actividades de control, información y comunicación, y el monitoreo.

C) AICPA-SAS

The American Institute of Certified Public Accountants' Consideration of the Internal Control Structure in a Financial Statement Audit (SAS 55), que ha sido modificado por el (SAS 78), 1995.

Da una guía a los auditores externos sobre el impacto del control interno en la planificación y desarrollo de una auditoría de estados financieros de las empresas, presentado como objetivos de control la información financiera, la efectividad y eficiencia de las operaciones y el cumplimiento de regulaciones, que desarrolla en los componentes de ambiente de control, valoración de riesgo, actividades de control, información, comunicación y monitoreo.

D) IFAC - NIA

La Federación Internacional de Contables IFAC (<http://www.ifac.org>) emitió las Normas Internacionales de Auditoría NIA 15, 16 y 20 en 1991. IFAC muestra en la NIA 15 (Auditoría en Entornos Informatizados) una referencia de controles para procesamiento electrónico de datos y la necesidad de estos cuando estamos en ambientes donde los instrumentos tradicionales del papel y demás pistas de auditoría no son visibles para los contables en el momento de realizar su trabajo.

La NIA 16 (Técnicas de Auditoría Asistida por Computador) describe técnicas y procedimientos de auditoría que se pueden hacer en entornos informatizados con ayuda de los computadores y otras tecnologías.

La NIA 20 nos presenta los efectos de un entorno informatizado en la evaluación de sistemas de información contables. Junto con las demás normas dan una guía al auditor de los controles en general a tener en cuenta en un ambiente informatizado y en las aplicaciones que procesan la

información, así como técnicas de auditoría asistidas por computador y su importancia.

E) SAC

The Institute of Internal Auditors Research Foundation's Systems Auditability and Control (SAC).

Realizado en 1991 y revisado posteriormente. Ofrece una guía de estándares y controles para los auditores internos en el área de auditoría de sistemas de información y tecnología. Tiene como objetivos de control la efectividad y eficiencia de las operaciones, la integridad de la información financiera y el cumplimiento de normas y regulaciones que explica en el ambiente de control, sistemas manuales y automatizados y procedimientos de control.

F) MAGERIT

Consejo superior de informática del ministerio de administraciones públicas de España MAGERIT (Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información). 1997

Es una metodología de análisis y gestión de riesgos de los sistemas de información de las administraciones públicas, emitida en el año 1997 por el consejo superior de informática y recoge las recomendaciones de las directivas de la Unión Europea en materia de seguridad de sistemas de información. Esta metodología presenta un objetivo definido en el estudio de los riesgos que afectan los sistemas de información y el entorno de ellos haciendo unas recomendaciones de las medidas apropiadas que deberían adoptarse para conocer, prevenir, evaluar y controlar los riesgos investigados. Magerit desarrolla el concepto de control de riesgos en las guías de procedimientos, técnicas, desarrollo de aplicaciones, personal y cumplimiento de normas legales.

G)EDP

La E.D.P. Auditors Foundation (EDPAF) fundada en 1976, es otra entidad de carácter educativo e investigador en los temas sobre estándares para la auditoría de los sistemas de información.

Esta fundación ha investigado sobre controles en los sistemas de información, generando los diez estándares generales de auditoría de sistemas y el código de ética para los auditores de sistemas que relacionamos a continuación.

6.4 AUDITORÍA DE LAS REDES DE ÁREA LOCAL.

Una Auditoría de Redes es, en esencia, una serie de mecanismos mediante los cuales se pone a prueba una red informática, evaluando su desempeño y seguridad, a fin de lograr una utilización más eficiente y segura de la información. El primer paso para iniciar una gestión responsable de la seguridad es identificar la estructura física (hardware, topología) y lógica (software, aplicaciones) del sistema (sea un equipo, red, intranet, extranet), y hacerle un Análisis de Vulnerabilidad para saber en qué grado de exposición nos encontramos; así, hecha esta "radiografía" de la red, se procede a localizar sus carencias más críticas, para proponer una Estrategia de Saneamiento de los mismos; un Plan de Contención ante posibles incidentes; y un Seguimiento Continuo del desempeño del sistema de ahora en más.

6.4.1 ETAPAS A IMPLEMENTAR EN LA AUDITORÍA DE REDES

Análisis de Vulnerabilidad

Éste es sin duda el punto más crítico de toda la Auditoría, ya que de él dependerá directamente el curso de acción a tomar en las siguientes etapas y el éxito de éstas.

Estrategia de Saneamiento

Identificadas las "brechas" en la red, se procede a "parchearlas", bien sea actualizando el software afectado, reconfigurándolo de una mejor manera ó remplazándolo por otro que consideremos más seguro y de mejor desempeño.

Las bases de datos, los servidores internos de correo, las comunicaciones sin cifrar, las estaciones de trabajo... todos los puntos críticos deben reducir el riesgo. En los casos más extremos, la misma infraestructura física de la red deberá ser replanteada, reorganizando y reconfigurando sus switches, routers y firewalls.

Plan de Contención

La red ha sido replanteada, el software ha sido reconfigurado (o rediseñado) y el riesgo ha sido reducido; aún así, constantemente se están reportando nuevos fallos de seguridad y la posibilidad de intrusión siempre está latente. Un disco puede fallar, una base de datos puede corromperse o una estación de trabajo puede ser infectada por un virus; para ello hay que elaborar un "Plan B", que prevea un incidente aún después de tomadas las medidas de seguridad, y que dé respuesta ante posibles eventualidades.

Seguimiento Continuo

La seguridad no es un producto, es un proceso. Constantemente surgen nuevos fallos de seguridad, nuevos virus, nuevas "herramientas" (exploits) que facilitan la intrusión en sistemas, como así también nuevas y

más efectivas tecnologías para prevenir estos problemas; por todo ello, la actitud ante la seguridad debe ser activa, procurando estar "al corriente" de lo que esté sucediendo en la materia, para ir cubriendo las nuevas brechas que vayan surgiendo y -cuando menos- para hacerle el trabajo más difícil a nuestros atacantes.

6.5 AUDITORÍA DE LA INFORMÁTICA PERSONAL

Entre los distintos servicios de auditoría (interna, perimetral, test de intrusión, etc.) que se pueden aplicar al ámbito de la Informática personal, destaca el Análisis forense como disciplina en auge debido a la proliferación de ataques informáticos así como la exposición de los datos contenidos en los archivos personales como consecuencia de la 'necesidad' de estar conectados a redes públicas para el desempeño del trabajo o el ocio.

Son innumerables los medios de acceder a los dispositivos personales (desde ordenadores personales a terminales móviles) y el riesgo de ser 'espiado' aumenta si no se toman unas medidas mínimas de seguridad, como software anti-malware, actualización de parches de seguridad, configuración del firewall, política de contraseñas, etc. Si estas medidas fallan, o bien se ha explotado una nueva vulnerabilidad de la que todavía no hay constancia, nuestros equipos personales pasan a estar controlados por terceros y toda la información en ellos contenida puede ser utilizada de forma fraudulenta (cuentas bancarias, claves de servicios web, imágenes, videos, correos personales, etc.)

Cuando hay sospecha de que nuestro equipo ha sido utilizado para llevar a cabo actividades ilícitas (reenvío de spam en nuestro nombre, anexas nuestra máquina a una botnet para ejecutar ataques tipo Denegación de Servicio, etc.) o bien ha dejado de funcionar al ser objeto de

un ataque (por virus, borrado de ficheros por un tercero, etc) deberemos obtener evidencias que certifiquen lo ocurrido.

6.5.1 ANÁLISIS FORENSE

6.5.1.1 INTRODUCCIÓN

La informática forense se ocupa de la investigación de acontecimientos sospechosos relacionados con sistemas informáticos, el esclarecimiento de situaciones creadas y sus autores, a través de la identificación, preservación, análisis y presentación de evidencias digitales. Los servicios de la informática forense no se limitan a aportar pruebas en procesos judiciales o administrativos. También se aplica a recuperar evidencias para su estudio y a la reconstrucción de determinados hechos con fines privados, empresariales, etc.

Con la aplicación de métodos científicos en la informática forense es posible estandarizar los procedimientos y dotarlos de mayor consistencia.

La informática forense se aplica allí donde:

- se presume una actividad delictiva en Internet, en entidades económicas, o sociales o en el ámbito privado
- cuando existen sospechas de robo datos, espionaje industrial, sabotaje o delitos por el estilo
- tenencia, producción y difusión de pornografía prohibida
- así como otras actividades ilícitas, las cuales se ejecutan con la ayuda de ordenadores.

El objetivo de una investigación forense tras una agresión son en general las siguientes:

- reconocimiento de los métodos o los puntos débiles que posibilitaron la agresión
- determinación de los daños ocasionados
- identificación del autor
- aseguramiento de las evidencias

De la formulación de estos objetivos se derivan las siguientes cuestiones:

- ¿Cómo puede verificarse el ataque?
- ¿Cómo debe asegurarse el sistema comprometido y su entorno?
- ¿Qué métodos deben emplearse para la captura de evidencias?
- ¿En qué secuencia deben preservarse las evidencias?
- ¿Dónde deben buscarse puntos de referencia y como pueden ser encontrados?
- ¿Cómo puede analizarse lo desconocido?

6.5.1.2 FASES DEL ANÁLISIS FORENSE

IDENTIFICACIÓN

La investigación forense comienza con la descripción exacta de la situación encontrada. Junto con la toma de los elementos existentes relativos al caso y las primeras presunciones, tienen que definirse los aspectos que deban ser esclarecidos. A continuación deberá estructurarse el material existente. Hecho esto deberán tomarse las decisiones inherentes a los medios necesarios para la preservación del material. Todo esto debe ser debidamente documentado.

PRESERVACIÓN

El primer paso en la preservación es el aseguramiento del lugar, el/los sistemas, los medios de almacenamiento de datos externos y otras posibles fuentes de evidencias. El objetivo fundamental es garantizar la integridad de las pruebas digitales.

ANÁLISIS

Tras la toma de datos probatorios relevantes y haberlos asegurado en los medios previstos, deberá procederse a los primeros análisis. Aquí se requerirán conocimientos sobre topología de red, aplicaciones, vulnerabilidades del sistema y una gran capacidad de improvisación.

El análisis forense es una metodología de estudio que se aplica una vez ocurrido un incidente, mediante el cual se trata de reconstruir cómo se ha penetrado en el sistema y se valoran los daños ocasionados.

Mediante el análisis forense es posible conocer los detalles de lo ocurrido y proponer la toma de medidas oportunas para prevenir futuros ataques, descubrir las vulnerabilidades que han hecho posible la intrusión, el origen, las acciones realizadas y las herramientas utilizadas.

En última instancia, es capaz de identificar al autor, el motivo y recomendar acciones legales. En caso de dudas, el proceso de análisis debe poder ser reproducido por expertos independientes (terceros).

El análisis no se realiza nunca sobre el sistema original y exige una documentación exhausta.

PRESENTACIÓN

La presentación constituye la conclusión de la investigación forense y en ella se prepara y redactan los resultados de todo el proceso. Estos deben ajustarse a la motivación de la investigación y a quien está dirigido.

Su contenido apuntará a la determinación del autor o autores, la fecha y hora, la descripción de los hechos, las proporciones alcanzadas y sus causas.

DOCUMENTACIÓN

La documentación de todo el proceso forense es de vital importancia. Todas las acciones ejecutadas deben ser pormenorizadamente protocolizadas. Esta protocolización debe ser oportuna, inmediatamente después de las acciones. Deben servir de garante de la actividad efectuada y facilitar la comprensión de la investigación.

Las actividades que no se documentan inmediatamente, generalmente no se registran. Al salvar datos volátiles en un sistema que se mantiene activo mientras se realiza el trabajo forense, debe hacerse con testigos, los cuales pueden corroborar que la preservación de los datos se realice correctamente y se eviten errores.

La importancia de mantener una protocolización detallada del proceso queda demostrada cuando los resultados del análisis forense son presentados y surgen dudas sobre algún aspecto. Además, la presentación se efectúa mucho después de haberse ejecutado las acciones, quizás uno o varios participantes en la investigación no puedan estar presentes, o simplemente alguien no pueda recordarse de algún detalle relevante.

Los protocolos deben recoger informaciones como:

- persona o grupo de personas que detectaron el caso
- hora y fecha de la comunicación
- el contenido exacto de la comunicación
- nombre de las personas y organizaciones que ejecuten la investigación
- nombre de quién dirige la investigación
- definición del procedimiento
- causa de la investigación
- lista de todos los sistemas, aparatos y aplicaciones incluidos en la investigación



- lista de todos los servicios y aplicaciones activos
- lista de todos los administradores relacionados con el sistema
- lista detallada de todos los pasos acometidos para encontrar evidencias, analizarlas y preservarlas
- registro de las personas que tienen acceso a las evidencias, incluida fecha y hora

Bibliografía:

Auditoría Informática: Un enfoque práctico. Piattini Velthuis, Mario G.; Peso Navarro, Emilio del ... [et al.]

Auditoría en sistemas computacionales. Carlos Muñoz Razo

Auditoría de sistemas. Una visión práctica. Alonso Tamayo Alzate

Auditoría Informática. Gonzalo Alonso Rivas

Autor:

Ramón Seoane Freijido

Director de Sistemas de Información Molduras del Noroeste

Colegiado del CPEIG

**7. LEY DE ACCESO ELECTRÓNICO
DE LOS CIUDADANOS A LOS
SERVICIOS PÚBLICOS. DECRETO
198/2010, POR EL QUE SE
REGULA EL DESARROLLO DE LA
ADMINISTRACIÓN ELECTRÓNICA
EN LA XUNTA DE GALICIA Y EN
LAS ENTIDADES DEPENDIENTES.
REAL DECRETO 3/2010, POR EL
QUE SE REGULA EL ESQUEMA
NACIONAL DE SEGURIDAD EN EL
ÁMBITO DE LA ADMINISTRACIÓN
ELECTRÓNICA. REAL DECRETO
4/2010, POR EL QUE SE REGULA
EL ESQUEMA NACIONAL DE
INTEROPERABILIDAD EN EL
ÁMBITO DE LA ADMINISTRACIÓN
ELECTRÓNICA.**

Tema 7.- Ley de acceso electrónico de los ciudadanos a los servicios públicos. Decreto 198/2010 por el que se regula el desarrollo de la administración electrónica en la Xunta de Galicia y sus entidades dependientes. Real decreto 3/2010 por el que se regula el esquema nacional de seguridad en el ámbito de la administración electrónica. Real decreto 4/2010 por el que se regula el esquema nacional de interoperabilidad en el ámbito de la administración electrónica.

INDICE

7.1 Ley de acceso electrónico de los ciudadanos a los servicios publicos

- 7.1.1 Introducción
- 7.1.2 Objeto de la ley
- 7.1.3 Ámbito de aplicación
- 7.1.4 Finalidades
- 7.1.5 Principios.

7.2 Decreto 198/2010 por el que se regula el desarrollo de la administración electrónica en la Xunta de Galicia y sus entidades dependientes.

- 7.2.1 Introducción
- 7.2.2 Objeto
- 7.2.3 Estructura

7.3 Real decreto 3/2010 por el que se regula el esquema nacional de seguridad en el ámbito de la administración electrónica

- 7.3.1 Introducción
- 7.3.2 Principios
- 7.3.3 Objetivos
- 7.3.4 Ámbito de aplicación.

7.4 Real decreto 4/2010 por el que se regula el esquema nacional de interoperabilidad en el ámbito de la administración electrónica.

- 7.4.1 Introducción

7.4.2 Objetivos

7.4.3 Ámbito aplicación y análisis

1.- LA LEY 11/2007 DE ACCESO ELECTRÓNICO DE LOS CIUDADANOS A LOS SERVICIOS PÚBLICOS. LA CALIDAD DE LOS SERVICIOS PÚBLICOS Y DE ATENCIÓN AL CIUDADANO.

1.1 Introducción.

Durante los últimos años se han producido numerosos cambios muy importantes en las relaciones entre Administración y Gobierno y ciudadanos, el progreso social, económico y tecnológico fomentaron el deseo de cambio y presionaron a la Administración para adaptarse a los nuevos problemas, las nuevas competencias y las necesidades ciudadanas.

La Administración Pública en cumplimiento de su deber de servir con objetividad a los intereses generales y actuar de acuerdo con los principios de eficacia, jerarquía, descentralización, desconcentración y coordinación con sometimiento pleno a la ley y el Derecho (art.103.1 CE) -, debe ser aquí una pieza fundamental para la implementación de las políticas de modernización de las administraciones públicas. Ha de ser capaz de adaptarse a las nuevas realidades para formar parte del proceso de desarrollo económico y social de las sociedades occidentales.

La mejora, y consecuentemente, la modernización de las administraciones públicas, debe ser un proceso continuo, dinámico y constante, en el que participen todos los que forman parte del sector público

En España, el punto de partida lo supuso el Acuerdo de Consejo de Ministros de 15 de noviembre de 1991, ya que en 1992 se aprobaría el Plan de Modernización de la Administración del Estado, compuesto por una serie de medidas que tenían como objetivo mejorar y modernizar la Administración Pública para responder a las necesidades cambiantes de los ciudadanos.

En la actualidad, las políticas de modernización están estrechamente ligadas con el desarrollo de la administración electrónica,

Siguiendo la definición dada por la Comisión Europea: la administración electrónica no es sino “el uso de las tecnologías en las Administraciones Públicas, combinado con cambios organizativos y nuevas aptitudes, con el fin de mejorar los servicios públicos y los procesos democráticos y reforzar el apoyo a las políticas públicas”.

Actualmente un elemento vertebrador del desarrollo de las tecnologías en la Administración lo constituye el denominado PLAN AVANZA II 2011-2015 (Aprobado por el Consejo de Ministros del 16 de julio de 2010)

Tomando como punto de partida el Plan Avanza aprobado en el año 2005, así como el marco europeo en el que se encuadran este tipo de iniciativas, se han identificado 34 retos concretos que debe abordar España en el ámbito de las TIC. En este contexto, la Estrategia 2011-2015 del Plan Avanza 2 va a centrar sus esfuerzos en la consecución de los siguientes 10 objetivos que facilitarán la superación de los retos definidos:

1. Promover procesos innovadores TIC(tecnologías información y comunicación) en las AAPP
2. Extender las TIC en la sanidad y el bienestar social

3. Potenciar la aplicación de las TIC al sistema educativo y formativo
4. Mejorar la capacidad y la extensión de las redes de telecomunicaciones
5. Extender la cultura de la seguridad entre la ciudadanía y las empresas
6. Incrementar el uso avanzado de servicios digitales por la ciudadanía
7. Extender el uso de soluciones TIC de negocio en la empresa
8. Desarrollar las capacidades tecnológicas del sector TIC
9. Fortalecer el sector de contenidos digitales garantizando la mejor protección de la propiedad intelectual en el actual contexto tecnológico y dentro del marco jurídico español y europeo.
10. Desarrollar las TIC verdes

Dentro de ese campo de actuación juega un papel decisivo en el desarrollo del mismo la Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los servicios públicos

La Ley 30/1992, de 26 de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común (LRJAP-PC) en su primera versión recogió, en su artículo 45, el impulso al empleo y aplicación de las técnicas y medios electrónicos, informáticos y telemáticos, por la Administración para el desarrollo de su actividad y el ejercicio de sus competencias y que permitió a los ciudadanos relacionarse con las Administraciones cuando fuese compatible con los “medios técnicos de que dispongan”. Además su artículo 38, y posteriormente la Ley 24/2001, pasaron de la informatización de los registros y archivos a los registros telemáticos como forma de relacionarse con la administración, siempre que el interesado señalase este medio como preferente.

Se pasa de una declaración de impulso de la Administración electrónica a la obligación de emplear medios telemáticos, ya que la Ley 11/2007, reconoce el derecho de los ciudadanos a relacionarse con la Administración a través de estos medios.

El servicio al ciudadano exige consagrar su derecho a comunicarse con las Administraciones por medios electrónicos, ya que estas están obligadas a hacerlo mediante el reconocimiento de la Ley del derecho de los ciudadanos a establecer relaciones electrónicas. De ahí que cada Administración (Estatad, Autonómica y local) deba facilitar al ciudadano, entre otros:

- El acceso a la información y servicios de su competencia.
- Presentar solicitudes y recursos.
- Los medios para dirigirse a las demás Administraciones, lo cual conlleva la colaboración entre administraciones.
- Efectuar pagos.
- Acceder a las notificaciones y comunicaciones que les remita la Administración.
- Encontrar información en un punto de acceso único sobre los servicios multicanal o aquellos que se ofrezcan por más de un medio o plataforma.

Los puntos más destacables de la Ley son:

- Los ciudadanos verán reconocidos nuevos derechos en sus relaciones con las Administraciones Públicas.
- La creación de la figura del Defensor del Usuario.
- Las Administraciones tendrán la obligación de hacer estos derechos efectivos a partir de 2009.
- Los trámites y gestiones podrán hacerse desde cualquier lugar, en cualquier momento.
- La Administración será más fácil, más ágil y más eficaz.
- Los ciudadanos pasan a tomar el mando en sus relaciones con la administración.

- Es una Ley de consenso. En su elaboración han participado todas las administraciones, de ciudadanos, de partidos, de empresas y asociaciones.

1.2 Objeto de la Ley

- Reconocer el derecho de los ciudadanos a relacionarse con las Administraciones Públicas por medios electrónicos.

- Regular los aspectos básicos de la utilización de las tecnologías de la información en la actividad administrativa, en las relaciones entre las Administraciones Públicas, así como en las relaciones de los ciudadanos con las mismas con la finalidad de garantizar sus derechos, un tratamiento común ante ellas y la validez y eficacia de la actividad administrativa en condiciones de seguridad jurídica.

- Utilizar, por parte de las AA.PP., las tecnologías de la información de acuerdo con lo dispuesto en la Ley, asegurando la disponibilidad, el acceso, la integridad, la autenticidad, la confidencialidad y la conservación de los datos, informaciones y servicios que gestionen en el ejercicio de sus competencias.

1.3 Ámbito de aplicación (Disposición final primera).

- Las Administraciones Públicas, entendiendo por tales la Administración General del Estado, las Administraciones de las Comunidades Autónomas y las Entidades que integran la Administración Local, así como las entidades de derecho público vinculadas o dependientes de las mismas.

- Los ciudadanos en sus relaciones con las Administraciones Públicas.

- Las relaciones entre las distintas Administraciones Públicas.

La Ley no será de aplicación a las Administraciones Públicas en las actividades que desarrollen en régimen de derecho privado.

1.4 Finalidades de la Ley

- Facilitar el ejercicio de derechos y el cumplimiento de deberes por medios electrónicos.
- Facilitar el acceso por medios electrónicos de los ciudadanos a la información y al procedimiento administrativo, con especial atención a la eliminación de las barreras que limiten dicho acceso.
- Crear las condiciones de confianza en el uso de los medios electrónicos, estableciendo las medidas necesarias para la preservación de la integridad de los derechos fundamentales, y en especial los relacionados con la intimidad y la protección de datos de carácter personal, por medio de la garantía de la seguridad de los sistemas, los datos, las comunicaciones, y los servicios electrónicos.
- Promover la proximidad con el ciudadano y la transparencia administrativa, así como la mejora continuada en la consecución del interés general.
- Contribuir a la mejora del funcionamiento interno de las Administraciones Públicas, incrementando la eficacia y la eficiencia de las mismas mediante el uso de las tecnologías de la información, con las debidas garantías legales en la realización de sus funciones.
- Simplificar los procedimientos administrativos y proporcionar oportunidades de participación y mayor transparencia, con las debidas garantías legales.
- Contribuir al desarrollo de la sociedad de la información en el ámbito de las Administraciones Públicas y en la sociedad en general.

1.5 Principios generales

- Limitaciones de la utilización de las tecnologías de la información:
 - Las establecidas por la Constitución.
 - El resto del ordenamiento jurídico.

- Principios:

1. El respeto al derecho a la protección de datos de carácter personal en los términos establecidos por la Ley Orgánica 15/1999, de Protección de los Datos de Carácter Personal, en las demás leyes específicas que regulan el tratamiento de la información y en sus normas de desarrollo, así como a los derechos al honor y a la intimidad personal y familiar.

2. Principio de igualdad con objeto de que en ningún caso el uso de medios electrónicos pueda implicar la existencia de restricciones o discriminaciones para los ciudadanos que se relacionen con las Administraciones Públicas por medios no electrónicos, tanto respecto al acceso a la prestación de servicios públicos como respecto a cualquier actuación o procedimiento administrativo sin perjuicio de las medidas dirigidas a incentivar la utilización de los medios electrónicos.

3. Principio de accesibilidad a la información y a los servicios por medios electrónicos en los términos establecidos por la normativa vigente en esta materia, a través de sistemas que permitan obtenerlos de manera segura y comprensible, garantizando especialmente la accesibilidad universal y el diseño para todos de los soportes, canales y entornos con objeto de que todas las personas puedan ejercer sus derechos en igualdad de condiciones, incorporando las características necesarias para garantizar la accesibilidad de aquellos colectivos que lo requieran.

4. Principio de legalidad en cuanto al mantenimiento de la integridad de las garantías jurídicas de los ciudadanos ante las Administraciones Públicas establecidas en la Ley 30/1992, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común.

5. Principio de cooperación en la utilización de medios electrónicos por las Administraciones Públicas al objeto de garantizar tanto la interoperabilidad de los sistemas y soluciones adoptados por cada una de ellas como, en su caso, la prestación conjunta de servicios

a los ciudadanos. En particular, se garantizará el reconocimiento mutuo de los documentos electrónicos y de los medios de identificación y autenticación que se ajusten a lo dispuesto en la presente Ley.

6. Principio de seguridad en la implantación y utilización de los medios electrónicos por las Administraciones Públicas, en cuya virtud se exigirá al menos el mismo nivel de garantías y seguridad que se requiere para la utilización de medios no electrónicos en la actividad administrativa.

7. Principio de proporcionalidad en cuya virtud sólo se exigirán las garantías y medidas de seguridad adecuadas a la naturaleza y circunstancias de los distintos trámites y actuaciones. Asimismo sólo se requerirán a los ciudadanos aquellos datos que sean estrictamente necesarios en atención a la finalidad para la que se soliciten.

2. DECRETO 198/2010 POR EL QUE SE REGULA EL DESARROLLO DE LA ADMINISTRACIÓN ELECTRÓNICA EN LA XUNTA DE GALICIA Y EN SUS ENTIDADES DEPENDIENTES:

2.1 Introducción.

La administración de la CCAA de Galicia no puede permanecer ajena a los incesantes y cada vez mas frecuentes cambios en el seno de las relaciones con al Administración desde el punto de vista tecnológico, es en este ámbito en donde, tal y como se recoge en la exposición de motivos del Decreto, se pretende conseguir una administración diferente, que tendrá a la electrónica como elemento central en su modernización donde sus efectos reales sobre la población irán encaminados a la utilización de medios y formas que reduzcan la brecha tecnológica creando las condiciones de confianza precisas para el uso de las tecnologías de la información y de la comunicación.

2.1 Objeto

Tiene por objeto regular el derecho de los ciudadanos a relacionarse con las administraciones públicas por medios electrónicos, la tramitación de los procedimientos administrativos incorporados a la tramitación telemática, la creación y regulación de la sede electrónica, la creación de la edición electrónica del Diario Oficial de Galicia y del Registro Electrónico, el impulso y desarrollo de los servicios electrónicos y el establecimiento de infraestructuras y servicios de interoperabilidad.

2.3 Estructura

El Decreto consta de 40 artículos, agrupados en nueve capítulos, con tres disposiciones adicionales, tres transitorias, una derogatoria y cuatro finales.

En el capítulo I de la norma recoge su objeto, el de regular el derecho de los ciudadanos a relacionarse con las administraciones públicas por medios electrónicos, la tramitación de los procedimientos administrativos incorporados a la tramitación telemática, la creación y regulación de la sede electrónica, la creación de la edición electrónica del Diario Oficial de Galicia y del Registro Electrónico, el impulso y desarrollo de los servicios electrónicos y el establecimiento de infraestructuras y servicios de interoperabilidad.

Establece como medidas de carácter general

- Ordenar e impulsar la Administración electrónica, a fin de mejorar la eficiencia interna, las relaciones intra e inter administrativas y las relaciones con los ciudadanos.
- Garantizar el derecho de los ciudadanos a relacionarse por medios electrónicos con la Administración pública autonómica.

- Contribuir al desarrollo de la sociedad de la información en el ámbito de las administraciones públicas de Galicia.
- Preservar la integridad de los derechos fundamentales relacionados con la intimidad de las personas, para la garantía de la seguridad de los datos y de las comunicaciones y para la protección de los servicios prestados en soporte electrónico.
- Facilitar el acceso de los ciudadanos a los servicios de la Administración electrónica en las oficinas telemáticas integradas de atención a los ciudadanos, basadas en la cooperación interadministrativa, ofreciendo servicios a los ciudadanos en oficinas públicas, con independencia de cual sea la Administración competente para conocer el asunto.
- Posibilitar la intermediación entre administraciones públicas para la resolución de trámites administrativos solicitados a los ciudadanos cuando sean de competencia de la Xunta de Galicia.

El capítulo II establece que la sede electrónica es la dirección electrónica, a través de la cual los ciudadanos acceden a la información, servicios y trámites electrónicos, que representa una fuente de información auténtica en la que el organismo titular identificado con la sede garantiza responsablemente la integridad, veracidad y actualización de la información y los servicios a los que se pueda acceder a través de esta.

La dirección electrónica de referencia de la sede electrónica de la Xunta de Galicia será <https://sede.xunta.es> que será accesible directamente, así como a través del portal www.xunta.es, configurándose como un conjunto de páginas web que asegurará:

- La calidad de la información y la coherencia en la navegación.
- La identificación y comunicación segura, mediante los correspondientes certificados electrónicos admitidos por la Xunta de Galicia.
- El acceso al Registro Electrónico, a las comunicaciones y notificaciones y a los formularios para iniciar los procedimientos administrativos o solicitar la prestación de servicios.
- Los principios de accesibilidad de acuerdo con las normas establecidas, estándares abiertos y, en su caso, aquellos otros que sean de uso general por los ciudadanos

El capítulo III regula la creación del Diario Oficial de Galicia en su edición electrónica que tendrá una consideración de publicación única, dotándola de validez jurídica, que sustituirá a la edición impresa.

El capítulo IV trata sobre los mecanismos de identificación y autenticación, estableciendo que los ciudadanos podrán utilizar los siguientes instrumentos de identificación para relacionarse con la Xunta de Galicia y las entidades incluidas en el ámbito de aplicación de este Decreto:

- a. En todo caso, los sistemas de firma electrónica incorporados al documento nacional de identidad, para personas físicas.
- b. Sistemas de firma electrónica avanzada, incluyendo los basados en certificado electrónico reconocido, admitidos por las administraciones públicas que tengan validez para la Xunta de Galicia y que se especifiquen en la sede electrónica.

c. Sistemas de firma electrónica, como la utilización de claves concertadas en un registro previo como persona usuaria inscrita en el registro de funcionarios habilitados por la Xunta de Galicia.

d. Otros sistemas de identificación que resulten proporcionales y seguros para la identificación de las personas interesadas

El capítulo V regula la tramitación de procedimientos administrativos en el ámbito de la administración electrónica, estableciendo que la gestión electrónica de la actividad administrativa respetará el ejercicio y la titularidad del órgano o entidad que tenga atribuidas sus competencias, así como la obligatoriedad de impulso de la administración electrónica,

Regula la iniciación y tramitación del procedimiento por medios electrónicos, reconociendo que cualquier persona interesada podrá iniciar y tramitar un procedimiento administrativo por medios electrónicos, ante y en relación con la Xunta de Galicia o las entidades incluidas en el ámbito de aplicación de este Decreto, conforme a las previsiones de estas y sin otras limitaciones que las establecidas en las normas y protocolos de aplicación en atención a razones tecnológicas.

Los capítulos VI y VII regulan los aspectos de la gestión y tramitación de los procedimientos administrativos, tanto en el ámbito interno, relativo a comunicaciones y notificaciones, establece que as entidades incluidas en el ámbito de aplicación del presente Decreto utilizarán un sistema de notificación electrónica que acredite la fecha y hora de puesta la disposición de la persona interesada del acto objeto de notificación, así como de la fecha y hora de acceso de ésta a su contenido mediante sistemas de sellado de tiempo, como en el ámbito externo relacionado, en concreto con las copias y documentos

electrónicos, define el documento electrónico este en los términos que se recogen en el anexo de la ley 11/2007, de administración electrónica “ Información de cualquier naturaleza en forma electrónica, archivada en un soporte electrónico según un formato determinado y susceptible de identificación y tratamiento diferenciado.”

El capítulo VIII trata sobre la interoperabilidad, tiene por objeto fomentar la cooperación interadministrativa, figura clave en el mismo es el denominado protocolo de interoperabilidad que es el documento que determinará el procedimiento para incorporar y consumir la información en soporte electrónico de las entidades incluidas en el ámbito de aplicación del presente Decreto.

El capítulo IX concreta las funciones que el órgano de dirección con competencias generales en materia de desarrollo de la administración electrónica lleva a cabo en relación con este Decreto, en desarrollo de las competencias y funciones que le atribuye el Decreto 325/2009, de 18 de junio, de estructura Orgánica de los órganos superiores dependientes de la Presidencia de la Xunta de Galicia para el impulso, gestión y coordinación de la Administración electrónica, como elemento indispensable para la modernización de la Administración pública, la dirección y gestión de todas las actuaciones de la Xunta en materia de tecnologías de la información y las comunicaciones y el establecimiento de directrices tecnológicas que deben seguir todos los órganos de la Xunta de Galicia.

3. REAL DECRETO 3/2010 POR EL QUE SE REGULA EL ESQUEMA NACIONAL DE SEGURIDAD EN EL AMBITO DE LA ADMINSTRACION ELECTRONICA.

3.1 Introducción

Tiene por objeto regular el Esquema Nacional de Seguridad establecido en el artículo 42 de la Ley 11/2007, de 22 de junio, y determinar la política de seguridad que se ha de aplicar en la utilización de los medios electrónicos a los que se refiere la citada ley y recoge y regula los principios básicos y requisitos mínimos que permitan una protección adecuada de la información.

La finalidad del Esquema Nacional de Seguridad es crear las condiciones necesarias para la confianza en el uso de los medios electrónicos, a través de medidas para garantizar la seguridad de los sistemas, los datos, las comunicaciones, y los servicios electrónicos, que permita el ejercicio de derechos y el cumplimiento de deberes a través de estos medios. Persigue fundamentar la confianza en que los sistemas de información prestarán sus servicios y custodiarán la información de acuerdo con sus especificaciones funcionales, sin interrupciones o modificaciones fuera de control y sin que la información pueda llegar al conocimiento de personas no autorizadas.

Al objeto de crear estas condiciones, el Esquema Nacional de Seguridad introduce los elementos comunes que han de guiar la actuación de las Administraciones Públicas en materia de seguridad de las tecnologías de la información. En particular, introduce los siguientes elementos principales:

Los principios básicos a ser tenidos en cuenta en las decisiones en materia de seguridad.

Los requisitos mínimos que permitan una protección adecuada de la información.

El mecanismo para lograr el cumplimiento de los principios básicos y requisitos mínimos mediante la adopción de medidas de

seguridad proporcionadas a la naturaleza de la información, el sistema y los servicios a proteger.

Tiene en cuenta las recomendaciones de la Unión Europea, la situación tecnológica de las diferentes Administraciones Públicas, así como los servicios electrónicos ya existentes, y la utilización de estándares abiertos así como, en su caso y de forma complementaria, estándares que sean de uso generalizado por los ciudadanos.

En su elaboración se han manejado, entre otros, referentes en materia de seguridad tales como directrices y guías de la OCDE, recomendaciones de la Unión Europea, normalización nacional e internacional, normativa sobre administración electrónica, protección de datos de carácter personal, firma electrónica y Documento Nacional de Identidad Electrónico, así como a referentes de otros países.

Se ha realizado en un proceso coordinado por el Ministerio de la Presidencia con el apoyo del Centro Criptológico Nacional (CCN), con la participación de todas las Administraciones Públicas. A lo largo de los últimos tres años más de un centenar de expertos de las Administraciones Públicas ha colaborado en su elaboración; a los que hay que sumar los numerosos expertos que también han aportado su opinión a través de las asociaciones profesionales del sector TIC; todo ello a la luz del estado del arte y de los principales referentes en materia de seguridad de la información.

3.2 Principios básicos del Esquema Nacional de Seguridad.

El objeto último de la seguridad de la información es asegurar que una organización administrativa podrá cumplir sus objetivos utilizando sistemas de información. En las decisiones en materia de seguridad deberán tenerse en cuenta los siguientes principios básicos:

- a) Seguridad integral.
- b) Gestión de riesgos.
- c) Prevención, reacción y recuperación.
- d) Líneas de defensa.
- e) Reevaluación periódica.
- f) Función diferenciada.

Recoge el Real Decreto los requisitos mínimos que deberán tener los sistemas de seguridad, y así el artículo 11 establece que “Todos los órganos superiores de las Administraciones públicas deberán disponer formalmente de su política de seguridad, que será aprobada por el titular del órgano superior correspondiente. Esta política de seguridad, se establecerá en base a los principios básicos indicados y se desarrollará aplicando los siguientes requisitos mínimos:

- a) Organización e implantación del proceso de seguridad.
- b) Análisis y gestión de los riesgos.
- c) Gestión de personal.
- d) Profesionalidad.
- e) Autorización y control de los accesos.
- f) Protección de las instalaciones.
- g) Adquisición de productos.
- h) Seguridad por defecto.
- i) Integridad y actualización del sistema.
- j) Protección de la información almacenada y en tránsito.
- k) Prevención ante otros sistemas de información interconectados.
- l) Registro de actividad.
- m) Incidentes de seguridad.
- n) Continuidad de la actividad.
- o) Mejora continua del proceso de seguridad.

3.3 Objetivos.

Crear las condiciones necesarias de confianza en el uso de los medios electrónicos, a través de medidas para garantizar la seguridad de los sistemas, los datos, las comunicaciones, y los servicios electrónicos, que permita a los ciudadanos y a las administraciones públicas, el ejercicio de derechos y el cumplimiento de deberes a través de estos medios.

Establecer la política de seguridad en la utilización de medios electrónicos en el ámbito de la Ley 11/2007, que estará constituida por los principios básicos y los requisitos mínimos para una protección adecuada de la información.

Introducir los elementos comunes que han de guiar la actuación de las administraciones públicas en materia de seguridad de las tecnologías de la información.

Aportar un lenguaje común para facilitar la interacción de las administraciones públicas, así como la comunicación de los requisitos de seguridad de la información a la industria.

En el Esquema Nacional de Seguridad se concibe la seguridad como una actividad integral, en la que no caben actuaciones puntuales o tratamientos coyunturales, debido a que la debilidad de un sistema la determina su punto más frágil y, a menudo, este punto es la coordinación entre medidas individualmente adecuadas pero deficientemente ensambladas.

Dada la naturaleza de la seguridad, la consecución de estos objetivos requiere un desarrollo que tenga en cuenta la complejidad técnica, la obsolescencia de la tecnología subyacente y el importante cambio que supone en la operativa de la administración la aplicación de la Ley 11/2007.

3.4 Ámbito de aplicación

Su ámbito de aplicación es el establecido en el artículo 2 de la Ley 11/2007, de 22 de junio, es decir tanto las Administraciones Públicas, entendiendo por tales la Administración General del Estado, las Administraciones de las Comunidades Autónomas y las Entidades que integran la Administración Local, así como las entidades de derecho público vinculadas o dependientes de las mismas, a los ciudadanos en sus relaciones con las Administraciones Públicas y a las relaciones entre las distintas Administraciones Públicas.

Estarán excluidos los sistemas que tratan información clasificada regulada por Ley 9/1968 de 5 de abril, de Secretos Oficiales, modificada por Ley 48/1978, de 7 de octubre y normas de desarrollo.

4. REAL DECRETO 4/2010 POR EL QUE SE REGULA EL ESQUEMA NACIONAL DE INTEROPERABILIDAD EN EL AMBITO DE LA ADMINSTRACION ELECTRONICA.

4.1 Introducción.

El Esquema Nacional de Interoperabilidad persigue la creación de las condiciones necesarias para garantizar el adecuado nivel de interoperabilidad técnica, semántica y organizativa de los sistemas y aplicaciones empleados por las Administraciones Públicas, que permita el ejercicio de derechos y el cumplimiento de deberes a través del acceso electrónico a los servicios públicos, a la vez que redunda en beneficio de la eficacia y la eficiencia.

Al objeto de crear estas condiciones, el Esquema Nacional de Interoperabilidad introduce los elementos comunes que han de guiar la actuación de las Administraciones Públicas en materia de

interoperabilidad. En particular, introduce los siguientes elementos principales:

- Se enuncian los principios específicos de la interoperabilidad.
- Se contemplan las dimensiones de la interoperabilidad organizativa, semántica y técnica a las que se refiere el artículo 41 de la Ley 11/2007, de 22 de junio.
- Se tratan las infraestructuras y los servicios comunes, elementos reconocidos de dinamización, simplificación y propagación de la interoperabilidad, a la vez que facilitadores de la relación multilateral.
- Se trata la reutilización, aplicada a las aplicaciones de las administraciones públicas, de la documentación asociada y de otros objetos de información, dado que la voz ‘compartir’ se encuentra presente en la definición de interoperabilidad recogida en la Ley 11/2007, de 22 de junio, y junto con la voz ‘reutilizar’, ambas son relevantes para la interoperabilidad y se encuentran entroncadas con las políticas de la Unión Europea en relación con la idea de compartir, reutilizar y colaborar.
- Se trata la interoperabilidad de la firma electrónica y de los certificados.
- Se atiende a la recuperación y conservación del documento electrónico, según lo establecido en la citada Ley 11/2007, de 22 de junio, como manifestación de la interoperabilidad a lo largo del tiempo, y que afecta de forma singular al documento electrónico.
- Por último, se crean las normas técnicas de interoperabilidad y los instrumentos para la interoperabilidad, para facilitar la aplicación del Esquema.

Tiene en cuenta las recomendaciones de la Unión Europea, la situación tecnológica de las diferentes Administraciones Públicas, así como los servicios electrónicos ya existentes, y la utilización de

estándares abiertos así como, en su caso y de forma complementaria, estándares que sean de uso generalizado por los ciudadanos.

En su elaboración se han manejado, entre otros, referentes en materia de desarrollo de la administración electrónica y, en particular, de interoperabilidad provenientes del ámbito de la Unión Europea, de actuaciones similares en otros países, de la normalización nacional e internacional; así como la normativa sobre administración electrónica, protección de datos de carácter personal, firma electrónica y Documento Nacional de Identidad Electrónico, entre otros.

Se ha realizado en un proceso coordinado por el Ministerio de la Presidencia, con la participación de todas las Administraciones Públicas. Se ha elaborado con la participación de todas las Administraciones Públicas. A lo largo de los últimos tres años ha colaborado en su elaboración más de un centenar de expertos de las Administraciones Públicas; a los que hay que sumar los numerosos expertos que también han aportado su opinión a través de las asociaciones profesionales del sector TIC; todo ello a la luz del estado del arte y de los principales referentes en materia de interoperabilidad.

4.2 Objetivos

Sus objetivos son los siguientes:

- Comprender los criterios y recomendaciones que deberán ser tenidos en cuenta por las administraciones públicas para la toma de decisiones tecnológicas que garanticen la interoperabilidad y que eviten la discriminación a los ciudadanos por razón de su elección tecnológica.

- Introducir los elementos comunes que han de guiar la actuación de las administraciones públicas en materia de interoperabilidad.

- Aportar un lenguaje común para facilitar la interacción de las administraciones públicas, así como la comunicación de los requisitos de interoperabilidad a la industria.

La interoperabilidad se concibe en consecuencia desde una perspectiva integral, de manera que no caben actuaciones puntuales o tratamientos coyunturales, debido a que la debilidad de un sistema la determina su punto más frágil y, a menudo, este punto es la coordinación entre medidas individualmente adecuadas pero deficientemente ensambladas.

Dada la naturaleza de la interoperabilidad, la consecución de estos objetivos requiere un desarrollo que tenga en cuenta la complejidad técnica, la obsolescencia de la tecnología subyacente y el importante cambio que supone en la operativa de la administración la aplicación de la Ley 11/2007.

4.3 Ámbito de aplicación y Análisis

Su ámbito de aplicación es el establecido en el artículo 42 de la Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos, es decir, a las Administraciones Públicas, entendiendo por tales la Administración General del Estado, las Administraciones de las Comunidades Autónomas y las Entidades que integran la Administración Local, así como las entidades de derecho público vinculadas o dependientes de las mismas.

A los ciudadanos en sus relaciones con las Administraciones Públicas.

A las relaciones entre las distintas Administraciones Públicas.

No será de aplicación a las Administraciones Públicas en las actividades que desarrollen en régimen de derecho privado



Como aspectos mas importantes a destacar se encuentran:

1.- Regula de forma clara los derechos de los ciudadanos en relación con la utilización de los medios electrónicos en la actividad administrativa, entre ellos

- A elegir, entre aquellos que en cada momento se encuentren disponibles, el canal a través del cual relacionarse por medios electrónicos con las Administraciones Públicas.
- A no aportar los datos y documentos que obren en poder de las Administraciones Públicas, las cuales utilizarán medios electrónicos para recabar dicha información siempre que, en el caso de datos de carácter personal, se cuente con el consentimiento de los interesados en los términos establecidos por la Ley Orgánica 15/1999, de Protección de Datos de Carácter Personal, o una norma con rango de Ley así lo determine, salvo que existan restricciones conforme a la normativa de aplicación a los datos y documentos recabados. El citado consentimiento podrá emitirse y recabarse por medios electrónicos.
- A la igualdad en el acceso electrónico a los servicios de las Administraciones Públicas.
- A conocer por medios electrónicos el estado de tramitación de los procedimientos en los que sean interesados, salvo en los supuestos en que la normativa de aplicación establezca restricciones al acceso a la información sobre aquéllos.

- A obtener copias electrónicas de los documentos electrónicos que formen parte de procedimientos en los que tengan la condición de interesado.
- A la conservación en formato electrónico por las Administraciones Públicas de los documentos electrónicos que formen parte de un expediente.
- A obtener los medios de identificación electrónica necesarios, pudiendo las personas físicas utilizar en todo caso los sistemas de firma electrónica del Documento Nacional de Identidad para cualquier trámite electrónico con cualquier Administración Pública.
- A la utilización de otros sistemas de firma electrónica admitidos en el ámbito de las Administraciones Públicas.
- A la garantía de la seguridad y confidencialidad de los datos que figuren en los ficheros, sistemas y aplicaciones de las Administraciones Públicas.
- A la calidad de los servicios públicos prestados por medios electrónicos.
- A elegir las aplicaciones o sistemas para relacionarse con las Administraciones Públicas siempre y cuando utilicen estándares abiertos o, en su caso, aquellos otros que sean de uso generalizado por los ciudadanos.

Regula el régimen jurídico de la Administración Electrónica, define la sede electrónica como aquella dirección electrónica disponible para los ciudadanos a través de redes de

telecomunicaciones cuya titularidad, gestión y administración corresponde a una Administración Pública, órgano o entidad administrativa en el ejercicio de sus competencias.

Regula la identificación y autenticación, disponiendo que las Administraciones Públicas admitirán, en sus relaciones por medios electrónicos, sistemas de firma electrónica que sean conformes a lo establecido en la Ley 59/2003, de 19 de diciembre, de Firma Electrónica y resulten adecuados para garantizar la identificación de los participantes y, en su caso, la autenticidad e integridad de los documentos electrónicos.

Los ciudadanos podrán utilizar los siguientes sistemas de firma electrónica para relacionarse con las Administraciones Públicas, de acuerdo con lo que cada Administración determine:

- En todo caso, los sistemas de firma electrónica incorporados al Documento Nacional de Identidad, para personas físicas.
- Sistemas de firma electrónica avanzada, incluyendo los basados en certificado electrónico reconocido, admitidos por las Administraciones Públicas.
- Otros sistemas de firma electrónica, como la utilización de claves concertadas en un registro previo como usuario, la aportación de información conocida por ambas partes u otros sistemas no criptográficos, en los términos y condiciones que en cada caso se determinen.

Con relación a los registros, comunicaciones y notificaciones dispone que las Administraciones Públicas crearan registros

electrónicos para la recepción y remisión de solicitudes, escritos y comunicaciones.

Los registros electrónicos podrán admitir: Documentos electrónicos normalizados correspondientes a los servicios, procedimientos y trámites que se especifiquen conforme a lo dispuesto en la norma de creación del registro, cumplimentados de acuerdo con formatos preestablecidos, y además cualquier solicitud, escrito o comunicación distinta de los mencionados en el apartado anterior dirigido a cualquier órgano o entidad del ámbito de la administración titular del registro.

Con respecto a las comunicaciones, los ciudadanos podrán elegir en todo momento la manera de comunicarse con las Administraciones Públicas, sea o no por medios electrónicos, excepto en aquellos casos en los que de una norma con rango de Ley se establezca o infiera la utilización de un medio no electrónico. La opción de comunicarse por unos u otros medios no vincula al ciudadano, que podrá, en cualquier momento, optar por un medio distinto del inicialmente elegido.

Con respecto a documentos y copias dispone que las Administraciones Públicas podrán emitir validamente por medios electrónicos los documentos administrativos a los que se refiere el artículo 46 de la Ley 30/1992, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común, siempre que incorporen una o varias firmas electrónicas.

Los documentos administrativos incluirán referencia temporal, que se garantizará a través de medios electrónicos cuando la naturaleza del documento así lo requiera.

Las copias realizadas por medios electrónicos de documentos electrónicos emitidos por el propio interesado o por las Administraciones Públicas, manteniéndose o no el formato original,

tendrán inmediatamente la consideración de copias auténticas con la eficacia prevista en el artículo 46 de la Ley 30/1992, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común, siempre que el documento electrónico original se encuentre en poder de la Administración, y que la información de firma electrónica y, en su caso, de sellado de tiempo permitan comprobar la coincidencia con dicho documento.

Regula la gestión electrónica de procedimientos, disponiendo que la gestión electrónica de la actividad administrativa respetará la titularidad y el ejercicio de la competencia por la Administración Pública, órgano o entidad que la tenga atribuida y el cumplimiento de los requisitos formales y materiales establecidos en las normas que regulen la correspondiente actividad. A estos efectos, y en todo caso bajo criterios de simplificación administrativa, se impulsará la aplicación de medios electrónicos a los procesos de trabajo y la gestión de los procedimientos y de la actuación administrativa

Por ultimo establece el R D un marco institucional de colaboración entre Administraciones disponiendo II Comité Sectorial de administración electrónica, dependiente de la Conferencia Sectorial de Administración Pública, es el órgano técnico de cooperación de la Administración General del Estado, de las administraciones de las Comunidades Autónomas y de las entidades que integran la Administración Local en materia de administración electrónica.

El Comité Sectorial de la administración electrónica velará por el cumplimiento de los fines y principios establecidos en esta Ley, y en particular desarrollará las siguientes funciones:



- Asegurar la compatibilidad e interoperabilidad de los sistemas y aplicaciones empleados por las Administraciones Públicas.
- Preparar planes programas conjuntos de actuación para impulsar el desarrollo de la administración electrónica en España.
- Asegurar la cooperación entre las administraciones públicas para proporcionar al ciudadano información administrativa clara, actualizada e inequívoca.

Autor:

Alfonso García Magariños

Director Asesoría Jurídica Municipal Concello de A Coruña

**8. LEY DE MEDIDAS DE
IMPULSO DE LA SOCIEDAD DE
LA INFORMACIÓN. FACTURA
ELECTRÓNICA. LEY DE FIRMA
ELECTRÓNICA. LEY DE
SERVICIOS DE LA SOCIEDAD
DE LA INFORMACIÓN Y
COMERCIO ELECTRÓNICO.
ACCESIBILIDAD. DECRETO
3/2010, DE 8 DE ENERO, POR EL
QUE SE REGULA EL SISTEMA
DE FACTURACIÓN
ELECTRÓNICA DE LA XUNTA
DE GALICIA.**

Tema 8. Ley de medidas de impulso de la sociedad de la información. Factura electrónica. Ley de firma electrónica. Ley de servicios de la sociedad de la información y comercio electrónico. Accesibilidad. Decreto 3/2010 de 8 de enero por el que se regula el sistema de facturación electrónica de la Xunta de Galicia

INDICE

- 8.1 Ley de medidas de impulso de la sociedad de la información
 - 8.1.1 Introducción
 - 8.1.2 Análisis de la ley
- 8.2 Factura electrónica.
- 8.3 Ley de firma electrónica
 - 8.3.1 Introducción
 - 8.3.2 Análisis
 - 8.3.3 Efectos jurídicos y análisis
- 8.4 Ley de servicios de la sociedad de la información y comercio electrónico
 - 8.4.1 Introducción
 - 8.4.2 Ámbito aplicación
 - 8.4.3 Principios y requisitos de actuación
- 8.5 Accesibilidad
- 8.6 Decreto 3 /2010 de 8 de enero por el que se regula el sistema de facturación electrónica de la Xunta de Galicia
 - 8.6.1 Introducción
 - 8.6.2 Estructura

8.1 LEY DE MEDIDAS DE IMPULSO DE LA SOCIEDAD DE LA INFORMACION.

8.1 1 Introducción

En fecha 29 de diciembre de 2007 se publica en el BOE la ley de medidas de impulso de la sociedad de la información, ley 56/2007 de 28 de diciembre) que se enmarca en el conjunto de medidas que constituyen el Plan 2006-2010 para el desarrollo de la Sociedad de la Información y de convergencia con Europa y entre Comunidades Autónomas y Ciudades Autónomas, (Plan Avanza, aprobado por el Gobierno en noviembre de 2005, siendo este complementado por el PLAN AVANZA II 2011-2015 Aprobado por el Consejo de Ministros del 16 de julio de 2010.)

Principales aspectos de la ley:

- Introducción de Internet en los principales servicios de interés para los ciudadanos. La Ley obliga a las grandes empresas de determinados sectores (electricidad, agua y gas, telecomunicaciones) a facilitar un medio de interlocución telemática con sus clientes.
- Impulso a la factura electrónica. El Gobierno o, en su caso, las Comunidades Autónomas con competencias, elaborarán un plan para generalizar su uso.
 - Desarrollo del comercio electrónico en España:
 - Regulación mínima de las subastas electrónicas entre empresas
 - Reglas de valoración de la firma electrónica en juicio
 - Flexibilización de las obligaciones relativas a las comunicaciones comerciales y a los requisitos para la contratación por vía electrónica, en particular, para su adecuación a la telefonía móvil de datos.

- Mayor seguridad en Internet. La Ley obliga a los proveedores de acceso a Internet a informar a sus usuarios sobre medios técnicos que permitan la protección frente a los problemas de seguridad en Internet (virus, herramientas para el filtrado de contenidos no deseados, etc.).
- Internet más accesible para discapacitados y personas de edad avanzada.
- Refuerzo de la protección de los derechos de los usuarios en materia de telecomunicaciones. La Ley tipifica de manera expresa como infracción administrativa la vulneración por parte de los operadores de los derechos de los consumidores y usuarios en el ámbito de las telecomunicaciones.
- Extensión de la conectividad de la Banda Ancha para alcanzar la mayor conectividad posible antes del 31 de diciembre de 2008
- Disponibilidad de nombres de dominio “.es” con caracteres propios de las lenguas españolas, como la “ñ” o la “ç”.
- Mejora de la información disponible del sector TIC en España
- Canalizaciones para el despliegue de redes de comunicaciones electrónicas en carreteras e infraestructuras ferroviarias.
- Mayor rapidez en la constitución de sociedades limitadas.
- Impulso para la cesión y puesta a disposición de la sociedad de contenidos digitales de las Administraciones Públicas.
- El Ministerio de Industria planificará frecuencias para la gestión individual del servicio de televisión local de proximidad por parte de entidades sin ánimo de lucro.
- Regulación del juego. El Gobierno presentará un Proyecto de Ley para regular las actividades de juego y apuestas atendiendo a los grupos especialmente sensibles de usuarios, así como a los consumidores en general. También deberá establecer un sistema de tributación sobre los servicios de juegos y apuestas por sistemas interactivos basados en comunicaciones electrónicas, que sólo podrán ejercerse por aquellos operadores autorizados por la Administración competente.

En esta línea, la presente Ley, por una parte, introduce una serie de innovaciones normativas en materia de facturación electrónica y de refuerzo de los derechos de los usuarios y, por otra parte, acomete las modificaciones necesarias en el ordenamiento jurídico para promover el impulso de la sociedad de la información.

En este sentido, se introducen una serie de modificaciones tanto de la Ley 34/2002, de 11 de julio, de Servicios de la Sociedad de la Información y de Comercio Electrónico, como de la Ley 59/2003, de 19 de diciembre, de firma electrónica, que constituyen dos piezas angulares del marco jurídico en el que se desenvuelve el desarrollo de la sociedad de la información.

Dicha revisión del ordenamiento jurídico se completa con otras modificaciones menores de la Ley 32/2003, de 3 de noviembre, General de Telecomunicaciones, de la Ley 11/1998, de 24 de abril, General de Telecomunicaciones y de la Ley 7/1996, de 15 de enero, de ordenación del comercio minorista.

8.1.2 Análisis.

El capítulo I de la Ley introduce sendos preceptos dirigidos a impulsar el empleo de la factura electrónica y del uso de medios electrónicos en todas las fases de los procesos de contratación y a garantizar una interlocución electrónica de los usuarios y consumidores con las empresas que presten determinados servicios de especial relevancia económica.

En materia de facturación electrónica, el artículo 1 establece la obligatoriedad del uso de la factura electrónica en el marco de la contratación con el sector público estatal en los términos que se precisen en el proyecto de Ley de contratos del sector público, define el concepto legal de factura electrónica y, asimismo, prevé actuaciones de

complemento y profundización del uso de medios electrónicos en los procesos de contratación.

El artículo 2, por su parte, establece la obligación de las empresas de determinados sectores con especial incidencia en la actividad económica (entre otras, compañías dedicadas al suministro de electricidad, agua y gas, telecomunicaciones, entidades financieras, aseguradoras, grandes superficies, transportes, agencias de viaje) de facilitar un medio de interlocución telemática a los usuarios de sus servicios que cuenten con certificados reconocidos de firma electrónica.

Finalmente, el artículo 3 tiene por finalidad establecer una regulación mínima de las subastas electrónicas entre empresarios (B2B) a fin de establecer un marco jurídico que dote a esta técnica de compra de la necesaria transparencia y seguridad jurídica.

El capítulo II de la Ley engloba las modificaciones legislativas que se han estimado necesarias para promover el impulso de la sociedad de la información y de las comunicaciones electrónicas.

Dichas modificaciones afectan principalmente a la Ley 34/2002, de 11 de julio, de Servicios de la Sociedad de la Información y de Comercio Electrónico y a la Ley 59/2003, de 19 de diciembre, de firma electrónica, si bien se incluyen también modificaciones de menor entidad de la Ley 32/2003, de 3 de noviembre, General de Telecomunicaciones, se modifica la Ley 7/1996, de 15 de enero, de ordenación del comercio minorista para incluir un nuevo tipo de infracción que respalde lo dispuesto en el artículo 2 de la presente Ley, se introducen una serie de cambios en la Ley 11/1998, de 24 de abril, General de Telecomunicaciones y se introducen, asimismo, modificaciones en la Ley de Propiedad Intelectual.

El artículo 4 de la Ley incluye las diferentes modificaciones necesarias en el vigente texto de la Ley 34/ 2002, de 11 de julio, de Servicios de la Sociedad de la Información y de Comercio Electrónico (LSSI).

Estas modificaciones tienen como finalidad, en primer lugar, revisar o eliminar obligaciones excesivas o innecesarias y, en segundo lugar, flexibilizar las obligaciones referidas a las comunicaciones comerciales y a la contratación electrónicas a fin de, entre otras razones, adecuar su aplicación al uso de dispositivos móviles

El artículo 5 de la Ley contempla las modificaciones necesarias en el articulado de la Ley 59/2003, de 19 de diciembre, de firma electrónica.

Estas modificaciones tienen por objeto clarificar las reglas de valoración de la firma electrónica en juicio y flexibilizar la obligación de los prestadores de servicios de certificación de comprobar los datos inscritos en registros públicos a fin de eliminar cargas excesivas.

El primer aspecto que se revisa del artículo 3 de la Ley de firma electrónica es la definición de «documento electrónico» que se modifica para alinearla en mayor medida con los conceptos utilizados en otras normas españolas de carácter general y en los países de nuestro entorno.

En segundo lugar, se aclara la redacción del apartado 8 del artículo 3, especificando que lo que debe comprobarse, en caso de impugnarse en juicio una firma electrónica reconocida, es si concurren los elementos constitutivos de dicho tipo de firma electrónica, es decir, que se trata de una firma electrónica avanzada basada en un certificado reconocido, que cumple todos los requisitos y condiciones establecidos en esta Ley para este tipo de certificados electrónicos, y que la firma se ha generado mediante un dispositivo seguro de creación de firma electrónica.

El artículo 6 incluye un nuevo tipo de infracción en el artículo 64 de la Ley 7/1996, de 15 de enero, de ordenación del comercio minorista, a fin de respaldar la nueva obligación de disponer de un medio de interlocución electrónica para la prestación de servicios al público de especial trascendencia económica establecido en el artículo 2 de la presente Ley.

El artículo 7 de la Ley, introduce una serie de modificaciones en la Ley 32/2003, de 3 de noviembre, General de Telecomunicaciones.

Con el fin de reforzar los derechos de los usuarios frente a los proveedores de redes y servicios de comunicaciones electrónicas, se modifican los artículos 53 y 54 de la Ley General de Telecomunicaciones, mediante la tipificación como infracción administrativa del incumplimiento por parte de los operadores de los derechos de los consumidores y usuarios en el ámbito de las telecomunicaciones.

Asimismo, se reestablece la exención de la antigua tasa por reserva de uso especial del espectro, a radioaficionados y usuarios de la Banda Ciudadana CB-27 que figuraba en la Ley 11/1998, de 24 de abril, General de Telecomunicaciones, para aquellos usuarios que a la fecha de devengo hubieran cumplido los 65 años de edad.

El artículo 8 establece un nuevo régimen aplicable a las tarifas por las tareas de asignación, renovación y otras operaciones registrales realizadas por la entidad pública empresarial Red.es en ejercicio de su función de Autoridad de Asignación de los nombres de dominio de Internet bajo el código de país correspondiente a España, que pasarán a tener la consideración de precio público. Con ello, se permite a la entidad pública empresarial Red.es comercializar los nombres de dominio «.es» en las mismas condiciones en las que se comercializan el resto de nombres de dominio genéricos y territoriales.

8.2.- FACTURA ELECTRÓNICA

Con carácter general se puede definir la factura como un documento que refleja la entrega de un producto o la provisión de un servicio, junto a la fecha de devengo, además de indicar la cantidad a pagar como contraprestación.

En la factura se encuentran los datos del expedidor y del destinatario, el detalle de los productos y servicios suministrados, los precios unitarios, los precios totales, los descuentos y los impuestos.

La facturación electrónica consiste en la transmisión de las facturas o documentos análogos entre emisor y receptor por medios electrónicos (ficheros informáticos) y telemáticos (de un ordenador a otro), firmados digitalmente con certificados reconocidos (o cualificados), con la misma validez legal que las facturas emitidas en papel.

Si buscamos una definición específica, podemos recurrir al artículo 1 de la Ley 56/2007: “La factura electrónica es un documento electrónico que cumple con los requisitos legal y reglamentariamente exigibles a las facturas y que, además, garantiza la autenticidad de su origen y la integridad de su contenido”.

Aunque existen varios mecanismos para garantizar la autenticidad del origen, la integridad del contenido y la legibilidad de una factura, ya sea en papel o en formato electrónico, desde el momento de su expedición hasta el final del período de conservación de la factura, en el caso de la factura electrónica, el uso de la firma electrónica es el más generalizado en España.

En este sentido, en el texto consensuado de la futura modificación de la Directiva 112/2006, se recoge, en lo que se refiere a su artículo 233:

“1. Se garantizará la autenticidad del origen, la integridad del contenido y la legibilidad de una factura, ya sea en papel o en formato electrónico, desde el momento de su expedición hasta el final del período de conservación de la factura. Cada sujeto pasivo determinará el modo de garantizar la autenticidad del origen, la integridad del contenido y la legibilidad de las facturas. Podrá realizarse mediante controles de gestión que creen un vínculo fiable de auditoría entre la factura y la entrega de bienes o la prestación de servicios.

Se entenderá por “autenticidad del origen”, la garantía de la identidad del proveedor de bienes o prestador de servicios o del emisor de la factura.

Por “integridad del contenido” se entenderá que el contenido requerido con arreglo a lo dispuesto en la presente Directiva no ha sido modificado.

2. Además de los tipos de control de la gestión contemplados por el segundo párrafo del apartado 1, otros ejemplos de tecnologías que garantizan la autenticidad del origen y la integridad del contenido de una factura electrónica son:

- La firma electrónica avanzada en el sentido del punto 2 del artículo 2 de la Directiva 1999/93/CE del Parlamento Europeo y del Consejo, de 13 de diciembre de 1999, por la que se establece un marco comunitario para la firma electrónica, basada en un certificado reconocido y creada mediante un dispositivo seguro de creación de firma, en el sentido de los puntos 6 y 10 de la Directiva 1999/93/CE.*

- El intercambio electrónico de datos (IED), tal como se define en el artículo 2 de la Recomendación 1994/820/CE de la Comisión, de 19 de octubre de 1994, relativa a los aspectos jurídicos del intercambio electrónico de datos, si el acuerdo relativo al intercambio contempla el uso de procedimientos que garanticen la autenticidad del origen y la integridad de los datos.”*

Esto significa que tras el período de transposición de la Directiva (1 de enero de 2013), la legislación española reflejará la posibilidad de que puedan enviarse facturas electrónicas entre empresas sin ningún requisito formal, si bien probablemente se mantengan los mismos requisitos que existen en la actualidad cuando el destinatario sea una administración pública.

En España, la adopción de la firma electrónica como mecanismo generalizado para garantizar la autenticidad e integridad de las facturas electrónicas se ha visto favorecido por la extensión del DNI electrónico y la amplia disponibilidad de certificados electrónicos de múltiples prestadores deservicios de certificación, así como por la disponibilidad de software gratuito que permite la generación y firma electrónica de las facturas electrónicas que se envían, así como su verificación en el caso de la recepción de facturas.

El proceso de facturación es un proceso importante para cualquier empresa, y culmina el proceso de compra y venta. Aunque tradicionalmente la relación entre empresas se ha basado en el intercambio de documentos en papel, esto implica el empleo de grandes cantidades de recursos y la realización de muchas tareas de forma manual. En un contexto de universalización de Internet, cada vez más las empresas se plantean la optimización de sus procesos para ganar eficiencia y ahorrar costes.

Y por ello se ha avanzado en la adopción de la facturación electrónica, que en España está regulada en el Reglamento de facturación publicado en Real Decreto 1496/2003 y modificado por el Real Decreto 87/2005.

Las denominaciones factura electrónica, factura telemática y factura digital son equivalentes, si bien la denominación generalmente utilizada en la normativa es remisión electrónica o remisión por medios electrónicos de

factura. Frecuentemente se distingue con la denominación factura digital a la modalidad de factura electrónica que utiliza la firma digital para garantizar la autenticidad e integridad de la factura.

Las facturas electrónicas se pueden emitir en diferentes formatos (EDIFACT, XML, PDF, html, doc, xls, gif, jpeg o txt, entre otros) siempre que se respete el contenido legal exigible a cualquier factura y que se cumplan los requisitos de autenticidad e integridad, por ejemplo con la incorporación de la firma electrónica reconocida (qualified Electronic signature, en inglés).

Sin embargo, tras la publicación de la Orden PRE/2971/2007, en se definió el uso obligatorio del formato XML facturae, cuando el destinatario sea una administración de la AGE (Administración General del Estado) y sus organismos públicos.

8.3. LEY DE FIRMA ELECTRÓNICA.

8.3.1 Introducción

Sin olvidar las referencias que sobre el tema de utilización de medios electrónicos establecía la ley 30/92 de 20 de noviembre (LRJPAC) es el Real Decreto-ley 14/1999, de 17 de septiembre, sobre firma electrónica, la norma pionera a la hora de fomentar la rápida incorporación de las nuevas tecnologías de seguridad de las comunicaciones electrónicas en la actividad de las empresas, los ciudadanos y las Administraciones públicas, actualmente le ley 59/2003 de firma electrónica, cuya ultima modificación tuvo lugar por la ley 56/2007 de medidas de impulso de la sociedad de la información

8.3.2 Estructura y análisis.

Desde el punto de vista de su estructura, la ley 59/2003 de firma electrónica consta de 36 artículos agrupados en seis títulos, 11 disposiciones adicionales, dos disposiciones transitorias, una disposición derogatoria y tres disposiciones finales.

El título I contiene los principios generales que delimitan los ámbitos subjetivo y objetivo de aplicación de la ley, los efectos de la firma electrónica y el régimen de empleo ante las Administraciones públicas y de acceso a la actividad de prestación de servicios de certificación.

El régimen aplicable a los certificados electrónicos se contiene en el título II, que dedica su primer capítulo a determinar quiénes pueden ser sus titulares y a regular las vicisitudes que afectan a su vigencia. El capítulo II regula los certificados reconocidos y el tercero el documento nacional de identidad electrónico.

El título III regula la actividad de prestación de servicios de certificación estableciendo las obligaciones a que están sujetos los prestadores -distinguiendo con nitidez las que solamente afectan a los que expiden certificados reconocidos-, y el régimen de responsabilidad aplicable.

El título IV establece los requisitos que deben reunir los dispositivos de verificación y creación de firma electrónica y el procedimiento que ha de seguirse para obtener sellos de calidad en la actividad de prestación de servicios de certificación.

Los títulos V y VI dedican su contenido, respectivamente, a fijar los regímenes de supervisión y sanción de los prestadores de servicios de certificación.

Por último, cierran el texto las disposiciones adicionales -que aluden a los regímenes especiales que resultan de aplicación preferente-, las disposiciones transitorias -que incorporan seguridad jurídica a la actividad desplegada al amparo de la normativa anterior-, la disposición derogatoria y las disposiciones finales relativas al fundamento constitucional, la habilitación para el desarrollo reglamentario y la entrada en vigor.

-
Supone la incorporación al ordenamiento interno de la regulación contenida en la Directiva 1999/93/ CE, de 13 de diciembre de 1999, del Parlamento Europeo y del Consejo, esta Ley parece tener presente en la elaboración de su contenido la Ley Modelo para las firmas electrónicas de la Comisión de las Naciones Unidas para el Derecho Mercantil Internacional (CNUDMI/ UNCITRAL), aprobada, junto a su Guía, el 5 de julio de 2001.

Tiene como principal finalidad reforzar el marco jurídico existente, incorporando a su texto «algunas novedades respecto del Real Decreto 14/1999, que contribuirán a dinamizar el mercado de la prestación de servicios de certificación, confiriendo seguridad a las comunicaciones a través de Internet, y configurando la firma electrónica como instrumento capaz de generar confianza en las transacciones telemáticas, además de agilizar el comercio electrónico. Se permitirá, en consecuencia, una comprobación de la procedencia y de la integridad de los mensajes intercambiados a través de redes de telecomunicaciones, ofreciendo las bases para evitar el repudio, si se adoptan las medidas oportunas basándose en fechas electrónicas»

Constituye su objeto, conforme dispone el art. 1, tanto la regulación de la firma electrónica, como elemento de seguridad de las comunicaciones en sus diversos aspectos, y su eficacia jurídica, como la prestación de servicios de certificación en sus diversos aspectos (objetivo: certificados, y subjetivo: prestadores de servicio de certificación)

El apartado 1 del art. 3 de la LFE define de forma general la firma electrónica como «el conjunto de datos en forma electrónica, consignados junto a otros o asociados con ellos, que pueden ser utilizados como medio de identificación del firmante».

Se trata de una definición amplia que puede englobar a todo conjunto de firmas electrónicas, desde aquellas más complejas, como la firma digital basada en sistemas biométricos como el iris, la propia palma de la mano, la huella dactilar, etc. hasta la más simples, como un nombre u otro elemento identificativos (por ejemplo, la firma manual digitalizada, o un password o contraseña), incluido al final del mensaje electrónico, o la existencia de una pregunta-respuesta, y un pin de acceso, lo que se denomina tecnología de secreto compartido, de tan escasa seguridad que plantean la cuestión de su valor probatorio a efectos de autenticación o identificación del autor

Asimismo, de este concepto amplio y tecnológicamente indefinido de firma que nos ofrece el citado precepto podemos resaltar las siguientes características de la firma electrónica:

- La firma electrónica es un conjunto de datos y no un símbolo, sello o grafía electrónica que sirve para identificar al firmante de un mensaje y para acreditar la identificación del mismo, como la integridad del contenido del mensaje.
- Se trata de una técnica para identificar al firmante de un documento electrónico.
- Los datos de firma electrónica puede forma parte del documento o ir asociados funcionalmente con ellos o, lo que es lo mismo, pueden aparecer como un conjunto

independiente. El modo concreto en que en cada momento se manifieste la firma electrónica dependerá del sistema técnico que se elija y de las aplicaciones prácticas que ofrezca cada modalidad

Define la ley que se considera documento electrónico, este es la información de cualquier naturaleza en forma electrónica, archivada en un soporte electrónico según un formato determinado y susceptible de identificación y tratamiento diferenciado.

Para que un documento electrónico tenga la naturaleza de documento público o de documento administrativo deberá cumplirse, o bien, estar firmados electrónicamente por funcionarios que tengan legalmente atribuida la facultad de dar fe pública, judicial, notarial o administrativa, siempre que actúen en el ámbito de sus competencias con los requisitos exigidos por la ley en cada caso, o bien tratarse de documento expedidos y firmados electrónicamente por funcionarios o empleados públicos en el ejercicio de sus funciones públicas, conforme a su legislación específica.

Al lado de la firma electrónica se encuentra la firma electrónica avanzada, que según la ley, artículo 3.2 “«La firma electrónica avanzada es la firma electrónica que permite identificar al firmante y detectar cualquier cambio ulterior de los datos firmados, que está vinculada al firmante de manera única y a los datos a que se refiere y que ha sido creada por medios que el firmante puede mantener bajo su exclusivo control»

La ley de firma electrónica frente a la regulación contenido tanto en el RDL 14/99 como en la Directiva, introduce un tercer tipo de firma, de mayor calidad y seguridad, como es la firma electrónica reconocida, definida en el art. 3.3 como «la firma electrónica avanzada basada en un

certificado reconocido y generada mediante un dispositivo seguro de creación de firma».

Supone, como señala la Exposición de Motivos de la Ley, «la creación de un concepto nuevo demandado por el sector, sin que ello implique modificación alguna de los requisitos sustantivos que tanto la Directiva 1999/93/CE como el propio Real Decreto Ley 14/1999 venían exigiendo.

El Art. 24 de la LFE, bajo el título «Dispositivo de firma electrónica», define los datos de creación de firma como «los datos únicos, como códigos o claves criptográficas privadas, que el firmante utiliza para crear la firma electrónica»

Como elemento característico de los mismos viene a establecerse el que éstos deben ser únicos

Por su parte, el Art. 25 de la LFE, bajo el título «Dispositivos de verificación de firma electrónica», define los «datos de verificación de firma» como «los datos, códigos o claves criptográficas públicas, que se utilizan para verificar la firma electrónica».

Por tanto, bajo el Título «Dispositivos de firma electrónica» se regula como nociones previas tanto para la aplicación del dispositivo de creación como para el de verificación los datos de creación y verificación de firma, respectivamente, que desde un punto de vista técnico constituyen además elementos que posibilitan la creación de una firma o su verificación

8.3.3 Efectos jurídicos de la firma electrónica

A la validez y eficacia de la firma electrónica dedica la LFE los apartados 4, 8, 9 y 10 del Art. 3, que coincide sustancialmente con lo dispuesto en el Art. 5 de la Directiva comunitaria, y en los que se equipara la firma electrónica reconocida a la firma manuscrita, se determina las

consecuencias de la impugnación de la autenticidad de la firma electrónica reconocida por la otra parte no firmante, se reconoce valor jurídico a la autonomía de la voluntad de las partes para dotar de eficacia a la firma electrónica y se especifica la admisibilidad de los datos firmados electrónicamente como prueba documental en juicio;

El Art 3.4 de la Ley establece la regla del equivalente funcional entre la firma electrónica reconocida y la firma manuscrita, al disponer que «la firma electrónica reconocida tendrá respecto de los datos consignados en forma electrónica, el mismo valor que la firma manuscrita en relación con los consignados en papel».

En consecuencia, sobre lo expuesto, para la plena operatividad de la regla de la equivalencia funcional de la firma electrónica reconocida con la firma manuscrita, que dispone el art. 3.4 de la LFE, en una interpretación conjunta con el art. 3.3 de esta misma Ley, es necesario el cumplimiento de los siguientes requisitos:

1.º Debe tratarse de una firma electrónica avanzada (art. 3.2 de la LFE).

2.º Dicha firma electrónica avanzada ha de estar basada en un certificado reconocido, es decir, aquel que cumple los requisitos de los arts. 11, 12 y 13 de la LFE, y que haya sido expedido por un prestador de servicios de certificación que cumpla con los requisitos previstos en el Art. 20 de la LFE.

3.º Dicha firma electrónica avanzada, además, debe haber sido producida por un dispositivo seguro de creación de firma que cumpla con los requisitos del apartado 3 del Art. 24 de la LFE

Regula también la ley la figura del DNI electrónico, este es el documento nacional de identidad que acredita electrónicamente la identidad personal de su titular y permite la firma electrónica de documentos, se impone la obligación de que todas las personas físicas o jurídicas, públicas o privadas, reconocerán la eficacia del documento

nacional de identidad electrónico para acreditar la identidad y los demás datos personales del titular que consten en el mismo, y para acreditar la identidad del firmante y la integridad de los documentos firmados con los dispositivos de firma electrónica en él incluidos.

LA ley regula la figura de los prestadores de servicios de certificación, siendo estos “la persona física o jurídica que expide certificados electrónicos o presta otros servicios en relación con la firma electrónica “

Para la expedición de certificados electrónicos al público, los prestadores de servicios de certificación únicamente podrán recabar datos personales directamente de los firmantes o previo consentimiento expreso de éstos, debiendo cumplir por tanto lo dispuesto en la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal y en sus normas de desarrollo.

Los prestadores de servicios de certificación que expidan certificados electrónicos deberán cumplir las siguientes obligaciones:

- No almacenar ni copiar los datos de creación de firma de la persona a la que hayan prestado sus servicios.
- Proporcionar al solicitante antes de la expedición del certificado la siguiente información mínima, que deberá transmitirse de forma gratuita, por escrito o por vía electrónica:
- Las obligaciones del firmante, la forma en que han de custodiarse los datos de creación de firma, el procedimiento que haya de seguirse para comunicar la pérdida o posible utilización indebida de dichos datos y determinados dispositivos de creación y de verificación de firma electrónica que sean

compatibles con los datos de firma y con el certificado expedido.

- Los mecanismos para garantizar la fiabilidad de la firma electrónica de un documento a lo largo del tiempo.
- El método utilizado por el prestador para comprobar la identidad del firmante u otros datos que figuren en el certificado.
- Las condiciones precisas de utilización del certificado, sus posibles límites de uso y la forma en que el prestador garantiza su responsabilidad patrimonial.
- Las certificaciones que haya obtenido, en su caso, el prestador de servicios de certificación y los procedimientos aplicables para la resolución extrajudicial de los conflictos que pudieran surgir por el ejercicio de su actividad.
- Las demás informaciones contenidas en la declaración de prácticas de certificación.
- La información citada anteriormente que sea relevante para terceros afectados por los certificados deberá estar disponible a instancia de éstos.
- Mantener un directorio actualizado de certificados en el que se indicarán los certificados expedidos y si están vigentes o si su vigencia ha sido suspendida o extinguida. La integridad del directorio se protegerá mediante la utilización de los mecanismos de seguridad adecuados.

- Garantizar la disponibilidad de un servicio de consulta sobre la vigencia de los certificados rápido y seguro

Regula la ley aspectos relacionados con la supervisión y control de la actividad de los prestadores de servicios, y así el Ministerio de Ciencia y Tecnología controlará el cumplimiento por los prestadores de servicios de certificación que expidan al público certificados electrónicos de las obligaciones establecidas en esta Ley y en sus disposiciones de desarrollo. Asimismo, supervisará el funcionamiento del sistema y de los organismos de certificación de dispositivos seguros de creación de firma electrónica.

El Ministerio de Ciencia y Tecnología realizará las actuaciones inspectoras que sean precisas para el ejercicio de su función de control, los funcionarios adscritos al Ministerio de Ciencia y Tecnología que realicen la inspección a que se refiere el apartado anterior tendrán la consideración de autoridad pública en el desempeño de sus cometidos.

Los prestadores de servicios de certificación, la entidad independiente de acreditación y los organismos de certificación tienen la obligación de facilitar al Ministerio de Ciencia y Tecnología toda la información y colaboración precisas para el ejercicio de sus funciones.

8.4.- LEY DE SERVICIOS DE SOCIEDAD DE INFORMACIÓN Y COMERCIO ELECTRÓNICO

8.4.1 Introducción.

La ley 34/2002 de 22 de julio tiene como objeto la incorporación al ordenamiento jurídico español de la Directiva 2000/31/CE, del Parlamento Europeo y del Consejo, de 8 de junio, relativa a determinados aspectos de los servicios de la sociedad de la información, en particular, el comercio electrónico en el mercado Interior (Directiva sobre el comercio electrónico). Asimismo, incorpora parcialmente la Directiva 98/27/CE, del Parlamento Europeo y del Consejo, de 19 de mayo, relativa a las acciones de cesación en materia de protección de los intereses de los consumidores, al regular, de conformidad con lo establecido en ella, una acción de cesación contra las conductas que contravengan lo dispuesto en esta Ley.

Lo que la Directiva 2000/31/CE denomina sociedad de la información viene determinado por la extraordinaria expansión de las redes de telecomunicaciones y, en especial, de Internet como vehículo de transmisión e intercambio de todo tipo de información. Su incorporación a la vida económica y social ofrece innumerables ventajas, como la mejora de la eficiencia empresarial, el incremento de las posibilidades de elección de los usuarios y la aparición de nuevas fuentes de empleo. Pero la implantación de Internet y las nuevas tecnologías tropieza con algunas incertidumbres jurídicas, que es preciso aclarar con el establecimiento de un marco jurídico adecuado, que genere en todos los actores intervinientes la confianza necesaria para el empleo de este nuevo medio.

Es objeto de la Ley la regulación del régimen jurídico de los servicios de la sociedad de la información y de la contratación por vía electrónica, en lo referente a las obligaciones de los prestadores de servicios incluidos los que actúen como intermediarios en la transmisión de contenidos por las redes de telecomunicaciones, las comunicaciones comerciales por vía electrónica, la información previa y posterior a la celebración de contratos electrónicos, las condiciones relativas a su validez y eficacia y el régimen sancionador aplicable a los prestadores de servicios de la sociedad de la información.

8.4.2 Ámbito aplicación

Se aplicará a los prestadores de servicios de la sociedad de la información establecidos en otro Estado miembro de la Unión Europea o del Espacio Económico Europeo cuando el destinatario de los servicios radique en España y los servicios afecten a las materias siguientes:

- a. Derechos de propiedad intelectual o industrial.
- b. Emisión de publicidad por instituciones de inversión colectiva.
- c. Actividad de seguro directo realizada en régimen de derecho de establecimiento o en régimen de libre prestación de servicios.
- d. Obligaciones nacidas de los contratos celebrados por personas físicas que tengan la condición de consumidores.
- e. Régimen de elección por las partes contratantes de la legislación aplicable a su contrato.
- f. Licitud de las comunicaciones comerciales por correo electrónico u otro medio de comunicación electrónica equivalente no solicitadas

La prestación de servicios de la sociedad de la información no estará sujeta a autorización previa

En caso de que un determinado servicio de la sociedad de la información atente o pueda atentar contra los principios que se expresan a continuación, los órganos competentes para su protección, en ejercicio de las funciones que tengan legalmente atribuidas, podrán adoptar las medidas necesarias para que se interrumpa su prestación o para retirar los datos que los vulneran.

8.4.3 Principios y requisitos de actuación

Los principios de aplicación son los siguientes:

- a. La salvaguarda del orden público, la investigación penal, la seguridad pública y la defensa nacional.
- b. La protección de la salud pública o de las personas físicas o jurídicas que tengan la condición de consumidores o usuarios, incluso cuando actúen como inversores.
- c. El respeto a la dignidad de la persona y al principio de no discriminación por motivos de raza, sexo, religión, opinión, nacionalidad, discapacidad o cualquier otra circunstancia personal o social, y
- d. La protección de la juventud y de la infancia.
- e. La salvaguarda de los derechos de propiedad intelectual

El prestador de servicios de la sociedad de la información estará obligado a disponer de los medios que permitan, tanto a los destinatarios del servicio como a los órganos competentes, acceder por medios electrónicos, de forma permanente, fácil, directa y gratuita, a la siguiente información:

- a. Su nombre o denominación social; su residencia o domicilio o, en su defecto, la dirección de uno de sus establecimientos permanentes en España; su dirección de correo electrónico y cualquier otro dato que permita establecer con él una comunicación directa y efectiva.
- b. Los datos de su inscripción en el Registro Mercantil en el que, en su caso, se encuentren inscritos o de aquel otro registro público en el que lo estuvieran para la adquisición de personalidad jurídica o a los solos efectos de publicidad.
- c. En el caso de que su actividad estuviese sujeta a un régimen de autorización administrativa previa, los datos relativos a dicha autorización y los identificativos del órgano competente encargado de su supervisión.

- d. Si ejerce una profesión regulada deberá indicar:
 - 1. Los datos del Colegio profesional al que, en su caso, pertenezca y número de colegiado.
 - 2. El título académico oficial o profesional con el que cuente.
 - 3. El Estado de la Unión Europea o del Espacio Económico Europeo en el que se expidió dicho título y, en su caso, la correspondiente homologación o reconocimiento.
 - 4. Las normas profesionales aplicables al ejercicio de su profesión y los medios a través de los cuales se puedan conocer, incluidos los electrónicos.
- e. El número de identificación fiscal que le corresponda.
- f. Cuando el servicio de la sociedad de la información haga referencia a precios, se facilitará información clara y exacta sobre el precio del producto o servicio, indicando si incluye o no los impuestos aplicables y, en su caso, sobre los gastos de envío o en su caso aquello que dispongan las normas de las Comunidades Autónomas con competencias en la materia.
- g. Los códigos de conducta a los que, en su caso, esté adherido y la manera de consultarlos electrónicamente

Los prestadores de servicios de la sociedad de la información estén sujetos a la responsabilidad civil, penal y administrativa establecida con carácter general en el ordenamiento jurídico, sin perjuicio de lo dispuesto en esta Ley

Los prestadores de servicios de la sociedad de la información que faciliten enlaces a otros contenidos o incluyan en los suyos directorios o instrumentos de búsqueda de contenidos no serán responsables por la información a la que dirijan a los destinatarios de sus servicios, siempre que:

- a. No tengan conocimiento efectivo de que la actividad o la información a la que remiten o recomiendan es ilícita o de que lesiona bienes o derechos de un tercero susceptibles de indemnización, o
- b. Si lo tienen, actúen con diligencia para suprimir o inutilizar el enlace correspondiente.

Las Administraciones públicas impulsarán, a través de la coordinación y el asesoramiento, la elaboración y aplicación de códigos de conducta voluntarios, por parte de las corporaciones, asociaciones u organizaciones comerciales, profesionales y de consumidores, en las materias reguladas en esta Ley. La Administración General del Estado fomentará, en especial, la elaboración de códigos de conducta de ámbito comunitario o internacional.

Los códigos de conducta podrán tratar, en particular, sobre los procedimientos para la detección y retirada de contenidos ilícitos y la protección de los destinatarios frente al envío por vía electrónica de comunicaciones comerciales no solicitadas, así como sobre los procedimientos extrajudiciales para la resolución de los conflictos que surjan por la prestación de los servicios de la sociedad de la información.

Los contratos celebrados por vía electrónica producirán todos los efectos previstos por el ordenamiento jurídico, cuando concurren el consentimiento y los demás requisitos necesarios para su validez

La prueba de la celebración de un contrato por vía electrónica y la de las obligaciones que tienen su origen en él se sujetará a las reglas generales del ordenamiento jurídico.

Cuando los contratos celebrados por vía electrónica estén firmados electrónicamente se estará a lo establecido en el artículo 3 de la Ley 59/2003, de 19 de diciembre, de firma electrónica

Los contratos celebrados por vía electrónica en los que intervenga como parte un consumidor se presumirán celebrados en el lugar en que éste tenga su residencia habitual

El prestador y el destinatario de servicios de la sociedad de la información podrán someter sus conflictos a los arbitrajes previstos en la legislación de arbitraje y de defensa de los consumidores y usuarios, y a los procedimientos de resolución extrajudicial de conflictos que se instauren por medio de códigos de conducta u otros instrumentos de autorregulación

8.5.-ACCESIBILIDAD.

La disposición adicional quinta de la ley de servicios de la sociedad de la información y del comercio electrónico (ley 34/2002 de 11 de julio) establece una norma relativa a accesibilidad para las personas con discapacidad y de edad avanzada a la información proporcionada por medios electrónicos y establece

“Las Administraciones públicas adoptarán las medidas necesarias para que la información disponible en sus respectivas páginas de Internet pueda ser accesible a personas con discapacidad y de edad avanzada, de acuerdo con los criterios de accesibilidad al contenido generalmente reconocidos, antes del 31 de diciembre de 2005.

A partir del 31 de diciembre de 2008, las páginas de Internet de las Administraciones Públicas satisfarán, como mínimo, el nivel medio de los criterios de accesibilidad al contenido generalmente reconocidos. Excepcionalmente, esta obligación no será aplicable cuando una funcionalidad o servicio no disponga de una solución tecnológica que permita su accesibilidad.

Las Administraciones Públicas exigirán que tanto las páginas de Internet cuyo diseño o mantenimiento financien total o parcialmente como las páginas de Internet de entidades y empresas que se encarguen de

gestionar servicios públicos apliquen los criterios de accesibilidad antes mencionados. En particular, será obligatorio lo expresado en este apartado para las páginas de Internet y sus contenidos de los Centros públicos educativos, de formación y universitarios, así como, de los Centros privados que obtengan financiación pública.

Las páginas de Internet de las Administraciones Públicas deberán ofrecer al usuario información sobre su nivel de accesibilidad y facilitar un sistema de contacto para que puedan transmitir las dificultades de acceso al contenido de las páginas de Internet o formular cualquier queja, consulta o sugerencia de mejora.

Igualmente, se promoverá la adopción de normas de accesibilidad por los prestadores de servicios y los fabricantes de equipos y software, para facilitar el acceso de las personas con discapacidad o de edad avanzada a los contenidos digitales.

Las Administraciones Públicas promoverán medidas de sensibilización, educación y formación sobre accesibilidad con objeto de promover que los titulares de otras páginas de Internet incorporen progresivamente los criterios de accesibilidad.

Los incumplimientos de las obligaciones de accesibilidad establecidas en esta Disposición adicional estarán sometidos al régimen de infracciones y sanciones vigente en materia de igualdad de oportunidades, no discriminación y accesibilidad universal de las personas con discapacidad.

Las páginas de Internet de las empresas que presten servicios al público en general de especial trascendencia económica, sometidas a la obligación establecida en el artículo 2 de la Ley 56/2007, de medidas de impulso de la sociedad de la información, deberán satisfacer a partir del 31 de diciembre de 2008, como mínimo, el nivel medio de los criterios de accesibilidad al contenido generalmente reconocidos. Excepcionalmente, esta obligación no será aplicable cuando una funcionalidad o servicio no disponga de una solución tecnológica que permita su accesibilidad.

El "Diseño Web Accesible" pretende establecer las técnicas y mecanismos para permitir que un sitio Web pueda ser utilizado por cualquier persona, independientemente de su discapacidad.

En diciembre de 2007 se aprobó la Ley 56/2007, de Medidas de Impulso de la Sociedad de la Información (BOE 29-12-2008). Por un lado, esta ley indica claramente que la accesibilidad de las páginas web de la administración pública está sujeta al régimen de infracciones y sanciones (Ley 49/2007). Por otro lado, la obligación de hacer sitios web accesibles se amplía al sector privado, en concreto a las empresas que presten servicios al público en general de especial trascendencia económica.

En diciembre de 2007 se aprobó la Ley 49/2007, por la que se establece el régimen de infracciones y sanciones en materia de igualdad de oportunidades, no discriminación y accesibilidad universal de las personas con discapacidad (BOE 27-12-2007). En esta ley se definen sanciones que pueden llegar hasta 1.000.000 de euros.

En noviembre de 2007 se aprobó el Real Decreto 1494/2007 por el que se aprueba el Reglamento sobre las condiciones básicas para el acceso de las personas con discapacidad a las tecnologías, productos y servicios relacionados con la sociedad de la información y medios de comunicación social (BOE 21-11-2007). Este Reglamento obliga a las administraciones públicas a que sus páginas web sean accesibles de acuerdo con el nivel 2 de la norma española UNE 139803:2004 antes del 2009.

La Ley IONDAU (Ley 51/2003, de 2 de diciembre, de Igualdad de Oportunidades, No Discriminación y Accesibilidad Universal de las Personas con Discapacidad. BOE 3-12-2003), fija varias fases: 1º a primeros de 2006 el Gobierno deberá haber establecido los criterios básicos de accesibilidad para las Tecnologías de la Sociedad de la Información; 2º en 2010 todos los nuevos productos y servicios de la Sociedad de la Información deberán ser

accesibles; 3º en 2014 todos los productos y servicios de la Sociedad de la Información deberán ser accesibles.

La Ley SSICE (Ley 34/2002, de 11 de julio, de Servicios de la Sociedad de la Información y de Comercio Electrónico. BOE 12-7-2002), en su disposición adicional 5ª (que hace referencia a la accesibilidad para las personas con discapacidad y de edad avanzada a la información proporcionada por medios electrónicos), obligaba a las Administraciones Públicas a tener sus Webs accesibles para todos antes de 2006.

En el ámbito Europeo existen numerosas normas e iniciativas en este sentido (como las iniciativas eEurope (an Information Society for All) 2002 y 2005 y la estrategia i2010), puesto que se habla de un 20% de la población europea afectada por algún tipo de discapacidad.

8.6.- DECRETO 3/2010 DE 8 DE ENERO POR EL QUE SE REGULA EL SISTEMA DE FACTURACIÓN ELECTRÓNICA DE LA XUNTA DE GALICIA

8.6.1 Introducción

La implantación de los medios electrónicos en el ámbito de la facturación y la contratación pública se enmarca en las políticas corporativas comunes del Gobierno gallego para el desarrollo de la administración electrónica y se integrará armónica y complementariamente con el resto de las aplicaciones comunes para toda la Xunta de Galicia.

El Decreto regula, por un lado, las líneas generales de empleo de los medios electrónicos, informáticos y telemáticos en los procedimientos de contratación y establece las condiciones de utilización de los citados medios en el marco del desarrollo de la administración electrónica de la Xunta de Galicia. Así mismo, configura las bases de un sistema que se asienta sobre varios ejes que se complementan estructurando todas las relaciones telemáticas entre los actores que intervienen en los procesos.

Así, en términos de servicios a los licitadores, ordena y estructura nuevos canales de información y participación del empresariado en los procesos de contratación creando la Plataforma de Contratos Públicos de Galicia y un Portal de Contratación Pública de la Comunidad Autónoma que potenciará los servicios en línea existentes e incorporará prestaciones relacionadas con la licitación electrónica. Por otro lado, en términos de servicios entre administraciones se prevén mecanismos de interoperatividad que, en primer lugar, refuerzan la accesibilidad a las plataformas y sistemas y aplicaciones existentes o futuras y, en segundo lugar, facilitan la cooperación y colaboración intra e interadministrativas a los efectos de tráfico de información.

8.6.2 Estructura

Respecto a la estructura, el Decreto consta de 18 artículos, agrupados en 5 capítulos.

El capítulo I regula el objeto del Decreto y su ámbito de aplicación.

El capítulo II regula la Plataforma de Contratos Públicos de Galicia, creada al amparo de lo dispuesto en el artículo 309.5 de la Ley 30/2007, de 30 de octubre, como servicio de información de las licitaciones del sector público gallego a través de internet.

El capítulo III regula el Sistema de Licitación Electrónica que permitirá la presentación de ofertas y proposiciones por vía telemática.

El capítulo IV regula determinados sistemas de tramitación y gestión electrónica de importante incidencia en la contratación y la facturación electrónica.

Finalmente, en el capítulo V se crea un Portal de Contratación Pública de la Comunidad Autónoma como punto central de acceso y entrada para los interesados a todas las aplicaciones y servicios que en materia de

contratación pública y por vía electrónica, se puedan realizar a través de internet.

El Decreto modifica también, en la disposición final, el Decreto 262/2001, de 20 septiembre, por el que se refunde la normativa reguladora del Registro General de Contratistas de la Comunidad Autónoma de Galicia al introducir la tramitación por medios electrónicos, informáticos y telemáticos (EIT) de los procesos de alta, modificación y baja del registro y un sistema de notificaciones electrónicas con las empresas registradas

Autor:

Alfonso García Magariños

Director Asesoría Jurídica Municipal Concello de A Coruña

9. NORMATIVA EN EL ÁMBITO DE LA PROPIEDAD INTELECTUAL. LA PROTECCIÓN JURÍDICA DE LOS PROGRAMAS DE ORDENADOR. TIPOS DE LICENCIAS. SOFTWARE DE FUENTES ABIERTAS (FLOSS).

Tema 9.- Normativa en el ámbito de la propiedad intelectual. La protección jurídica de los programas de ordenador. Tipos de licencias: Software de fuentes abiertas (FLOSS)

INDICE

9.1 Normativa en el ámbito de la propiedad intelectual.

9.1.1 Estatal

9.1.2 Comunitaria

9.1.3 Internacional

9.2 Protección jurídica programas ordenador

9.2.1 Introducción

9.2.2 Normativa Estatal

9.3 Tipos de licencias

9.4 Software de fuentes abiertas FLOSS

9.1- NORMATIVA EN EL ÁMBITO DE LA PROPIEDAD INTELECTUAL.

Según la Organización Mundial de la Propiedad Intelectual, la propiedad intelectual (P.I.) tiene que ver con las creaciones de la mente: las invenciones, las obras literarias y artísticas, los símbolos, los nombres, las imágenes y los dibujos y modelos utilizados en el comercio.

La propiedad intelectual se divide en dos categorías: la propiedad industrial, que incluye las invenciones, patentes, marcas, dibujos y modelos industriales e indicaciones geográficas de procedencia; y el derecho de autor, que abarca las obras literarias y artísticas, tales como las novelas, los poemas y las obras de teatro, las películas, las obras musicales, las obras de arte, tales como los dibujos, pinturas, fotografías y esculturas, y los diseños arquitectónicos. Los derechos relacionados con el derecho de autor son los derechos de los artistas intérpretes y ejecutantes sobre sus interpretaciones y ejecuciones, los derechos de los productores de fonogramas sobre sus grabaciones y los derechos de los organismos de radiodifusión sobre sus programas de radio y de televisión

Por lo que respecta a los derechos que conforman la propiedad intelectual se distinguen los derechos morales y los derechos patrimoniales:

Derechos morales:

Frente a los sistemas de corte anglosajón, la legislación española es claramente defensora de los derechos morales, reconocidos para los autores y para los artistas intérpretes o ejecutantes. Estos derechos son

irrenunciables e inalienables, acompañan al autor o al artista intérprete o ejecutante durante toda su vida y a sus herederos o causahabientes al fallecimiento de aquellos. Entre ellos destaca el derecho al reconocimiento de la condición de autor de la obra o del reconocimiento del nombre del artista sobre sus interpretaciones o ejecuciones, y el de exigir el respeto a la integridad de la obra o actuación y la no alteración de las mismas.

Derechos de carácter patrimonial:

Hay que distinguir entre:

Derechos relacionados con la explotación de la obra o prestación protegida, que a su vez se subdividen en derechos exclusivos y en derechos de remuneración:

1.-Los derechos exclusivos son aquellos que permiten a su titular autorizar o prohibir los actos de explotación de su obra o prestación protegida por el usuario, y a exigir de este una retribución a cambio de la autorización que le conceda.

2.-Los derechos de remuneración, a diferencia de los derechos exclusivos, no facultan a su titular a autorizar o prohibir los actos de explotación de su obra o prestación protegida por el usuario, aunque si obligan a este al pago de una cantidad dineraria por los actos de explotación que realice, cantidad esta que es determinada, bien por la ley o en su defecto por las tarifas generales de las entidades de gestión.

3.-Derechos compensatorios, como el derecho por copia privada que compensa los derechos de propiedad intelectual dejados de percibir por razón de las reproducciones de las obras o prestaciones protegidas para uso exclusivamente privado del copista

9.1.1 Normativa Estatal

La propiedad intelectual es el conjunto de derechos que corresponden a los autores y a otros titulares (artistas, productores, organismos de radiodifusión...) respecto de las obras y prestaciones fruto de su creación.

La propiedad intelectual, tal y como establece el Código Civil en sus artículos 428 y 429, forma parte de las llamadas propiedades especiales, y viene a constituir una forma especial de ejercer el derecho de propiedad sobre determinados objetos jurídicos que, por su cualidad, especializan el dominio.

Como propiedad especial, el Código Civil remite su regulación a una ley especial, y declara la aplicación supletoria de las reglas generales establecidas en el mismo sobre la propiedad para lo no específicamente previsto en dicha ley especial. Esta ley es la Ley de Propiedad Intelectual (LPI), cuyo Texto Refundido fue aprobado por el Real Decreto Legislativo 1/1996, de 12 de abril.

El citado Texto fue objeto de sucesivas modificaciones entre las que debemos destacar la operada por la ley 5/1998, de 6 de marzo, y la ley 23/2006 de 7 de julio, (responde esta a la necesidad de incorporar al derecho español una de las últimas directivas aprobadas en materia de propiedad intelectual, la Directiva 2001/29/CE del Parlamento Europeo y del Consejo, de 22 de mayo de 2001, relativa a la armonización de determinados aspectos de los derechos de autor y derechos afines a los derechos de autor en la sociedad de la información, con la que la Unión Europea, a su vez, ha querido cumplir los Tratados de la Organización Mundial de la Propiedad Intelectual (OMPI) de 1996 sobre Derecho de Autor y sobre Interpretación o Ejecución y Fonogramas)

Cabe también destacar la ley 19/2006, de 5 de junio, por la que se amplían los medios de tutela de los derechos de propiedad intelectual e industrial y se establecen normas procesales para facilitar la aplicación de diversos reglamentos comunitarios.

9.1.2 Normativa comunitaria:

1.-Directiva 92/100/CEE, de 19 de noviembre de 1992, sobre derechos de alquiler y préstamo y otros derechos afines a los derechos de autor en el ámbito de la propiedad intelectual. Esta Directiva, entre otros aspectos, reconoce el derecho de autorizar o prohibir el alquiler y préstamo de originales y copias de obras protegidas.

2.-Directiva 93/98/CEE, de 29 de octubre de 1993, relativa a la armonización del plazo de protección del derecho de autor y de determinados derechos afines. En esta Directiva se armoniza el plazo de protección del derecho de autor, fijándolo en un período de setenta años tras la muerte del autor o desde el momento de la primera difusión lícita entre el público, y por lo que se refiere a los derechos afines, en cincuenta años desde que se produce el hecho generador.

3.-Directiva 96/9/CE, de 11 de marzo de 1996, sobre la protección jurídica de las bases de datos. Reconoce un derecho de autor al creador de la estructura de la base de datos, y un derecho "sui generis" al fabricante de la misma, entendiendo por tal la persona física o jurídica que ha realizado una inversión sustancial para la fabricación de las bases de datos.

4.-Directiva 2001/29/CE, de 22 de mayo de 2001, relativa a la armonización de determinados aspectos de los derechos de autor y derechos afines en la sociedad de la información, adecua el sistema de derechos de autor y conexos al entorno digital, asumiendo al mismo tiempo

las obligaciones contraídas por la Unión Europea y sus Estados Miembros en el marco de los Tratados Digitales OMPI (WCT y WPPT).

5.-Directiva 2000/31/CE del Parlamento Europeo y del Consejo, de 8 de junio de 2000 (DOCE de 17 de julio) relativa a determinados aspectos jurídicos de los servicios de la sociedad de la información, en particular el comercio electrónico (Directiva sobre el comercio electrónico). En esa Directiva se regula, entre otros aspectos y por lo que interesa a la materia de propiedad intelectual, la responsabilidad de los prestadores de servicios intermediarios (artículos 12 a 15 de la Directiva).

9.1.3 Normativa internacional:

1.-El Convenio de Berna, que protege las obras literarias y artísticas, datando su acta originaria de 1886, siendo España socio fundador del mismo. Entre los principios informadores del Convenio se encuentran el de trato nacional (o asimilación del extranjero al nacional), el de protección automática, el de independencia de la protección, y el de protección mínima (para lograr un conjunto dispositivo uniformemente aplicable).

2.-Tratado OMPI sobre Derecho de Autor (Tratado WCT, 1996): como resultado de la Conferencia Diplomática de la OMPI sobre ciertas cuestiones de derechos de autor y de derechos conexos –celebrada en Ginebra en diciembre de 1996-, se adoptó éste tratado, orientado a ofrecer la necesaria respuesta legislativa a los problemas planteados por la tecnología digital, y particularmente por Internet.

3.-ISO 12083. Marcaje de documentos electrónicos

9.2.- PROTECCIÓN JURÍDICA DE PROGRAMAS DE ORDENADOR.

9.2.1 Introducción

Debemos partir, dada su importancia de la Directiva del Consejo de 14 de mayo de 1991 sobre la protección jurídica de programas de ordenador, allí nos indica que a efectos de la presente Directiva, el término «programa de ordenador» incluye programas en cualquier forma, incluso los que están incorporados en el «hardware»; que este término designa también el trabajo preparatorio de concepción que conduce al desarrollo de un programa de ordenador, siempre que la naturaleza del trabajo preparatorio sea tal que más tarde pueda originar un programa de ordenador

Dicha directiva fue objeto de transposición al ordenamiento español por la ley 16/1993 de 23 de diciembre, siendo esta a su vez derogada por el Real Decreto Legislativo 1/1996, de 12 de abril, por el que se aprueba el Texto Refundido de la Ley de Propiedad Intelectual, regularizando, aclarando y armonizando las disposiciones legales vigentes sobre la materia.

La Directiva establece que los Estados miembros protegerán mediante derechos de autor los programas de ordenador como obras literarias tal como se definen en el Convenio de Berna para la protección de las obras literarias y artísticas.

A los fines de la presente Directiva, la expresión «programas de ordenador» comprenderá su documentación preparatoria

Respecto a la titularidad de los derechos; se considerará autor del programa de ordenador a la persona física o grupo de personas físicas que lo hayan creado o, cuando la legislación de los Estados miembros lo permita, a la persona jurídica que sea considerada titular del derecho por dicha legislación. Cuando la legislación de un Estado miembro reconozca las obras colectivas, la persona física o jurídica que según dicha legislación haya creado el programa, será considerada su autor.

Cuando un programa de ordenador se cree conjuntamente por varias personas físicas, los derechos exclusivos serán propiedad común.

Cuando un trabajador asalariado cree un programa de ordenador en el ejercicio de las funciones que le han sido confiadas, o siguiendo las instrucciones de su empresario, la titularidad de los derechos económicos correspondientes al programa de ordenador así creado corresponderán, exclusivamente, al empresario, salvo pacto en contrario.

La protección se concederá a todas las personas físicas y jurídicas que cumplan los requisitos establecidos en la legislación nacional sobre derechos de autor aplicable a las obras literarias

De conformidad con la Directiva, los derechos exclusivos del titular incluirán el derecho de realizar o de autorizar:

a) la reproducción total o parcial de un programa de ordenador por cualquier medio y bajo cualquier forma, ya fuere permanente o transitoria.

Cuando la carga, presentación, ejecución, transmisión o almacenamiento de un programa necesitan tal reproducción del mismo, estos actos estarán sujetos a la autorización del titular del derecho;

b) la traducción, adaptación, arreglo y cualquier otra transformación de un programa de ordenador y la reproducción de los resultados de tales actos, sin perjuicio de los derechos de la persona que transforme el programa de ordenador;

c) cualquier forma de distribución pública, incluido el alquiler, del programa de ordenador original o de sus copias. La primera venta en la Comunidad de una copia de un programa por el titular de los derechos o con su consentimiento, agotará el derecho de distribución en la Comunidad de

dicha copia, salvo el derecho de controlar el subsiguiente alquiler del programa o de una copia del mismo.

No obstante lo anterior, salvo que existan disposiciones contractuales específicas, no necesitarán la autorización del titular los actos indicados en las letras a) y b) anteriormente citadas cuando dichos actos sean necesarios para la utilización del programa de ordenador por parte del adquirente legítimo con arreglo a su finalidad propuesta, incluida la corrección de errores.

La realización de una copia de salvaguardia por parte de una persona con derecho a utilizar el programa no podrá impedirse por contrato en tanto en cuanto resulte necesaria para dicha utilización.

El usuario legítimo de la copia de un programa estará facultado para observar, estudiar o verificar su funcionamiento, sin autorización previa del titular, con el fin de determinar las ideas y principios implícitos en cualquier elemento del programa, siempre que lo haga durante cualquiera de las operaciones de carga, visualización, ejecución, transmisión o almacenamiento del programa, que tiene derecho a hacer.

9.2.2 Normativa Estatal

Desde el punto de vista de la normativa estatal se regula en el título VII del RD 1/1996, de 12 de abril, por el que se aprueba el Texto Refundido de la Ley de Propiedad Intelectual, que deroga a la citada ley 16/1993 de 23 de diciembre de transposición de la Directiva 91/250/CEE

El derecho de autor sobre los programas de ordenador se regirá por los preceptos del presente Título VII y, en lo que no esté específicamente previsto en el mismo, por las disposiciones que resulten aplicables de la Ley.

A los efectos de la Ley se entenderá por programa de ordenador toda secuencia de instrucciones o indicaciones destinadas a ser utilizadas, directa o indirectamente, en un sistema informático para realizar una función o una tarea o para obtener un resultado determinado, cualquiera que fuere su forma de expresión y fijación.

A los mismos efectos, la expresión programas de ordenador comprenderá también su documentación preparatoria. La documentación técnica y los manuales de uso de un programa gozarán de la misma protección que este Título dispensa a los programas de ordenador.

El programa de ordenador será protegido únicamente si fuese original, en el sentido de ser una creación intelectual propia de su autor.

La protección prevista se aplicará a cualquier forma de expresión de un programa de ordenador. Asimismo, esta protección se extiende a cualesquiera versiones sucesivas del programa así como a los programas derivados, salvo aquellas creadas con el fin de ocasionar efectos nocivos a un sistema informático.

Cuando los programas de ordenador formen parte de una patente o un modelo de utilidad gozarán, de la protección que pudiera corresponderles por aplicación del régimen jurídico de la propiedad industrial.

No estarán protegidos mediante los derechos de autor las ideas y principios en los que se basan cualquiera de los elementos de un programa de ordenador incluidos los que sirven de fundamento a sus interfaces.

1.-Titularidad

Será considerado autor del programa de ordenador la persona o grupo de personas naturales que lo hayan creado, o la persona jurídica que sea contemplada como titular de los derechos de autor en los casos expresamente previstos por la ley, cuando se trate de una obra colectiva tendrá la consideración de autor, salvo pacto en contrario, la persona natural o jurídica que la edite y divulgue bajo su nombre.

Los derechos de autor sobre un programa de ordenador que sea resultado unitario de la colaboración entre varios autores serán propiedad común y corresponderán a todos éstos en la proporción que determinen.

Cuando un trabajador asalariado cree un programa de ordenador, en el ejercicio de las funciones que le han sido confiadas o siguiendo las instrucciones de su empresario, la titularidad de los derechos de explotación correspondientes al programa de ordenador así creado, tanto el programa fuente como el programa objeto, corresponderán, exclusivamente, al empresario, salvo pacto en contrario.

La protección se concederá a todas las personas naturales y jurídicas que cumplan los requisitos establecidos en la ley para la protección de los derechos de autor.

2.-Duración de la protección.

Cuando el autor sea una persona natural la duración de los derechos de explotación de un programa de ordenador será, según los distintos supuestos que pueden plantearse, la prevista en el Capítulo I del Título III del RD 1/1996, de 12 de abril, por el que se aprueba el Texto Refundido de la Ley de Propiedad Intelectual,

Cuando el autor sea una persona jurídica la duración de los derechos a que se refiere el párrafo anterior será de setenta años, computados desde el día

1 de enero del año siguiente al de la divulgación lícita del programa o al de su creación si no se hubiera divulgado.

3.-Contenido de los derechos de explotación.

Los derechos exclusivos de la explotación de un programa de ordenador por parte de quien sea su titular, incluirán el derecho de realizar o de autorizar:

- a) La reproducción total o parcial, incluso para uso personal, de un programa de ordenador, por cualquier medio y bajo cualquier forma, ya fuere permanente o transitoria. Cuando la carga, presentación, ejecución, transmisión o almacenamiento de un programa necesiten tal reproducción deberá disponerse de autorización para ello, que otorgará el titular del derecho.
- b) La traducción, adaptación, arreglo o cualquier otra transformación de un programa de ordenador y la reproducción de los resultados de tales actos, sin perjuicio de los derechos de la persona que transforme el programa de ordenador.
- c) Cualquier forma de distribución pública incluido el alquiler del programa de ordenador original o de sus copias.

A tales efectos, cuando se produzca cesión del derecho de uso de un programa de ordenador, se entenderá, salvo prueba en contrario, que dicha cesión tiene carácter no exclusivo e intransferible, presumiéndose, asimismo, que lo es para satisfacer únicamente las necesidades del usuario. La primera venta en la Unión Europea de una copia de un programa por el titular de los derechos o con su consentimiento, agotará el derecho de distribución de dicha copia, salvo el derecho de controlar el subsiguiente alquiler del programa o de una copia del mismo.

4.-Límites a los derechos de explotación.

No necesitarán autorización del titular, salvo disposición contractual en contrario,

a) La reproducción o transformación de un programa de ordenador incluida la corrección de errores, cuando dichos actos sean necesarios para la utilización del mismo por parte del usuario legítimo, con arreglo a su finalidad propuesta.

b) La realización de una copia de seguridad por parte de quien tiene derecho a utilizar el programa no podrá impedirse por contrato en cuanto resulte necesaria para dicha utilización.

c) El usuario legítimo de la copia de un programa estará facultado para observar, estudiar o verificar su funcionamiento, sin autorización previa del titular, con el fin de determinar las ideas y principios implícitos en cualquier elemento del programa, siempre que lo haga durante cualquiera de las operaciones de carga, visualización, ejecución, transmisión o almacenamiento del programa que tiene derecho a hacer.

El autor, salvo pacto en contrario, no podrá oponerse a que el cesionario titular de derechos de explotación realice o autorice la realización de versiones sucesivas de su programa ni de programas derivados del mismo.

No será necesaria la autorización del titular del derecho cuando la reproducción del código y la traducción de su forma sea indispensable para obtener la información necesaria para la interoperabilidad de un programa creado de forma independiente con otros programas, siempre que se cumplan los siguientes requisitos:

1.-Que tales actos sean realizados por el usuario legítimo o por cualquier otra persona facultada para utilizar una copia del programa, o, en su nombre, por parte de una persona debidamente autorizada.

2.-Que la información necesaria para conseguir la interoperabilidad no haya sido puesta previamente y de manera fácil y rápida, a disposición de las personas a que se refiere el párrafo anterior.

3.-Que dichos actos se limiten a aquellas partes del programa original que resulten necesarias para conseguir la interoperabilidad.

5.-Protección registral.

Los derechos sobre los programas de ordenador, así como sobre sus sucesivas versiones y los programas derivados, podrán ser objeto de inscripción en el Registro de la Propiedad Intelectual.

6.-Infracción de los derechos.

De acuerdo con la normativa vigente tendrán la consideración de infractores de los derechos de autor quienes, sin autorización del titular de los mismos, realicen los actos siguientes previstos en el artículo 99 al indicar este que

“La reproducción total o parcial, incluso para uso personal, de un programa de ordenador, por cualquier medio y bajo cualquier forma, ya fuere permanente o transitoria. Cuando la carga, presentación, ejecución, transmisión o almacenamiento de un programa necesiten tal reproducción deberá disponerse de autorización para ello, que otorgará el titular del derecho.

b. La traducción, adaptación, arreglo o cualquier otra transformación de un programa de ordenador y la reproducción de los resultados de tales actos, sin perjuicio de los derechos de la persona que transforme el programa de ordenador.

c. Cualquier forma de distribución pública incluido el alquiler del programa de ordenador original o de sus copias.”

Además en particular, se considerarn infractores:

- 1.- Quienes pongan en circulación una o más copias de un programa de ordenador conociendo o pudiendo presumir su naturaleza ilegítima.
- 2.-Quienes tengan con fines comerciales una o más copias de un programa de ordenador, conociendo o pudiendo presumir su naturaleza ilegítima.
- 3.-Quienes pongan en circulación o tengan con fines comerciales cualquier instrumento cuyo único uso sea facilitar la supresión o neutralización no autorizadas de cualquier dispositivo técnico utilizado para proteger un programa de ordenador.

7.- Medidas de protección.

El titular de los derechos reconocidos sobre programas de ordenador que, se disponen en la ley, es decir

- 1.- Podrá pedir el cese de la actividad ilícita, que podrá comprender, la suspensión de la explotación o actividad infractora,
- 2.-La prohibición al infractor de reanudar la explotación o actividad infractora,
- 3.-La retirada del comercio de los ejemplares ilícitos y su destrucción,

4.-La retirada de los circuitos comerciales, la inutilización, y, en caso necesario, la destrucción de los moldes, planchas, matrices, negativos y demás elementos materiales, equipos o instrumentos destinados principalmente a la reproducción, a la creación o fabricación de ejemplares ilícitos,

5.-La remoción o el precinto de los aparatos utilizados en la comunicación pública no autorizada de obras o prestaciones.

6.- La remoción o el precinto de los instrumentos utilizados para facilitar la supresión o la neutralización no autorizadas de cualquier dispositivo técnico utilizado para proteger obras o prestaciones aunque aquélla no fuera su único uso,

7.-Lla suspensión de los servicios prestados por intermediarios a terceros que se valgan de ellos para infringir derechos de propiedad intelectual

Además las medidas cautelares procedentes, conforme a lo dispuesto en la Ley de Enjuiciamiento Civil.

9.3.-TIPOS DE LICENCIAS

Software Libre o Free Software es un software disponible para cualquiera que desee utilizarlo, copiarlo y distribuirlo, ya sea en su forma original o con modificaciones. La posibilidad de modificaciones implica que el código fuente está disponible. Si un programa es libre, puede ser potencialmente incluido en un sistema operativo también libre. Es importante no confundir software libre con software gratis, porque la libertad asociada al software libre de copiar, modificar y redistribuir, no significa gratuidad. Existen programas gratuitos que no pueden ser modificados ni redistribuidos. Y existen programas pagos.

Copyleft.

La mayoría de las licencias usadas en la publicación de software libre permite que los programas sean modificados y redistribuidos. Estas

prácticas están generalmente prohibidas por la legislación internacional de copyright, que intenta impedir que alteraciones y copias sean efectuadas sin la autorización del o los autores. Las licencias que acompañan al software libre hacen uso de la legislación de copyright para impedir la utilización no autorizada, pero estas licencias definen clara y explícitamente las condiciones bajo las cuales pueden realizarse copias, modificaciones y redistribuciones, con el fin de garantizar las libertades de modificar y redistribuir el software registrado. A esta versión de copyright, se le da el nombre de copyleft.

GPL.

La Licencia Pública General GNU (GNU General Public License GPL) es la licencia que acompaña los paquetes distribuidos por el Proyecto GNU, más una gran variedad de software que incluye el núcleo del sistema operativo Linux. La formulación de GPL es tal que en vez de limitar la distribución del software que protege, llega hasta impedir que este software sea integrado en software propietario. La GPL se basa en la legislación internacional de copyright, lo que debe garantizar cobertura legal para el software licenciado con GPL.

Debian.

La licencia Debian es parte del contrato realizado entre Debian y la comunidad de usuarios de software libre, y se denomina Debian Free Software Guidelines (DFSG). En esencia, esta licencia contiene criterios para la distribución que incluyen, además de la exigencia de publicación del código fuente: (a) la redistribución libre ; (b) el código fuente debe ser incluido y debe poder ser redistribuido; (c) todo trabajo derivado debe poder ser redistribuido bajo la misma licencia del original; (d) puede haber restricciones en cuanto a la redistribución del código fuente, si el original fue modificado; (e) la licencia no puede discriminar a ninguna persona o grupo de personas, así como tampoco ninguna forma de utilización del software; (f) los derechos otorgados no dependen del sitio en el que el

software se encuentra; y (g) la licencia no puede 'contaminar' a otro software.

BSD.

La licencia BSD cubre las distribuciones de software de Berkeley Software Distribution, además de otros programas. Ésta es una licencia considerada 'permisiva', ya que impone pocas restricciones sobre la forma de uso, alteraciones y redistribución del software. El software puede ser vendido y no hay obligaciones de incluir el código fuente. Esta licencia garantiza el crédito a los autores del software pero no intenta garantizar que las modificaciones futuras permanezcan siendo software libre.

X.org.

El Consorcio X distribuye X Window System bajo una licencia que lo hace software libre, aunque sin adherirse al copyleft. Existen distribuciones bajo la licencia de la X.org que son software libre, y otras distribuciones que no lo son. Existen algunas versiones no-libres del sistema de ventanas X11 para estaciones de trabajo y ciertos dispositivos de IBM-PC que son las únicas funciones disponibles, sin otros similares que sean distribuidos como software libre.

Software con Dominio Público.

El Software con dominio público es software sin copyright. Algunos tipos de copia o versiones modificadas pueden no ser libres si el autor impone restricciones adicionales en la redistribución del original o de trabajos derivados.

Software Semi-libre.

El Software semi-libre es un software que no es libre pero permite que otros individuos lo usen, lo copien, lo distribuyan y hasta lo modifiquen. Ejemplos de software semi-libre son las primeras versiones de Internet

Explorer de Microsoft, o algunas versiones de browsers de Netscape, y StarOffice.

Freeware.

El término freeware no posee una definición ampliamente aceptada, pero es utilizada para programas que permiten la redistribución pero no la modificación, y que incluyen su código fuente. Estos programas no son software libre.

Shareware.

Shareware es el software disponible con el permiso para que sea redistribuido, pero su utilización implica el pago. Generalmente, el código fuente no se encuentra disponible, y por lo tanto es imposible realizar modificaciones.

Software Propietario.

El Software propietario es aquel cuya copia, redistribución o modificación están, en alguna medida, prohibidos por su propietario. Para usar, copiar o redistribuir, se debe solicitar permiso al propietario o pagar.

Software Comercial.

El Software comercial es el software desarrollado por una empresa con el objetivo de lucrar con su utilización. Nótese que "comercial" y "propietario" no son lo mismo. La mayor parte del software comercial es propietario, pero existe software libre que es comercial, y existe software no-libre que no es comercial.

9.4 .-SOFTWARE DE FUENTES ABIERTAS.

El software libre y de código abierto (también conocido como FOSS o FLOSS, siglas de free/libre and open source software, en inglés) es el

software que está licenciado de tal manera que los usuarios pueden estudiar, modificar y mejorar su diseño mediante la disponibilidad de su código fuente.

El término "software libre y de código abierto" abarca los conceptos de software libre y software de código abierto, que, si bien comparten modelos de desarrollo similares, tienen diferencias en sus aspectos filosóficos. El software libre se enfoca en las libertades filosóficas que les otorga a los usuarios mientras que el software de código abierto se enfoca en las ventajas de su modelo de desarrollo. "FOSS" es un término imparcial respecto a ambas filosofías.

El software gratis no necesariamente tiene que ser libre o de código abierto

Comparación entre software libre y de código abierto

Para que un software sea definido como libre o de código abierto, o ambos, debe cumplir ciertas reglas o normas para poseer esta denominación:

Las 4 libertades del software libre

- 1.- Ejecutar el programa con cualquier propósito (libertad 0)
(privado, educativo, público, comercial, militar, etc.)
- 2.-Estudiar y modificar el programa (libertad 1)
(para lo cual es necesario poder acceder al código fuente)
- 3.-Distribuir el programa de manera que se pueda ayudar al prójimo (libertad 2).
- 4.-Distribuir las versiones modificadas propias (libertad 3)

Las 10 premisas del software de código abierto

- 1.-Libre redistribución: el software debe poder ser regalado o vendido libremente.

- 2.-Código fuente: el código fuente debe estar incluido u obtenerse libremente.
- 3.-Trabajos derivados: la redistribución de modificaciones debe estar permitida
- 4.-Integridad del código fuente del autor: las licencias pueden requerir que las modificaciones sean redistribuidas sólo como parches.
- 5.- Sin discriminación de personas o grupos: nadie puede dejarse fuera.
- 6.-Sin discriminación de áreas de iniciativa: los usuarios comerciales no pueden ser excluidos.
- 7.-Distribución de la licencia: deben aplicarse los mismos derechos a todo el que reciba el programa.
- 8.-La licencia no debe ser específica de un producto: el programa no puede licenciarse solo como parte de una distribución mayor.
- 9.-La licencia no debe restringir otro software: la licencia no puede obligar a que algún otro software que sea distribuido con el software abierto deba también ser de código abierto.
- 10.-La licencia debe ser tecnológicamente neutral: no debe requerirse la aceptación de la licencia por medio de un acceso por clic de ratón o de otra forma específica del medio de soporte del software.

Organizaciones y licencias tras el FOSS

Existen organizaciones detrás de cada iniciativa de distinción del software.

Por parte del software libre, existe la Free Software Foundation (FSF); apoyando el concepto de software de código abierto existe la Open Source Initiative (OSI). Ambas se enfocan en diferentes aspectos del uso y distribución del software, y su disponibilidad y responsabilidades que competen al usuario tener. Por este motivo existen diferentes licencias que las diferencian:



Licencias de código abierto (para el software de código abierto), licencias de software libre (para el software libre), entre otras, sin protección heredada y con protección heredada.

Autor:

Alfonso García Magariños

Director Asesoría Jurídica Municipal Concello de A Coruña

10. LEY 32/2003, GENERAL DE TELECOMUNICACIONES. REGULACIÓN DEL MERCADO DE LAS TELECOMUNICACIONES.

Tema 10.- Ley 32/2003 general telecomunicaciones. Regulación del mercado de telecomunicaciones.

INDICE

10.1 Ley general de telecomunicaciones.

10.1.1 Introducción

10.1.2 Aspectos Básicos

10.1.3 Estructura y Objetivos

10.1.- LEY 32/2003 GENERAL DE TELECOMUNICACIONES. REGULACIÓN DEL MERCADO

10.1.1 Introducción

Si bien la ley 11/1998, de 24 de abril, General de Telecomunicaciones, instauró un régimen plenamente liberalizado en la prestación de servicios y el establecimiento y explotación de redes de telecomunicaciones, abriendo el sector a la libre competencia entre operadores, dicha regulación había quedado en cierto modo desfasada, derivado ello fundamentalmente de la hiperactividad normativa de la Unión Europea.

La ley incorpora al ordenamiento jurídico español el contenido de la normativa comunitaria citada, respetando plenamente los principios recogidos en ella.

10.1.2 Aspectos Básicos

Como notas más importantes de la ley cabe destacar las siguientes:

En primer lugar, se dirige a regular exclusivamente el sector de las telecomunicaciones, en ejercicio de la competencia exclusiva del Estado prevista en el artículo 149.1.21^a de la Constitución. La Ley excluye expresamente de su regulación los contenidos difundidos a través de medios audiovisuales, que constituyen parte del régimen de los medios de comunicación social, y que se caracterizan por ser transmitidos en un solo sentido de forma simultánea a una multiplicidad de usuarios. Igualmente se excluye de su regulación la prestación de servicios sobre las redes de telecomunicaciones que no consistan principalmente en el transporte de señales a través de dichas redes. Estos últimos son objeto de regulación en la Ley 34/2002, de 11 de julio, de Servicios de la Sociedad de la Información y de Comercio Electrónico. No obstante, las redes utilizadas

como soporte de los servicios de radiodifusión sonora y televisiva, las redes de televisión por cable y los recursos asociados, como parte integrante de las comunicaciones electrónicas, estarán sujetos a lo establecido en la Ley.

Toda la regulación de las comunicaciones electrónicas se entiende incluida en el concepto más amplio de telecomunicaciones y, por lo tanto, dictada por el Estado en virtud de su atribución competencial exclusiva del artículo 149.1.21ª de la Constitución.

Se avanza en la liberalización de la prestación de servicios y la instalación y explotación de redes de comunicaciones electrónicas. En este sentido, cumpliendo con el principio de intervención mínima, se entiende que la habilitación para dicha prestación y explotación a terceros viene concedida con carácter general e inmediato por la Ley. Únicamente será requisito previo la notificación a la Comisión del Mercado de las Telecomunicaciones para iniciar la prestación del servicio. Desaparecen, pues, las figuras de las autorizaciones y licencias previstas en la Ley 11/1998, de 24 de abril, General de Telecomunicaciones, como títulos habilitantes individualizados de que era titular cada operador para la prestación de cada red o servicio.

Se refuerzan las competencias y facultades de la Comisión del Mercado de las Telecomunicaciones en relación con la supervisión y regulación de los mercados. Se contempla un sistema que gana en flexibilidad, mediante el cual este organismo realizará análisis periódicos de los distintos mercados de referencia, detectando aquellos que no se estén desarrollando en un contexto de competencia efectiva e imponiendo, en ese caso, obligaciones específicas a los operadores con poder significativo en el mercado. Es novedoso también el cambio en la definición de este tipo de operadores, pasando de un concepto «formal», esto es, basado en la superación de una determinada cuota de mercado, a uno «material», más cercano al tradicional derecho de la competencia, es decir, basado en la posición de

fuerza del operador que le permite actuar con independencia de sus competidores o de los consumidores que sean personas físicas y usuarios.

En relación con la garantía de los derechos de los usuarios, la Ley recoge la ampliación de las prestaciones, que, como mínimo esencial, deben garantizarse a todos los ciudadanos, bajo la denominación de «servicio universal». Se incluye el acceso funcional a internet, ya incorporado anticipadamente por la Ley 34/2002, de 11 de julio, de Servicios de la Sociedad de la Información y de Comercio Electrónico, y la posibilidad de que se ofrezcan opciones tarifarias especiales que permitan un mayor control del gasto por los usuarios. Además, se amplía el catálogo de derechos de los consumidores que sean personas físicas y usuarios reconocidos con rango legal.

La regulación de la ocupación del dominio público o la propiedad privada para la instalación de redes, pretende establecer unos criterios generales, que deberán ser respetados por las Administraciones públicas titulares del dominio público. De este modo, se reconocen derechos de ocupación a todos los operadores que practiquen la notificación a la Comisión del Mercado de las Telecomunicaciones, en la medida que sea necesario para la instalación de sus redes, a la vez que se detallan los principios básicos que garanticen el ejercicio de dicho derecho en condiciones de igualdad y transparencia, con independencia de la Administración o el titular del dominio público o la propiedad privada.

En lo referente al dominio público radioeléctrico, se regula la garantía del uso eficiente del espectro radioeléctrico, como principio superior que debe guiar la planificación y la asignación de frecuencias por la Administración y el uso de éstas por los operadores. Asimismo, se abre la posibilidad de la cesión de derechos de uso del espectro radioeléctrico, en las condiciones que se determinen reglamentariamente. En los supuestos en que las bandas de frecuencias asignadas a determinados servicios sean

insuficientes para atender la demanda de los operadores, se prevé la celebración de procedimientos de licitación. Como requisito esencial en la prestación de servicios mediante tecnologías que usen el dominio público radioeléctrico, se establece el respeto a los límites de las emisiones radioeléctricas establecidas en la normativa vigente.

La Ley también tiene como objetivo el establecimiento de una serie de criterios que guíen la actuación en la imposición de tasas que afecten a los servicios de telecomunicaciones. Distingue entre aquellas tasas que respondan a la necesidad de compensar actuaciones administrativas, donde la cuantía se fijará en función de su coste, de aquellas impuestas sobre el uso de recursos asociados, como el dominio público, las frecuencias o la numeración. En este último caso se perseguirá garantizar su uso óptimo, teniendo en cuenta el valor del bien y su escasez. Como principios básicos de estas exacciones se establecen la transparencia, la proporcionalidad y su justificación objetiva.

En la tipificación de infracciones y la imposición de las correspondientes sanciones se han reforzado las potestades administrativas, como necesario contrapunto a una mayor simplificación en las condiciones para obtener la habilitación para prestar servicios. Con ello, el control «ex ante» que suponía la obtención de una autorización individualizada para cada operador con la Ley 11/1998, de 24 de abril, General de Telecomunicaciones, viene a ser sustituido por uno «ex post», mediante la posibilidad de obtener información de los operadores, de imponer medidas cautelares en el procedimiento sancionador o de inhabilitar a las empresas que cometan infracciones muy graves.

10.1.3 Estructura y Objetivos

Contiene la ley 7 títulos.

El título I contiene las disposiciones generales de la ley, así, declara que las telecomunicaciones son servicios de interés general que se prestan en régimen de libre competencia,

Los objetivos y principios de esta Ley son los siguientes:

Fomentar la competencia efectiva en los mercados de telecomunicaciones y, en particular, en la explotación de las redes y en la prestación de los servicios de comunicaciones electrónicas y en el suministro de los recursos asociados a ellos. Todo ello promoviendo una inversión eficiente en materia de infraestructuras y fomentando la innovación.

Garantizar el cumplimiento de las referidas condiciones y de las obligaciones de servicio público en la explotación de redes y la prestación de servicios de comunicaciones electrónicas, en especial las de servicio universal.

Promover el desarrollo del sector de las telecomunicaciones, así como la utilización de los nuevos servicios y el despliegue de redes, y el acceso a éstos, en condiciones de igualdad, e impulsar la cohesión territorial, económica y social.

Hacer posible el uso eficaz de los recursos limitados de telecomunicaciones, como la numeración y el espectro radioeléctrico, y la adecuada protección de este último, y el acceso a los derechos de ocupación de la propiedad pública y privada.

Defender los intereses de los usuarios

Fomentar, en la medida de lo posible, la neutralidad tecnológica en la regulación.

Promover el desarrollo de la industria de productos y servicios de telecomunicaciones.

Contribuir al desarrollo del mercado interior de servicios de comunicaciones electrónicas en la Unión Europea.

Recoge también que las redes, servicios, instalaciones y equipos de telecomunicaciones que desarrollen actividades esenciales para la defensa

nacional integran los medios destinados a ésta, se reservan al Estado y se rigen por su normativa específica

El título II regula la explotación de redes y prestación de servicios de comunicaciones electrónicas en régimen de libre competencia

La explotación de las redes y la prestación de los servicios de comunicaciones electrónicas se realizarán en régimen de libre competencia sin más limitaciones que las establecidas en esta Ley y su normativa de desarrollo

Podrán explotar redes y prestar servicios de comunicaciones electrónicas a terceros las personas físicas o jurídicas nacionales de un Estado miembro de la Unión Europea o con otra nacionalidad, cuando, en el segundo caso, así esté previsto en los acuerdos internacionales que vinculen al Reino de España. Para el resto de personas físicas o jurídicas, el Gobierno podrá autorizar excepciones de carácter general o particular a la regla anterior.

En todo caso, las personas físicas o jurídicas que exploten redes o presten servicios de comunicaciones electrónicas a terceros deberán designar una persona responsable a efecto de notificaciones domiciliada en España, sin perjuicio de lo que puedan prever los acuerdos internacionales.

Los interesados en la explotación de una determinada red o en la prestación de un determinado servicio de comunicaciones electrónicas deberán, con anterioridad al inicio de la actividad, notificarlo fehacientemente a la Comisión del Mercado de las Telecomunicaciones en los términos que se determinen mediante Real Decreto, sometiéndose a las condiciones previstas para el ejercicio de la actividad que pretendan realizar. Quedan exentos de esta obligación quienes exploten redes y se presten servicios de comunicaciones electrónicas en régimen de autoprestación.

Cuando la Comisión del Mercado de las Telecomunicaciones constate que la notificación no reúne los requisitos establecidos en el apartado anterior, dictará resolución motivada en un plazo máximo de 15 días, no teniendo por realizada aquélla.

Se crea, dependiente de la Comisión del Mercado de las Telecomunicaciones, el Registro de operadores. Dicho registro será de carácter público y su regulación se hará por Real Decreto. En él deberán inscribirse los datos relativos a las personas físicas o jurídicas que hayan notificado su intención de explotar redes o prestar servicios de comunicaciones electrónicas, las condiciones para desarrollar la actividad y sus modificaciones

Los operadores de redes públicas de comunicaciones electrónicas tendrán el derecho y, cuando se solicite por otros operadores de redes públicas de comunicaciones electrónicas, la obligación de negociar la interconexión mutua con el fin de prestar servicios de comunicaciones electrónicas disponibles al público, con el objeto de garantizar así la prestación de servicios y su interoperabilidad

Cuando se impongan obligaciones a un operador de redes públicas de comunicaciones electrónicas para que facilite acceso, la Comisión del Mercado de las Telecomunicaciones podrá establecer determinadas condiciones técnicas u operativas al citado operador o a los beneficiarios de dicho acceso cuando ello sea necesario para garantizar el funcionamiento normal de la red, conforme se establezca reglamentariamente

La Comisión del Mercado de las Telecomunicaciones, podrá imponer a los operadores que, de conformidad con dicho artículo, hayan sido declarados con poder significativo en el mercado obligaciones en materia de:

- 1.-Transparencia, en relación con la interconexión y el acceso, conforme a las cuales los operadores deberán hacer público determinado tipo de información, como la relativa a contabilidad, especificaciones técnicas, características de las redes, condiciones de suministro y utilización, y precios. En particular, cuando se impongan obligaciones de no discriminación a un operador, se le podrá exigir que publique una oferta de referencia.
- 2.-No discriminación, que garantizarán, en particular, que el operador aplique condiciones equivalentes en circunstancias semejantes a otros operadores que presten servicios equivalentes y proporcione a terceros servicios e información de la misma calidad que los que proporcione para sus propios servicios o los de sus filiales o asociados y en las mismas condiciones.
- 3.-Separación de cuentas, en el formato y con la metodología que, en su caso, se especifiquen.
- 4.-Acceso a recursos específicos de las redes y a su utilización.
- 5.-Control de precios, tales como la orientación de los precios en función de los costes, y contabilidad de costes, para evitar precios excesivos o la compresión de los precios en detrimento de los usuarios finales.

Para los servicios de comunicaciones electrónicas disponibles al público se proporcionarán los números y direcciones que se necesiten para permitir su efectiva prestación, tomándose esta circunstancia en consideración en los planes nacionales de numeración y direccionamiento, respectivamente

Los planes nacionales y sus disposiciones de desarrollo designarán los servicios para los que puedan utilizarse los números y, en su caso, direcciones y nombres correspondientes, incluido cualquier requisito relacionado con la prestación de tales servicios.

El contenido de los citados planes y el de los actos derivados de su desarrollo y gestión serán públicos, salvo en lo relativo a materias que puedan afectar a la seguridad nacional.

Se regulan las obligaciones de servicio público y derechos y obligaciones de carácter público en la explotación de redes y en la prestación de servicios de comunicaciones electrónicas

Los operadores están sometidos a las siguientes categorías de obligaciones de servicio público:

El servicio universal en los términos siguientes:

Se entiende por servicio universal el conjunto definido de servicios cuya prestación se garantiza para todos los usuarios finales con independencia de su localización geográfica, con una calidad determinada y a un precio asequible

Se debe garantizar:

1.- Que todos los usuarios finales puedan obtener una conexión a la red telefónica pública desde una ubicación fija y acceder a la prestación del servicio telefónico disponible al público, siempre que sus solicitudes se consideren razonables en los términos que reglamentariamente se determinen. La conexión debe ofrecer al usuario final la posibilidad de efectuar y recibir llamadas telefónicas y permitir comunicaciones de fax y datos a velocidad suficiente para acceder de forma funcional a Internet. No obstante, la conexión deberá permitir comunicaciones en banda ancha, en los términos que se definan por la normativa vigente.

2.- Que se ponga a disposición de los abonados al servicio telefónico disponible al público una guía general de números de abonados, ya sea impresa o electrónica, o ambas, y se actualice, como mínimo, una vez al año. Asimismo, que se ponga a disposición de todos los usuarios finales de dicho servicio, incluidos los usuarios de teléfonos públicos de pago, al menos un servicio de información general sobre números de abonados. Todos los abonados al servicio telefónico disponible al público tendrán derecho a figurar en la mencionada guía general, sin perjuicio, en todo

caso, del respeto a las normas que regulen la protección de los datos personales y el derecho a la intimidad.

3.- Que exista una oferta suficiente de teléfonos públicos de pago, en todo el territorio nacional, que satisfaga razonablemente las necesidades de los usuarios finales, en cobertura geográfica, en número de aparatos, accesibilidad de estos teléfonos por los usuarios con discapacidades y calidad de los servicios y, que sea posible efectuar gratuitamente llamadas de emergencia desde los teléfonos públicos de pago sin tener que utilizar ninguna forma de pago, utilizando el número único de llamadas de emergencia 112 y otros números de emergencia españoles. Asimismo, en los términos que se definan por la normativa vigente para el servicio universal, que exista una oferta suficiente de equipos terminales de acceso a Internet de banda ancha.

4.- Que los usuarios finales con discapacidad tengan acceso al servicio telefónico disponible al público desde una ubicación fija y a los demás elementos del servicio universal citados en este artículo en condiciones equiparables a las que se ofrecen al resto de usuarios finales.

5.- Que, cuando así se establezca reglamentariamente, se ofrezcan a los consumidores que sean personas físicas, de acuerdo con condiciones transparentes, públicas y no discriminatorias, opciones o paquetes de tarifas que difieran de las aplicadas en condiciones normales de explotación comercial, con objeto de garantizar, en particular, que las personas con necesidades sociales especiales puedan tener acceso al servicio telefónico disponible al público o hacer uso de éste.

6.- Que se apliquen, cuando proceda, opciones tarifarias especiales o limitaciones de precios, tarifas comunes, equiparación geográfica u otros regímenes similares, de acuerdo con condiciones transparentes, públicas y no discriminatorias.

El Gobierno podrá, por necesidades de la defensa nacional, de la seguridad pública o de los servicios que afecten a la seguridad de las personas o a la protección civil, imponer otras obligaciones de servicio público distintas de las de servicio universal a los operadores.

El Gobierno podrá, asimismo, imponer otras obligaciones de servicio público, previo informe de la Comisión del Mercado de las Telecomunicaciones, motivadas por:

- 1.-Razones de cohesión territorial.
- 2.-Razones de extensión del uso de nuevos servicios y tecnologías, en especial a la sanidad, a la educación, a la acción social y a la cultura.
- 3.-Razones de facilitar la comunicación entre determinados colectivos que se encuentren en circunstancias especiales y estén insuficientemente atendidos con la finalidad de garantizar la suficiencia de su oferta.
- 4.-Por necesidad de facilitar la disponibilidad de servicios que comporten la acreditación de fehaciencia del contenido del mensaje remitido o de su remisión o recepción.

Los operadores tendrán derecho, a la ocupación del dominio público en la medida en que ello sea necesario para el establecimiento de la red pública de comunicaciones electrónicas de que se trate.

Los operadores también tendrán derecho, a la ocupación de la propiedad privada cuando resulte estrictamente necesario para la instalación de la red en la medida prevista en el proyecto técnico presentado y siempre que no existan otras alternativas económicamente viables, ya sea a través de su expropiación forzosa o mediante la declaración de servidumbre forzosa de paso para la instalación de infraestructura de redes públicas de comunicaciones electrónicas. En ambos casos tendrán la condición de beneficiarios en los expedientes que se tramiten, conforme a lo dispuesto en la legislación sobre expropiación forzosa.

Las Administraciones públicas fomentarán la celebración de acuerdos voluntarios entre operadores para la ubicación compartida y el uso compartido de infraestructuras situadas en bienes de titularidad pública o privada.

Secreto de las comunicaciones

Los operadores que exploten redes públicas de comunicaciones electrónicas o que presten servicios de comunicaciones electrónicas disponibles al público deberán garantizar el secreto de las comunicaciones de conformidad con los artículos 18.3 y 55.2 de la Constitución, debiendo adoptar las medidas técnicas necesarias.

1.- Los operadores están obligados a realizar las interceptaciones que se autoricen de acuerdo con lo establecido en la ley

Los sujetos obligados deberán facilitar al agente facultado, salvo que por las características del servicio no estén a su disposición y sin perjuicio de otros datos que puedan ser establecidos mediante real decreto, los datos indicados en la orden de interceptación legal, de entre los que se relacionan a continuación:

a) Identidad o identidades del sujeto objeto de la medida de la interceptación.

b) Identidad o identidades de las otras partes involucradas en la comunicación electrónica.

c) Servicios básicos utilizados.

d) Servicios suplementarios utilizados.

e) Dirección de la comunicación.

f) Indicación de respuesta.

g) Causa de finalización.

h) Marcas temporales.

i) Información de localización.

j) Información intercambiada a través del canal de control o señalización.

El título IV regula la conformidad de aparatos

El Ministerio de Ciencia y Tecnología velará por que los operadores de redes públicas de comunicaciones electrónicas publiquen las especificaciones técnicas precisas y adecuadas de las interfaces de red ofrecidas en España, con anterioridad a la posibilidad de acceso público a los servicios prestados a través de dichas interfaces y por que publiquen las especificaciones técnicas actualizadas cuando se produzca alguna modificación en aquéllas

Los aparatos de telecomunicación, entendiendo por tales cualquier dispositivo no excluido expresamente del reglamento que desarrolle este título que sea equipo radioeléctrico o equipo terminal de telecomunicación, o ambas cosas a la vez, deberán evaluar su conformidad con los requisitos esenciales recogidos en las disposiciones que lo determinen, ser conformes con todas las disposiciones que se establezcan e incorporar el marcado correspondiente como consecuencia de la evaluación realizada. Podrá exceptuarse de la aplicación de lo dispuesto en este título el uso de determinados equipos de radioaficionados contruidos por el propio usuario y no disponibles para venta en el mercado, conforme a lo dispuesto en su regulación específica

Los aparatos de telecomunicación que hayan evaluado su conformidad con los requisitos esenciales en otro Estado miembro de la Unión Europea o en virtud de los acuerdos de reconocimiento mutuo celebrados por ella con terceros países, y cumplan con las demás disposiciones aplicables en la materia, tendrán la misma consideración,

.

El Ministerio de Ciencia y Tecnología establecerá los procedimientos para el reconocimiento de la conformidad de los aparatos de telecomunicación

afectos a los acuerdos de reconocimiento mutuo que establezca la Unión Europea con terceros países

La prestación a terceros de servicios de instalación o mantenimiento de equipos o sistemas de telecomunicación se realizará en régimen de libre competencia sin más limitaciones que las establecidas en esta Ley y su normativa de desarrollo.

Regula el título V el dominio público radioeléctrico

El espectro radioeléctrico es un bien de dominio público, cuya titularidad, gestión, planificación, administración y control corresponden al Estado. Dicha gestión se ejercerá de conformidad con lo dispuesto en este título y en los tratados y acuerdos internacionales en los que España sea parte, atendiendo a la normativa aplicable en la Unión Europea y a las resoluciones y recomendaciones de la Unión Internacional de Telecomunicaciones y de otros organismos internacionales.

La administración, gestión, planificación y control del espectro radioeléctrico incluyen, entre otras funciones, la elaboración y aprobación de los planes generales de utilización, el establecimiento de las condiciones para el otorgamiento del derecho a su uso, la atribución de ese derecho y la comprobación técnica de las emisiones radioeléctricas. Asimismo, se integra dentro de la administración, gestión, planificación y control del referido espectro la inspección, detección, localización, identificación y eliminación de las interferencias perjudiciales, irregularidades y perturbaciones en los sistemas de telecomunicaciones, iniciándose, en su caso, el oportuno procedimiento sancionador.

La utilización del dominio público radioeléctrico mediante redes de satélites se incluye dentro de la gestión, administración y control del espectro de frecuencias.

La gestión del dominio público radioeléctrico tiene por objetivo el establecimiento de un marco jurídico que asegure unas condiciones armonizadas para su uso y que permita su disponibilidad y uso eficiente. A tales efectos:

Los derechos de uso privativo del dominio público radioeléctrico se otorgarán por plazos que se fijarán reglamentariamente, renovables en función de las disponibilidades y previsiones de la planificación de dicho dominio público. Los derechos de uso privativo sin limitación de número se otorgarán por un período que finalizará el 31 de diciembre del año natural en que cumplan su quinto año de vigencia, prorrogable por períodos de cinco años. Por su parte, los derechos de uso privativo con limitación de número tendrán la duración prevista en los correspondientes procedimientos de licitación que en todo caso será de un máximo de veinte años renovables.

Facultades del Gobierno para la gestión del dominio público radioeléctrico

El Gobierno desarrollará reglamentariamente las condiciones de gestión del dominio público radioeléctrico, la elaboración de los planes para su utilización y los procedimientos de otorgamiento de los derechos de uso de dicho dominio. En dicho reglamento se regulará, como mínimo, lo siguiente:

El procedimiento de determinación, control e inspección de los niveles de emisión radioeléctrica tolerable y que no supongan un peligro para la salud pública, en concordancia con lo dispuesto por las recomendaciones de la Comisión Europea. Tales límites deberán ser respetados, en todo caso, por el resto de Administraciones públicas, tanto autonómicas como locales.

El procedimiento para la elaboración de los planes de utilización del espectro radioeléctrico, que incluyen el cuadro nacional de atribución de frecuencias, los planes técnicos nacionales de radiodifusión y televisión, cuya aprobación corresponderá al Gobierno, y las necesidades de espectro radioeléctrico para la defensa nacional. Los datos relativos a esta última materia tendrán el carácter de reservados.

Los procedimientos de otorgamiento de derechos de uso del dominio público radioeléctrico. Los procedimientos de otorgamiento de derechos de uso del dominio público radioeléctrico tendrán en cuenta, entre otras circunstancias, la tecnología utilizada, el interés de los servicios, las bandas y su grado de aprovechamiento. También tendrán en consideración la valoración económica, para el interesado, del uso del dominio público, que éste es un recurso escaso y, en su caso, las ofertas presentadas por los licitadores.

La habilitación para el ejercicio de los derechos de uso del dominio público radioeléctrico revestirá la forma de afectación, concesión o autorización administrativa. El plazo para el otorgamiento de las autorizaciones y concesiones de dominio público radioeléctrico será de seis semanas desde la entrada de la solicitud en cualquiera de los registros del órgano administrativo competente, sin perjuicio de lo dispuesto en el apartado siguiente. Dicho plazo no será de aplicación cuando sea necesaria la coordinación internacional de frecuencias o afecte a reservas de posiciones orbitales.

La adecuada utilización del espectro radioeléctrico mediante el empleo de equipos y aparatos.

Cuando sea preciso para garantizar el uso eficaz del espectro radioeléctrico, el Ministerio de Ciencia y Tecnología podrá, previa audiencia a las partes interesadas, incluidas las asociaciones de consumidores y

usuarios, limitar el número de concesiones demaniales a otorgar sobre dicho dominio para la explotación de redes públicas y la prestación de servicios de comunicaciones electrónicas. Esta limitación será revisable por el propio ministerio, de oficio o a instancia de parte, en la medida en que desaparezcan las causas que la motivaron

El derecho de uso del dominio público radioeléctrico se otorgará por la Agencia Estatal de Radiocomunicaciones, a través de la afectación demanial o de la concesión o autorización administrativa, el uso común del dominio público radioeléctrico será libre.

El otorgamiento del derecho al uso del dominio público radioeléctrico revestirá la forma de autorización administrativa en los siguientes supuestos:

Si se trata de una reserva del derecho de uso especial no privativo del dominio público. Tendrán la consideración de uso especial del dominio público el del espectro radioeléctrico por radioaficionados y otros sin contenido económico, como los de banda ciudadana, estableciéndose mediante reglamento el plazo de su duración y las condiciones asociadas exigibles.

Si se otorga el derecho de uso privativo para autoprestación por el solicitante, salvo en el caso de Administraciones públicas que requerirán de afectación demanial. No se otorgarán derechos de uso privativo del dominio público radioeléctrico para su uso en autoprestación en los supuestos en que la demanda supere a la oferta. En los restantes supuestos, el derecho al uso privativo del dominio público radioeléctrico requerirá concesión administrativa. Para el otorgamiento de dicha concesión demanial, será requisito previo que los solicitantes acrediten su condición de operador. Las resoluciones mediante las cuales se otorguen

las concesiones de dominio público radioeléctrico se dictarán y publicarán en la forma y plazos que se establezcan mediante Real Decreto.

El título VI regula la administración de las telecomunicaciones

Tendrán la consideración de Autoridad Nacional de Reglamentación de Telecomunicaciones:

El Gobierno.

Los órganos superiores y directivos del Ministerio de Ciencia y Tecnología que, de conformidad con la estructura orgánica del departamento, asuman las competencias de esta Ley.

Los órganos superiores y directivos del Ministerio de Economía en materia de regulación de precios.

La Comisión del Mercado de las Telecomunicaciones.

La Agencia Estatal de Radiocomunicaciones.

. Se crea, con la denominación de Agencia Estatal de Radiocomunicaciones, un organismo público con carácter de organismo autónomo, de acuerdo con lo previsto en el artículo 43.1.a) de la Ley 6/1997, de 14 de abril, de Organización y Funcionamiento de la Administración General del Estado, con personalidad jurídico-pública diferenciada y plena capacidad de obrar

Dicha Agencia se adscribe, a través de la Secretaría de Estado de Telecomunicaciones y para la Sociedad de la Información, al Ministerio de Ciencia y Tecnología,

A la Agencia, dentro de la esfera de sus competencias, le corresponden las potestades administrativas para el cumplimiento de sus fines, en los términos que prevea su Estatuto y de acuerdo con la legislación aplicable.

La Agencia tendrá por objeto la ejecución de la gestión del dominio público radioeléctrico en el marco de las directrices fijadas por el Gobierno, el Ministerio de Ciencia y Tecnología y la Secretaría de Estado de

Telecomunicaciones y para la Sociedad de la Información, así como en la normativa correspondiente.

la Agencia desarrollará las siguientes funciones :

- a) La propuesta de planificación, la gestión y la administración del dominio público radioeléctrico, así como la tramitación y el otorgamiento de los títulos habilitantes para su utilización, salvo cuando se limite su número de acuerdo con lo previsto en el apartado 2 del artículo 44 .
- b) El ejercicio de las funciones atribuidas a la Administración General del Estado en materia de autorización e inspección de instalaciones radioeléctricas en relación con los niveles de emisión radioeléctrica permitidos , en el ámbito de la competencia exclusiva que corresponde al Estado sobre las telecomunicaciones, de acuerdo con el artículo 149.1.21ª de la Constitución.
- c) La gestión de un registro público de radiofrecuencias, accesible a través de internet, en el que constarán los titulares de concesiones administrativas para el uso privativo del dominio público radioeléctrico.
- d) La elaboración de proyectos y desarrollo de los planes técnicos nacionales de radiodifusión y televisión.
- e) La comprobación técnica de emisiones radioeléctricas para la identificación, localización y eliminación de interferencias perjudiciales, infracciones, irregularidades y perturbaciones de los sistemas de radiocomunicación.
- f) El control y la inspección de las telecomunicaciones, así como la propuesta de incoación de expedientes sancionadores en la materia. En materias de competencia del Ministerio de Ciencia y Tecnología o de la Comisión del Mercado de Telecomunicaciones, y a su solicitud, la Agencia Estatal de Radiocomunicaciones realizará las funciones de inspección que le sean requeridas.
- g) La gestión de la asignación de los recursos órbita-espectro para comunicaciones por satélite.

- h) La gestión en período voluntario de la tasa por reserva del dominio público radioeléctrico establecida en la ley
- i) La elaboración de estudios e informes y, en general, el asesoramiento de la Administración General del Estado en todo lo relativo a la gestión del dominio público radioeléctrico.
- j) La colaboración con la Secretaría de Estado de Telecomunicaciones y para la Sociedad de la Información en la participación en los organismos internacionales relacionados con la planificación del espectro radioeléctrico.
- k) La elaboración y elevación al Ministerio de Ciencia y Tecnología de un informe anual sobre su actuación.

La Comisión del Mercado de las Telecomunicaciones es un organismo regulador de los previstos por el artículo 8 de la Ley 2/2011, de 4 de marzo, de Economía Sostenible, dotado de personalidad jurídica propia y plena capacidad pública y privada.

La Comisión del Mercado de las Telecomunicaciones tendrá por objeto el establecimiento y supervisión de las obligaciones específicas que hayan de cumplir los operadores en los mercados de telecomunicaciones y el fomento de la competencia en los mercados de los servicios audiovisuales, conforme a lo previsto por su normativa reguladora y en el apartado 1 del artículo 10 de la Ley 2/2011, de 4 de marzo, de Economía sostenible, la resolución de los conflictos entre los operadores y, en su caso, el ejercicio como órgano arbitral de las controversias entre los mismos.

La Comisión del Mercado de las Telecomunicaciones ejercerá las siguientes funciones

1.-Arbitrar en los conflictos que puedan surgir entre los operadores del sector de las comunicaciones electrónicas, así como en aquellos otros casos que puedan establecerse por vía reglamentaria, cuando los interesados lo acuerden.

2.-El ejercicio de esta función arbitral no tendrá carácter público. El procedimiento arbitral se ajustará a los principios esenciales de audiencia, libertad de prueba, contradicción e igualdad, y será indisponible para las partes.

3.-Asignar la numeración a los operadores, para lo que dictará las resoluciones oportunas, en condiciones objetivas, transparentes y no discriminatorias, de acuerdo con lo que reglamentariamente se determine. La Comisión velará por la correcta utilización de los recursos públicos de numeración asignados. Asimismo, autorizará la transmisión de dichos recursos, estableciendo, mediante resolución, las condiciones de aquélla.

4.-Ejercer las funciones que en relación con el servicio universal y su financiación le encomiende la ley.

5.- La resolución vinculante de los conflictos que se susciten entre los operadores en materia de acceso e interconexión de redes, así como en materias relacionadas con las guías telefónicas, la financiación del servicio universal y el uso compartido de infraestructuras.

6.- Adoptar las medidas necesarias para salvaguardar la pluralidad de oferta del servicio, el acceso a las redes de comunicaciones electrónicas por los operadores, la interconexión de las redes y la explotación de red en condiciones de red abierta, y la política de precios y comercialización por los prestadores de los servicios.

Inspección y régimen sancionador

La función inspectora en materia de telecomunicaciones corresponde a:

La Agencia Estatal de Radiocomunicaciones.

La Comisión del Mercado de las Telecomunicaciones.

El Ministerio de Ciencia y Tecnología.

Responsabilidad por las infracciones en materia de telecomunicaciones

La responsabilidad administrativa por las infracciones de las normas reguladoras de las telecomunicaciones será exigible:

1.-En el caso de incumplimiento de las condiciones establecidas para la explotación de redes o la prestación de servicios de comunicaciones electrónicas, a la persona física o jurídica que desarrolle la actividad.

2.-En las cometidas con motivo de la explotación de redes o la prestación de servicios sin haber efectuado la notificación a que se refiere el artículo 6 de esta Ley, a la persona física o jurídica que realice la actividad o, subsidiariamente, a la que tenga la disponibilidad de los equipos e instalaciones por cualquier título jurídico válido en derecho o careciendo de éste.

3.-En las cometidas por los usuarios o por otras personas que, sin estar comprendidas en los párrafos anteriores, realicen actividades reguladas en la normativa sobre telecomunicaciones, a la persona física o jurídica cuya actuación se halle tipificada por el precepto infringido o a la que las normas correspondientes atribuyen específicamente la responsabilidad

Se consideran infracciones muy graves:

a) La realización de actividades sin título habilitante cuando sea legalmente necesario o utilizando parámetros técnicos diferentes de los propios del título y la utilización de potencias de emisión notoriamente superiores a las permitidas o de frecuencias radioeléctricas sin autorización o distintas de las autorizadas, siempre que, en estos dos últimos casos, se produzcan daños graves a las redes o a la prestación de los servicios de comunicaciones electrónicas.

b) El uso, en condiciones distintas a las autorizadas, del espectro radioeléctrico que provoque alteraciones que impidan la correcta prestación de otros servicios por otros operadores.

c) El incumplimiento grave o reiterado por los titulares de concesiones, afectaciones demaniales o autorizaciones para el uso del dominio público radioeléctrico de las condiciones esenciales que se les impongan por el Ministerio de Ciencia y Tecnología.

- d) La transmisión total o parcial de concesiones o autorizaciones para el uso privativo del dominio público radioeléctrico, sin cumplir con los requisitos establecidos a tal efecto por la normativa.
- e) La producción deliberada de interferencias definidas como perjudiciales según la ley de telecomunicaciones, incluidas las causadas por estaciones radioeléctricas que estén instaladas o en funcionamiento a bordo de un buque, de una aeronave o de cualquier otro objeto flotante o aerotransportado que transmita emisiones desde fuera del territorio español para su posible recepción total o parcial en éste.

Se consideran infracciones graves:

- a) La realización de actividades sin título habilitante cuando sea legalmente necesario o utilizando parámetros técnicos diferentes de los propios del título y la utilización de potencias de emisión notoriamente superiores a las permitidas o de frecuencias radioeléctricas sin autorización o distintas de las autorizadas, siempre que las referidas conductas no constituyan infracción muy grave.
- b) La instalación de estaciones radioeléctricas sin autorización, cuando, de acuerdo con lo dispuesto en la normativa reguladora de las telecomunicaciones, sea necesaria, o de estaciones radioeléctricas a bordo de un buque, de una aeronave o de cualquier otro objeto flotante o aerotransportado, que, en el mar o fuera de él, posibilite la transmisión de emisiones desde el exterior para su posible recepción total o parcial en territorio nacional.
- c) La mera producción de interferencias definidas como perjudiciales en esta Ley que no sean muy graves.
- d) La emisión de señales de identificación falsas o engañosas.
- e) El uso, en condiciones distintas de las autorizadas, del espectro radioeléctrico que provoque alteraciones que dificulten la correcta prestación de otros servicios por otros operadores.

f) No atender el requerimiento hecho por la autoridad competente para el cese de las emisiones radioeléctricas, en los supuestos de producción de interferencias.

Se consideran infracciones leves:

La producción de cualquier tipo de emisión radioeléctrica no autorizada, salvo que deba ser considerada como infracción grave o muy grave.

La mera producción de interferencias cuando no deba ser considerada como infracción grave o muy grave.

Carecer de los preceptivos cuadros de tarifas o de precios cuando su exhibición se exija por la normativa vigente.

No facilitar los datos requeridos por la Administración o retrasar injustificadamente su aportación cuando resulte exigible conforme a lo previsto por la normativa reguladora de las comunicaciones electrónicas.

Cualquier otro incumplimiento de las obligaciones impuestas a operadores de redes o de servicios de comunicaciones electrónicas o de sus usuarios, previsto en las leyes vigentes, salvo que deba ser considerado como infracción grave o muy grave, conforme a lo dispuesto en los artículos anteriores

Las infracciones reguladas en la ley de telecomunicaciones prescribirán, las muy graves, a los tres años; las graves, a los dos años, y las leves, a los seis meses

Autor:

Alfonso García Magariños

Director Asesoría Jurídica Municipal Concello de A Coruña

**11. LEGISLACIÓN SOBRE
PROTECCIÓN DE DATOS.
NORMATIVA COMUNITARIA.
LEY ORGÁNICA 15/1999, DE
PROTECCIÓN DE DATOS DE
CARÁCTER PERSONAL, REAL
DECRETO 1720/2007, DE 21 DE
DICIEMBRE, POR EL QUE SE
APRUEBA EL REGLAMENTO DE
DESARROLLO DE LA DE LA
LEY ORGÁNICA 15/1999, DE 13
DE DICIEMBRE, DE
PROTECCIÓN DE DATOS DE
CARÁCTER PERSONAL.**

Tema 11.- Legislación sobre protección de datos. Normativa Comunitaria. Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal. Real Decreto 1720/2007 por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.

INDICE

11.1 Legislación sobre protección de datos

11.2 Normativa Comunitaria

11.2.1 General

11.2.2 Reglamentos

11.2.3 Directivas

11.2.4 Decisiones

11.2.5 Convenios:

11.3.- Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal

11.3.1 Introducción

11.3.2 Principios.

11.3.3 Derechos

11.3.4 Ficheros Públicos y Privados

11.3.5 Agencia Protección Datos.

11.4.- Real Decreto 1720/2007 por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal

11.4.1 Introducción

11.4.2 Análisis

10.1 LEGISLACION SOBRE PROTECCION DE DATOS.

Sin perjuicio del desarrollo a lo largo del tema de las normas más importantes, cabe destacar:

1.-Constitución Española de 1978.

2.-Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.

3.-Ley 2/2011, de 4 de marzo, de Economía Sostenible. Modificación de la LOPD. Disposición final quincuagésima sexta.

4.-Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal.

5.-Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica (DA.4ª)

6.-Real Decreto 1665/2008, de 17 de octubre, por el que se modifica el Estatuto de la Agencia Española de Protección de Datos, aprobado por el Real Decreto 428/1993, de 26 de marzo.

7.-Real Decreto 156/1996, de 2 de febrero, por el que se modifica el Estatuto de la Agencia Española de Protección de Datos.

8.-Real Decreto 428/1993, de 26 de marzo, por el que se aprueba el Estatuto de la Agencia Española de Protección de Datos

11.2 NORMATIVA COMUNITARIA

11.2.1 General

En la Carta de los derechos fundamentales de la Unión Europea, de 7 de diciembre de 2000, el artículo 8 dispone:

“Toda persona tiene derecho a la protección de los datos de carácter personal que la conciernan.

Estos datos se tratarán de modo leal, para fines concretos y sobre la base del consentimiento de la persona afectada o en virtud de otro fundamento legítimo previsto por la ley. Toda persona tiene derecho a acceder a los datos recogidos que la conciernan y a su rectificación.

El respeto de estas normas quedará sujeto al control de una autoridad independiente.”

En las versiones consolidadas del Tratado de la Unión Europea y del Tratado de Funcionamiento de la Unión Europea. Publicadas en el Diario Oficial de la Unión Europea el 30 de marzo de 2010, se recogen aspectos relacionados con la protección de datos, así en el artículo 16 del Tratado de Funcionamiento de la U. E se dispone *“Toda persona tiene derecho a la protección de los datos de carácter personal que le conciernan.*

2. El Parlamento Europeo y el Consejo establecerán, con arreglo al procedimiento legislativo ordinario, las normas sobre protección de las personas físicas respecto del tratamiento de datos de carácter personal por las instituciones, órganos y organismos de la Unión, así como por los Estados miembros en el ejercicio de las actividades comprendidas en el

ámbito de aplicación del Derecho de la Unión, y sobre la libre circulación de estos datos. El respeto de dichas normas estará sometido al control de autoridades independientes.

Las normas que se adopten en virtud del presente artículo se entenderán sin perjuicio de las normas específicas previstas en el artículo 39 del Tratado de la Unión Europea. “

El artículo 39 del Tratado de la Unión Europea establece “De conformidad con el artículo 16 del Tratado de Funcionamiento de la Unión Europea, y no obstante lo dispuesto en su apartado 2, el Consejo adoptará una decisión que fije las normas sobre protección de las personas físicas respecto del tratamiento de datos de carácter personal por los Estados miembros en el ejercicio de las actividades comprendidas en el ámbito de aplicación del presente capítulo, y sobre la libre circulación de dichos datos. El respeto de dichas normas estará sometido al control de autoridades independientes.

11.2.2 Reglamentos:

1.- Reglamento del Eurodac, No 2725/2000 Del Consejo de 11 de diciembre de 2000 relativo a la creación del sistema «Eurodac» para la comparación de las impresiones dactilares para la aplicación efectiva del Convenio de Dublín, allí se crea un sistema denominado «Eurodac», cuya finalidad será ayudar a determinar el Estado miembro responsable, con arreglo al Convenio de Dublín, del examen de las solicitudes de asilo presentadas en los Estados miembros y, además, facilitar la aplicación del Convenio de Dublín en las condiciones establecidas en el presente Reglamento, se considera que Las impresiones dactilares constituyen un elemento importante para determinar la identidad exacta de dichas personas. Es necesario crear un sistema para comparar sus datos dactiloscópicos, considerando los mismos como datos de carácter personal.

2.- Reglamento (CE) No 45/2001 del Parlamento Europeo y del Consejo de 18 de diciembre de 2000 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales, allí se establece que las instituciones y los organismos creados por los Tratados constitutivos de las Comunidades comunitarios», garantizarán, de conformidad con el presente Reglamento, la protección de los derechos y las libertades fundamentales de las personas físicas, y en particular su derecho a la intimidad, en lo que respecta al tratamiento de los datos personales, y no limitarán ni prohibirán la libre circulación de datos personales entre ellos o entre ellos y destinatarios sujetos al Derecho nacional de los Estados miembros adoptado en aplicación de la Directiva 95/46/CE.

La autoridad de control independiente establecida por el presente Reglamento, denominada «Supervisor Europeo de Protección de Datos», supervisará la aplicación de las disposiciones del presente Reglamento a todas las operaciones de tratamiento realizadas por las instituciones y organismos comunitarios.

Se entiende por «datos personales»: toda información sobre una persona física identificada o identificable ; se considerará identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un número de identificación o uno o varios elementos específicos, característicos de su identidad física, fisiológica, psíquica, económica, cultural o social;

«tratamiento de datos personales» cualquier operación o conjunto de operaciones, efectuadas o no mediante procedimientos automatizados, aplicadas a datos personales, como la recogida, registro, organización, conservación, adaptación o modificación, extracción, consulta, utilización, comunicación por transmisión, difusión o cualquier otra forma que permita el acceso a los mismos, así como la alineación o interconexión, y el bloqueo, supresión o destrucción;

Las disposiciones del Reglamento se aplicarán al tratamiento de datos personales por parte de todas las instituciones y organismos comunitarios, en la medida en que dicho tratamiento se lleve a cabo para el ejercicio de actividades que pertenecen al ámbito de aplicación del Derecho comunitario

Los datos personales deberán ser:

- a) tratados de manera leal y lícita;
- b) recogidos con fines determinados, explícitos y legítimos, y no ser tratados posteriormente de manera incompatible con dichos fines; no se considerará incompatible el tratamiento posterior de datos con fines históricos, estadísticos o científicos, siempre y cuando el responsable del tratamiento establezca las garantías oportunas, en particular para asegurar que los datos no serán tratados con otros fines y que no se utilizarán en favor de medidas o decisiones que afecten a personas concretas;
- c) adecuados, pertinentes y no excesivos con relación a los fines para los que se recaben y para los que se traten posteriormente;
- d) exactos y, si fuera necesario, actualizados; se tomarán todas las medidas razonables para la supresión o rectificación de los datos inexactos o incompletos en relación con los fines para los que fueron recogidos o para los que son tratados posteriormente;
- e) conservados en una forma que permita la identificación de los interesados durante un período no superior al necesario para la consecución de los fines para los que fueron recogidos o para los que se traten posteriormente. La institución o el organismo comunitario establecerá para los datos personales que deban ser archivados por un período más largo del mencionado para fines históricos, estadísticos o científicos, que dichos datos se archiven bien únicamente en forma anónima, o, cuando ello no sea posible, sólo con la identidad codificada

del interesado. En cualquier caso, deberá imposibilitarse el uso de los datos salvo para fines históricos, estadísticos o científicos.

3.- Decisión del Consejo de 13 de septiembre de 2004 por la que se adoptan las normas de desarrollo del Reglamento (CE) no 45/2001 del Parlamento Europeo y del Consejo relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por las instituciones y los organismos comunitarios y a la libre circulación de estos datos.

11.2.3 Directivas:

1.-Directiva 2009/136/CE del Parlamento Europeo y del Consejo, de 25 de noviembre de 2009, por la que se modifican la Directiva 2002/22/CE relativa al servicio universal y los derechos de los usuarios en relación con las redes y los servicios de comunicaciones electrónicas, la Directiva 2002/58/CE relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas y el Reglamento (CE) no 2006/2004 sobre la cooperación en materia de protección de los consumidores

2.-Directiva 2006/24/CE, del Parlamento Europeo y del Consejo de 15 de marzo de 2006, sobre la conservación de datos generados o tratados en relación con la prestación de servicios de comunicaciones electrónicas de acceso público o de redes públicas de comunicaciones y por la que se modifica la Directiva 2002/58/CE.

3.-Directiva 2004/82/CE, del Consejo de 29 de abril de 2004, sobre la obligación de los transportistas de comunicar los datos de las personas transportadas.

4.-Directiva 2002/58/CE del Parlamento Europeo y del Consejo de 12 de julio de 2002, relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas (Directiva sobre privacidad y las comunicaciones electrónicas).

5.-Directiva 2002/22/CE del Parlamento Europeo y del Consejo, de 7 de marzo de 2002, relativa al servicio universal y los derechos de los usuarios en relación con las redes y los servicios de comunicaciones electrónicas (Directiva servicio universal).

6.-Directiva 2002/21/CE, del parlamento Europeo y del Consejo de 29 de abril de 2004, sobre la obligación de los transportistas de comunicar los datos de las personas transportadas.

7.-Directiva 2002/20/CE, del Parlamento Europeo y del Consejo, de 7 de marzo de 2002, relativa a la autorización de redes y servicios de comunicaciones electrónicas (Directiva de autorización).

8.-Directiva 2002/19/CE, del Parlamento Europeo y del Consejo, de 7 de marzo de 2002, relativa al acceso a las redes de comunicaciones electrónicas y recursos asociados, y a su interconexión (Directiva de acceso).

9.-Directiva 2000/31/CE, del Parlamento Europeo y del Consejo, de 8 de junio de 2000, relativa a determinados aspectos jurídicos de los servicios de la sociedad de la información, en particular el comercio electrónico en el mercado interior (Directiva sobre el comercio electrónico).

10.-Directiva 1999/93/CE, del Parlamento Europeo y del Consejo, de 13 de diciembre de 1999, por la que se establece un marco comunitario para la firma electrónica.

11.-Directiva 97/66/CE del Parlamento Europeo y del Consejo de 15 de diciembre de 1997 relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las telecomunicaciones. (Derogada por la Directiva 2002/58/CE).

12.-Directiva 95/46/CE del Parlamento Europeo y del Consejo de 24 de octubre de 1995 relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos.

11.2.4 Decisiones:

1.-Decisión de la Comisión de 31 de enero de 2011 de conformidad con la Directiva 95/46/CE del Parlamento Europeo y del Consejo, relativa a la protección adecuada de los datos personales por el Estado de Israel en lo que respecta al tratamiento automatizado de los datos personales

2.-Decisión de la Comisión de 19 de octubre de 2010 de conformidad con la Directiva 95/46/CE del Parlamento Europeo y del Consejo, relativa a la adecuada protección de los datos personales en Andorra

3.-Decisión de la Comisión de 5 de marzo de 2010 con arreglo a la Directiva 95/46/CE del Parlamento Europeo y del Consejo, relativa a la protección adecuada dada en la Ley de las Islas Feroe sobre el tratamiento de datos personales

4.-Decisión de la Comisión (2010/87/UE), de 5 de febrero de 2010, relativa a las cláusulas contractuales tipo para la transferencia de datos personales a los encargados del tratamiento establecidos en terceros países, de conformidad con la Directiva 95/46/CE del Parlamento Europeo y del Consejo.

5.-Decisión de la Comisión de 8 de mayo de 2008 de conformidad con la Directiva 95/46/CE del Parlamento Europeo y del Consejo, relativa a la protección adecuada de los datos personales en Jersey

6.-Decisión de la Comisión de 6 de septiembre de 2005, relativa al carácter adecuado de la protección de los datos personales incluidos en los registros de nombres de los pasajeros (PNR) que se transfieren a la Agencia de Servicios de Fronteras de Canadá.

7.-Decisión de la Comisión de 27 de diciembre de 2004, por la que se modifica la Decisión 2001/497/CE en lo relativo a la introducción de un conjunto alternativo de cláusulas contractuales tipo para la transferencia de datos personales a terceros países.

8.-Decisión de la Comisión de 14 de mayo de 2004 relativa al carácter adecuado de la protección de los datos personales incluidos en los registros de nombres de los pasajeros que se transfieren al Servicio de aduanas y protección de fronteras de los Estados Unidos (Bureau of Customs and Border Protection).

9.-Decisión de la Comisión de 29 de abril de 2004 por la que se establece una lista de organismos cuyos investigadores pueden acceder, con fines científicos, a datos confidenciales.

10.-Decisión de la Comisión de 28 de abril de 2004 relativa al carácter adecuado de la protección de datos personales en la Isla de Man.

11.-Decisión de la Comisión de noviembre de 2003, relativa al carácter adecuado de la protección de datos personales en Guernsey.

12.-Decisión de la Comisión de 30 de junio de 2003, con arreglo a la Directiva 95/46/CE del Parlamento Europeo y del Consejo sobre la adecuación de la protección de los datos personales en Argentina.

13.-Decisión reguladora de la Unidad de Cooperación Judicial Eurojust.

14.-Decisión 2002/16/CE de la Comisión, de 27 de diciembre de 2001, relativa a 'Cláusulas contractuales tipo para la transferencia de datos personales a los encargados del tratamiento establecidos en terceros países, de conformidad con la Directiva 95/46/CE. (queda derogada a partir de 15 de mayo de 2010)..

15.-Decisión de la comisión de 20 de diciembre de 2001 con arreglo a la Directiva 95/46/CE del Parlamento Europeo y del Consejo, sobre la adecuación de la protección de los datos personales conferida por la ley canadiense Personal Information and Electronic Documents Act.

16.-Decisión 2001/497/CE de la Comisión, de 15 de junio de 2001, relativa a 'Cláusulas contractuales tipo para la transferencia de datos personales a un tercer país previstas en la Directiva 95/46/CE.

17.-Decisión de la Comisión de 26 de julio de 2000 con arreglo a la Directiva 95/46/CE del Parlamento Europeo y del Consejo relativa al nivel de protección adecuado de los datos personales en Suiza.

18.-Decisión de la Comisión de 26 de Julio de 2000 con arreglo a la Directiva 95/46/CE del Parlamento Europeo y del Consejo relativa a la protección adecuada de los datos personales en Hungría.

19.-Decisión de la Comisión de 26 de Julio de 2000 con arreglo a la Directiva 95/46/CE del Parlamento Europeo y del Consejo, sobre la adecuación conferida por los principios de puerto seguro para la

protección de la vida privada y las correspondientes preguntas más frecuentes, publicadas por el Departamento de Comercio de Estados Unidos de América.

11.2.5 Convenios:

1.-Convenio de Europol.

2.-Convenio de Schengen.

3.-Convenio del Sistema de Información de Aduanas.

11.3 LEY ORGÁNICA 15/1999, DE 13 DE DICIEMBRE, DE PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL.

11.3.1 Introducción

La Ley tiene por objeto garantizar y proteger, en lo que concierne al tratamiento de los datos personales, las libertades públicas y los derechos fundamentales de las personas físicas, y especialmente de su honor e intimidad personal y familiar

Será de aplicación a los datos de carácter personal registrados en soporte físico que los haga susceptibles de tratamiento, y a toda modalidad de uso posterior de estos datos por los sectores público y privado

A los efectos de la Ley Orgánica se entenderá por

a) Datos de carácter personal: Cualquier información concerniente a personas físicas identificadas o identificables.

b) Fichero: Todo conjunto organizado de datos de carácter personal, cualquiera que fuere la forma o modalidad de su creación, almacenamiento, organización y acceso.

c) Tratamiento de datos: Operaciones y procedimientos técnicos de carácter automatizado o no, que permitan la recogida, grabación, conservación, elaboración, modificación, bloqueo y cancelación, así como las cesiones de datos que resulten de comunicaciones, consultas, interconexiones y transferencias.

d) Responsable del fichero o tratamiento: Persona física o jurídica, de naturaleza pública o privada, u órgano administrativo, que decida sobre la finalidad, contenido y uso del tratamiento.

e) Afectado o interesado: Persona física titular de los datos que sean objeto del tratamiento a que se refiere el apartado c) del presente artículo.

f) Procedimiento de disociación: Todo tratamiento de datos personales de modo que la información que se obtenga no pueda asociarse a persona identificada o identificable.

g) Encargado del tratamiento: La persona física o jurídica, autoridad pública, servicio o cualquier otro organismo que, solo o conjuntamente con otros, trate datos personales por cuenta del responsable del tratamiento.

h) Consentimiento del interesado: Toda manifestación de voluntad, libre, inequívoca, específica e informada, mediante la que el interesado consienta el tratamiento de datos personales que le conciernen.

i) Cesión o comunicación de datos: Toda revelación de datos realizada a una persona distinta del interesado.

j) Fuentes accesibles al público: Aquellos ficheros cuya consulta puede ser realizada por cualquier persona, no impedida por una norma limitativa, o sin más exigencia que, en su caso, el abono de una contraprestación. Tienen la consideración de fuentes de acceso público, exclusivamente, el censo promocional, los repertorios telefónicos en los términos previstos por su normativa específica y las listas de personas pertenecientes a grupos de profesionales que contengan únicamente los datos de nombre, título, profesión, actividad, grado académico, dirección e indicación de su pertenencia al grupo. Asimismo, tienen el carácter de fuentes de acceso público, los Diarios y Boletines oficiales y los medios de comunicación.

11.3.2 Principios.

1.- Calidad de los datos, los datos de carácter personal sólo se podrán recoger para su tratamiento, así como someterlos a dicho tratamiento, cuando sean adecuados, pertinentes y no excesivos en relación con el ámbito y las finalidades determinadas, explícitas y legítimas para las que se hayan obtenido.

2.- Derecho de información en la recogida de datos, los interesados a los que se soliciten datos personales deberán ser previamente informados de modo expreso, preciso e inequívoco:

a) De la existencia de un fichero o tratamiento de datos de carácter personal, de la finalidad de la recogida de éstos y de los destinatarios de la información.

b) Del carácter obligatorio o facultativo de su respuesta a las preguntas que les sean planteadas.

c) De las consecuencias de la obtención de los datos o de la negativa a suministrarlos.

d) De la posibilidad de ejercitar los derechos de acceso, rectificación, cancelación y oposición.

e) De la identidad y dirección del responsable del tratamiento o, en su caso, de su representante.

3.- Principio del consentimiento del afectado, el tratamiento de los datos de carácter personal requerirá el consentimiento inequívoco del afectado, salvo que la Ley disponga otra cosa.

4.- Comunicación de datos, los datos de carácter personal objeto del tratamiento sólo podrán ser comunicados a un tercero para el cumplimiento de fines directamente relacionados con las funciones legítimas del cedente y del cesionario con el previo consentimiento del interesado.

5.- Deber de secreto, el responsable del fichero y quienes intervengan en cualquier fase del tratamiento de los datos de carácter personal están obligados al secreto profesional respecto de los mismos y al deber de guardarlos, obligaciones que subsistirán aun después de finalizar sus relaciones con el titular del fichero o, en su caso, con el responsable del mismo.

6.- Especial protección a determinados datos, nadie podrá ser obligado a declarar sobre su ideología, religión o creencias.

7.- Seguridad de los datos. El responsable del fichero, y, en su caso, el encargado del tratamiento, deberán adoptar las medidas de índole técnica y organizativas necesarias que garanticen la seguridad de los datos de carácter personal y eviten su alteración, pérdida, tratamiento o acceso no autorizado, habida cuenta del estado de la tecnología, la naturaleza de los datos almacenados y los riesgos a que están expuestos, ya provengan de la acción humana o del medio físico o natural.

11.3.3 Derechos de las personas

Los ciudadanos tienen derecho a no verse sometidos a una decisión con efectos jurídicos, sobre ellos o que les afecte de manera significativa, que se base únicamente en un tratamiento de datos destinados a evaluar determinados aspectos de su personalidad, cabe destacar :

1.-Derecho de consulta al Registro General de Protección de Datos, cualquier persona podrá conocer, recabando a tal fin la información oportuna del Registro General de Protección de Datos, la existencia de tratamientos de datos de carácter personal, sus finalidades y la identidad del responsable del tratamiento. El Registro General será de consulta pública y gratuita

2.-Derecho de acceso, el interesado tendrá derecho a solicitar y obtener gratuitamente información de sus datos de carácter personal sometidos a tratamiento, el origen de dichos datos, así como las comunicaciones realizadas o que se prevén hacer de los mismos

3.-Derecho de rectificación y cancelación. El responsable del tratamiento tendrá la obligación de hacer efectivo el derecho de rectificación o cancelación del interesado en el plazo de diez días

4.-Derecho de tutela, las actuaciones contrarias a lo dispuesto en la Ley pueden ser objeto de reclamación por los interesados ante la Agencia Española de Protección de Datos.

5.- Derecho indemnización. Los interesados que, como consecuencia del incumplimiento de lo dispuesto en la presente Ley por el responsable o el encargado del tratamiento, sufran daño o lesión en sus bienes o derechos tendrán derecho a ser indemnizados.

11.3.4 Ficheros Públicos y Privados.

La creación, modificación o supresión de los ficheros de las Administraciones públicas sólo podrán hacerse por medio de disposición general publicada en el Boletín Oficial del Estado o Diario oficial correspondiente.

Las disposiciones de creación o de modificación de ficheros deberán indicar:

a.-La finalidad del fichero y los usos previstos para el mismo.

b.-Las personas o colectivos sobre los que se pretenda obtener datos de carácter personal o que resulten obligados a suministrarlos.

- c.-El procedimiento de recogida de los datos de carácter personal.
- d.-La estructura básica del fichero y la descripción de los tipos de datos de carácter personal incluidos en el mismo.
- e.-Las cesiones de datos de carácter personal y, en su caso, las transferencias de datos que se prevean a países terceros.
- f.-Los órganos de las Administraciones responsables del fichero.
- g.-Los servicios o unidades ante los que pudiesen ejercitarse los derechos de acceso, rectificación, cancelación y oposición.
- h.-Las medidas de seguridad con indicación del nivel básico, medio o alto exigible.

Podrán crearse ficheros de titularidad privada que contengan datos de carácter personal cuando resulte necesario para el logro de la actividad u objeto legítimos de la persona, empresa o entidad titular y se respeten las garantías que esta Ley establece para la protección de las personas.

Toda persona o entidad que proceda a la creación de ficheros de datos de carácter personal lo notificará previamente a la Agencia Española de Protección de Datos.

Entre los extremos que debe contener la notificación, figurarán necesariamente el responsable del fichero, la finalidad del mismo, su ubicación, el tipo de datos de carácter personal que contiene, las medidas de seguridad, con indicación del nivel básico, medio o alto exigible y las cesiones de datos de carácter personal que se prevean realizar y, en su caso, las transferencias de datos que se prevean a países terceros.

Deberán comunicarse a la Agencia Española de Protección de Datos los cambios que se produzcan en la finalidad del fichero automatizado, en su responsable y en la dirección de su ubicación.

El Registro General de Protección de Datos inscribirá el fichero si la notificación se ajusta a los requisitos exigibles.

En caso contrario podrá pedir que se completen los datos que falten o se proceda a su subsanación.

Transcurrido un mes desde la presentación de la solicitud de inscripción sin que la Agencia Española de Protección de Datos hubiera resuelto sobre la misma, se entenderá inscrito el fichero automatizado a todos los efectos.

11.3.5 Agencia Protección Datos

La Agencia Española de Protección de Datos es un ente de derecho público, con personalidad jurídica propia y plena capacidad pública y privada, que actúa con plena independencia de las Administraciones públicas en el ejercicio de sus funciones

Son funciones de la Agencia Española de Protección de Datos:

- 1.-Velar por el cumplimiento de la legislación sobre protección de datos y controlar su aplicación, en especial en lo relativo a los derechos de información, acceso, rectificación, oposición y cancelación de datos.
- 2.-Emitir las autorizaciones previstas en la Ley o en sus disposiciones reglamentarias.

3.-Dictar, en su caso, y sin perjuicio de las competencias de otros órganos, las instrucciones precisas para adecuar los tratamientos a los principios de la Ley.

4.-Atender las peticiones y reclamaciones formuladas por las personas afectadas.

5.-Proporcionar información a las personas acerca de sus derechos en materia de tratamiento de los datos de carácter personal.

6.-Requerir a los responsables y los encargados de los tratamientos, previa audiencia de éstos, la adopción de las medidas necesarias para la adecuación del tratamiento de datos a las disposiciones de esta Ley y, en su caso, ordenar la cesación de los tratamientos y la cancelación de los ficheros, cuando no se ajuste a sus disposiciones.

7.-Ejercer la potestad sancionadora en los términos previstos por la ley orgánica de protección da datos.

8.-Informar, con carácter preceptivo, los proyectos de disposiciones generales que desarrollen esta Ley.

9.-Recabar de los responsables de los ficheros cuanta ayuda e información estime necesaria para el desempeño de sus funciones.

10.-Velar por la publicidad de la existencia de los ficheros de datos con carácter personal, a cuyo efecto publicará periódicamente una relación de dichos ficheros con la información adicional que el Director de la Agencia determine.

11.-Redactar una memoria anual y remitirla al Ministerio de Justicia.

12.-Ejercer el control y adoptar las autorizaciones que procedan en relación con los movimientos internacionales de datos, así como desempeñar las funciones de cooperación internacional en materia de protección de datos personales.

13.-Velar por el cumplimiento de las disposiciones que la Ley de la Función Estadística Pública establece respecto a la recogida de datos estadísticos y al secreto estadístico, así como dictar las instrucciones precisas, dictaminar sobre las condiciones de seguridad de los ficheros constituidos con fines exclusivamente estadísticos

Las resoluciones de la Agencia Española de Protección de Datos se harán públicas, una vez hayan sido notificadas a los interesados. La publicación se realizará preferentemente a través de medios informáticos o telemáticos.

11.3.6 Infracciones y Sanciones.

Los responsables de los ficheros y los encargados de los tratamientos estarán sujetos al régimen sancionador establecido en la presente Ley.

Las infracciones se calificarán como leves, graves o muy graves.

Son infracciones leves:

1.-No remitir a la Agencia Española de Protección de Datos las notificaciones previstas en esta Ley o en sus disposiciones de desarrollo.

2.-No solicitar la inscripción del fichero de datos de carácter personal en el Registro General de Protección de Datos.

3.-El incumplimiento del deber de información al afectado acerca del tratamiento de sus datos de carácter personal cuando los datos sean recabados del propio interesado.

4.-La transmisión de los datos a un encargado del tratamiento sin dar cumplimiento a los deberes formales establecidos en la Ley.

Son infracciones graves:

1.-Proceder a la creación de ficheros de titularidad pública o iniciar la recogida de datos de carácter personal para los mismos, sin autorización de disposición general, publicada en el Boletín Oficial del Estado o diario oficial correspondiente.

2.-Tratar datos de carácter personal sin recabar el consentimiento de las personas afectadas, cuando el mismo sea necesario conforme a lo dispuesto en la Ley y sus disposiciones de desarrollo.

3.-Tratar datos de carácter personal o usarlos posteriormente con conculcación de los principios y garantías establecidos en la Ley y las disposiciones que lo desarrollan, salvo cuando sea constitutivo de infracción muy grave.

4.-La vulneración del deber de guardar secreto acerca del tratamiento de los datos de carácter personal

5.-El impedimento o la obstaculización del ejercicio de los derechos de acceso, rectificación, cancelación y oposición.

6.-El incumplimiento del deber de información al afectado acerca del tratamiento de sus datos de carácter personal cuando los datos no hayan sido recabados del propio interesado.

7.-El incumplimiento de los restantes deberes de notificación o requerimiento al afectado

8.-Mantener los ficheros, locales, programas o equipos que contengan datos de carácter personal sin las debidas condiciones de seguridad que por vía reglamentaria se determinen.

9.-No atender los requerimientos o apercibimientos de la Agencia Española de Protección de Datos o no proporcionar a aquélla cuantos documentos e informaciones sean solicitados por la misma.

10.-La obstrucción al ejercicio de la función inspectora.

11.-La comunicación o cesión de los datos de carácter personal sin contar con legitimación para ello salvo que la misma sea constitutiva de infracción muy grave.

Son infracciones muy graves:

1.-La recogida de datos en forma engañosa o fraudulenta.

2.-Tratar o ceder los datos de carácter personal especialmente protegidos (ideología, afiliación sindical, religión y creencias, origen racial, a la salud y a la vida sexual, comisión de infracciones penales o administrativas)

3.-No cesar en el tratamiento ilícito de datos de carácter personal cuando existiese un previo requerimiento del Director de la Agencia Española de Protección de Datos para ello.

4.-La transferencia internacional de datos de carácter personal con destino a países que no proporcionen un nivel de protección equiparable sin

autorización del Director de la Agencia Española de Protección de Datos salvo en los supuestos en los que dicha autorización no resulta necesaria.

Tipo de sanciones.

Las infracciones leves serán sancionadas con multa de 900 a 40.000 euros.

Las infracciones graves serán sancionadas con multa de 40.001 a 300.000 euros.

Las infracciones muy graves serán sancionadas con multa de 300.001 a 600.000 euros.

La cuantía de las sanciones se graduará atendiendo a los siguientes criterios:

a.-El carácter continuado de la infracción.

b.-El volumen de los tratamientos efectuados.

c.-La vinculación de la actividad del infractor con la realización de tratamientos de datos de carácter personal.

d.-El volumen de negocio o actividad del infractor.

e.-Los beneficios obtenidos como consecuencia de la comisión de la infracción.

f.-El grado de intencionalidad.

g.-La reincidencia por comisión de infracciones de la misma naturaleza.

h.-La naturaleza de los perjuicios causados a las personas interesadas o a terceras personas.

i.-La acreditación de que con anterioridad a los hechos constitutivos de infracción la entidad imputada tenía implantados procedimientos adecuados de actuación en la recogida y tratamiento de los datos de carácter personal, siendo la infracción consecuencia de una anomalía en el funcionamiento de dichos procedimientos no debida a una falta de diligencia exigible al infractor.

j.-Cualquier otra circunstancia que sea relevante para determinar el grado de antijuridicidad y de culpabilidad presentes en la concreta actuación infractora.

11.4 Real Decreto 1720/2007 por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal

11.4.1 Introducción

La Ley Orgánica 15/1999, de 13 de diciembre de Protección de datos de carácter personal adaptó nuestro ordenamiento a lo dispuesto por la Directiva 95/46/CE del Parlamento Europeo y del Consejo de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos, derogando a su vez la hasta entonces vigente Ley Orgánica 5/1992, de 29 de octubre, de Regulación del tratamiento automatizado de datos de carácter personal.

El Reglamento comparte con la Ley Orgánica la finalidad de hacer frente a los riesgos que para los derechos de la personalidad pueden suponer el

acopio y tratamiento de datos personales. Por ello, ha de destacarse que esta norma reglamentaria nace con la vocación de no reiterar los contenidos de la norma superior y de desarrollar, no sólo los mandatos contenidos en la Ley Orgánica de acuerdo con los principios que emanan de la Directiva, sino también aquellos que en estos años de vigencia de la Ley se ha demostrado que precisan de un mayor desarrollo normativo.

El reglamento parte de la necesidad de dotar de coherencia a la regulación reglamentaria en todo lo relacionado con la transposición de la Directiva y de desarrollar los aspectos novedosos de la Ley Orgánica 15/1999, junto con aquellos en los que la experiencia ha aconsejado un cierto grado de precisión que dote de seguridad jurídica al sistema.

11.4.2 Análisis

El título I contempla el objeto y ámbito de aplicación del reglamento. A lo largo de la vigencia de la Ley Orgánica 15/1999, se ha advertido la conveniencia de aclarar qué se entiende por ficheros y tratamientos relacionados con actividades personales o domésticas, aspecto muy relevante dado que está excluido de la normativa sobre protección de datos de carácter personal.

Se aporta un conjunto de definiciones que ayudan al correcto entendimiento de la norma, lo que resulta particularmente necesario en un ámbito tan tecnificado como el de la protección de datos personales. Por otra parte, fija el criterio a seguir en materia de cómputo de plazos con el fin de homogeneizar esta cuestión evitando distinciones que suponen diferencias de trato de los ficheros públicos respecto de los privados.

El título II, se refiere a los principios de la protección de datos. Reviste particular importancia la regulación del modo de captación del consentimiento atendiendo a aspectos muy específicos como el caso de

los servicios de comunicaciones electrónicas y, muy particularmente, la captación de datos de los menores. Asimismo, se ofrece lo que no puede definirse sino como un estatuto del encargado del tratamiento, que sin duda contribuirá a clarificar todo lo relacionado con esta figura. Las previsiones en este ámbito se completan con lo dispuesto en el título VIII en materia de seguridad dotando de un marco coherente a la actuación del encargado.

El título III se ocupa de una cuestión tan esencial como los derechos de las personas en este ámbito. Estos derechos de acceso, rectificación, cancelación y oposición al tratamiento, según ha afirmado el Tribunal Constitucional en su sentencia número 292/2000, constituyen el haz de facultades que emanan del derecho fundamental a la protección de datos y sirven a la capital función que desempeña este derecho fundamental: garantizar a la persona un poder de control sobre sus datos personales, lo que sólo es posible y efectivo imponiendo a terceros los mencionados deberes de hacer.

A continuación, los títulos IV a VII permiten clarificar aspectos importantes para el tráfico ordinario, como la aplicación de criterios específicos a determinado tipo de ficheros de titularidad privada que por su trascendencia lo requerían -los relativos a la solvencia patrimonial y crédito y los utilizados en actividades de publicidad y prospección comercial-, el conjunto de obligaciones materiales y formales que deben conducir a los responsables a la creación e inscripción de los ficheros, los criterios y procedimientos para la realización de las transferencias internacionales de datos, y, finalmente, la regulación de un instrumento, el código tipo, llamado a jugar cada vez un papel más relevante como elemento dinamizador del derecho fundamental a la protección de datos.

El título VIII regula un aspecto esencial para la tutela del derecho fundamental a la protección de datos, la seguridad, que repercute sobre

múltiples aspectos organizativos, de gestión y aún de inversión, en todas las organizaciones que traten datos personales. La repercusión del deber de seguridad obligaba a un particular rigor ya que en esta materia han confluído distintos elementos muy relevantes. Por una parte, la experiencia dimanante de la aplicación del Real Decreto 994/1999 permitía conocer las dificultades que habían enfrentado los responsables e identificar los puntos débiles y fuertes de la regulación. Por otra, se reclamaba la adaptación de la regulación en distintos aspectos. En este sentido, el reglamento trata de ser particularmente riguroso en la atribución de los niveles de seguridad, en la fijación de las medidas que corresponda adoptar en cada caso y en la revisión de las mismas cuando ello resulte necesario. Por otra parte, ordena con mayor precisión el contenido y las obligaciones vinculadas al mantenimiento del documento de seguridad. Además, se ha pretendido regular la materia de modo que contemple las múltiples formas de organización material y personal de la seguridad que se dan en la práctica. Por último, se regula un conjunto de medidas destinadas a los ficheros y tratamientos estructurados y no automatizados que ofrezca a los responsables un marco claro de actuación.

Finalmente en el título IX, dedicado a los procedimientos tramitados por la Agencia Española de Protección de Datos, se ha optado por normar exclusivamente aquellas especialidades que diferencian a los distintos procedimientos tramitados por la Agencia de las normas generales previstas para los procedimientos en la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común, cuya aplicación se declara supletoria al presente Reglamento.

Autor:

Alfonso García Magariños

Director Asesoría Jurídica Municipal Concello de A Coruña

**12. PLAN DIRECTOR DE
SEGURIDAD DE INFORMACIÓN
DE LA XUNTA DE GALICIA.
DECRETO 230/2008, POR EL
QUE SE ESTABLECEN LAS
NORMAS DE BUENAS
PRÁCTICAS EN LA UTILIZACIÓN
DE LOS SISTEMAS DE
INFORMACIÓN DE LA
ADMINISTRACIÓN DE LA
COMUNIDAD AUTÓNOMA DE
GALICIA. ADMINISTRACIÓN
ELECTRÓNICA Y SOCIEDAD DE
LA INFORMACIÓN.**

Tema 12.- Plan Director de Seguridad e Información de la Xunta de Galicia. Decreto 230/2008 por el que se establecen las normas de buenas practicas en la utilización de sistemas de informacion en la Administración de la CCAA de Galicia.

INDICE

12.1 Plan Director de Seguridad e Información de la Xunta de Galicia

- 12.1.1.Introducción
- 12.1.2 Responsabilidades
- 12.1.3 Objetivos
- 12.1.4 Agentes involucrados

12.2 Decreto 230/2008 por el que se establecen las normas de buenas practicas en la utilización de sistemas de informacion en la Administración de la CCAA de Galicia.

- 12.2.1 Objeto y ámbito de aplicación
- 12.2.2 Órganos responsables y de coordinación
- 12.2.3 Acceso a información, redes de comunicaciones e Internet
- 12.2.4 Servicio de mensajería corporativo
- 12.2.5 Deber de personas usuarias
- 12.2.6 Inspección
- 12.2.7 Responsabilidad de personas usuarias que tengan la condición de empleados públicos

12.1 PLAN DIRECTOR DE SEGURIDAD E INFORMACION DE LA XUNTA DE GALICIA

12.1.1 Introducción.

El Plan Director de Seguridad de la Información establece las actuaciones a llevar a cabo por la Administración de la Comunidad Autónoma de Galicia en materia de seguridad de la información así como los agentes involucrados y sus respectivas responsabilidades. Además, define las directrices necesarias para gestionar de forma segura los sistemas de información de la Administración y manifiesta el reconocimiento de la importancia que tiene la seguridad de la información sobre la confianza que los ciudadanos depositan en la administración.

Las tecnologías de la información y las comunicaciones (TIC) constituyen un instrumento de alto nivel estratégico por su potencial para impulsar la modernización de la Administración de la Comunidad Autónoma Gallega, así como por su capacidad para estimular y sustentar el desarrollo social y económico de Galicia.

Este plan contempla todos los sistemas de información de la Xunta de Galicia. Nace con la voluntad de ser aplicado progresivamente al conjunto de Consellerías de la Administración autonómica, a sus organismos autónomos, sociedades públicas, fundaciones del sector público autonómico y demás entidades de derecho público vinculadas o dependientes de la Comunidad Autónoma de Galicia. Sin perjuicio del anterior, está directamente destinado a garantizar la seguridad de los sistemas corporativos.

Dentro de este plan, corresponde a la Secretaría General de Modernización e Innovación Tecnológica el análisis de necesidades, planificación, diseño, gestión e implantación de los sistemas de información y elementos tecnológicos en los órganos de la Administración de Justicia en Galicia, en coordinación con las administraciones y órganos competentes en la materia de sistemas de información de justicia.

En este Plan también se perfilan una serie de iniciativas orientadas a asesorar y sensibilizar al personal de la Administración Local en materia de protección de datos, de seguridad informática y de acceso electrónico de los ciudadanos a los servicios públicos.

El alcance temporal del presente plan abarca el período 2010 - 2014. En el plan se efectúa una priorización de las distintas actuaciones en orden a su urgencia e impacto. La seguridad de la información requiere una visión global que recoja una mejora pragmática y asequible a corto plazo y, a la vez, un modelo objetivo ambicioso y de largo plazo.

12.1.2 Responsabilidades.

A la Secretaría General de Modernización e Innovación Tecnológica según el Decreto 325/2009, del 18 de junio, de estructura orgánica de los órganos superiores dependientes de la Presidencia de la Xunta de Galicia, le corresponde establecer la política de seguridad informática corporativa de la Xunta de Galicia y la promoción de buenas prácticas en lo relativo al tratamiento de datos de carácter personal. A través del Centro de Seguridad de la Información (CSI), elaborará los planes, medidas y directrices de seguridad informática, supervisará el cumplimiento de todas las medidas de seguridad informática en los diferentes ámbitos y departamentos y diseñará y realizará las acciones encaminadas a garantizar el cumplimiento de la normativa vigente en materia de

Protección de Datos de Carácter Personal en la Administración de la Comunidad Autónoma.

Las Consellerías de la Administración de la Comunidad Autónoma de Galicia, según el Decreto 230/2008, de 18 de septiembre, por lo que se establecen las normas de buenas prácticas en la utilización de los sistemas de información de la Administración de la Comunidad Autónoma de Galicia designarán el órgano que será responsable de los sistemas de información de su propiedad y de establecer los medios tecnológicos que necesitan las personas a su servicio, así como de velar por el correcto funcionamiento de las infraestructuras y del equipamiento informático y de comunicaciones de que dispongan. Cuando estas atribuciones no estén asignadas reglamentariamente a un órgano, la designación se hará por las secretarías generales de cada departamento. Asimismo, cada departamento de la Xunta de Galicia deberá designar a una persona como responsable de seguridad

El Comité de Seguridad de los Sistemas de Información (CSSI), creado en el Decreto de buenas prácticas, es un órgano colegiado formado por las personas responsables de seguridad de los distintos departamentos de la Xunta de Galicia, que tiene como objetivo definir la política de seguridad corporativa. Este comité estará coordinado y asesorado por el órgano competente en materia de seguridad corporativa a través del Centro de seguridad de la Información

Las personas que prestan servicios a la Administración de la Comunidad Autónoma de Galicia, además de cumplir a con las medidas indicadas en el Decreto de buenas prácticas tienen deber de sigilo y confidencialidad respecto de la información a la que puedan tener acceso por razón de sus funciones, limitándose a emplearla para el estricto cumplimiento de las tareas encomendadas.

La Xunta de Galicia expresa su compromiso con la seguridad, de forma que dará a conocer este Plan Director de Seguridade entre todo el persoal que preste sus servicios en la Administración de la Comunidade Autónoma, velará por su cumplimiento e impulsará la implantación y difusión de la gestión de la seguridad de la información en las personas y empresas de Galicia

12.1.3 Objetivos

El presente plan trata de mejorar el nivel de seguridad existente en la Administración de la Comunidad Autónoma de Galicia. Esto significa gestionar la seguridad de la información de tal forma que las medidas de seguridad implantadas alcancen un alto grado de efectividad que reduzca al máximo el impacto de las incidencias de seguridad

Con este fin, la Xunta de Galicia se fija, en materia de seguridad de la información, los siguientes objetivos:

- . Concienciar e implicar en la gestión de la seguridad a toda la dirección y personal de la Administración autonómica, a sus organismos autónomos, sociedades públicas, fundaciones del sector público autonómico y demás entidades de derecho público vinculadas o dependientes de la Comunidad Autónoma de Galicia, contando con la colaboración de proveedores y especialistas
- . Promover el máximo aprovechamiento de las tecnologías de la información y las comunicaciones en la actividad administrativa y asegurar a la vez el respecto de las garantías y derechos de los ciudadanos en sus relaciones con la Administración, estableciendo que la seguridad en los sistemas sea atendida, revisada y auditada por personal calificado y que su configuración y diseño garanticen la seguridad por defecto.

- . Gestionar los riesgos que puedan afectar a los componentes de los sistemas de información para poder identificarlos y evaluarlos y tomar las medidas de seguridad informática adecuadas (físicas, lógicas, técnicas, normativas y organizativas).
- . Garantizar la disponibilidad de los sistemas de información de acuerdo con los requisitos establecidos para los servicios prestados, gestionando y controlando el acceso físico y lógico, certificando que los productos de seguridad usados para dar servicio al ciudadano cumplen con los estándares establecidos, revisando el nivel de actualización, asegurando la confidencialidad de la información gestionada por la Administración y evitando accesos o alteraciones indebidas y pérdidas de información, implantando la seguridad perimetral necesaria ante los posibles riesgos de interconexión con otros sistemas de redes externas y registrando toda actividad de los usuarios que accedan al sistema.
- . Gestionar la continuidad de los servicios TIC proporcionados por la Administración, estableciendo los sistemas de protección a nivel organizativo, lógico y físico que permitan reducir la probabilidad de que se produzca un incidente y, en caso de que se produzca, acortar el tiempo de vuelta a la normalidad y minimizar su impacto.
- . Evaluar periódicamente el sistema de gestión de seguridad, basándose en el registro y tratamiento de incidencias, garantizando que las medidas implantadas alcancen un nivel de madurez optimizado con políticas, normas, procedimientos y estructuras organizacionales que promuevan la concienciación y formación continua de los usuarios en temas de seguridad de la información.
- . Proporcionar un contorno de seguridad que garantice el cumplimiento de los requisitos legales para la validez y eficacia de los procedimientos administrativos que utilicen los medios electrónicos, informáticos y

telemáticos, estableciendo para cada sistema de información responsables diferenciados de la información, del servicio y de la seguridad.

. La Xunta de Galicia actuará como elemento generador de e-confianza que promueva un tejido empresarial sólido en seguridad de la información e incremente la confianza y la protección de los derechos de la ciudadanía gallega en la Sociedad de la información.

12.1.4 Agentes involucrados

1.- Subdirección general de calidad, interoperabilidad y seguridad (sxcis). La Subdirección General de Calidad, Interoperabilidad y Seguridad (SXCIS) de la SXMIT tiene, entre sus funciones, la de que establezca la política de seguridad informática corporativa de la Xunta de Galicia y la de promover las buenas prácticas en lo relativo al tratamiento de datos de carácter personal.

Para eso, se creó, dentro de la SXCIS, el Servicio de Calidad y Seguridad Informática con las siguientes competencias en materia de seguridad de la información:

. Dirección de las políticas corporativas de seguridad informática de la Xunta de Galicia a través del Centro de Seguridad de la Información.

. Elaboración de los planes, medidas y directrices de seguridad informática para el conjunto de órganos y unidades de la Xunta.

. Supervisión del cumplimiento de todas las medidas de seguridad informática en los distintos ámbitos y departamentos de la Xunta.

. Diseño y realización de acciones encaminadas a garantizar el cumplimiento de la normativa vigente en materia de protección de datos

de carácter personal en la Administración de la Comunidad Autónoma de Galicia

2.- Centro de Seguridad de la información (CSI)

El Centro de Seguridad de la Información tiene una función transversal dentro de la Xunta. Entre sus atribuciones, se encuentra la resolución de incidencias de seguridad y el asesoramiento a las distintas consejerías en materia de seguridad de la información, tanto en materia de protección de datos como en la evaluación de soluciones de seguridad

El CSI supervisará la seguridad de los sistemas corporativos de la Administración de la Comunidad Autónoma de Galicia y será el centro de resolución de incidentes de seguridad (ataques activos y pasivos, pérdida de información, falta de disponibilidad, etc.).

Dentro de los servicios de apoyo y asesoramiento a las distintas consejerías en su cometido de adecuación de sus sistemas de información a las exigencias de la legislación vigente en materia de protección de datos, el Centro de Seguridad de la Información será el interlocutor con la Agencia Española de Protección de Datos.

El Centro de Seguridad de la Información se encargará de evaluar, analizar y probar en una contornea controlada las distintas soluciones de seguridad existentes en el mercado y de aplicación e interés para la Administración de la Comunidad Autónoma de Galicia. Los resultados de estas evaluaciones se reflejarán en una serie de informes de análisis y de estudios comparativos. Asimismo, podrán realizarse demostraciones a las consejerías, ya sea a través de la contornea de pruebas o mediante charlas divulgativas. Estas evaluaciones podrán realizarse en función de las necesidades detectadas por el propio Centro de Seguridad de la

Información o en base a la valoración de peticiones de los distintos departamentos y podrán referirse la seguridad perimetral, de centros de proceso de datos, de aplicaciones, de puesto informático, etc.

Con el fin de promover el desarrollo del presente Plan en las diferentes consejerías, se incluirán dentro de las funciones del CSI, las siguientes tareas

- . Realizar el seguimiento y revisar el presente Plan Director de forma periódica.
- . Apoyar y asesorar a las consejerías para alcanzar los objetivos fijados en el presente Plan
- . Impulsar y apoyar el Comité de Seguridad de los Sistemas de Información de la Xunta.
- . Velar por la mejora del nivel de seguridad de la información de la Administración de la Comunidad Autónoma de Galicia.

Para el desarrollo de estas funciones el Centro de Seguridad de la Información dispone de un amplio conocimiento en el campo de la seguridad de la información, y podrá contar con el asesoramiento de expertos externos.

3.- Consellerías da Xunta .

Las Consellerías son las máximas responsables del estado de seguridad de sus sistemas de información. Deberán velar por su seguridad garantizando la confidencialidad, integridad y disponibilidad de la información. Son también las responsables de acometer las actuaciones recomendadas en el presente Plan Director y alcanzar los objetivos marcados.

Dentro de cada consellería, el personal de soporte técnico desempeñará funciones de asesoría técnica, ejecución, propuesta, coordinación y supervisión de los planes de informatización.

Asimismo, los órganos responsables de los sistemas de información de cada departamento de la Xunta de Galicia, con el apoyo del personal de soporte técnico, serán los competentes para velar por el cumplimiento de los objetivos de este Plan. Les corresponderá a ellos asegurarse de que los equipos se utilizan adecuadamente y atendiendo a la finalidad a la que están destinados.

4.- Comité de seguridad de sistemas de información.(CSSI).

El Comité de Seguridad de los Sistemas de Información, tiene como objetivo establecer el marco de trabajo que impulse la implantación y difusión de la gestión de la seguridad de la información en el ámbito de la Administración de la Comunidad Autónoma de Galicia.

Los miembros del Comité se reúnen para revisar el estado de la seguridad de la información en la Administración de la Comunidad Autónoma de Galicia, aprobar las políticas de seguridad, revisar y aprobar los proyectos de seguridad, revisar los procesos de monitorización de las incidencias de seguridad y realizar otras tareas de gestión de la seguridad de alto nivel que sean necesarias.

Las principales funciones asumidas por este Comité son las que se presentan a continuación:

- .Identificar, revisar y proponer objetivos estratégicos en materia de seguridad de la información.
- . Establecer roles y responsabilidades en materia de seguridad de la información.

- . Proponer y aprobar políticas, normas y directrices de seguridad de la información para la Xunta de Galicia y velar por su cumplimiento.
- . Proveer un soporte al esfuerzo de seguridad de la información, dando una visión más transversal para el análisis y decisiones, a fin de lograr la mejor relación coste-efectividad en su gestión.
- . Constituir el canal primario de discusión de aspectos de seguridad de la información que se deban abordar en la Administración de la Comunidad Autónoma de Galicia.
- . Apoyar a los coordinadores de seguridad en el desarrollo de estrategias de mitigación de riesgos, basándose en el conocimiento que sus integrantes tienen de sus respectivas áreas.
- . Impulsar la implantación y difusión de la gestión de la seguridad de la información
- . Revisar y aprobar anualmente la Política de Seguridad.
- . Realizar otras tareas de gestión de la seguridad de alto nivel que sean necesarias.
- . Revisar periódicamente el presente Plan Director.

Para el desarrollo de estas funciones, el CSSI podrá contar con el apoyo, en materia de actualización normativa, de la Asesoría Jurídica General. Puntualmente, podrá solicitar la colaboración de la Junta Consultiva de Contratación Administrativa de la Xunta de Galicia y del equipo de auditores y analistas de gestión del rendimiento y calidad forma de la Dirección General de Evaluación y Reforma Administrativa de la Consellería de Presidencia, Administraciones Públicas y Justicia.

5.- Asesoría Jurídica General.

El papel del derecho en las tecnologías de la información es amplio y abarca varios campos como pueden ser los que enunciamos a continuación:

- . Protección de datos de carácter personal.
- . Propiedad Intelectual.

- . Servicios de la sociedad de la información.
- . Firma electrónica.
- . Constitución de prueba por medios informáticos.
- . Uso de herramientas informática por el personal.

La Asesoría Jurídica General, acercará al Comité de Seguridad de los Sistemas de Información su conocimiento en el ámbito legal como apoyo a la actualización normativa, mediante la emisión de dictámenes o informes en derecho, la formulación de criterios generales de asesoramiento jurídico y el estudio de los proyectos de reglamentos con examen de su adecuación al ordenamiento constitucional, estatutario y legal.

Por su conocimiento en materias jurídicas vinculadas al derecho de las tecnologías de la información, asegurará que las iniciativas del Comité de Seguridad de los Sistemas de Información y de la Secretaría General competente son acordes a la legislación vigente aplicable. Por otra banda, la Asesoría Jurídica de cada Consellería le prestará un servicio de apoyo en las materias anteriormente mencionadas.

6.- Junta Consultiva Contratación Administrativa

La Junta Consultiva de Contratación Administrativa de la Comunidad Autónoma de Galicia, esta adscrita a la Consejería responsable de los asuntos tributarios como un órgano consultivo específica en materia de contratación administrativa.

Dentro de las funciones y competencias de la Junta , se encuentran:

∴. Elaborar y proponer las normas, instrucciones y medidas que considere precisas para la mejora y eficacia de la contratación de la Administración autonómica, sus organismos y sociedades, fundaciones del sector público y demás entidades de derecho público de ella dependientes.

. Realizar estudios e investigaciónes sobre contratación administrativa, trasladando a los órganos de contratación las recomendaciones que se deriven a la sazón

La Xunta de Galicia recurre a proveedores para la prestación de servicios como pueden ser desarrollo de nuevas aplicaciones, infraestructuras, externalización de una actividad.

Es importante para garantizar la seguridad de la información gestionar la actuación de los proveedores. Por eso es necesario identificar los requisitos de seguridad vinculados a la prestación del servicio e incluirlos en los contratos.

Por tanto, la Junta Consultiva de Contratación Administrativa trasladará a los órganos de contratación todas las recomendaciones que considere oportunas en orden a que se incluyan cláusulas sobre disponibilidad, confidencialidad, integridad y autenticidad de la información manejada por los sistemas de información.

Con la finalidad de asegurar este aspecto, ejercerá una función de análisis y propuesta de inclusión en las frunces de contratación de cláusulas medio ambientales, sociales, de comercio justo y de protección de datos que los adjudicatarios deberán cumplir en función del servicio contratado.

7. Equipo de auditores e analistas de gestión do rendimientto y calidad

El equipo de auditores y analistas de gestión del rendimiento y calidad forma de la Dirección General de Evaluación y Reforma Administrativa de la Consellería de Presidencia, Administraciones Públicas y Justicia.

Esta Dirección tiene entre otras las siguientes competencias:

. En materia de evaluación del rendimiento y gestión de la calidad:

1.-El desarrollo y la gestión de las medidas para la implantación de sistemas de mejora de la calidad tendiendo a promover la mejora continua de los servicios de la Administración autonómica, tanto de los que se prestan directamente al ciudadano como los servicios internos.

. En materia de racionalización y simplificación de procedimientos administrativos:

1.-Coordinar la aplicación de la normativa europea y estatal sobre simplificación y mejora de la gestión administrativa.

. En materia de información administrativa y atención al ciudadano:

1.-Evaluar periódicamente la calidad del sistema de información administrativa, proponiendo las medidas de mejoras convenientes con el fin de facilitar a los ciudadanos y usuarios los servicios que solicitan.

2.- Tramitar, sin perjuicio de las competencias que corresponden a las secretarías generales y en colaboración con estas, las quejas y las propuestas que formulen los ciudadanos y usuarios sobre el funcionamiento de los servicios prestados por la Administración autonómica de acuerdo con lo establecido en los artículos 25 y siguientes del Decreto 164/2005, del 16 de junio.

Entre los principios de protección de datos se encuentran el principio de información y el principio de consentimiento. El principio de información, que se regula en el artículo 5 de la LOPD, establece que el interesado debe estar informado el momento de la recogida de datos. En cuanto al principio de consentimiento exige que se obtenga el consentimiento del afectado para el tratamiento de los datos, salvo excepciones recogidas en la LOPD. Estos derechos fundamentales deben garantizarse no sólo para cumplir con la legislación vigente sino también para garantizar la calidad del servicio prestado al ciudadano.

Los procedimientos administrativos son unos de los puntos en los que es necesario prestar atención teniendo en cuenta que recogen, a menudo, datos de carácter personal.

Cuando la recogida de datos se realiza mediante formulario bien sea en formato papel o en formato electrónico se introducirá una cláusula informativa en el formulario cubriendo las exigencias del artículo 5 de la Ley Orgánica protección datos. Con respecto al consentimiento se recogerá mediante la firma del formulario papel y la aprobación del formulario electrónico.

El equipo revisa los procedimientos administrativos antes de su publicación en el DOG.

12.2 DECRETO 230/2008 DE 18 DE SEPTIEMBRE POR EL QUE SE ESTABLECEN BUENAS PRACTICAS

12.2.1 Objeto y ámbito de aplicación.

Este Decreto tiene por objeto regular las normas de utilización de los sistemas de información y de comunicaciones, fijos y móviles, de los que dispone la Administración de la Comunidad Autónoma de Galicia, estableciendo los derechos y los deberes de las personas usuarias de estos sistemas en lo relativo a su seguridad y buen uso.

La finalidad de la presente norma es conseguir el mejor aprovechamiento de las tecnologías de la información y las comunicaciones en la actividad administrativa, así como garantizar la protección de la información de las personas y de las empresas en sus relaciones con la Administración de la Comunidad Autónoma de Galicia

Será de aplicación a todas las personas que presten servicios para la Administración de la Comunidad Autónoma de Galicia y utilicen para el desempeño de sus funciones los sistemas de información o las redes de comunicaciones propiedad de la Administración autonómica.

El contenido de este Decreto será de aplicación en la utilización del equipamiento informático y de comunicaciones, fijo y móvil, incluyendo cualquier dispositivo puesto a disposición de las personas que prestan servicios para la Administración autonómica

12.2.2 Órganos responsables y de coordinación.

1.- Órganos responsables

Las secretarías generales designarán, dentro de cada departamento de la Xunta de Galicia, al órgano que será responsable de los sistemas de su propiedad y de establecer los medios tecnológicos que necesitan las personas a su servicio, así como de velar por el correcto funcionamiento de las infraestructuras y del equipamiento informático y de comunicaciones de que dispongan. En aquellos casos en que dichas atribuciones ya estén asignadas reglamentariamente a un órgano, no será precisa esta designación.

Estos órganos, con el apoyo del personal de soporte técnico, son los competentes para velar por el cumplimiento de las normas contenidas en este Decreto. Le corresponderá a ellos asegurarse de que los equipos se utilizan adecuadamente y atendiendo a la finalidad a la que están destinados.

Para el mejor cumplimiento de estas atribuciones sobre los sistemas, cada departamento de la Xunta de Galicia deberá designar a una persona como responsable de seguridad. Las personas designadas deberán comunicar,

dentro de su ámbito, las normas, procedimientos y políticas de seguridad para su conocimiento por el personal, así como impulsar su implantación.

2.- Órganos de coordinación.

Son órganos de coordinación:

a) La Comisión de Informática de la Xunta de Galicia, regulada por el Decreto 290/1992, de 8 de octubre .

b) La Dirección General de Calidad y Evaluación de las Políticas Públicas de la Consellería de Presidencia, Administraciones Públicas y Justicia.

c) El Comité de Seguridad de los Sistemas de Información de la Xunta de Galicia. Es un órgano colegiado, adscrito a la Consellería de Presidencia, Administraciones Públicas y Justicia, formado por las personas responsables de seguridad de los distintos departamentos de la Xunta de Galicia, que tiene como objetivo definir la política de seguridad corporativa. Este comité estará coordinado y asesorado por la dirección general competente a través del Centro de Seguridad Informática. Su régimen básico de funcionamiento se regulará por orden de la Consellería de Presidencia, Administraciones Públicas y Justicia.

12.2.3 Acceso a información, redes de comunicaciones e Internet.

1.- Acceso a informacion

Las personas usuarias tendrán autorizado el acceso únicamente a aquella información y recursos que precisen para el desarrollo de sus funciones. El acceso a la información contenida en los sistemas de la Administración de la Comunidad Autónoma de Galicia estará restringido a aquellas personas poseedoras de la correspondiente autorización, que será personal e

intransferible y compuesta al menos de un identificador y de una contraseña.

Los órganos responsables de los sistemas establecerán los mecanismos adecuados para evitar que las personas puedan acceder o modificar datos sin autorización. Exclusivamente el personal de soporte técnico, conforme a los criterios establecidos por el responsable de cada uno de los sistemas de información, podrá conceder, alterar o anular la autorización de acceso a los datos y recursos.

No se podrán obtener derechos de acceso a la información distintos a los autorizados, ni se utilizará el identificador de otra persona, aunque se disponga de permiso de ésta, salvo indicación expresa y puntual del órgano responsable de dicha información o recurso. Con este fin, las unidades de personal de los distintos departamentos de la Xunta de Galicia comunicarán al servicio de informática todos los cambios que se produzcan en los puestos de trabajo.

Las personas al servicio de la Administración de la Comunidad Autónoma de Galicia deberán velar por la seguridad de los datos a los que tengan acceso por las tareas de su puesto de trabajo, especialmente los confidenciales o de carácter personal.

Por motivos de seguridad, la Administración de la Comunidad Autónoma de Galicia podrá monitorizar los accesos a la información contenida en sus sistemas, cumpliendo los requisitos que al efecto establezca la normativa vigente.

2 Redes de comunicaciones.

. La conexión a la red corporativa de la Xunta de Galicia será facilitada por la Dirección General de Calidad y Evaluación de las Políticas Públicas en

uso de las competencias atribuidas en el decreto de estructura orgánica de la Consellería de Presidencia, Administraciones Públicas y Justicia.

No se podrá conectar a esta red de comunicaciones ningún dispositivo por medios distintos a los definidos y autorizados por el Centro de Gestión de Red de dicha dirección general.

En el caso de aquellas redes de comunicaciones de la Administración de la Comunidad Autónoma de Galicia ya gestionadas por otras consellerías, la conexión a las mismas será facilitada por el órgano responsable de cada una de ellas.

3 Internet

La Administración de la Comunidad Autónoma de Galicia proveerá de conexión a Internet a las personas a su servicio con una finalidad exclusivamente profesional.

El equipo que tenga acceso a Internet, a través de las redes de comunicación gestionadas por la Administración de la Comunidad Autónoma de Galicia, deberá disponer de «software» de protección frente a virus y demás códigos maliciosos.

Los datos de conexión y tráfico serán monitorizados y se guardará un registro durante el tiempo que establece la normativa vigente en cada supuesto. En ningún caso esta retención de datos afectará al secreto de las comunicaciones.

Las conexiones a sitios Web que contengan material ofensivo o software malicioso serán bloqueadas, salvo excepciones debidamente autorizadas

12.2.4 Servicio de mensajería corporativo

La Administración de la Comunidad Autónoma de Galicia proveerá de servicio de mensajería a las personas a su servicio con una finalidad exclusivamente profesional.

Por razones de seguridad y rendimiento, los órganos responsables del servicio podrán monitorizar el servicio de mensajería corporativa. Esta monitorización no será nunca selectiva o discriminatoria sino que será realizada de forma sistemática o aleatoria y sin vulneración de la intimidad personal ni del secreto de las comunicaciones.

Aquellas cuentas en las que se detecte un uso inadecuado, que se definirá en el documento de política de seguridad corporativa, podrán ser bloqueadas o suspendidas temporalmente. En ningún caso, se podrá utilizar el servicio de mensajería para:

- a) La difusión de mensajes ofensivos o discriminatorios.
- b) El uso de la cuenta de correo corporativo para expresar opiniones personales en foros temáticos fuera del ámbito de las administraciones.
- c) La difusión masiva no autorizada; suscripción indiscriminada a listas de correo o cualquier ataque con el objeto de impedir o dificultar el servicio de correo.

12.2.5 Deber de personas usuarias

Las personas que prestan servicios a la Administración de la Comunidad Autónoma de Galicia, además de cumplir con las medidas indicadas en este Decreto relativas al equipamiento informático y de comunicaciones, a las aplicaciones informáticas, a la información y al uso de los servicios corporativos, son responsables del buen uso de los medios electrónicos,

informáticos, telemáticos y de comunicaciones, fijos y móviles, puestos a su disposición para las actividades propias de las funciones que desarrollan.

No se podrá acceder a los recursos informáticos y telemáticos para desarrollar actividades que persigan o tengan como consecuencia:

- a) La degradación de los servicios.
- b) La destrucción o modificación no autorizada de la información de manera premeditada.
- c) La violación de la intimidad, del secreto de las comunicaciones y del derecho a la protección de datos personales.
- d) El deterioro intencionado del trabajo de otras personas.
- e) El uso de los sistemas de información para fines ajenos a los de la Administración.
- f) Incurrir en actividades ilícitas de cualquier tipo.
- g) Dañar intencionadamente los recursos informáticos de la Administración de la Comunidad Autónoma de Galicia o de otras instituciones.
- h) Instalar o utilizar «software» que no disponga de la licencia correspondiente.

3. Para garantizar unos mínimos de seguridad en el equipamiento asignado, se deberá:

a) Utilizar y guardar en secreto la contraseña que protege la cuenta de acceso, responsabilidad directa de la persona usuaria. Ésta debe cerrar su cuenta al final de cada sesión o cuando deja desatendido el equipo, con el fin de que no pueda ser usado por terceras personas.

b) Revisar de forma periódica sus ordenadores, eliminando cualquier virus, programa o fichero que pueda causar daños a otros equipos de la red u otras actuaciones que contravengan la legislación vigente.

c) En el caso de que su equipo contenga información importante que no esté guardada en un servidor, realizar copias de seguridad periódicas para garantizar su disponibilidad.

Las personas usuarias, en el ejercicio de sus funciones, deberán colaborar con el órgano competente en materia de seguridad de los sistemas de información y seguir sus recomendaciones y, en particular, las del Centro de Seguridad Informática, en aplicación de la política de seguridad corporativa definida por el Comité de Seguridad de los Sistemas de Información de la Xunta de Galicia.

También estarán obligadas al cumplimiento de aquellas otras medidas adicionales que especifiquen los órganos responsables de los sistemas.

12.2.6 Inspección

La Administración de la Comunidad Autónoma de Galicia, mediante los medios tecnológicos y personales que estime oportunos, revisará periódica y puntualmente, por razones de seguridad y de calidad del servicio, el estado de los equipos, dispositivos y redes de comunicaciones de su responsabilidad, así como su correcta utilización, con el objeto de verificar su correcto funcionamiento, eficiencia y el cumplimiento de las medidas y protocolos de seguridad establecidos en la legislación vigente.

La dirección general competente en materia de seguridad corporativa velará por el cumplimiento de la presente normativa e informará al Comité de Seguridad de los Sistemas de Información de la Xunta de Galicia sobre los incumplimientos o deficiencias de seguridad observados, con el objeto de que tomen las medidas oportunas.

Los servicios para los que se detecte un uso inadecuado o que no cumplan los requisitos de seguridad, que se definirán en el documento de política de seguridad corporativa, podrán ser bloqueados o suspendidos temporalmente para aquellas cuentas en las que se detecte un daño para los de los sistemas de información y de comunicaciones. El servicio se restablecerá cuando la causa de su degradación desaparezca

12.2.7 Responsabilidad de personas usuarias que tengan la condición de empleados públicos

La Administración de la Comunidad Autónoma de Galicia exigirá de los empleados públicos la responsabilidad en la que incurriesen por dolo, culpa o descuido graves de las que se deriven daños y perjuicios en sus bienes o derechos o indemnizaciones para particulares, previa instrucción del procedimiento correspondiente en los términos previstos en la normativa de aplicación.

El incumplimiento de los deberes y obligaciones impuestos por el presente Decreto, que sean constitutivos de infracción disciplinaria, según la tipificación efectuada en la normativa aplicable, dará lugar a la incoación del correspondiente procedimiento disciplinario que se tramitará conforme a lo establecido en la normativa aplicable a los empleados públicos en función de la naturaleza jurídica de su vínculo con la Administración. No obstante lo anterior, la incoación de los expedientes y la imposición de las

sanciones requerirá informe previo de la Dirección General de Calidad y Evaluación de las Políticas Públicas.

Autor:

Alfonso García Magariños

Director Asesoría Jurídica Municipal Concello de A Coruña

**13. IMPLANTACIÓN DE LA
ADMINISTRACIÓN
ELECTRÓNICA. SEDE
ELECTRÓNICA Y SERVICIOS DE
SEDE. REGISTRO
ELECTRÓNICO. EXPEDIENTE
ELECTRÓNICO. ARCHIVO
ELECTRÓNICO DE
DOCUMENTOS.
DIGITALIZACIÓN, COMPULSA
ELECTRÓNICA. FACTURA Y
LICITACIÓN ELECTRÓNICAS.**

BLOQUE: ADMINISTRACIÓN ELECTRÓNICA Y SOCIEDAD DE LA INFORMACIÓN

TEMA 13. IMPLANTACIÓN DE LA ADMINISTRACIÓN ELECTRÓNICA. SEDE ELECTRÓNICA Y SERVICIOS DE SEDE. REGISTRO ELECTRÓNICO. EXPEDIENTE ELECTRÓNICO. ARCHIVO ELECTRÓNICO DE DOCUMENTOS. DIGITALIZACIÓN, COMPULSA ELECTRÓNICA. FACTURA Y LICITACIÓN ELECTRÓNICAS.

13.1.IMPLANTACIÓN DE LA ADMINISTRACIÓN ELECTRÓNICA

13.2.SEDE ELECTRÓNICA Y SERVICIOS DE LA SEDE

13.3.REGISTRO ELECTRÓNICO

13.4.EXPEDIENTE ELECTRÓNICO

13.5.ARCHIVO ELECTRÓNICO DE DOCUMENTOS

13.6.DIGITALIZACIÓN, COMPULSA ELECTRÓNICA.

13.7.FACTURA Y LICITACIÓN ELECTRÓNICAS

13.8.REFERENCIAS

13.1.IMPLANTACIÓN DE LA ADMINISTRACIÓN ELECTRÓNICA

Según establece la Comisión Europea, la Administración electrónica se define como el uso de las Tecnologías de la Información y las Comunicaciones en las Administraciones Públicas, combinada con cambios organizativos y nuevas aptitudes, con el fin de mejorar los servicios públicos y los procesos democráticos y reforzar el apoyo a las políticas públicas.

La e-Administración o Administración electrónica hace referencia a la incorporación de las tecnologías de la información y las comunicaciones en dos vertientes:

- Desde un punto de vista organizativo, transformando las oficinas tradicionales, convirtiendo los procesos en papel en procesos electrónicos.
- Desde una perspectiva de las relaciones externas, habilitando la vía electrónica como un nuevo medio para la relación con el ciudadano, empresas y otras instituciones.

La idea clave sobre la administración electrónica es que no se trata simplemente de llevar las TIC a la actividad administrativa, sino que constituye un elemento fundamental en los procesos de modernización administrativa dentro de los cuales se enmarca que debe llevar a la mejora y simplificación de los servicios.

La Administración electrónica tiene su mayor impulso en la última década, motivado en parte por un marco legal que ha permitido llevar las garantías jurídicas que existen en el mundo real al mundo virtual y en otra parte por la evolución de las tecnologías relacionadas y el desarrollo de proyectos emblemáticos, como el DNI electrónico.

Puede mencionarse como antecedente el RD 263/1996, de 16 de febrero, por el que se regula la utilización de técnicas electrónicas, informáticas y telemáticas por la Administración General del Estado (ampliado posteriormente por RD 209/2003).

En este proceso destaca especialmente la Ley 59/2003, de 19 de diciembre, de firma electrónica, que establece, entre muchas otras cuestiones, el concepto de firma electrónica reconocida y la equipara jurídicamente a la firma manuscrita o en papel, dotándola así de plena validez legal para las transacciones electrónicas públicas y privadas. La primera regulación de la firma electrónica en España había producido mediante el Real Decreto 14/1999, transposición de la directiva europea 1999/93/CE sobre firma electrónica.

Por otra parte, con la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal y su reglamento de desarrollo (mediante Real Decreto 1720/2007), se establecen las garantías de confidencialidad de los datos proporcionados por las personas físicas en estas transacciones.

Pero sobre todo es necesario hacer mención a la Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos, muchas veces denominada simplemente "Ley de Administración Electrónica" o mencionada por siglas LAECSPC¹, que consagra el concepto de Administración electrónica en el marco jurídico español y la eleva a la categoría de derecho de los ciudadanos.

La LAECSPC es la primera norma legal con rango de ley que se centra enteramente en la problemática propia de la Administración Electrónica, es por tanto la norma legal de referencia en esta materia y establece un marco homogéneo para las tres administraciones en la materia.

Su principal objetivo es reconocer y garantizar el derecho del ciudadano a relacionarse por medios electrónicos con las Administraciones Públicas. Por otra parte se pretende impulsar el uso de los servicios electrónicos en la Administración creando las condiciones necesarias, y de manera indirecta ejercer con ello un efecto arrastre sobre la sociedad de la información en general.

Las Administraciones Públicas tienen la obligación de posibilitar el acceso a todos sus servicios electrónicos, incluyendo registro, pago, notificaciones y la consulta del estado de tramitación de sus procedimientos desde el 31 de diciembre del 2009. En este sentido es especialmente exigente con la Administración del Estado, condicionando la obligatoriedad para las

¹ Dadas las múltiples referencias que se hacen en este texto a dicha Ley, optaremos habitualmente por utilizar esta expresión o bien simplemente Ley 11/2007.

Comunidades Autónomas y Administración Local a la disponibilidad de financiación suficiente para la implantación de estos servicios.

La LAECSPC además ha supuesto el punto de partida para un desarrollo normativo que permite avanzar en aspectos concretos, y que también se mencionarán en estos capítulos y aparecen en el apartado de referencias.

En particular, y con respecto a los aspectos técnicos, destacan el Esquema Nacional de Seguridad y el Esquema Nacional de Interoperabilidad, y con respecto a este último, las recientes Normas Técnicas de Interoperabilidad, que hacen referencia a los distintos apartados estudiados en este bloque. Todos están mencionados en el apartado de referencias.

Además de reconocer el derecho de los ciudadanos a relacionarse con las Administraciones Públicas por medios electrónicos, regula los aspectos básicos de la utilización de las tecnologías de la información en la actividad administrativa, en las relaciones entre las Administraciones Públicas, así como en las relaciones de los ciudadanos con las mismas con la finalidad de garantizar sus derechos, un tratamiento común ante ellas y la validez y eficacia de la actividad administrativa en condiciones de seguridad jurídica.

La LAECSPC obliga a las Administraciones a asegurar la disponibilidad, el acceso, la integridad, la autenticidad, la confidencialidad y la conservación de los datos, informaciones y servicios que gestionen en el ejercicio de sus competencias.

También establece una serie de fines, que definen con claridad que debe perseguir todo proyecto de Administración Electrónica:

1. Facilitar el ejercicio de derechos y el cumplimiento de deberes por medios electrónicos.

2. Facilitar el acceso por medios electrónicos de los ciudadanos a la información y al procedimiento administrativo, con especial atención a la eliminación de las barreras que limiten dicho acceso.
3. Crear las condiciones de confianza en el uso de los medios electrónicos, estableciendo las medidas necesarias para la preservación de la integridad de los derechos fundamentales, y en especial los relacionados con la intimidad y la protección de datos de carácter personal, por medio de la garantía de la seguridad de los sistemas, los datos, las comunicaciones, y los servicios electrónicos.
4. Promover la proximidad con el ciudadano y la transparencia administrativa, así como la mejora continuada en la consecución del interés general.
5. Contribuir a la mejora del funcionamiento interno de las Administraciones Públicas, incrementando la eficacia y la eficiencia de las mismas mediante el uso de las tecnologías de la información, con las debidas garantías legales en la realización de sus funciones.
6. Simplificar los procedimientos administrativos y proporcionar oportunidades de participación y mayor transparencia, con las debidas garantías legales.
7. Contribuir al desarrollo de la sociedad de la información en el ámbito de las Administraciones Públicas y en la sociedad en general.

La utilización de las tecnologías de la información tendrá las limitaciones establecidas por la Constitución y el resto del ordenamiento jurídico, respetando el pleno ejercicio por los ciudadanos de los derechos que tienen reconocidos, y ajustándose a los siguientes principios:

- a. El respeto al derecho a la protección de datos de carácter personal en los términos establecidos por la Ley Orgánica 15/1999, de Protección de los Datos de Carácter Personal, en las demás leyes específicas que regulan el tratamiento de la información y en sus



normas de desarrollo, así como a los derechos al honor y a la intimidad personal y familiar.

- b. Principio de igualdad con objeto de que en ningún caso el uso de medios electrónicos pueda implicar la existencia de restricciones o discriminaciones para los ciudadanos que se relacionen con las Administraciones Públicas por medios no electrónicos, tanto respecto al acceso a la prestación de servicios públicos como respecto a cualquier actuación o procedimiento administrativo sin perjuicio de las medidas dirigidas a incentivar la utilización de los medios electrónicos.
- c. Principio de accesibilidad a la información y a los servicios por medios electrónicos en los términos establecidos por la normativa vigente en esta materia, a través de sistemas que permitan obtenerlos de manera segura y comprensible, garantizando especialmente la accesibilidad universal y el diseño para todos de los soportes, canales y entornos con objeto de que todas las personas puedan ejercer sus derechos en igualdad de condiciones, incorporando las características necesarias para garantizar la accesibilidad de aquellos colectivos que lo requieran.
- d. Principio de legalidad en cuanto al mantenimiento de la integridad de las garantías jurídicas de los ciudadanos ante las Administraciones Públicas establecidas en la Ley 30/1992, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común.
- e. Principio de cooperación en la utilización de medios electrónicos por las Administraciones Públicas al objeto de garantizar tanto la interoperabilidad de los sistemas y soluciones adoptados por cada una de ellas como, en su caso, la prestación conjunta de servicios a los ciudadanos. En particular, se garantizará el reconocimiento mutuo de los documentos electrónicos y de los medios de identificación y autenticación que se ajusten a lo dispuesto en la presente Ley.
- f. Principio de seguridad en la implantación y utilización de los medios electrónicos por las Administraciones Públicas, en cuya virtud se

exigirá al menos el mismo nivel de garantías y seguridad que se requiere para la utilización de medios no electrónicos en la actividad administrativa.

- g. Principio de proporcionalidad en cuya virtud sólo se exigirán las garantías y medidas de seguridad adecuadas a la naturaleza y circunstancias de los distintos trámites y actuaciones. Asimismo sólo se requerirán a los ciudadanos aquellos datos que sean estrictamente necesarios en atención a la finalidad para la que se soliciten.
- h. Principio de responsabilidad y calidad en la veracidad y autenticidad de las informaciones y servicios ofrecidos por las Administraciones Públicas a través de medios electrónicos.
- i. Principio de neutralidad tecnológica y de adaptabilidad al progreso de las técnicas y sistemas de comunicaciones electrónicas garantizando la independencia en la elección de las alternativas tecnológicas por los ciudadanos y por las Administraciones Públicas, así como la libertad de desarrollar e implantar los avances tecnológicos en un ámbito de libre mercado. A estos efectos las Administraciones Públicas utilizarán estándares abiertos así como, en su caso y de forma complementaria, estándares que sean de uso generalizado por los ciudadanos.
- j. Principio de simplificación administrativa, por el cual se reduzcan de manera sustancial los tiempos y plazos de los procedimientos administrativos, logrando una mayor eficacia y eficiencia en la actividad administrativa.
- k. Principio de transparencia y publicidad del procedimiento, por el cual el uso de medios electrónicos debe facilitar la máxima difusión, publicidad y transparencia de las actuaciones administrativas.

A nivel técnico, se puede destacar el principio de neutralidad tecnológica y uso de estándares abiertos en el uso de las TIC.

Se reconoce a los ciudadanos el derecho a relacionarse con las Administraciones Públicas utilizando medios electrónicos (la LAECSPC, como la mayoría de la normativa que guarda relación, utiliza normalmente este término en lugar de otros como “telemáticos”) para el ejercicio de los derechos previstos en el artículo 35 de la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común, así como para obtener informaciones, realizar consultas y alegaciones, formular solicitudes, manifestar consentimiento, entablar pretensiones, efectuar pagos, realizar transacciones y oponerse a las resoluciones y actos administrativos.

Además, los ciudadanos tienen en relación con la utilización de los medios electrónicos en la actividad administrativa, y en los términos previstos en la presente Ley, los siguientes derechos:

- a. A elegir, entre aquellos que en cada momento se encuentren disponibles, el canal a través del cual relacionarse por medios electrónicos con las Administraciones Públicas.
- b. A no aportar los datos y documentos que obren en poder de las Administraciones Públicas, las cuales utilizarán medios electrónicos para recabar dicha información siempre que, en el caso de datos de carácter personal, se cuente con el consentimiento de los interesados en los términos establecidos por la Ley Orgánica 15/1999, de Protección de Datos de Carácter Personal, o una norma con rango de Ley así lo determine, salvo que existan restricciones conforme a la normativa de aplicación a los datos y documentos recabados. El citado consentimiento podrá emitirse y recabarse por medios electrónicos.
- c. A la igualdad en el acceso electrónico a los servicios de las Administraciones Públicas (entendida como no discriminación de personas que no tenga un acceso fácil a los medios electrónicos).

- d. A conocer por medios electrónicos el estado de tramitación de los procedimientos en los que sean interesados, salvo en los supuestos en que la normativa de aplicación establezca restricciones al acceso a la información sobre aquéllos.
- e. A obtener copias electrónicas de los documentos electrónicos que formen parte de procedimientos en los que tengan la condición de interesado.
- f. A la conservación en formato electrónico por las Administraciones Públicas de los documentos electrónicos que formen parte de un expediente.
- g. A obtener los medios de identificación electrónica necesarios, pudiendo las personas físicas utilizar en todo caso los sistemas de firma electrónica del Documento Nacional de Identidad para cualquier trámite electrónico con cualquier Administración Pública.
- h. A la utilización de otros sistemas de firma electrónica admitidos en el ámbito de las Administraciones Públicas.
- i. A la garantía de la seguridad y confidencialidad de los datos que figuren en los ficheros, sistemas y aplicaciones de las Administraciones Públicas.
- j. A la calidad de los servicios públicos prestados por medios electrónicos.
- k. A elegir las aplicaciones o sistemas para relacionarse con las Administraciones Públicas siempre y cuando utilicen estándares abiertos o, en su caso, aquellos otros que sean de uso generalizado por los ciudadanos.

En particular, en los procedimientos relativos al acceso a una actividad de servicios y su ejercicio, los ciudadanos tienen derecho a la realización de la tramitación a través de una ventanilla única, por vía electrónica y a distancia, y a la obtención de la siguiente información a través de medios electrónicos, que deberá ser clara e inequívoca:

- a. Los requisitos aplicables a los prestadores establecidos en territorio español, en especial los relativos a los procedimientos y trámites necesarios para acceder a las actividades de servicio y para su ejercicio.
- b. Los datos de las autoridades competentes en las materias relacionadas con las actividades de servicios, así como los datos de las asociaciones y organizaciones distintas de las autoridades competentes a las que los prestadores o destinatarios puedan dirigirse para obtener asistencia o ayuda.
- c. Los medios y condiciones de acceso a los registros y bases de datos públicos relativos a prestadores de actividades de servicios.
- d. Las vías de reclamación y recurso en caso de litigio entre las autoridades competentes y el prestador o el destinatario, o entre un prestador y un destinatario, o entre prestadores.

Las Administraciones Públicas deberán habilitar diferentes canales o medios para la prestación de los servicios electrónicos, garantizando en todo caso el acceso a los mismos a todos los ciudadanos, con independencia de sus circunstancias personales, medios o conocimientos, en la forma que estimen adecuada.

La Administración General del Estado garantizará el acceso de todos los ciudadanos a los servicios electrónicos proporcionados en su ámbito a través de un sistema de varios canales que cuente, al menos, con los siguientes medios:

- a. Las oficinas de atención presencial que se determinen, las cuales pondrán a disposición de los ciudadanos de forma libre y gratuita los medios e instrumentos precisos para ejercer los derechos reconocidos en el artículo 6 de la LAECSPC, debiendo contar con asistencia y orientación sobre su utilización, bien a cargo del personal

de las oficinas en que se ubiquen o bien por sistemas incorporados al propio medio o instrumento.

- b. Puntos de acceso electrónico, consistentes en sedes electrónicas creadas y gestionadas por los departamentos y organismos públicos y disponibles para los ciudadanos a través de redes de comunicación. En particular se creará un Punto de acceso general a través del cual los ciudadanos puedan, en sus relaciones con la Administración General del Estado y sus Organismos Públicos, acceder a toda la información y a los servicios disponibles. Este Punto de acceso general contendrá la relación de servicios a disposición de los ciudadanos y el acceso a los mismos, debiendo mantenerse coordinado, al menos, con los restantes puntos de acceso electrónico de la Administración General del Estado y sus Organismos Públicos.
- c. Servicios de atención telefónica que, en la medida en que los criterios de seguridad y las posibilidades técnicas lo permitan, faciliten a los ciudadanos el acceso a las informaciones y servicios electrónicos a los que se refieren los apartados anteriores.

Con el fin de que los ciudadanos puedan ejercer su derecho a no aportar datos que ya obren en poder de la Administración Pública, cada Administración deberá facilitar el acceso de las restantes Administraciones Públicas a los datos relativos a los interesados que obren en su poder y se encuentren en soporte electrónico, especificando las condiciones, protocolos y criterios funcionales o técnicos necesarios para acceder a dichos datos con las máximas garantías de seguridad, integridad y disponibilidad, de conformidad con lo dispuesto en la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal y su normativa de desarrollo.

La disponibilidad de tales datos estará limitada estrictamente a aquellos que son requeridos a los ciudadanos por las restantes Administraciones

para la tramitación y resolución de los procedimientos y actuaciones de su competencia de acuerdo con la normativa reguladora de los mismos.

13.2. SEDE ELECTRÓNICA Y SERVICIOS DE LA SEDE

La LAECSPC define la sede electrónica como aquella dirección electrónica disponible para los ciudadanos a través de redes de telecomunicaciones cuya titularidad, gestión y administración corresponde a una Administración Pública, órgano o entidad administrativa en el ejercicio de sus competencias.

El establecimiento de una sede electrónica conlleva la responsabilidad del titular respecto de la integridad, veracidad y actualización de la información y los servicios a los que pueda accederse a través de la misma.

Cada Administración Pública determinará las condiciones e instrumentos de creación de las sedes electrónicas, con sujeción a los principios de publicidad oficial, responsabilidad, calidad, seguridad, disponibilidad, accesibilidad, neutralidad e interoperabilidad. En todo caso deberá garantizarse la identificación del titular de la sede, así como los medios disponibles para la formulación de sugerencias y quejas.

Las sedes electrónicas dispondrán de sistemas que permitan el establecimiento de comunicaciones seguras siempre que sean necesarias. Este apartado cobra especial importancia cuando se ofrecen servicios de tramitación.

La publicación en las sedes electrónicas de informaciones, servicios y transacciones respetará los principios de accesibilidad y usabilidad de acuerdo con las normas establecidas al respecto, estándares abiertos y, en su caso, aquellos otros que sean de uso generalizado por los ciudadanos.

La publicación de los diarios o boletines oficiales en las sedes electrónicas de la Administración, Órgano o Entidad competente tendrá, en las condiciones y garantías que cada Administración Pública determine, los mismos efectos que los atribuidos a su edición impresa. La publicación del *Boletín Oficial del Estado* en la sede electrónica del organismo competente tendrá carácter oficial y auténtico en las condiciones y con las garantías que se determinen reglamentariamente, derivándose de dicha publicación los efectos previstos en el título preliminar del Código Civil y en las restantes normas aplicables.

La publicación de actos y comunicaciones que, por disposición legal o reglamentaria deban publicarse en tablón de anuncios o edictos podrá ser sustituida o complementada por su publicación en la sede electrónica del organismo correspondiente.

Por lo tanto, la sede electrónica se diferencia de cualquier sede institucional tradicional en entorno telemático por la responsabilidad del titular, el hecho de que la publicación de diarios o boletines oficiales reviste los mismos efectos que la publicación impresa y que puede actuar como sustituta o complemento al tablón de anuncios o edictos. Además, han de tenerse en cuenta las condiciones que han de cumplir las sedes electrónicas de la Administración General del Estado en el marco del Real Decreto 1671/2009. Para el resto de las Administraciones Públicas, si bien están fuera su ámbito, es indudable su validez como elemento de referencia.

En todo caso, a través de su articulado, la LAECSP establece los siguientes requisitos para las sedes electrónicas:

- Debe permitir el acceso de los ciudadanos para la realización de cualquier tipo de trámite o interacción con la Administración.



- Debe permitir a los ciudadanos realizar consultas sobre el estado de tramitación de expedientes en los que tengan la condición de interesado.
- Tanto la sede como los elementos y contenidos de la misma deben basarse en aplicaciones y sistemas que utilicen estándares abiertos o sean de uso generalizado por los ciudadanos.
- Debe contener la información sobre los pasos a seguir para cada uno de los trámites y procedimientos de las Administraciones Públicas.
- Debe contener la información sobre las autoridades competentes para cada actividad de los servicios ofrecidos por las Administraciones Públicas.
- La AGE deberá disponer de una sede electrónica que sirva como Punto de acceso general único a los servicios que presta la AGE y sus Organismos.
- El Punto de acceso general creado por la AGE deberá estar integrado con el resto de sedes de la AGE y Organismos Públicos para la prestación de los distintos servicios.
- Debe garantizar la identificación de su titular.
- Debe permitir establecer las conexiones seguras cuando sean necesarias.
- Debe cumplir los principios de accesibilidad y usabilidad de acuerdo con las normas establecidas al respecto (Según el BOE n. 141 de 13/6/2003 en la disposición 7, artículo 2: se deben cumplir los requisitos AA).
- Permitirá la publicación de actos y comunicaciones que, por disposición legal o reglamentaria deban publicarse en tablón de anuncios o edictos.
- Debe contener la lista de sistemas de firma electrónica avanzada admitidos.
- Debe contener la lista de sellos electrónicos utilizados por cada Administración.
- Debe contener las disposiciones de creación de registros electrónicos.

- La sede permitirá la publicación electrónica del boletín oficial de la Administración, órgano o Entidad competente.
- Debe contener los distintos tipos de escritos, comunicaciones, solicitudes, etc. que pueden presentarse.
- Deberá publicar los medios electrónicos disponibles para que el ciudadano se relacione con las Administraciones Públicas.
- Deberá mostrar de manera visible la fecha y hora garantizando su integridad.
- Deberá publicar una lista con los días considerados inhábiles.
- En aquéllas administraciones que tengan lenguas cooficiales, se debe garantizar el acceso en ambas lenguas.

Desde el punto de vista técnico, la sede electrónica no presenta características tecnológicas distintas a la de cualquier sitio web tradicional, si bien es necesario establecer las medidas de seguridad que permitan garantizar la responsabilidad establecida por la LAECSP.

En particular, es importante la identificación segura de la sede electrónica. En este sentido, la Ley establece la posibilidad de creación de certificados de sede electrónica con este propósito.

La Fábrica Nacional de la Moneda y Timbre – Real Casa de la Moneda (FNMT-RCM), que ya ofrecía certificados de identificación segura, dispone ya de la versión actualizada para el cumplimiento de la LAECSP (son los llamados genéricamente certificados APE). Los "Certificados de identificación de sede electrónica" son aquellos certificados expedidos por la FNMT-RCM bajo la Declaración de Prácticas de Certificación de la Administración Pública del Estado y que vinculan unos datos de verificación de firma a los datos identificativos de una sede electrónica en la que existe una persona física que actúa como firmante o custodio de la clave y titular del certificado, junto con la entidad de la administración a la que pertenece y que es titular de la dirección electrónica a través de la que

se accede la sede electrónica (sólo la titularidad es compartida, no siendo así la custodia). Esta persona física es la que tiene el control sobre dicho certificado y los datos de creación y verificación de firma y es responsable de su custodia de forma diligente.

Constituyen los límites de uso de este tipo de certificados la identificación de sedes electrónicas de la Administración Pública, Organismos y entidades públicas vinculadas o dependientes así como el establecimiento de comunicaciones seguras con éstas.

Además, las sedes electrónicas pueden contar con requisitos técnicos adicionales según los servicios que presten, pudiendo por ejemplo, ser necesario garantizar la integridad y contenido de sus páginas a una fecha y hora determinada mediante la firma con sellado de tiempo de dicho contenido, y lo mismo se puede decir de los documentos emitidos o recibidos.

13.3. REGISTRO ELECTRÓNICO

Las tareas fundamentales del registro electrónico son tomar una referencia de tiempo, anotar el asiento de la entrada/salida, guardar los datos de la presentación de información, y devolver un acuse de recibo con el número de registro y momento de la presentación.

El registro podrá asimismo incluir funcionalidades adicionales, como por ejemplo, el sellado de tiempo para obtener la referencia temporal, el cotejo/compulsa electrónica de documentos presentados físicamente o el funcionamiento como registro único para toda la Administración.

Con respecto a los registros electrónicos, la LAECSP establece que las Administraciones Públicas crearán registros electrónicos para la recepción y

remisión de solicitudes, escritos y comunicaciones. Los registros electrónicos podrán admitir:

- a. Documentos electrónicos normalizados correspondientes a los servicios, procedimientos y trámites que se especifiquen conforme a lo dispuesto en la norma de creación del registro, cumplimentados de acuerdo con formatos preestablecidos.
- b. Cualquier solicitud, escrito o comunicación distinta de los mencionados en el apartado anterior dirigido a cualquier órgano o entidad del ámbito de la administración titular del registro.

En cada Administración Pública existirá, al menos, un sistema de registros electrónicos suficiente para recibir todo tipo de solicitudes, escritos y comunicaciones dirigidos a dicha Administración Pública. Las Administraciones Públicas podrán, mediante convenios de colaboración, habilitar a sus respectivos registros para la recepción de las solicitudes, escritos y comunicaciones de la competencia de otra Administración que se determinen en el correspondiente convenio.

En el ámbito de la Administración General del Estado se automatizarán las oficinas de registro físicas a las que se refiere el artículo 38 de la Ley 30/1992, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común, a fin de garantizar la interconexión de todas sus oficinas y posibilitar el acceso por medios electrónicos a los asientos registrales y a las copias electrónicas de los documentos presentados.

Las disposiciones de creación de registros electrónicos se publicarán en el Diario Oficial correspondiente y su texto íntegro deberá estar disponible para consulta en la sede electrónica de acceso al registro. En todo caso, las disposiciones de creación de registros electrónicos especificarán el órgano o unidad responsable de su gestión, así como la fecha y hora oficial y los

días declarados como inhábiles a los efectos previstos en el artículo siguiente.

En la sede electrónica de acceso al registro figurará la relación actualizada de las solicitudes, escritos y comunicaciones que pueden presentarse en el mismo.

Los registros electrónicos emitirán automáticamente un recibo consistente en una copia autenticada del escrito, solicitud o comunicación de que se trate, incluyendo la fecha y hora de presentación y el número de entrada de registro.

Podrán aportarse documentos que acompañen a la correspondiente solicitud, escrito o comunicación, siempre que cumplan los estándares de formato y requisitos de seguridad que se determinen en los Esquemas Nacionales de Interoperabilidad y de Seguridad.

Los registros electrónicos generarán recibos acreditativos de la entrega de estos documentos que garanticen la integridad y el no repudio de los documentos aportados.

Los registros electrónicos se regirán a efectos de cómputo de los plazos imputables tanto a los interesados como a las Administraciones Públicas por la fecha y hora oficial de la sede electrónica de acceso, que deberá contar con las medidas de seguridad necesarias para garantizar su integridad y figurar visible.

Los registros electrónicos permitirán la presentación de solicitudes, escritos y comunicaciones todos los días del año durante las veinticuatro horas.

A los efectos del cómputo de plazo fijado en días hábiles o naturales, y en lo que se refiere a cumplimiento de plazos por los interesados, la presentación en un día inhábil se entenderá realizada en la primera hora

del primer día hábil siguiente, salvo que una norma permita expresamente la recepción en día inhábil.

El inicio del cómputo de los plazos que hayan de cumplir los órganos administrativos y entidades de derecho público vendrá determinado por la fecha y hora de presentación en el propio registro o, en el caso previsto en el apartado 2.b del artículo 24 de la LAECSP, por la fecha y hora de entrada en el registro del destinatario. En todo caso, la fecha efectiva de inicio del cómputo de plazos deberá ser comunicada a quien presentó el escrito, solicitud o comunicación.

Cada sede electrónica en la que esté disponible un registro electrónico determinará, atendiendo al ámbito territorial en el que ejerce sus competencias el titular de aquella, los días que se considerarán inhábiles a los efectos de los apartados anteriores. En todo caso, no será de aplicación a los registros electrónicos lo dispuesto en el artículo 48.5 de la Ley 30/1992, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común, que establece que cuando un día fuese hábil en el municipio o Comunidad Autónoma en que residiese el interesado, e inhábil en la sede del órgano administrativo, o a la inversa, se considerará inhábil en todo caso.

Desde el punto de vista técnico, el registro electrónico debe permitir la presentación de documentación en formato electrónico y la generación del correspondiente asiento en el registro de entrada y salida de la Administración. Ello implica probablemente la necesidad de integración con un sistema de gestión de registro de entrada y salida general, que permita la introducción de asientos manual desde los distintos departamentos.

Además, para poder realizar esta función con las suficientes garantías, debe permitir lo siguiente:

- a) Presentar la documentación en formato electrónico y firmada por el ciudadano mediante el correspondiente certificado electrónico que garantice su autenticidad, integridad y no repudio.
- b) Registrar de modo fehaciente el proceso de registro de dicha documentación. A tal efecto se puede utilizar algún tipo de resguardo firmado mediante el uso de un certificado de la Administración Pública (previsiblemente un certificado de sello electrónico) que incluya sellado de tiempo para garantizar la fecha y hora de entrega.
- c) Entregar al ciudadano el resguardo de dicho registro en formato electrónico, convenientemente firmado por la Administración, en el que constará la fecha y hora de entrada y los documentos entregados, y pudiendo incorporar un checksum o sistema de equivalente que permita verificar que los contenidos presentados son los que constan en dicho resguardo.

Los documentos deberían entrar a formar parte del sistema de gestión de documentos electrónicos, recibiendo por lo tanto una identificación única dentro del sistema y el tratamiento que corresponda en cada caso. Así por ejemplo, de ser necesario entrarían a formar parte del correspondiente expediente electrónico.

13.4. EXPEDIENTE ELECTRÓNICO

La LAECSP define expediente electrónico como el conjunto de documentos electrónicos correspondientes a un procedimiento administrativo, cualquiera que sea el tipo de información que contengan.

El foliado de los expedientes electrónicos se llevará a cabo mediante un índice electrónico, firmado por la Administración, órgano o entidad actuante, según proceda.

Este índice garantizará la integridad del expediente electrónico y permitirá su recuperación siempre que sea preciso, siendo admisible que un mismo documento forme parte de distintos expedientes electrónicos.

La remisión de expedientes podrá ser sustituida a todos los efectos legales por la puesta a disposición del expediente electrónico, teniendo el interesado derecho a obtener copia del mismo.

Desde el punto de vista técnico, el expediente viene definido por el índice ordenado de documentos que ha sido firmado electrónicamente, por lo que no puede ser modificado sin la pérdida de validez de dicha firma. Los documentos como tal pueden ser almacenados de forma independiente, previsiblemente estarán a su vez firmados para garantizar su integridad y no repudio, y deben contar con un código que los identifique de forma unívoca dentro de la organización y no sólo dentro del ámbito del expediente. De este modo, un mismo documento puede ser referenciado desde varios índices, o lo que es lo mismo, formar parte de distintos expedientes.

13.5.ARCHIVO ELECTRÓNICO DE DOCUMENTOS

Las Administraciones Públicas podrán emitir válidamente por medios electrónicos los documentos administrativos a los que se refiere el artículo 46 de la Ley 30/1992, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común, siempre que incorporen una o varias firmas electrónicas conforme a lo establecido en la Sección III del Capítulo II de la LAECSP.

Los documentos administrativos incluirán referencia temporal, que se garantizará a través de medios electrónicos cuando la naturaleza del documento así lo requiera.

La Administración General del Estado, en su relación de prestadores de servicios de certificación electrónica, especificará aquellos que con carácter general estén admitidos para prestar servicios de sellado de tiempo.

Podrán almacenarse por medios electrónicos todos los documentos utilizados en las actuaciones administrativas.

Los documentos electrónicos que contengan actos administrativos que afecten a derechos o intereses de los particulares deberán conservarse en soportes de esta naturaleza, ya sea en el mismo formato a partir del que se originó el documento o en otro cualquiera que asegure la identidad e integridad de la información necesaria para reproducirlo. Se asegurará en todo caso la posibilidad de trasladar los datos a otros formatos y soportes que garanticen el acceso desde diferentes aplicaciones.

Los medios o soportes en que se almacenen documentos, deberán contar con medidas de seguridad que garanticen la integridad, autenticidad, confidencialidad, calidad, protección y conservación de los documentos almacenados. En particular, asegurarán la identificación de los usuarios y el control de accesos, así como el cumplimiento de las garantías previstas en la legislación de protección de datos.

Desde el punto de vista técnico, el almacenamiento y tratamiento de documentos en formato electrónico implica la utilización de una firma avanzada que permita garantizar su integridad y el no repudio. En caso de tratarse de documentos en otro formato, como el papel, puede ser necesaria su conversión previa a algún formato electrónico mediante técnicas como la del escaneado.

Además, el sistema informático de soporte debe garantizar la seguridad de los documentos tanto desde el punto de vista de la disponibilidad como del control de acceso. Por último, implica también la implantación sistema de custodia de documentos electrónicos con mecanismos que permitan garantizar su validez a lo largo del tiempo, mediante el uso, por ejemplo, de firmas longevas o de la actualización periódica de formatos para evitar su obsolescencia.

13.6. DIGITALIZACIÓN, COMPULSA ELECTRÓNICA.

En primer lugar, debemos distinguir entre cotejo o copia compulsada y copia auténtica:

- El cotejo y la compulsa de documentos es la técnica consistente en la comprobación de que una copia coincide con su original, que lleva a poder afirmar que la misma es exacta. La copia cotejada o compulsada en ningún caso acredita la autenticidad del documento original.
- La copia auténtica de un documento acredita la autenticidad de los datos contenidos en la misma, no sólo desde la perspectiva de su identidad con el documento original, si no por sus efectos certificativos, en cuanto que garantiza, igualmente, la autenticidad de los datos contenidos en este último.

Por consiguiente, la copia auténtica goza de la misma validez y eficacia que el documento original, no limitando sus efectos a un procedimiento administrativo concreto.

Las copias realizadas por medios electrónicos de documentos electrónicos emitidos por el propio interesado o por las Administraciones Públicas,

manteniéndose o no el formato original, tendrán inmediatamente la consideración de copias auténticas con la eficacia prevista en el artículo 46 de la Ley 30/1992, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común, siempre que el documento electrónico original se encuentre en poder de la Administración, y que la información de firma electrónica y, en su caso, de sellado de tiempo permitan comprobar la coincidencia con dicho documento.

Las copias realizadas por las Administraciones Públicas, utilizando medios electrónicos, de documentos emitidos originalmente por las Administraciones Públicas en soporte papel tendrán la consideración de copias auténticas siempre que se cumplan los requerimientos y actuaciones previstas en el artículo 46 de la Ley 30/1992, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común.

Las Administraciones Públicas podrán obtener imágenes electrónicas de los documentos privados aportados por los ciudadanos, con su misma validez y eficacia, a través de procesos de digitalización que garanticen su autenticidad, integridad y la conservación del documento imagen, de lo que se dejará constancia. Esta obtención podrá hacerse de forma automatizada, mediante el correspondiente sello electrónico.

En los supuestos de documentos emitidos originalmente en soporte papel de los que se hayan efectuado copias electrónicas de acuerdo con lo dispuesto en este artículo, podrá procederse a la destrucción de los originales en los términos y con las condiciones que por cada Administración Pública se establezcan.

Las copias realizadas en soporte papel de documentos públicos administrativos emitidos por medios electrónicos y firmados electrónicamente tendrán la consideración de copias auténticas siempre

que incluyan la impresión de un código generado electrónicamente u otros sistemas de verificación que permitan contrastar su autenticidad mediante el acceso a los archivos electrónicos de la Administración Pública, órgano o entidad emisora.

Desde el punto de vista técnico, la compulsa y creación de copias auténticas implica la firma de un documento electrónico mediante el uso de un certificado electrónico. En caso de que dicho documento se encuentre en formato papel, debe ser previamente digitalizado mediante un procedimiento establecido y seguro.

El proceso tecnológico de conversión a formato electrónico se denomina “digitalización certificada”, entendiendo como tal la definición dada compatible con el término “digitalización” que se puede encontrar en el Anexo del Esquema Nacional de Interoperabilidad (RD 4/2010).

Al ser necesario que la copia sea fiel e íntegra, el proceso de digitalización debe cumplir una serie de características:

- a) Debe ser completamente automático y realizarse de forma atómica, obteniendo como entrada el documento original e devolviendo como resultado la copia electrónica. Así, no será posible la intervención humana en ninguna fase do proceso que pueda alterar por error o de forma deliberada el contenido previsto.
- b) El proceso tecnológico debe ser diseñado de tal forma que non produzca alteración con respecto al documento original. En este aspecto hay que tener en cuenta que la obtención de la copia implica la realización de distintas operaciones. Así por ejemplo, será necesario en un primer momento obtener a partir del contenido en papel una representación en formato electrónico, posiblemente mediante una operación de escaneado o similar. En esta fase será

importante definir las características técnicas de los dispositivos a utilizar, y parámetros del proceso como puede ser el nivel de resolución (término definido en el Anexo del RD 4/2010) mínima. A partir de esta información, ya en formato electrónico, muy probablemente será necesario además realizar conversiones entre formatos o aplicar algoritmos de compresión con o sin pérdida de información, para los que será necesario establecer unos límites de tolerancia.

Para la firma, la LAECSP establece la posibilidad de utilizar certificados de personal adscrito a la Administración o funcionario.

La Fábrica Nacional de la Moneda y Timbre – Real Casa de la Moneda (FNMT-RCM), que ya ofrecía certificados de identificación segura, dispone ya de la versión actualizada para el cumplimiento de la LAECSP. Los Certificados emitidos por la FNMT-RCM para el personal al servicio de las administraciones públicas cuya política y Declaración Particular se definen en la DPC de la APE, son certificados reconocidos según lo definido en la Ley de Firma Electrónica 59/2003 y la norma ETSI 101 456 y válidos para la realización de firma electrónica por parte del personal al servicio de las administraciones públicas y según lo definido en la Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos (LAECSP).

El certificado para el personal de la Administración Pública, es la certificación electrónica emitida por la FNMT-RCM que vincula a su titular con unos datos de verificación de firma y confirma, de forma conjunta:

- la identidad de su titular, número de identificación personal, cargo, puesto de trabajo y/o condición de autorizado.

- al órgano, organismo o entidad de la Administración Pública, bien sea ésta General, autonómica, Local o institucional, donde ejerce sus competencias, presta sus servicios, o desarrolla su actividad.

El ámbito de uso de este tipo de Certificados lo componen las diferentes competencias y funciones propias de los titulares de acuerdo con su cargo, empleo y, en su caso, condiciones de autorización.

13.7. FACTURA Y LICITACIÓN ELECTRÓNICAS

13.7.1. FACTURA ELECTRÓNICA

La facturación electrónica es un equivalente funcional de la factura en papel y consiste en la transmisión de las facturas o documentos análogos entre emisor y receptor por medios electrónicos (ficheros informáticos) y telemáticos (de un ordenador a otro), firmados digitalmente con certificados reconocidos.

La Ley 57/2007, de Medidas de Impulso de la Sociedad de la Información, define la factura electrónica como “un documento electrónico que cumple con los requisitos legal y reglamentariamente exigibles a las facturas y que, además, garantiza la autenticidad de su origen y la integridad de su contenido, lo que permite atribuir la factura a su obligado tributario emisor”.

De esta definición extendida en todo el mercado, se transmite tres condicionantes para la realización de e-Factura:

- Se necesita un formato electrónico de factura de mayor o menor complejidad (EDIFACT, XML, PDF, html, doc, xls, gif, jpeg o txt, entre otros).

- Es necesario una transmisión telemática (tiene que partir de un ordenador, y ser recogida por otro ordenador).
- Este formato electrónico y transmisión telemática, deben garantizar su integridad y autenticidad a través de una firma electrónica reconocida. El artículo 3.3 de la Ley 59/2003 de 19 de diciembre define la firma electrónica reconocida como: “la firma electrónica avanzada basada en un certificado reconocido y generada mediante un dispositivo seguro de creación de firma”.

El certificado que se usa es el del expedidor real de la factura. Ya sea éste el obligado tributario, un tercero que actúe en su nombre o el destinatario de la factura, si se ha acordado auto-facturación.

Por último y para que tuviera la facturación electrónica la misma validez legal que una factura en papel, se necesita el consentimiento de ambas partes (emisor y receptor).

Adicionalmente, y como requisito de todas las facturas independientemente de cómo se transmitan, en papel o en formato electrónico, el artículo 6 del RD 1496/2003 que regula el contenido de una factura establece que los campos obligatorios de una factura son:

- Número de factura
- Fecha expedición
- Razón Social emisor y receptor
- NIF emisor y “receptor”
- Domicilio emisor y receptor
- Descripción de las operaciones (base imponible)
- Tipo impositivo
- Cuota tributaria
- Fecha prestación del servicio (si distinta a expedición)

Para cumplir con la norma y que una factura electrónica tenga la misma validez legal que una emitida en papel, el documento electrónico que la representa debe contener los campos obligatorios exigibles a toda factura, estar firmado mediante una firma electrónica avanzada basado en certificado reconocido y ser transmitido de un ordenador a otro recogiendo el consentimiento de ambas partes.

Para homogenizar estos aspectos técnicos se ha desarrollado la Orden PRE/2971/2007, sobre la expedición de facturas por medios electrónicos cuando el destinatario de las mismas sea la Administración General del Estado u organismos públicos vinculados o dependientes de aquélla y sobre la presentación ante la Administración General del Estado o sus organismos públicos vinculados o dependientes de facturas expedidas entre particulares.

En esta orden se crea el formato de factura electrónica Facturae, junto con la previsión de compatibilidad en futuras con normas como UBL (Universal Business Language). Facturae define fundamentalmente las tecnologías de firma a utilizar en las facturas y una estructura en XML que éstas deben cumplir. Se puede encontrar amplia información sobre este formato en el sitio web <http://www.facturae.es/>.

También es posible crear extensiones del formato. Una extensión es una definición estructurada de información específica, de un sector determinado, que no está contemplada en el núcleo del formato Facturae y que es de interés para emisores y receptores. Facturae permite la inclusión de extensiones a nivel de línea, de factura o de lote de facturas.

Se facilita la divulgación de las extensiones a través de la publicación de enlaces a repositorios de extensiones relevantes. Estas extensiones se constituirán en un modelo de uso común susceptible de utilización mayoritaria por los usuarios de Facturae del sector correspondiente.

Para que una extensión figure en la tabla de enlaces, es necesario cumplir una serie de requisitos. Para la creación de la extensión, si bien es responsabilidad de la asociación encargada, se facilita un documento de recomendaciones generales:

Obligaciones legales del expedidor:

1. Reglamento sobre Facturación Electrónica. La Orden 962/2007, de 10 de abril, desarrolla determinadas disposiciones sobre facturación telemática y conservación electrónica de facturas, contenidas en el Real Decreto 1496/2003, que es el reglamento de facturación. Al respecto del consentimiento del destinatario, se encuentra recogido en el Artículo 2 de la citada Orden, donde dice que el consentimiento podrá formularse de forma expresa por cualquier medio, verbal o escrito.
2. Creación de la factura. Mediante una aplicación informática, con los contenidos obligatorios mínimos requeridos.
3. Uso de firma electrónica reconocida
4. Remisión telemática
5. Conservación de copia o matriz de la factura. Esta obligación se regula en el artículo 1 del RD 1496/2003, donde se especifica la obligación de expedir, entregar y conservar facturas.
También han existido dudas sobre si las facturas electrónicas pueden emitirse en copia o sólo se debe guardar la matriz. Al respecto la Agencia Tributaria lo ha aclarado en el borrador antes citado (Art. 5) con la siguiente definición:
“Se entiende por Matriz de una factura (...) un conjunto de datos, tablas, base de datos o sistemas de ficheros que contienen todos los datos reflejados en las facturas junto a los programas que permitieron la generación de las facturas....”
6. Contabilización y anotación en registros de IVA

7. Conservación durante el período de prescripción
8. Garantía de accesibilidad completa. Deber de gestionar las facturas de modo que se garantice una accesibilidad completa: visualización, búsqueda selectiva, copia o descarga en línea e impresión. Esta es una obligación inherente a la conservación de las facturas por medios electrónicos que el legislador denomina acceso completo a datos, tratando de facilitar la auditoria e inspección de las facturas electrónicas. (Artículo 9 del RD 1496/2003)
9. Subcontratación a un tercero. Todas las fases anteriores pueden ser subcontratadas a un tercero, sin perder su responsabilidad. Regulado en el artículo 5.1 del RD 1496/2003 el legislador deja claro en ese mismo párrafo que, aunque se permite la subfacturación a terceros, es el obligado tributario el responsable de cumplir todas estas obligaciones.

Obligaciones legales del destinatario:

1. Recepción de la factura por medio electrónico
 - Verificación de los contenidos mínimos exigibles
 - Verificación segura de la firma electrónica. Regulado en el artículo 21 e inherente a las obligaciones de la conservación de las facturas electrónicas se indica que: “el destinatario se debe asegurar de la legibilidad en el formato original en el que se haya recibido, así como, en su caso, de los datos asociados y mecanismo de verificación de firma”.

A diferencia del emisor, al que se permite construir la factura desde la matriz, el destinatario debe conservar los originales firmados.
2. Contabilización y anotación en registros de IVA
3. Conservación durante el período de prescripción. Deber de gestionar las facturas de modo que se garantice una accesibilidad completa.
4. Todas las fases anteriores puede subcontratarlas a un tercero, sin perder su responsabilidad.

La obligación del uso de facturas electrónicas nace de las previsiones de la Ley 30/2007, de Contratos del Sector Público, la cual regula, entre otras muchas materias, el establecimiento de una plataforma de contratación electrónica del Estado y la utilización de medios electrónicos, informáticos o telemáticos por parte de las empresas del sector privado para la contratación con Administraciones Públicas.

Por otra parte, establece un calendario de implantación progresiva del uso obligatorio de la facturación electrónica por parte de las empresas del sector privado que accedan a contratos del sector público como proveedores del mismo. En este calendario se pueden destacar principalmente dos hitos: un período de transición que finalizó el 1 de agosto del año 2009 e implica que las sociedades que no presenten cuenta de pérdidas y ganancias abreviada ya están obligadas a presentar facturas electrónicas a sus clientes que sean entidades pertenecientes al sector público estatal.

13.7.2. LICITACIÓN ELECTRÓNICA

La Ley 30/2007, de Contratos del Sector Público, en su disposición final novena, dedicada a la habilitación normativa en materia de uso de medios electrónicos, informáticos o telemáticos, y uso de factura electrónica, dice lo siguiente:

1. Se autoriza al Ministro de Economía y Hacienda para aprobar, previo dictamen del Consejo de Estado, las normas de desarrollo de la disposición adicional decimonovena que puedan ser necesarias para hacer plenamente efectivo el uso de medios electrónicos, informáticos o telemáticos en los procedimientos regulados en esta Ley.

2. Igualmente, el Ministro de Economía y Hacienda, mediante Orden, definirá las especificaciones técnicas de las comunicaciones de datos que deban efectuarse en cumplimiento de la presente Ley y establecerá los modelos que deban utilizarse.

3. En el plazo máximo de un año desde la entrada en vigor de la Ley, el Ministro de Economía y Hacienda aprobará las normas de desarrollo necesarias para hacer posible el uso de las facturas electrónicas en los contratos que se celebren por las entidades del sector público estatal.

4. Transcurridos tres meses desde la entrada en vigor de las normas a que se refiere el apartado anterior la presentación de facturas electrónicas será obligatoria en la contratación con el sector público estatal para las sociedades que no puedan presentar cuenta de pérdidas y ganancias abreviada.

Por Orden conjunta de los Ministros de Economía y Hacienda y de Industria, Turismo y Comercio, se extenderá progresivamente la obligatoriedad del uso de las facturas electrónicas para otras personas físicas y jurídicas en función de sus características y el volumen de su cifra de negocios. En todo caso, transcurridos dieciocho meses desde la entrada en vigor de las normas a que se refiere el apartado anterior, el uso de la factura electrónica será obligatorio en todos los contratos del sector público estatal; no obstante, en los contratos menores, la utilización de la factura electrónica será obligatoria cuando así se establezca expresamente en estas Órdenes de extensión.

5. El Consejo de Ministros, a propuesta de los Ministros de Economía y Hacienda y de Industria, Turismo y Comercio, adoptará las medidas necesarias para facilitar la emisión de facturas electrónicas por las personas y entidades que contraten con el sector público estatal, garantizando la gratuidad de los servicios de apoyo que se establezcan

para las empresas cuya cifra de negocios en el año inmediatamente anterior y para el conjunto de sus actividades sea inferior al umbral que se fije en la Orden a que se refiere el párrafo anterior.

En la práctica, un sistema de licitación electrónica debe permitir:

- Consultar en Internet las convocatorias de los contratos y obtener los pliegos. Para ello se crea la figura del Perfil del contratante, donde es posible consultar toda la información relativa a expedientes de contratación. El perfil del contratante debe garantizar técnicamente la fecha y hora de la publicación, así como la integridad del contenido. Esto se lleva a la práctica mediante un sistema por el cual el contenido que va a ser publicado es primero firmado electrónicamente, incluyendo la firma un sellado de tiempo.
- Presentar por medios electrónicos solicitudes de participación, ofertas y documentos. Los licitantes deben poder presentar durante el plazo previsto ofertas de modo telemático. Para ello podrán hacer uso del correspondiente registro electrónico. Tal y como se explicó en dicho apartado, los licitantes podrán obtener el correspondiente resguardo.
- Obtener información sobre el desarrollo del procedimiento mediante la consulta de un tablón de anuncios electrónico. Nuevamente a través del perfil del contratante.
- Recibir notificaciones telemáticamente. Para la emisión de notificaciones telemáticas de modo fehaciente (de no ser así, en ocasiones se denominan simplemente comunicaciones), se dispone de servicios como el Sistema de Notificaciones Telemáticas Seguras creado por la Sociedad Estatal de Correos y Telégrafos. En este sistema, el ciudadano dispone de un buzón al que son enviadas las notificaciones. El ciudadano tiene la posibilidad de ignorar, aceptar o rechazar las notificaciones, con las mismas garantías que por el canal tradicional, y el servicio informa a la Administración de la situación en cada caso.

Un sistema de licitación electrónica debe además garantizar que, en función del procedimiento de contratación establecido, las ofertas sólo podrán ser accedidas en la fase de tramitación prevista. Permitirá por lo tanto definir las mesas de contratación, si es el caso, y establecerá los mecanismos necesarios para que las ofertas no puedan ser abiertas hasta que éstas se hayan constituido formalmente.

Técnicamente, esto se resuelve mediante la creación de sobres electrónicos, siguiendo los pasos que se detallan a continuación:

PREPARACIÓN DE LA LICITACIÓN

- Se identifica a los miembros de la mesa. El sistema debe tener acceso a la clave pública de cada uno de los miembros.

PRESENTACIÓN DE OFERTAS:

- En el momento de la presentación de las ofertas, se genera un par de claves pública y privada para cada una, y la oferta es cifrada con la clave pública, creando el sobre electrónico.
- Dicho sobre sólo puede ser abierto mediante la correspondiente clave privada. Sin embargo, la clave privada no se almacena en el sistema. En su lugar, se le aplica un algoritmo que la divide en varias partes.
- Cada parte es asignada a un miembro de la mesa y cifrada con su clave pública, de tal modo que es la única persona que puede acceder a ella con su clave privada.

APERTURA DE OFERTAS:

- En el día y hora de constitución de la mesa de contratación, el sistema considera abierta la mesa de contratación y los miembros pueden acceder al sistema.
- Cada uno de los miembros pueden acceder a la parte de la clave privada del sobre que le corresponde. Para ello, puesto que está cifrada con su clave pública, deben utilizar su clave privada, identificándolos fehacientemente.
- Una vez el sistema dispone de suficientes partes de la clave privada (no es necesario que participen todos los miembros de la mesa, sino

que es posible establecer previamente un quórum), recompone la clave privada del sobre.

- Con la clave privada del sobre, el sistema ya puede extraer y mostrar la oferta.

Por último, el sistema de licitación electrónica debe contar con un componente de gestión de expedientes que permita llevar a cabo todos los trámites en la secuencia correcta, así como garantizar el acceso a la documentación generada (actas, informes, etc.) y almacenada.

13.8. REFERENCIAS

- Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común.
- Ley 15/1999, de 13 de diciembre, de Protección de datos de carácter personal
- Ley 53/1999, de 19 de diciembre, de Firma electrónica.
- Ley 34/2002, de 11 de julio, de Servicios de la sociedad de la información y de comercio electrónico.
- Ley 11/2007, de 22 de junio, de Acceso electrónico dos ciudadanos a los servicios públicos.
- Ley 30/2007, de 30 de octubre, de Contratos do Sector Público.
- Ley 37/2007, de 16 de noviembre, sobre Reutilización de la información del sector público.
- Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley 15/1999, de 13 de diciembre, de protección de datos de carácter personal.
- Ley 56/2007, de 28 de diciembre, de Medidas de impulso de la sociedad de la Información.
- Real Decreto 1494/2007, de 12 de noviembre, por el que se aprueba el Reglamento sobre las condiciones básicas para el acceso de las personas con discapacidad a las tecnologías, productos y servicios relacionados con la sociedad de la información y medios de comunicación social.

- Ley 17/2009, de 23 de noviembre, sobre el Libre acceso a las actividades de servicios y su ejercicio.
- Ley 25/2009, de 22 de diciembre, de Modificación de diversas leyes para su adaptación a la Ley 17/2009, de 23 de noviembre, sobre el Libre acceso a las actividades de servicios y su ejercicio.
- Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito da Administración Electrónica.
- Real Decreto 4/2010, de 8 de enero, por el que se regula el Esquema Nacional de Interoperabilidad en el ámbito da Administración Electrónica.
- Decreto 198/2010, de 2 de diciembre, por el que se regula el Desarrollo de la Administración Electrónica en la Xunta de Galicia y en las entidades dependientes.
- Resoluciones de la Secretaría de Estado para la Función Pública por la que se aprueban distintas normas técnicas de interoperabilidad.

- “Manual práctico de supervivencia de la Administración Electrónica”, de Alberto López Tallón, publicado bajo licencia Creative Commons.
- “Anotacións e comentarios ao Decreto de Administración Electrónica da Xunta de Galicia”, editado polo Colexio Profesional de Enxeñaría en Informática de Galicia coa colaboración da Xunta de Galicia. ISBN 978-84-614-7362-5.
- “Las relaciones de la empresa con la Administración Electrónica”, editado polo Colexio Profesional de Enxeñaría en Informática de Galicia. ISBN 978-84-614-9865-9.
- “Empresa, protección de datos y Administración Electrónica”, editado polo Colexio Profesional de Enxeñaría en Informática de Galicia. ISBN 978-84-614-4014-6.

Autor: Jesús Rodríguez Castro

Jefe del Servicio de Informática del Concello de Santiago de
Compostela

Colegiado del CPEIG

**14. INTEROPERABILIDAD.
COORDINACIÓN
INTERADMINISTRATIVA E
INTEROPERABILIDAD EN EL
MARCO DE LA
ADMINISTRACIÓN
ELECTRÓNICA. INICIATIVAS DE
DESARROLLO DE LA
ADMINISTRACIÓN
ELECTRÓNICA: @FIRMA, DNI
ELECTRÓNICO.**

BLOQUE: ADMINISTRACIÓN ELECTRÓNICA Y SOCIEDAD DE LA INFORMACIÓN

TEMA 14. INTEROPERABILIDAD. COORDINACIÓN ADMINISTRATIVA E INTEROPERABILIDAD EN EL MARCO DE LA ADMINISTRACIÓN ELECTRÓNICA. INICIATIVAS DE DESARROLLO DE LA ADMINISTRACIÓN ELECTRÓNICA: @FIRMA, DNI ELECTRÓNICO

14.1.INTEROPERABILIDAD.

14.2.COORDINACIÓN INTERADMINISTRATIVA E INTEROPERABILIDAD EN EL MARCO DE LA ADMINISTRACIÓN ELECTRÓNICA.

14.3.INICIATIVAS DE DESARROLLO DE LA ADMINISTRACIÓN ELECTRÓNICA: @FIRMA, DNI ELECTRÓNICO.

14.3.1. @FIRMA

14.3.2. DNI ELECTRÓNICO

14.4.REFERENCIAS

14.1.INTEROPERABILIDAD.

La interoperabilidad es la capacidad de los sistemas de información y de los procedimientos a los que éstos dan soporte, de compartir datos y posibilitar el intercambio de información y conocimiento entre ellos.

Resulta necesaria para la cooperación, el desarrollo, la integración y la prestación de servicios conjuntos por las Administraciones públicas; para la ejecución de las diversas políticas públicas; para la realización de diferentes principios y derechos; para la transferencia de tecnología y la reutilización de aplicaciones en beneficio de una mejor eficiencia; para la cooperación entre diferentes aplicaciones que habiliten nuevos servicios;

todo ello facilitando el desarrollo de la administración electrónica y de la sociedad de la información.

En el ámbito de las Administraciones públicas, la consagración del derecho de los ciudadanos a comunicarse con ellas a través de medios electrónicos comporta una obligación correlativa de las mismas. Esta obligación tiene, como premisas, la promoción de las condiciones para que la libertad y la igualdad sean reales y efectivas, así como la remoción de los obstáculos que impidan o dificulten el ejercicio pleno del principio de neutralidad tecnológica y de adaptabilidad al progreso de las tecnologías de la información y las comunicaciones, garantizando con ello la independencia en la elección de las alternativas tecnológicas por los ciudadanos, así como la libertad de desarrollar e implantar los avances tecnológicos en un ámbito de libre mercado.

La Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los servicios públicos (LAECSP), reconoce el protagonismo de la interoperabilidad y se refiere a ella como uno de los aspectos en los que es obligado que las previsiones normativas sean comunes y debe ser, por tanto, abordado por la regulación del Estado.

El Real Decreto 4/2010, de 8 de enero (BOE de 29 de enero. Publicada el 10 de marzo una corrección de errores), por el que se regula el Esquema Nacional de Interoperabilidad en el ámbito de la administración electrónica, regula el citado Esquema previsto en el artículo 42 de la LAECSP, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos. Su objeto es comprender el conjunto de criterios y recomendaciones en materia de seguridad, conservación y normalización de la información, de los formatos y de las aplicaciones que deberán ser tenidos en cuenta por las Administraciones Públicas para la toma de decisiones tecnológicas que garanticen la interoperabilidad. En materia de seguridad, véase el Esquema Nacional de Seguridad regulado en el Real Decreto 3/2010, de 8 de enero.

El Esquema Nacional de Interoperabilidad persigue la creación de las condiciones necesarias para garantizar el adecuado nivel de interoperabilidad técnica, semántica y organizativa de los sistemas y aplicaciones empleados por las Administraciones Públicas, que permita el ejercicio de derechos y el cumplimiento de deberes a través del acceso electrónico a los servicios públicos, a la vez que redunda en beneficio de la eficacia y la eficiencia.

Al objeto de crear estas condiciones, el Esquema Nacional de Interoperabilidad introduce los elementos comunes que han de guiar la actuación de las Administraciones Públicas en materia de interoperabilidad. En particular, introduce los siguientes elementos principales:

- Se enuncian los principios específicos de la interoperabilidad.
- Se contemplan las dimensiones de la interoperabilidad organizativa, semántica y técnica a las que se refiere el artículo 41 de la LAECSP.
- Se tratan las infraestructuras y los servicios comunes, elementos reconocidos de dinamización, simplificación y propagación de la interoperabilidad, a la vez que facilitadores de la relación multilateral.
- Se trata la reutilización, aplicada a las aplicaciones de las administraciones públicas, de la documentación asociada y de otros objetos de información, dado que la voz ‘compartir’ se encuentra presente en la definición de interoperabilidad recogida en la LAECSP, y junto con la voz ‘reutilizar’, ambas son relevantes para la interoperabilidad y se encuentran entroncadas con las políticas de la Unión Europea en relación con la idea de compartir, reutilizar y colaborar.
- Se trata la interoperabilidad de la firma electrónica y de los certificados.
- Se atiende a la recuperación y conservación del documento electrónico, según lo establecido en la citada LAECSP como

manifestación de la interoperabilidad a lo largo del tiempo, y que afecta de forma singular al documento electrónico.

- Por último, se crean las normas técnicas de interoperabilidad y los instrumentos para la interoperabilidad, para facilitar la aplicación del Esquema.
- Tiene en cuenta las recomendaciones de la Unión Europea, la situación tecnológica de las diferentes Administraciones Públicas, así como los servicios electrónicos ya existentes, y la utilización de estándares abiertos así como, en su caso y de forma complementaria, estándares que sean de uso generalizado por los ciudadanos.
- En su elaboración se han manejado, entre otros, referentes en materia de desarrollo de la administración electrónica y, en particular, de interoperabilidad provenientes del ámbito de la Unión Europea, de actuaciones similares en otros países, de la normalización nacional e internacional; así como la normativa sobre administración electrónica, protección de datos de carácter personal, firma electrónica y Documento Nacional de Identidad Electrónico, entre otros.

Se ha realizado en un proceso coordinado por el Ministerio de la Presidencia, con la participación de todas las Administraciones Públicas.

Sus objetivos son los siguientes:

- Comprender los criterios y recomendaciones que deberán ser tenidos en cuenta por las administraciones públicas para la toma de decisiones tecnológicas que garanticen la interoperabilidad y que eviten la discriminación a los ciudadanos por razón de su elección tecnológica.
- Introducir los elementos comunes que han de guiar la actuación de las administraciones públicas en materia de interoperabilidad.

- Aportar un lenguaje común para facilitar la interacción de las administraciones públicas, así como la comunicación de los requisitos de interoperabilidad a la industria.

La interoperabilidad se concibe en consecuencia desde una perspectiva integral, de manera que no caben actuaciones puntuales o tratamientos coyunturales, debido a que la debilidad de un sistema la determina su punto más frágil y, a menudo, este punto es la coordinación entre medidas individualmente adecuadas pero deficientemente ensambladas.

Dada la naturaleza de la interoperabilidad, la consecución de estos objetivos requiere un desarrollo que tenga en cuenta la complejidad técnica, la obsolescencia de la tecnología subyacente y el importante cambio que supone en la operativa de la administración la aplicación de la LAECSP.

El Esquema Nacional de Interoperabilidad en el ámbito de la Administración Electrónica establece, en su disposición adicional primera, el desarrollo de la serie de Normas Técnicas de Interoperabilidad que son de obligado cumplimiento por parte de las Administraciones públicas.

Las Normas Técnicas de Interoperabilidad desarrollan aspectos concretos de diversas cuestiones necesarios para asegurar los aspectos más prácticos y operativos de la interoperabilidad entre las Administraciones públicas y con el ciudadano. La relación de normas incluida en la citada disposición adicional primera es la siguiente¹:

- Catálogo de estándares.
- Documento electrónico(*).
- Digitalización de documentos (*).

¹ Las Normas Técnicas marcadas con el símbolo (*) han sido ya desarrolladas y publicadas en el Boletín Oficial del Estado número 182 del 30 de julio de 2011.

- Expediente electrónico (*).
- Política de firma electrónica y de certificados de la Administración (*).
- Protocolos de intermediación de datos.
- Relación de modelos de datos que tengan el carácter de comunes en la Administración y aquellos que se refieran a materias sujetas a intercambio de información con los ciudadanos y otras administraciones.
- Política de gestión de documentos electrónicos.
- Requisitos de conexión a la Red de comunicaciones de las Administraciones Públicas españolas (*).
- Procedimientos de copiado auténtico y conversión entre documentos electrónicos, así como desde papel u otros medios físicos a formatos electrónicos (*).
- Modelo de Datos para el intercambio de asientos entre las Entidades Registrales (*).

Se están elaborando con la participación de todas las Administraciones públicas, Administración General del Estado, Comunidades Autónomas, Corporaciones Locales a través de la FEMP y Universidades Públicas a través de la CRUE.

Los Ministerios de Política Territorial y Administración Pública y de Industria, Turismo y Comercio lanzaron en 2009 el Proyecto Aporta (<http://www.aporta.es>), con el objetivo de impulsar el sector de la reutilización de la información del sector público (RISP) en nuestro país.

14.2.COORDINACIÓN INTERADMINISTRATIVA E INTEROPERABILIDAD EN EL MARCO DE LA ADMINISTRACIÓN ELECTRÓNICA.

La LAECSP determina que el Comité Sectorial de administración electrónica, dependiente de la Conferencia Sectorial de Administración Pública, es el órgano técnico de cooperación de la Administración General

del Estado, de las administraciones de las Comunidades Autónomas y de las entidades que integran la Administración Local en materia de administración electrónica.

El Comité Sectorial de la administración electrónica velará por el cumplimiento de los fines y principios establecidos en la LAECSP, y en particular desarrollará las siguientes funciones:

- Asegurar la compatibilidad e interoperabilidad de los sistemas y aplicaciones empleados por las Administraciones Públicas.
- Preparar planes programas conjuntos de actuación para impulsar el desarrollo de la administración electrónica en España.
- Asegurar la cooperación entre las administraciones públicas para proporcionar al ciudadano información administrativa clara, actualizada e inequívoca.

Cuando por razón de las materias tratadas resulte de interés podrá invitarse a las organizaciones, corporaciones o agentes sociales que se estime conveniente en cada caso a participar en las deliberaciones del comité sectorial.

Los grupos de trabajo que tiene definidos actualmente son los siguientes:

- Red SARA, a través de la cual se interconectan todas las Administraciones Públicas: Unión Europea, Administración General del Estado, Comunidades Autónomas y Ayuntamientos.
- Identificación y firma electrónica, trabaja en servicios y aspectos relacionado con la armonización de firma electrónica y la expansión del DNI electrónico.
- Mejora de Procesos Software: pretende elaborar unas directrices que permitan mejorar el desarrollo del software, y los procedimientos para su adquisición por parte de las administraciones públicas.

- Observatorio Administración Electrónica (OBSAE): Permite conocer el estado de la Administración electrónica en las administraciones públicas y cuyo principal producto es el informe CAE.
- Programas Libres y reutilización de los sistemas de información: Trabaja en la coordinación entre las diversas distribuciones GNU/Linux autonómicas; la promoción de los estándares abiertos; la consolidación del apoyo a las actuaciones de normalización en curso en materia del Formato Abierto de Documentos (Proyecto ISO/IEC DIS 26300) y en materia de compatibilidad del hardware con GNU/Linux (Grupo Técnico de AENOR AEN GT22). Para reutilización se ha realizado un sistema automatizado que trata la información del inventario de aplicaciones de todas las CCAA y se pretende obtener un marco de reutilización de objetos.

Las Administraciones Públicas utilizarán las tecnologías de la información en sus relaciones con las demás administraciones y con los ciudadanos, aplicando medidas informáticas, tecnológicas, organizativas, y de seguridad, que garanticen un adecuado nivel de interoperabilidad técnica, semántica y organizativa y eviten discriminación a los ciudadanos por razón de su elección tecnológica.

- El Esquema Nacional de Interoperabilidad comprende el conjunto de criterios y recomendaciones en materia de seguridad, conservación y normalización de la información, de los formatos y de las aplicaciones que deberán ser tenidos en cuenta por las Administraciones Públicas para la toma de decisiones tecnológicas que garanticen la interoperabilidad.
- El Esquema Nacional de Seguridad tiene por objeto establecer la política de seguridad en la utilización de medios electrónicos en el ámbito de la presente Ley, y está constituido por los principios

básicos y requisitos mínimos que permitan una protección adecuada de la información.

Ambos Esquemas se han elaborado con la participación de todas las Administraciones y han sido aprobados por Real Decreto del Gobierno, a propuesta de la Conferencia Sectorial de Administración Pública y previo informe de la Comisión Nacional de Administración Local, debiendo mantenerse actualizados de manera permanente.

En la elaboración de ambos Esquemas se tendrán en cuenta las recomendaciones de la Unión Europea, la situación tecnológica de las diferentes Administraciones Públicas, así como los servicios electrónicos ya existentes. A estos efectos considerarán la utilización de estándares abiertos así como, en su caso y de forma complementaria, estándares que sean de uso generalizado por los ciudadanos.

La Administración General del Estado, las Administraciones Autonómicas y las entidades que integran la Administración Local, así como los consorcios u otras entidades de cooperación constituidos a tales efectos por éstas, adoptarán las medidas necesarias e incorporarán en sus respectivos ámbitos las tecnologías precisas para posibilitar la interconexión de sus redes con el fin de crear una red de comunicaciones que interconecte los sistemas de información de las Administraciones Públicas españolas y permita el intercambio de información y servicios entre las mismas, así como la interconexión con las redes de las Instituciones de la Unión Europea y de otros Estados Miembros.

Las Administraciones Públicas podrán suscribir convenios de colaboración con objeto de articular medidas e instrumentos de colaboración para la implantación coordinada y normalizada de una red de espacios comunes o ventanillas únicas.

En particular, y de conformidad con lo dispuesto en el apartado anterior, se implantarán espacios comunes o ventanillas únicas para obtener la información prevista en el artículo 6.3 de la LAECSP y para realizar los trámites y procedimientos a los que hace referencia el apartado a de dicho artículo.

REUTILIZACIÓN DE APLICACIONES Y TRANSFERENCIA DE TECNOLOGÍA

A este respecto, la LAECSP establece que las administraciones titulares de los derechos de propiedad intelectual de aplicaciones, desarrolladas por sus servicios o cuyo desarrollo haya sido objeto de contratación, podrán ponerlas a disposición de cualquier Administración sin contraprestación y sin necesidad de convenio.

Las aplicaciones a las que se refiere el apartado anterior podrán ser declaradas como de fuentes abiertas, cuando de ello se derive una mayor transparencia en el funcionamiento de la Administración Pública o se fomente la incorporación de los ciudadanos a la Sociedad de la información

Las Administraciones Públicas mantendrán directorios actualizados de aplicaciones para su libre reutilización, especialmente en aquellos campos de especial interés para el desarrollo de la administración electrónica y de conformidad con lo que al respecto se establezca en el Esquema Nacional de Interoperabilidad.

La Administración General del Estado, a través de un centro para la transferencia de la tecnología, mantendrá un directorio general de aplicaciones para su reutilización, prestará asistencia técnica para la libre reutilización de aplicaciones e impulsará el desarrollo de aplicaciones, formatos y estándares comunes de especial interés para el desarrollo de la administración electrónica en el marco de los esquemas nacionales de interoperabilidad y seguridad.

En el sitio web del Consejo Superior de Administración Electrónica o CSAE, cuya dirección es <http://www.csae.map.es/>, o a través del Portal de Administración Electrónica o PAE, cuya dirección es <http://administracionelectronica.gob.es/>, es posible acceder al Centro de Transferencia de Tecnología (CTT).

El Centro de Transferencia de Tecnología (CTT) publica un directorio general de aplicaciones y/o iniciativas cuyo objetivo es favorecer la reutilización de soluciones por todas las Administraciones Públicas. Este portal informa de proyectos, iniciativas, servicios, normativa y soluciones que se están desarrollando en materia de Administración electrónica. Además, desde la forja del CTT se permite el desarrollo colaborativo de aplicaciones de las administraciones públicas.

El CTT cuenta con dos entornos tecnológicos en los que trabajar en función de diferentes necesidades.

- El entorno CTT-PAe o directorio de iniciativas del CTT es el lugar indicado para encontrar una iniciativa, proyecto o/y servicio para reutilizar en tu administración. En este entorno está disponible la información divulgativa de todas las iniciativas recogidas en el CTT y se ofrecen diferentes opciones de descarga y de colaboración en ellas.
- El entorno de la forja-CTT, es un entorno de desarrollo colaborativo para aplicaciones de las administraciones públicas en el que pueden participar activamente administraciones, empresas y particulares. Cuenta con funcionalidades de descargas, documentos, novedades, foros, registros de incidencias, bugs, sugerencias, encuestas, distribución de tareas, listas de distribución de correo y gestión del código fuente.

La Ley 37/2007, de 16 de noviembre, sobre reutilización de la información del sector público tiene por objeto la regulación básica del régimen jurídico aplicable a la reutilización de los documentos elaborados o custodiados por las Administraciones y organismos del sector público.

CENATIC es el Centro Nacional de Referencia de Aplicación de las Tecnologías de la Información y la Comunicación (TIC) basadas en fuentes abiertas.

CENATIC es una Fundación Pública Estatal, promovida por el Ministerio de Industria, Turismo y Comercio (a través de la Secretaría de Telecomunicaciones y para la Sociedad de la Información y la entidad pública Red.es) y la Junta de Extremadura, que además cuenta en su Patronato con las comunidades autónomas de Andalucía, Asturias, Aragón, Cantabria, Cataluña, Illes Balears, País Vasco y Xunta de Galicia. También forma parte del Patronato de CENATIC la empresa Telefónica.

CENATIC es el único proyecto estratégico del Gobierno de España para impulsar el conocimiento y uso del software de fuentes abiertas, en todos los ámbitos de la sociedad.

La vocación de la Fundación es posicionarse como centro de excelencia nacional, con proyección internacional tanto en el ámbito europeo como iberoamericano.

14.3. INICIATIVAS DE DESARROLLO DE LA ADMINISTRACIÓN ELECTRÓNICA: @FIRMA, DNI ELECTRÓNICO.

La comunicación a través de medios telemáticos y la administración electrónica requiere el uso de la firma electrónica en la administración. La firma electrónica constituye un instrumento capaz de permitir una

comprobación de la procedencia y de la integridad de los mensajes intercambiados a través de redes de telecomunicaciones, ofreciendo las bases para evitar el repudio, si se adoptan las medidas oportunas basándose en fechas electrónicas.

La utilización de la firma electrónica en la administración pública está regulada en la siguiente normativa, entre otra:

- Directiva 1999/93/CE del Parlamento Europeo y del Consejo, de 13 de diciembre de 1999, por la que se establece un marco comunitario para la firma electrónica
- Ley 59/2003, de 19 de diciembre, de firma electrónica
- LEY 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos.
- Real Decreto 1671/2009, de 6 de noviembre, por el que se desarrolla parcialmente la Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los servicios público.
- Real Decreto 3/2010, de 8 de enero, por el se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica
- Real Decreto 4/2010, de 8 de enero, por el que se regula el Esquema Nacional de Interoperabilidad en el ámbito de la Administración Electrónica

14.3.1. @FIRMA

@firma es una plataforma de validación y firma electrónica multi-PKI, que se pone a disposición de las Administraciones Públicas, proporcionando servicios para implementar la autenticación y firma electrónica avanzada de una forma rápida y efectiva.

Se trata de un proyecto de la Dirección General para el Impulso de la Administración Electrónica, dependiente del Ministerio de Política Territorial y Administración Pública.

Las Administraciones Públicas ofrecen a los ciudadanos, servicios públicos electrónicos en los que se necesita firma electrónica y métodos avanzados de identificación o autenticación basados en certificados digitales. Debido a los múltiples certificados que pueden utilizarse para la identificación y la firma, implantar sistemas que soporten todas las funcionalidades y relaciones con las CA puede resultar complejo y costoso.

Este proyecto se centra en facilitar a las aplicaciones los complementos de seguridad necesarios para implementar la autenticación y firma electrónica avanzada basada en certificados digitales de una forma eficaz y efectiva. Se ofrecen así servicios que impulsan el uso de la certificación y firma electrónica en los sistemas de información de las diferentes Administraciones públicas que así lo requieran.

Es una solución de referencia para cumplir con las medidas de identificación y autenticación descritas en el Capítulo II de la LAECSP.

Desde el punto de vista tecnológico, construye una capa de abstracción de seguridad a nivel de aplicación que desacopla la lógica de negocio de las aplicaciones de la introducción de mecanismos de seguridad a nivel de control de accesos, firma, cifrado, control del no repudio y validez de los certificados, etc.

Facilita la creación de redes de confianza y de reconocimiento mutuo de servicios de validación entre autoridades de validación y los prestadores de certificación acreditados así como primera base para cumplir con el plan de acción i2010 en materia de interoperatividad del IDM (gestión de identidades electrónicas) de la Unión Europea.

El objetivo de esta plataforma de validación es comprobar que el certificado utilizado por el ciudadano es un certificado válido y que no ha

sido revocado y que por tanto sigue teniendo plena validez para identificar a su propietario.

Los servicios de la plataforma son aplicables a todos los certificados electrónicos cualificados publicados por cualquier proveedor de servicio de certificación acreditado en España, incluidos los certificados de la tarjeta del DNle del ciudadano.

A través del conjunto de aplicaciones de la suite @firma se proporcionan unos servicios horizontales de firma y unos componentes informáticos. Estos servicios y aplicaciones se ponen a disposición de las administraciones públicas que lo deseen:

- @firma: Plataforma de validación de certificados y firmas del Ministerio de Política Territorial y Administración Pública
- ClientE de @firma: Applet de generación de firmas en diferentes formatos
- Autoridad de sellado de tiempo del Ministerio de Política Territorial y Administración Pública
- Valide: Aplicación web para el usuario final de validación de firmas y certificados. Demostrador de @firma
- Portafirmas: Componente para la integración de la firma en los flujos de trabajo organizativos
- Stork: Proyecto para conseguir el reconocimiento paneuropeo de las identidades electrónicas, y en concreto la aceptación del DNI electrónico e identificadores similares en Servicios de Administración Electrónica de otras administraciones europeas
- Política de firma y certificados: directrices y normas técnicas aplicables a la utilización de certificados y firma electrónica en la Administración General del Estado

Cuando el ciudadano interacciona con la Administración, para realizar un

trámite personal, es necesario conocer su identidad, que telemáticamente se realiza a través del DNI electrónico o un certificado electrónico. La Administración comprueba el estado del certificado o el DNLe con el que el ciudadano se está identificando o firmando la solicitud. Para esta comprobación se utiliza la plataforma de validación @firma, delegando en ella la verificación de las credenciales del certificado o DNLe utilizado.

Además, dispone de múltiples utilidades de valor añadido, entre las que se encuentran la generación y validación de firmas electrónicas en múltiples formatos, auditoría de las transacciones y documentos firmados, sellado de tiempos o la compatibilidad con certificados digitales generados por múltiples prestadores de servicios de certificación.

La plataforma de validación del Ministerio de la Política Territorial y Administración Pública funciona como un servicio no intrusivo o cerrado, que puede ser utilizado por todos los servicios telemáticos ofrecidos por las distintas Administraciones Públicas.

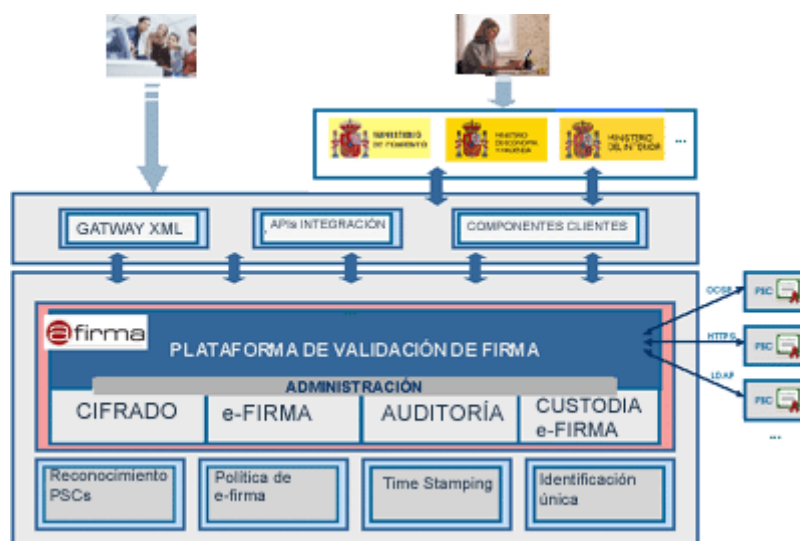
Los servicios ofrecidos a los organismos se pueden catalogar en cuatro bloques, basándose la mayoría en la publicación de un catálogo amplio de servicios web compatible con las tecnologías java y Microsoft. Todos los servicios web se encuentran disponibles tanto en castellano como en inglés, facilitando así la integración e interoperabilidad con soluciones existentes en las implantaciones de los organismos usuarios.

1. Servicios de validación: servicios web de validación de firmas digitales en múltiples formatos y certificados electrónicos de diferentes perfiles y prestadores.
2. Servicios de firma electrónica: firma electrónica de servidor simple, en paralelo (cosign), en cascada (countersign) o en bloque. En estos momentos estos servicios no se están manteniendo y actualizando, por ello se proporciona un componente de firma

electrónica para entorno de usuario final. Actualización de firmas electrónicas a un formato más avanzado, para ello es posible especificar el formato al que se desea extender la firma. Los distintos valores pueden ser: BES, EPES, T, C, X, X-1, X-2, X-L, X-L-1, X-L-2 y A. Soporta los algoritmos de hash SHA1 y SHA2 y los algoritmos de firma RSA y curvas elípticas. Validación longeva de firmas.

3. Servicios de soporte a la Operación: a través de servicios de soporte a la integración, apoyo a la evolución hacia nuevos estándares de firma electrónica, etc.

Esquema de funcionamiento de la plataforma de validación.



La plataforma de validación @firma en su versión 5.5 proporciona servicios de validación de certificados y de firma electrónica de los principales Prestadores de Servicios de Certificación reconocidos de nuestro país, entre ellos la Dirección General de Policía.

Los servicios que ofrece son:

1. Funcionalidades de verificación: Validación de certificados X.509 según la RFC 3280, de las Autoridades de Certificación incluidas en la plataforma. Entre las funcionalidades de validación se pueden destacar:
 - Reconocimiento y validación del DNI electrónico emitido por la Dirección General de la Policía, y de múltiples prestadores.
 - Validación de certificados X.509 según la RFC 3280, de todas las Autoridades de Certificación reconocidas en el país por el Ministerio de Industria
 - Validación Multinivel de certificados (en el caso de estructura de certificación de más de dos niveles).
 - Obtención mediante un análisis en XML, de la información correspondiente a los campos del certificado, según la Política de Confianza definida para el tipo de certificado de que se trate.
 - Caché de validación configurable en tiempo, para evitar tener que acceder al Proveedor de Servicios de Certificación ante validaciones de un mismo certificado en un corto período de tiempo.

2. Funcionalidades de Firma: La plataforma permite varias modalidades de firma como de servidor, de bloque, en dos fases y en tres fases (En estos momentos los servicios de firma en servidor no se están manteniendo y actualizando). Además:
 - Hace transparente para las aplicaciones el uso de diferentes formatos de firma electrónica como PKCS#7, CMS, XML signature, PDF, ODF, XAdES y CAdES
 - Se ofrece un Cliente de firma que permite la firmar electrónica de documentos por parte de los ciudadanos que accedan a los servicios de Administración Electrónica. Para ello se emplean los certificados digitales de usuario que se hallan instalados en el navegador o disponibles a través de un módulo PKCS#11 instalado en el navegador. Dicho cliente es compatible con los S.O. Windows XP, 2000 y Linux; y con navegadores Mozilla Firefox e Internet Explorer.

- Validación de firma vía servicios web (WS) de un elemento firmado, indicando si la firma es correcta y la validez, fechado de tiempo, etc. También se realiza la interpretación de los campos de los certificados a un XML homogéneo.
 - Permite la actualización de firmas electrónicas a un formato más avanzado, para ello es posible especificar el formato al que se desea extender la firma. Los distintos valores pueden ser: BES, EPES, T, C, X, X-1, X-2, X-L, X-L-1, X-L-2 y A.
 - En estos momentos los algoritmos de hash soportados son SHA1 y SHA2 (el resto se hallan obsoletos).
 - En estos momentos los algoritmos de firma digital soportados son RSA y curvas elípticas.
3. Sellado de Tiempo (TSA) Se incluye un servicio de sellado de tiempo según el estándar RFC 3161 para certificar temporalmente todas las operaciones de validación y firma que se realizan a través de la plataforma.
4. Gestión y administración: La plataforma realiza la gestión y administración de los Prestadores de Servicios de Certificación adheridos. Todas las operaciones realizadas en la plataforma son registradas para la auditoria y trazabilidad del sistema.

Los beneficios que la plataforma facilita a los organismos son:

1. El reconocimiento de múltiples certificados.
2. Independencia del prestadores de servicios de certificación ya que soporta de varios protocolos de validación de certificados (OCSP, HTTP, LDAP).
3. El uso de Políticas de Seguridad para garantizar la confidencialidad, autenticidad e integridad de todas las transacciones realizadas.
4. Mayor eficiencia y menor coste en la utilización de la firma electrónica en los servicios telemáticos prestados.

5. Hace transparente para las aplicaciones el uso de diferentes formatos de firma electrónica como PKCS#7, CMS, XML signature, XAdES y CAdES
6. La interoperabilidad con los servicios proporcionados por las Administraciones Públicas. Se ha ce extensible la interoperabilidad al ámbito Europeo y al de sus organismos e instituciones al ser contempladas las especificaciones de compatibilidad con la Unión Europea.
7. Reducción de costes: el servicio permite optimizar el coste de los servicios de validación de certificados por cada aplicación.
8. Innovación: la plataforma de la validación multi-PKI se ha convertido en el primer servicio centralizado principal que proporciona servicios electrónicos horizontales a todas las Administraciones Públicas del país gratuitamente.
9. Buenas prácticas: trasladar el modelo español a foros europeos y a los grupos de trabajo de e-signature de IDABC.

Se puede encontrar en el Portal PAE-CTT la documentación necesaria sobre cada actualización en los servicios, así como los recursos actualizados (esquemas y descriptores de servicio).

Además, en la dirección <https://valide.redsara.es/valide/> se puede acceder a VALIDe, el servicio de validación y demostrador de firma electrónica.

14.3.2. DNI ELECTRÓNICO

Además de toda la legislación relativa a la utilización de certificados electrónicos, el DNle electrónico se encuentra regulado en el Real Decreto 1553/2005, de 23 de diciembre, por el que se regula la expedición del Documento Nacional de Identidad y sus certificados de firma electrónica (BOE núm. 307, de 24 de diciembre de 2005). Se transcriben a

continuación los principales artículos, especialmente los relativos a la incorporación y utilización de certificados electrónicos.

El Documento Nacional de Identidad es un documento personal e intransferible emitido por el Ministerio del Interior que goza de la protección que a los documentos públicos y oficiales otorgan las leyes. Su titular estará obligado a la custodia y conservación del mismo.

Dicho Documento tiene suficiente valor, por sí solo, para acreditar la identidad y los datos personales de su titular que en él se consignan, así como la nacionalidad española del mismo.

A cada Documento Nacional de Identidad, se le asignará un número personal que tendrá la consideración de identificador numérico personal de carácter general.

Igualmente, el Documento Nacional de Identidad permite a los españoles mayores de edad y que gocen de plena capacidad de obrar la identificación electrónica de su titular, así como realizar la firma electrónica de documentos, en los términos previstos en la Ley 59/2003, de 19 de diciembre, de firma electrónica.

La firma electrónica realizada a través del Documento Nacional de Identidad tendrá respecto de los datos consignados en forma electrónica el mismo valor que la firma manuscrita en relación con los consignados en papel.

Será competencia del Ministerio del Interior el ejercicio de las funciones relativas a la gestión, dirección, organización, desarrollo y administración de todos aquellos aspectos referentes a la expedición y confección del Documento Nacional de Identidad, conforme a lo previsto en la legislación en materia de seguridad ciudadana y de firma electrónica.

El ejercicio de las competencias a que se refiere el apartado anterior, incluida la emisión de los certificados de firma electrónica reconocidos, será realizado por la Dirección General de la Policía, a quien corresponderá también la custodia y responsabilidad de los archivos y ficheros, automatizados o no, relacionados con el Documento Nacional de Identidad. A tal efecto, la Dirección General de la Policía quedará sometida a las obligaciones impuestas al responsable del fichero por la Ley Orgánica 15/1999, de 13 de septiembre, de Protección de Datos de Carácter Personal.

El Documento Nacional de Identidad se expedirá a solicitud del interesado en la forma y lugares que al efecto se determinen, para lo cual deberá aportar los documentos que se establecen en el artículo 5.1 de este Real Decreto.

Para solicitar la expedición del Documento Nacional de Identidad será imprescindible la presencia física de la persona a quien se haya de expedir, el abono de la tasa legalmente establecida en cada momento y la presentación de la correspondiente documentación.

Con carácter general el Documento Nacional de Identidad tendrá un período de validez, a contar desde la fecha de la expedición o de cada una de sus renovaciones, de:

- a) Cinco años, cuando el titular no haya cumplido los treinta al momento de la expedición o renovación
- b) Diez años, cuando el titular haya cumplido los treinta y no haya alcanzado los setenta.
- c) Permanente cuando el titular haya cumplido los setenta años.

De forma excepcional se podrá otorgar validez distinta al Documento Nacional de Identidad en los siguientes supuestos de expedición y renovación:

- a) Permanente, a personas mayores de treinta años que acrediten la condición de gran inválido.
- b) Por un año, en los supuestos del apartado segundo del artículo 5 y del mismo apartado del artículo 7.

Transcurrido el período de validez que para cada supuesto se contempla en el artículo anterior, el Documento Nacional de Identidad se considerará caducado y quedarán sin efecto las atribuciones y efectos que le reconoce el ordenamiento jurídico, estando su titular obligado a proceder a la renovación del mismo. Dicha renovación se llevará a cabo mediante la presencia física del titular del Documento.

Independientemente de los supuestos del apartado anterior se deberá proceder a la renovación del Documento Nacional de Identidad en los supuestos de variación de los datos que se recogen en el mismo, en cuyo caso será preciso aportar, además de lo establecido en el apartado anterior, los documentos justificativos que acrediten dicha variación.

El extravío, sustracción, destrucción o deterioro del Documento Nacional de Identidad, conllevará la obligación de su titular de proveerse inmediatamente de un duplicado, que será expedido en la forma y con los requisitos indicados para la renovación prevista en el apartado primero del artículo anterior. La validez de estos duplicados será la misma que tenían los Documentos a los que sustituyen, salvo que éstos se hallen dentro de los últimos 90 días de su vigencia, en cuyo caso se expedirán con la misma validez que si se tratara de una renovación.

La entrega del Documento Nacional de Identidad deberá realizarse personalmente a su titular, y cuando éste sea menor de 14 años o incapaz

se llevará a cabo en presencia de la persona que tenga encomendada la patria potestad o tutela, o persona apoderada por estas últimas. En el momento de la entrega del Documento Nacional de Identidad se proporcionará la información a que se refiere el artículo 18. b) de la Ley 59/2003, de 19 de diciembre.

La activación de la utilidad informática a que se refiere el artículo 1.4, que tendrá carácter voluntario, se llevará a cabo mediante una clave personal secreta, que el titular del Documento Nacional de Identidad podrá introducir reservadamente en el sistema.

Al entregar el Documento renovado, se procederá a la retirada del anterior para su inutilización física. Una vez inutilizado podrá ser devuelto a su titular si éste lo solicita.

El material, formato y diseño de la tarjeta soporte del Documento Nacional de Identidad se determinará por el Ministerio del Interior, teniendo en cuenta en su elaboración la utilización de procedimientos y productos conducentes a la consecución de condiciones de calidad e inalterabilidad y máximas garantías para impedir su falsificación. Llevará incorporado un chip electrónico al objeto de posibilitar la utilidad informática a que se refiere el artículo 1.4 de este Real Decreto.

El Documento Nacional de Identidad recogerá gráficamente los siguientes datos de su titular:

- En el anverso: Apellidos y nombre, fecha de nacimiento, sexo, nacionalidad, Número personal del Documento Nacional de Identidad y carácter de verificación correspondiente al Número de Identificación Fiscal, fotografía, firma manuscrita.

- En el reverso: Lugar de nacimiento, provincia-nación, nombre de los padres, domicilio, lugar de domicilio, provincia, nación, Caracteres OCR-B de lectura mecánica.

Los datos de filiación se reflejarán en los mismos términos en que consten en la certificación a la que se alude en el artículo 5.1.a) de este Real Decreto, excepto en el campo de caracteres OCR-B de lectura mecánica, en que por aplicación de acuerdos o convenios internacionales la transcripción literal de aquellos datos impida o dificulte la lectura mecánica y finalidad de aquellos caracteres.

Igualmente constarán los siguientes datos referentes al propio Documento y a la tarjeta soporte: Fecha de caducidad y número de soporte.

El chip incorporado a la tarjeta soporte contendrá:

- Datos de filiación del titular.
- Imagen digitalizada de la fotografía.
- Imagen digitalizada de la firma manuscrita.
- Plantilla de la impresión dactilar del dedo índice de la mano derecha o, en su caso, del que corresponda según lo indicado en el artículo 5.3 de este Real Decreto.
- Certificados reconocidos de autenticación y de firma, y certificado electrónico de la autoridad emisora, que contendrán sus respectivos períodos de validez.
- Claves privadas necesarias para la activación de los certificados mencionados anteriormente.

Con independencia de lo que establece el artículo 6.1 sobre la validez del Documento Nacional de Identidad, los certificados electrónicos reconocidos incorporados al mismo tendrán un período de vigencia de treinta meses.

A la extinción de la vigencia del certificado electrónico, podrá solicitarse la expedición de nuevos certificados reconocidos, manteniendo la misma tarjeta del Documento Nacional de Identidad mientras dicho Documento continúe vigente. Para la solicitud de un nuevo certificado deberá mediar la presencia física del titular en la forma y con los requisitos que se determinen por el Ministerio del Interior, de acuerdo con lo previsto en la Ley 59/2003, de 19 de diciembre.

El cumplimiento del período establecido en el apartado anterior implicará la inclusión de los certificados en la lista de certificados revocados que será mantenida por la Dirección General de la Policía, bien directamente o a través de las entidades a las que encomiende su gestión.

La pérdida de validez del Documento Nacional de Identidad llevará aparejada la pérdida de validez de los certificados reconocidos incorporados al mismo. La renovación del Documento Nacional de Identidad o la expedición de duplicados del mismo implicará, a su vez, la expedición de nuevos certificados electrónicos.

También serán causas de extinción de la vigencia del certificado reconocido las establecidas en la Ley 59/2003, de 19 de diciembre, que resulten de aplicación, y, entre otras, el fallecimiento del titular del Documento Nacional de Identidad electrónico.

De acuerdo y en cumplimiento del artículo 19 de la Ley 59/2003, de 19 de diciembre, el Ministerio del Interior formulará una Declaración de Prácticas y Políticas de Certificación. Dicha Declaración de Prácticas y Políticas de Certificación estará disponible al público de manera permanente y fácilmente accesible en la página de Internet del Ministerio del Interior.

La documentación requerida para la expedición del Documento Nacional de Identidad en el artículo 5.1 de este Real Decreto no será exigible cuando

sea posible remitir ésta desde los órganos competentes por medios telemáticos a la Dirección General de la Policía, de conformidad con lo que se establezca mediante Convenio.

En estos casos, por Orden del Ministro del Interior se establecerá el régimen de aportación de dichos documentos.

Con la llegada de la Sociedad de la Información y la generalización del uso de Internet se hace necesario adecuar los mecanismos de acreditación de la personalidad a la nueva realidad y disponer de un instrumento eficaz que traslade al mundo digital las mismas certezas con las que operamos cada día en el mundo físico y que, esencialmente, son:

- Acreditar electrónicamente y de forma indubitada la identidad de la persona
- Firmar digitalmente documentos electrónicos, otorgándoles una validez jurídica equivalente a la que les proporciona la firma manuscrita

Para responder a estas nuevas necesidades nace el Documento Nacional de Identidad electrónico (DNle), similar al tradicional y cuya principal novedad es que incorpora un pequeño circuito integrado (chip), capaz de guardar de forma segura información y de procesarla internamente.

Para poder incorporar este chip, el Documento Nacional de Identidad cambia su soporte tradicional (cartulina plastificada) por una tarjeta de material plástico, dotada de nuevas y mayores medidas de seguridad. A esta nueva versión del Documento Nacional de Identidad nos referimos como DNI electrónico nos permitirá, además de su uso tradicional, acceder a los nuevos servicios de la Sociedad de la Información, que ampliarán nuestras capacidades de actuar a distancia con las Administraciones Públicas, con las empresas y con otros ciudadanos.

La Autoridad de Validación es el componente que tiene como tarea suministrar información sobre la vigencia de los certificados electrónicos que, a su vez, hayan sido registrados por una Autoridad de Registro y certificados por la Autoridad de Certificación.

La información sobre los certificados electrónicos revocados (no vigentes) se almacena en las denominadas listas de revocación de certificados (CRL).

En la Infraestructura de Clave Pública (PKI) adoptada para el DNI electrónico, se ha optado por asignar las funciones de Autoridad de Validación a entidades diferentes de la Autoridad de Certificación, a fin de aislar la comprobación de la vigencia de un certificado electrónico de los datos de identidad de su titular.

Así, la Autoridad de Certificación (Ministerio del Interior – Dirección General de la Policía) no tiene en modo alguno acceso a los datos de las transacciones que se realicen con los certificados que ella emite y las Autoridades de Validación no tiene acceso a la identidad de los titulares de los certificados electrónico que maneja, reforzando la transparencia del sistema.

Para la validación del DNI electrónico se dispone de dos prestadores de Servicios de Validación:

- Fábrica Nacional de Moneda y Timbre – Real Casa de la Moneda, que prestará sus servicios de validación con carácter universal: ciudadanos, empresas y Administraciones Públicas.
- Ministerio de la Presidencia, que prestará los servicios de validación al conjunto de las Administraciones Públicas.

La prestación de estos servicios de validación se realiza en base al protocolo Online Certificate Status Protocol (OCSP), lo que, en esencia, supone que un cliente OCSP envía una petición sobre el estado del certificado a la Autoridad de Validación, la cual, tras consultar su base de datos, ofrece vía HTTP una respuesta sobre el estado del certificado. El servicio de validación está disponible de forma ininterrumpida todos los días del año.

El DNI electrónico incluye dos certificados electrónicos, que son el conjunto de datos incluidos en el chip, que permiten la identificación de su titular (Certificado de Autenticación) y la firma electrónica de documentos (Certificado de Firma).

Los datos se alojan en dos partes del chip de la tarjeta: pública y privada. La primera contiene los datos básicos de los certificados y una clave pública, mientras que la parte privada contiene la clave privada de la tarjeta, sólo conocida por su titular. La generación de claves se realiza dentro de la tarjeta criptográfica y en presencia de su titular.

Para poder realizar transacciones electrónicas con el DNI electrónico es necesario:

- Un lector de tarjetas inteligentes (con chip), con sus correspondiente drivers.
- La librería para hacer uso del DNle: CSP (para S.O. Microsoft) o PKCS#11
- Una conexión a Internet para realizar las transacciones telemáticas.

El lector de DNle debe cumplir las características técnicas siguientes:

- Debe cumplir el estándar ISO 7816 (1, 2 y 3)
- Debe soportar tarjetas asíncronas basadas en protocolos T=0 (y T=1)
- Debe soportar velocidades de comunicación mínimas de 9.600 bps.
- Debe soportar los estándares siguientes:

- API PC/SC (Personal Computer/Smart Card)
- CSP (Cryptographic Service Provider, Microsoft)
- API PKCS#11

En la estructura de las tarjetas inteligentes que cumplen con el estándar PKCS#15 existe un fichero elemental denominado CDF (Certificate Directory File). La finalidad de este fichero es contener certificados o índices a certificados. En el caso del DNle el CDF contiene una estructura con codificación ASN.1 que incorpora la referencia interna a los certificados de ciudadano y los atributos countryName, serialNumber, surname, givenName y commonName que aparecen en el certificado x509 v3 de autenticación del ciudadano. También se han incorporado a la estructura los atributos organizationName, organizationalUnitName y el commonName de la autoridad de certificación subordinada que expidió el certificado del ciudadano. El EF implicado tiene como identificador 6004.

Con el fin de facilitar y fomentar el uso del DNle, se ha puesto a disposición de los ciudadanos un sitio web con la dirección <http://www.dnielectronico.es/>.

14.4. REFERENCIAS

- Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común.
- Ley 15/1999, de 13 de diciembre, de Protección de datos de carácter personal
- Ley 53/1999, de 19 de diciembre, de Firma electrónica.
- Ley 34/2002, de 11 de julio, de Servicios de la sociedad de la información y de comercio electrónico.
- Real Decreto 1553/2005, de 23 de diciembre, por el que se regula la expedición del Documento Nacional de Identidad y sus certificados de firma electrónica (BOE núm. 307, de 24 de diciembre de 2005).
- Ley 11/2007, de 22 de junio, de Acceso electrónico dos cidadanos a los servicios públicos.
- Ley 37/2007, de 16 de noviembre, sobre Reutilización de la información del sector público.
- Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley 15/1999, de 13 de diciembre, de protección de datos de carácter personal.
- Ley 56/2007, de 28 de diciembre, de Medidas de impulso de la sociedad de la Información.
- Real Decreto 1494/2007, de 12 de noviembre, por el que se aprueba el Reglamento sobre las condiciones básicas para el acceso de las personas con discapacidad a las tecnologías, productos y servicios relacionados con la sociedad de la información y medios de comunicación social.
- Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito da Administración Electrónica.
- Real Decreto 4/2010, de 8 de enero, por el que se regula el Esquema Nacional de Interoperabilidad en el ámbito da Administración Electrónica.

- Decreto 198/2010, de 2 de diciembre, por el que se regula el Desarrollo de la Administración Electrónica en la Xunta de Galicia y en las entidades dependientes.
- Resoluciones de la Secretaría de Estado para la Función Pública por la que se aprueban distintas normas técnicas de interoperabilidad.
- “Manual práctico de supervivencia de la Administración Electrónica”, de Alberto López Tallón, publicado bajo licencia Creative Commons.
- “Anotacións e comentarios ao Decreto de Administración Electrónica da Xunta de Galicia”, editado polo Colexio Profesional de Enxeñaría en Informática de Galicia coa colaboración da Xunta de Galicia. ISBN 978-84-614-7362-5.
- “Construyendo la identidad digital. Situación actual de la firma electrónica y de las entidades de certificación”, editado polo Colexio Profesional de Enxeñaría en Informática de Galicia. ISBN 978-84-614-6072-4.
- “Las relaciones de la empresa con la Administración Electrónica”, editado polo Colexio Profesional de Enxeñaría en Informática de Galicia. ISBN 978-84-614-9865-9.
- “Empresa, protección de datos y Administración Electrónica”, editado polo Colexio Profesional de Enxeñaría en Informática de Galicia. ISBN 978-84-614-4014-6.

Autor: Jesús Rodríguez Castro

Jefe del Servicio de Informática del Concello de Santiago de
Compostela

Colegiado del CPEIG

**15. SERVICIOS HORIZONTALES
DE ADMINISTRACIÓN
ELECTRÓNICA.
IDENTIFICACIÓN Y
AUTENTICACIÓN DE LOS
FUNCIONARIOS, CIUDADANOS
Y DE LAS ADMINISTRACIONES
PÚBLICAS. ACREDITACIÓN Y
REPRESENTACIÓN DE LOS
CIUDADANOS. FIRMA
ELECTRÓNICA, INTERCAMBIO
DE CERTIFICADOS, SELLADO
DE TIEMPO (TIME-STAMPING).
PAGO ELECTRÓNICO Y
NOTIFICACIONES
TELEMÁTICAS.**

BLOQUE: ADMINISTRACIÓN ELECTRÓNICA Y SOCIEDAD DE LA INFORMACIÓN

TEMA 15. SERVICIOS HORIZONTALES DE LA ADMINISTRACIÓN ELECTRÓNICA. IDENTIFICACIÓN Y AUTENTIFICACIÓN DE LOS FUNCIONARIOS, DE LOS CIUDADANOS, Y DE LAS ADMINISTRACIONES PÚBLICAS. ACREDITACIÓN Y REPRESENTACIÓN DE LOS CIUDADANOS. FIRMA ELECTRÓNICA, INTERCAMBIO DE CERTIFICADOS, SELLADO DE TEMPO (TIME-STAMPING). PAGO ELECTRÓNICO Y NOTIFICACIONES TELEMÁTICAS.

15.1.SERVICIOS HORIZONTALES DE LA ADMINISTRACIÓN ELECTRÓNICA.

15.2.IDENTIFICACIÓN Y AUTENTIFICACIÓN DE LOS FUNCIONARIOS, DE LOS CIUDADANOS, Y DE LAS ADMINISTRACIONES PÚBLICAS.

15.3.ACREDITACIÓN Y REPRESENTACIÓN DE LOS CIUDADANOS.

15.4.FIRMA ELECTRÓNICA, INTERCAMBIO DE CERTIFICADOS, SELLADO DE TEMPO (TIME-STAMPING).

15.4.1. FIRMA ELECTRÓNICA

15.4.2. INTERCAMBIO DE CERTIFICADOS

15.4.3. SELLADO DE TIEMPO (TIME-STAMPING)

15.5.PAGO ELECTRÓNICO Y NOTIFICACIONES TELEMÁTICAS.

15.5.1. PAGO ELECTRÓNICO

15.5.2. NOTIFICACIONES TELEMÁTICAS

15.6.REFERENCIAS

15.1.SERVICIOS HORIZONTALES DE LA ADMINISTRACIÓN ELECTRÓNICA.

Uno de los objetivos de la Administración Electrónica es ofrecer servicios públicos electrónicos que contribuyan a mejorar la vida de los ciudadanos.

Para ello se han desarrollado un conjunto de servicios horizontales, utilizables por cualquier Administración, que ayudan a acelerar el proceso de implantación de la Administración Electrónica.

Dichos servicios comunes se agrupan en las siguientes materias:

- Interconexión entre Administraciones.
- Firma Electrónica
- Tramitación electrónica
- Normativa, Regulación y Recomendaciones
- Servicios integrales
- Información y difusión
- Herramientas de apoyo
- Gestión de Recursos Humanos en la Administración General del Estado

RED SARA

El artículo 43 de la ley 11/2007 establece la obligación de crear una red de comunicaciones que interconecte las Administraciones Públicas españolas entre sí y con otras redes de las Instituciones Europeas y de otros Estados miembros, para el intercambio de información y servicios entre ellas.

La Red SARA permite la interconexión de las Administraciones Públicas, facilitando el intercambio de información y servicios entre ellas. A través de la Red SARA los Ministerios, las Comunidades Autónomas, los Entes Locales y otros organismos públicos pueden interconectar sus redes de una manera fiable, segura, capaz y flexible.

Además, a través del enlace de la Red SARA con la red transeuropea sTESTA las Administraciones Públicas españolas se pueden interconectar con redes de instituciones europeas y de administraciones de otros Estados

miembros de la UE, para el despliegue y acceso a los servicios paneuropeos de Administración electrónica.

Características de SARA

- **Fiabilidad:** La red SARA está diseñada con tecnología de última generación VPLS (Virtual Private LAN Services) que la dota de gran capacidad de transmisión de datos y muy alta disponibilidad.
- **Seguridad:** La red SARA implementa medidas de seguridad entre las que destaca el establecimiento de VPNs. Es una red extremadamente segura en la que todo el tráfico circula cifrado por la Troncal.
- **Capacidad:** La red SARA cuenta con un ancho de banda de 1 Gbps en Ministerios y CPDs, y 100 Mbps en cada Comunidad Autónoma.
- **Calidad de Servicio (QoS):** La tecnología VPLS permite dotar a la red de mecanismos de calidad de servicio para todo tipo de tráfico.
- **Punto-Multipunto:** La red SARA está diseñada con un modelo de conexión punto-multipunto mediante el cual no existe un nodo central en el que convergen todas las conexiones y por tanto se eliminan posibles puntos únicos de fallo. Los mecanismos de seguridad están distribuidos en cada nodo, si bien la política es homogénea y con gestión centralizada.
- **Flexibilidad:** La red SARA está diseñada para poder evolucionar y crecer a la medida que lo hagan las necesidades de la Administración.

La red SARA permite que las administraciones compartan entre ellas todos los servicios que estimen necesarios. Además existen servicios comunes que facilitan el despliegue de la oferta de Administración electrónica, y a los que las diferentes administraciones pueden acceder, tales como los siguientes:

- Verificación de los datos de identidad y residencia.

- Plataforma de validación de firma electrónica (@firma).
- Solicitud de cambio de domicilio.
- Notificación electrónica fehaciente.
- Pasarela de pago.
- Registro electrónico común.
- Consultas del estado de expedientes.
- Catálogos de procedimientos de las AAPP.
- Videoconferencia.
- Voz IP.
- Entornos de trabajo en colaboración.

PLAN DE DIRECCIONAMIENTO E INTERCONEXIÓN DE REDES

El Plan de direccionamiento e interconexión de redes en la Administración define un espacio de direccionamiento privado común para los Centros de la Administración. Este Plan permite que cada entidad u organismo pueda establecer de manera independiente sus planes de numeración IP, en función de su infraestructura de red, o distribución orgánica o departamental, pero manteniendo una coordinación con el resto de Administraciones Públicas que evite el uso de direcciones duplicadas.

SUITE DE PRODUCTOS RELACIONADOS CON LA FIRMA ELECTRÓNICA

Se ha creado una suite de productos relacionados con la firma electrónica para impulsar y facilitar la implantación de sistemas de firma y autenticación en la Administración Pública, que son objeto de estudio en otros apartados de esta documentación.

SERVICIOS COMUNES PARA EL INTERCAMBIO DE DATOS

Se han desarrollado una serie de productos para impulsar y facilitar la verificación y consulta de datos en la Administración Pública, fomentando

la reutilización de soluciones con la finalidad primordial de ofrecer un punto centralizado de servicios de verificación de datos como es la Plataforma de Intermediación, facilitando la interoperabilidad entre las Administraciones Públicas.

Es una solución de referencia para cumplir el artículo 6.2b de la LAECSP.

Se proporcionan unos servicios horizontales de consulta y verificación de datos, así como componentes y aplicaciones informáticas que los desarrollan, y se ponen a disposición de las Administraciones Públicas que lo deseen de manera gratuita:

- Plataforma de Intermediación: Ofrece un conjunto de servicios de verificación y consulta de datos que permite a cualquier organismo público verificar, en tiempo real, los datos relativos a un ciudadano que ha iniciado un trámite con una entidad y que son necesarios para la resolución del trámite.
- SCSP: Es un protocolo que facilita la interoperabilidad e intercambio de datos entre las AAPP con el objetivo de evitar que el ciudadano tenga que presentar certificados en papel, de datos que la Administración ya tiene. Estos certificados se sustituyen por un intercambio de datos entre Administraciones Públicas.
- Broker SCCD: Servicio web para permitir la comunicación del cambio de domicilio desde los Ayuntamientos (y Comunidades Autónomas) hacia los organismos tramitadores de la Administración General del Estado (AEAT, DGP, TGSS, INSS, MUFACE, etc...)

SUITE DE PRODUCTOS RELACIONADOS CON LA GESTIÓN DE RECURSOS HUMANOS EN LA ADMINISTRACIÓN GENERAL DEL ESTADO.

Dentro de los servicios comunes proporcionados por la Dirección General para el Impulso de la Administración Electrónica se ha creado una suite de

productos relacionados con la gestión de RRHH en la Administración General del Estado para fomentar la reutilización de soluciones con la finalidad primordial de ofrecer servicios para la confección de nóminas, gestión de los procedimientos de RRHH departamentales e interdepartamentales, gestión del Plan de Pensiones de la AGE, consulta de información para la toma de decisiones en el ámbito de los RRHH de las Administraciones Públicas y del Registro Central de Personal, y presentación de propuestas de modificación de Relaciones de Puestos de Trabajo a la Comisión Ejecutiva de la Comisión Interministerial de Retribuciones CECIR.

A través del conjunto de aplicaciones de gestión de RRHH de la AGE se proporcionan unos servicios horizontales de gestión y unos componentes informáticos. Estos servicios y aplicaciones se ponen a disposición de la Administración General del Estado:

- Portal del empleado Funciona: Portal de información y servicios que proporciona un espacio virtual de relación, colaboración y gestión del conocimiento para el personal de la Administración General del Estado.
- Sistema de Nómina Estándar de la Administración del Estado: Gestión completa de nómina de centros, entidades y organismos de la Administración del Estado.
- Sistema de Información del Registro Central de Personal (RCP): El RCP inscribe al personal al servicio de la Administración General del Estado y anota los actos relevantes de su vida administrativa. Los sistemas de información son:
 - Sistema de Información del Registro Central de Personal (RCP): Anotaciones registrales, relaciones de puestos de trabajo y estructura orgánica de la AGE.
 - Sistema de información a la Dirección y minería de datos SID – eSIR.

- Sistema de archivo electrónico de imágenes de documentos registrales.
- Sistema de Gestión BADARAL: Sistema de información integrado con el Registro Central de Personal y el Portal CECIR para apoyo a los gestores de RRHH de la AGE. Gestión de Concursos, Plan de Pensiones AGE, permisos y licencias, Situaciones de Incapacidad Temporal, entre otros.
- Sistema Integrado de Gestión de Personal SIGP: Sistema para la gestión electrónica de procedimientos de gestión de RRHH de la AGE.
- Portal CECIR: Espacio de trabajo para los gestores de Recursos Humanos de los Departamentos Ministeriales y la CECIR.

15.2. IDENTIFICACIÓN Y AUTENTIFICACIÓN DE LOS FUNCIONARIOS, DE LOS CIUDADANOS, Y DE LAS ADMINISTRACIONES PÚBLICAS.

La LAECSP establece que las Administraciones Públicas admitirán, en sus relaciones por medios electrónicos, sistemas de firma electrónica que sean conformes a lo establecido en la Ley 59/2003, de 19 de diciembre, de Firma electrónica y resulten adecuados para garantizar la identificación de los participantes y, en su caso, la autenticidad e integridad de los documentos electrónicos.

Los ciudadanos podrán utilizar los siguientes sistemas de firma electrónica para relacionarse con las Administraciones Públicas, de acuerdo con lo que cada Administración determine:

- a) En todo caso, los sistemas de firma electrónica incorporados al Documento Nacional de Identidad, para personas físicas.
- b) Sistemas de firma electrónica avanzada, incluyendo los basados en certificado electrónico reconocido, admitidos por las Administraciones Públicas.

- c) Otros sistemas de firma electrónica, como la utilización de claves concertadas en un registro previo como usuario, la aportación de información conocida por ambas partes u otros sistemas no criptográficos, en los términos y condiciones que en cada caso se determinen.

Por otro lado, las Administraciones Públicas podrán utilizar los siguientes sistemas para su identificación electrónica y para la autenticación de los documentos electrónicos que produzcan:

- a) Sistemas de firma electrónica basados en la utilización de certificados de dispositivo seguro o medio equivalente que permita identificar la sede electrónica y el establecimiento con ella de comunicaciones seguras.
- b) Sistemas de firma electrónica para la actuación administrativa automatizada.
- c) Firma electrónica del personal al servicio de las Administraciones Públicas.
- d) Intercambio electrónico de datos en entornos cerrados de comunicación, conforme a lo específicamente acordado entre las partes.

Las personas físicas podrán, en todo caso y con carácter universal, utilizar los sistemas de firma electrónica incorporados al Documento Nacional de Identidad en su relación por medios electrónicos con las Administraciones Públicas.

Los ciudadanos, además de los sistemas de firma electrónica incorporados al Documento Nacional de Identidad, podrán utilizar sistemas de firma electrónica avanzada para identificarse y autenticar sus documentos.

La relación de sistemas de firma electrónica avanzada admitidos, con carácter general, en el ámbito de cada Administración Pública, deberá ser pública y accesible por medios electrónicos. Dicha relación incluirá, al menos, información sobre los elementos de identificación utilizados así como, en su caso, las características de los certificados electrónicos admitidos, los prestadores que los expiden y las especificaciones de la firma electrónica que puede realizarse con dichos certificados.

Los certificados electrónicos expedidos a Entidades sin personalidad jurídica, previstos en la Ley 59/2003, de 19 de diciembre, de Firma Electrónica podrán ser admitidos por las Administraciones Públicas en los términos que estas determinen.

Las Administraciones Públicas podrán determinar, teniendo en cuenta los datos e intereses afectados, y siempre de forma justificada, los supuestos y condiciones de utilización por los ciudadanos de otros sistemas de firma electrónica, tales como claves concertadas en un registro previo, aportación de información conocida por ambas partes u otros sistemas no criptográficos.

En aquellos supuestos en los que se utilicen estos sistemas para confirmar información, propuestas o borradores remitidos o exhibidos por una Administración Pública, ésta deberá garantizar la integridad y el no repudio por ambas partes de los documentos electrónicos concernidos.

Cuando resulte preciso, las Administraciones Públicas certificarán la existencia y contenido de las actuaciones de los ciudadanos en las que se hayan usado formas de identificación y autenticación a que se refiere este artículo.

Las sedes electrónicas utilizarán, para identificarse y garantizar una comunicación segura con las mismas, sistemas de firma electrónica basados en certificados de dispositivo seguro o medio equivalente.

Para la identificación y la autenticación del ejercicio de la competencia en la actuación administrativa automatizada, cada Administración Pública podrá determinar los supuestos de utilización de los siguientes sistemas de firma electrónica:

- a) Sello electrónico de Administración Pública, órgano o entidad de derecho público, basado en certificado electrónico que reúna los requisitos exigidos por la legislación de firma electrónica.

Los certificados de sello electrónico vinculan unos datos de verificación de firma (clave pública) a los datos identificativos de una unidad organizativa (unidad que se realiza la actuación administrativa automatizada: área, sección, departamento, etc.) de una entidad de la Administración Pública y la persona física que tiene la máxima responsabilidad sobre dicha unidad organizativa. Un ejemplo son los certificados APE de la FNMT-RCM, del cual se puede obtener información en <http://cert.fntm.es/>. Pueden ser utilizados para el intercambio de información entre sistemas informáticos o la generación automática de documentos.

- b) Código seguro de verificación vinculado a la Administración Pública, órgano o entidad y, en su caso, a la persona firmante del documento, permitiéndose en todo caso la comprobación de la integridad del documento mediante el acceso a la sede electrónica correspondiente.

Desde el punto de vista técnico, este sistema funciona mediante la asignación de un código único a cada documento emitido por la Administración, y el almacenamiento de una copia en una base de

datos documental. En la sede electrónica está disponible un servicio que, previa introducción del código de documento, muestra el contenido almacenado. De este modo, cualquier ciudadano puede verificar la validez de un documento impreso o en formato electrónico comparándolo con la copia que obra en poder de la Administración.

La relación de sellos electrónicos utilizados por cada Administración Pública, incluyendo las características de los certificados electrónicos y los prestadores que los expiden, deberá ser pública y accesible por medios electrónicos. Además, cada Administración Pública adoptará las medidas adecuadas para facilitar la verificación de sus sellos electrónicos.

Sin perjuicio de lo previsto en los artículos 17 y 18 de la LAECSP, la identificación y autenticación del ejercicio de la competencia de la Administración Pública, órgano o entidad actuante, cuando utilice medios electrónicos, se realizará mediante firma electrónica del personal a su servicio.

Cada Administración Pública podrá proveer a su personal de sistemas de firma electrónica, los cuales podrán identificar de forma conjunta al titular del puesto de trabajo o cargo y a la Administración u órgano en la que presta sus servicios. La firma electrónica basada en el Documento Nacional de Identidad podrá utilizarse estos efectos.

Los documentos electrónicos transmitidos en entornos cerrados de comunicaciones establecidos entre Administraciones Públicas, órganos y entidades de derecho público, serán considerados válidos a efectos de autenticación e identificación de los emisores y receptores en las condiciones establecidas en el presente artículo. Cuando los participantes en las comunicaciones pertenezcan a una misma Administración Pública, ésta determinará las condiciones y garantías por las que se regirá que, al

menos, comprenderá la relación de emisores y receptores autorizados y la naturaleza de los datos a intercambiar. Cuando los participantes pertenezcan a distintas administraciones, las condiciones y garantías citadas en el apartado anterior se establecerán mediante convenio. En todo caso deberá garantizarse la seguridad del entorno cerrado de comunicaciones y la protección de los datos que se transmitan.

La comunicación a través de medios telemáticos y la Administración Electrónica requiere el uso de la firma electrónica en la Administración. La firma electrónica constituye un instrumento capaz de permitir una comprobación de la procedencia y de la integridad de los mensajes intercambiados a través de redes de telecomunicaciones, ofreciendo las bases para evitar el repudio, si se adoptan las medidas oportunas basándose en fechas electrónicas.

La utilización de la firma electrónica en la Administración pública está regulada en la siguiente normativa, entre otra:

- Directiva 1999/93/CE del Parlamento Europeo y del Consejo, de 13 de diciembre de 1999, por la que se establece un marco comunitario para la firma electrónica.
- Ley 59/2003, de 19 de diciembre, de firma electrónica.
- Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos.
- Real Decreto 1671/2009, de 6 de noviembre, por el que se desarrolla parcialmente la Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos.
- Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica.
- Real Decreto 4/2010, de 8 de enero, por el que se regula el Esquema Nacional de Interoperabilidad en el ámbito de la Administración Electrónica

En el caso concreto de la Xunta de Galicia, y en aplicación de lo estipulado en la LAECSP, fue aprobada la ORDEN de 25 de mayo de 2011 por la que se regula la tarjeta del personal al servicio del sector público autonómico.

Tal y como se establece en la orden, el artículo 35.b) de la Ley 30/1992, de 26 de noviembre, de régimen jurídico de las Administraciones Públicas y del procedimiento administrativo común, establece que los ciudadanos, en sus relaciones con las Administraciones Públicas, tienen derecho a identificar a las autoridades y el personal al servicio de las Administraciones Públicas, bajo cuya responsabilidad se tramiten los procedimientos.

El avance de las nuevas tecnologías y los sistemas de comunicaciones tiene su reflejo en el ámbito de la Comunidad Autónoma de Galicia en el Decreto 198/2010, de 2 de diciembre, por el que se regula el desarrollo de la Administración Electrónica de la Xunta de Galicia y en las entidades de ella dependientes, que recoge como la primera de sus finalidades de carácter general en su artículo 2.1.A) «a) Ordenar e impulsar la Administración Electrónica, a fin de mejorar la eficiencia interna, las relaciones intra e interadministrativas y las relaciones con los ciudadanos», regulando la identificación electrónica de los empleados públicos en su artículo 18 mediante sistemas de firma electrónica, y pudiendo determinarse su aplicación para otros usos.

Es necesario así, y para el conjunto del sector público autonómico, regulado en la Ley 16/2010, de 17 de diciembre, establecer una tarjeta que sirva tanto para la identificación presencial del empleado/a ante los ciudadanos como para permitir al personal y a la Administración acceder a las prestaciones y servicios derivados del avance de las nuevas tecnologías y la implantación de la Administración Electrónica.

La tarjeta acreditativa del personal al servicio del sector público autonómico será de utilización obligatoria para el siguiente personal:

- a) Los altos cargos incluidos en el ámbito de aplicación de la Ley 9/1996, de 18 de octubre, de incompatibilidades de los miembros de la Xunta de Galicia y altos cargos de la Administración autonómica, modificada por la Ley 4/2006, de 30 de junio, de transparencia y de buenas prácticas de la Administración pública gallega.
- b) Personal funcionario, laboral y estatutario al servicio de la Administración general de la Comunidad Autónoma de Galicia.
- c) Personal de las entidades instrumentales del sector público autonómico, según lo define y regula la Ley 16/2010, de 17 de diciembre, de organización y funcionamiento de la Administración general y del sector público autonómico de Galicia.
- d) El personal eventual que no esté incluido en el ámbito de aplicación de las leyes a las que hace referencia el apartado a) de este artículo.
- e) La tarjeta no será de aplicación al personal que preste servicios en centros sanitarios y centros educativos.

La tarjeta tendrá las siguientes finalidades:

- a) Identificar y acreditar a su titular como personal al servicio del sector público autonómico, en los ámbitos de la Administración general de la comunidad autónoma, y de las entidades instrumentales.
- b) El personal que desempeñe funciones de atención presencial al ciudadano deberá llevar, en un lugar visible, la tarjeta.
- c) La identificación electrónica de los empleados públicos, de conformidad con lo dispuesto en el artículo 18 del Decreto 198/2010, de 2 de diciembre, por el que se regula el desarrollo de la Administración Electrónica en la Xunta de Galicia y en las entidades de ella dependientes.
- d) Permitir el acceso a sistemas de información y áreas restringidas.

- e) Mejorar el control del acceso a los edificios e instalaciones.
- f) El seguimiento del cumplimiento del horario y jornada laboral por los empleados públicos, facilitando el control de los supuestos de disminución y reducción de jornada, y la implantación del horario flexible y el teletrabajo.

Las tarjetas deberán llevar la fotografía de su titular, su nombre y apellidos y el número del DNI con el formato que se recoge en el anexo de la presente orden.

A nivel tecnológico dispondrá de las siguientes capacidades:

- a) Chip criptográfico que permitirá el almacenamiento de varios certificados digitales (entre ellos, el certificado para personal al servicio de las Administraciones Públicas y el certificado de persona física).
- b) Identificación por radiofrecuencia (chip RFID de cercanía) que permitirá el control de acceso a lugares de acceso restringido y a instalaciones con acceso controlado mediante elementos de impedimento de paso.
- c) Banda magnética como contenedor de datos del profesional para su utilización en sistemas de información que requieran de estos datos.

15.3. ACREDITACIÓN Y REPRESENTACIÓN DE LOS CIUDADANOS.

Los certificados electrónicos reconocidos emitidos por prestadores de servicios de certificación serán admitidos por las Administraciones Públicas como válidos para relacionarse con las mismas, siempre y cuando el prestador de servicios de certificación ponga a disposición de las Administraciones Públicas la información que sea precisa en condiciones

que resulten tecnológicamente viables y sin que suponga coste alguno para aquellas.

Los sistemas de firma electrónica utilizados o admitidos por alguna Administración Pública distintos de los basados en los certificados a los que se refiere el apartado anterior podrán ser asimismo admitidos por otras Administraciones, conforme a principios de reconocimiento mutuo y reciprocidad.

La Administración General del Estado dispondrá, al menos, de una plataforma de verificación del estado de revocación de todos los certificados admitidos en el ámbito de las Administraciones Públicas que será de libre acceso por parte de todos los Departamentos y Administraciones. Cada Administración Pública podrá disponer de los mecanismos necesarios para la verificación del estado de revocación y la firma con los certificados electrónicos admitidos en su ámbito de competencia.

En los supuestos en que para la realización de cualquier operación por medios electrónicos se requiera la identificación o autenticación del ciudadano mediante algún instrumento de los previstos de los que aquel no disponga, tal identificación o autenticación podrá ser válidamente realizada por funcionarios públicos mediante el uso del sistema de firma electrónica del que estén dotados.

Para la eficacia de lo dispuesto en el apartado anterior, el ciudadano deberá identificarse y prestar su consentimiento expreso, debiendo quedar constancia de ello para los casos de discrepancia o litigio.

Cada Administración Pública mantendrá actualizado un registro de los funcionarios habilitados para la identificación o autenticación.

Sin perjuicio de lo dispuesto en el [artículo 13.2](#) de la LAECSP, donde se determinan los posibles medios de identificación de los ciudadanos, las Administraciones Públicas podrán habilitar con carácter general o específico a personas físicas o jurídicas autorizadas para la realización de determinadas transacciones electrónicas en representación de los interesados. Dicha habilitación deberá especificar las condiciones y obligaciones a las que se comprometen los que así adquieran la condición de representantes, y determinará la presunción de validez de la representación salvo que la normativa de aplicación prevea otra cosa. Las Administraciones Públicas podrán requerir, en cualquier momento, la acreditación de dicha representación.

15.4.FIRMA ELECTRÓNICA, INTERCAMBIO DE CERTIFICADOS, SELLADO DE TEMPO (TIME-STAMPING).

15.4.1. FIRMA ELECTRÓNICA

La política de firma electrónica y certificados en el ámbito de la Administración General del Estado y de sus organismos públicos, según se establece en el artículo 24 del Real Decreto 1671/2009, por el que se desarrolla parcialmente la LAECSP, está constituida por las directrices y normas técnicas aplicables a la utilización de certificados y firma electrónica dentro de su ámbito de aplicación.

El artículo 18 del Real Decreto 4/2010 por el que se regula el Esquema Nacional de Interoperabilidad, establece que la política de firma electrónica y de certificados de la Administración General del Estado, servirá de marco general de interoperabilidad para la autenticación y el reconocimiento mutuo de firmas electrónicas dentro de su ámbito de actuación. También establece que dicha política podrá ser utilizada como referencia por otras Administraciones públicas para definir las políticas de certificados y firmas a reconocer dentro de sus ámbitos competenciales.

En términos generales una política de firma electrónica contiene una serie de normas relativas a la firma electrónica, organizadas alrededor de los conceptos de generación y validación de firma, en un contexto particular (contractual, jurídico, legal,...), definiendo las reglas y obligaciones de todos los actores involucrados en dicho proceso. El objetivo de este proceso es determinar la validez de la firma electrónica para una transacción en particular, especificando la información que debiera incluir el firmante en el proceso de generación de la firma, y la información que debiera comprobar el verificador en el proceso de validación de la misma.

Objetivo

La política de firma la Administración General del Estado representa el conjunto de criterios comunes asumidos esta Administración y sus organismos públicos vinculados o dependientes, en relación con la firma electrónica.

- incluye las normas relativas a la firma electrónica, organizadas alrededor de los conceptos de generación y validación de firma asociada a un contexto dado.
- permite reforzar la confianza en las transacciones electrónicas.
- define las reglas y obligaciones de todos los actores involucrados en un proceso de firma.
- permite determinar la validez de la firma electrónica para una transacción en particular.

En el Boletín Oficial del Estado con fecha 31 de julio de 2011 fue publicada la Resolución de 19 de julio de 2011, de la Secretaría de Estado para la Función Pública, por la que se aprueba la Norma Técnica de Interoperabilidad de Política de Firma Electrónica y de certificados de la Administración.

15.4.2. INTERCAMBIO DE CERTIFICADOS

Uno de los servicios horizontales de la Administración Electrónica mencionados anteriormente es el SCSP, cuya finalidad es sustituir la presentación de certificados en papel ante una Administración por una transmisión de datos entre el organismo que requiere los datos y el organismo que los custodia y proporciona, con las garantías jurídicas descritas en el RD 263/1996 (redacción del RD 209/2003) por transmisiones de datos. El sistema tiene en cuenta la normativa referente a la protección de datos.

Actualmente están disponibles los siguientes datos que cumplen con la especificación de SCSP: Identidad, residencia, situación de desempleo, títulos universitarios, títulos no universitarios, datos catastrales, certificación catastral, importes de prestación de desempleo percibidos, estar al corriente de pago de las obligaciones tributarias, consulta de deuda con la Seguridad Social, alta en la Tesorería General de la Seguridad Social, certificado de Renta, domicilio fiscal, impuesto de actividades económicas.

Las ventajas de este sistema: Ahorro de tiempo y coste al disminuir el número de trámites que debe realizar, agilidad de resolución en los trámites al no tener que esperar por datos que la Administración puede obtener en línea, y todos los trámites del procedimiento puede realizarse de forma electrónica..

El funcionamiento del servicio es el siguiente:

- Petición de datos: el organismo petionario identifica la solicitud, genera y envía firmado el mensaje de petición completo.
- Autorización de organismos: para cada petición el organismo emisor comprueba que el organismo tramitador está autorizado para pedir esos datos.
- Validación del esquema de petición: el organismo emisor analiza el esquema XML del mensaje de petición.

- Transmisiones emitidas: cada petición es guardada y tramitada en el organismo emisor. Genera, firma, y almacena las respuestas a cada petición con el mismo identificador de la petición. El tiempo de almacenamiento de la transmisión será el que marque la Ley en cada caso.
- Transmisiones recibidas: el organismo peticionario valida, tramita y almacena cada una de las respuestas recibidas.
- Conexión con el backoffice: incluye un módulo de conexión con el backoffice configurable a medida del organismo.

Además de este proyecto, diferentes organismos como la AEAT, la DGT, o la DGP han desarrollado o están desarrollando sus propios sistemas de intercambio telemático de información, y firmando convenios de colaboración que permiten su uso con otras Administraciones.

15.4.3. SELLADO DE TIEMPO

En el artículo 29.2 de la LAEPD se indica que: "Los documentos administrativos incluirán referencia temporal, que se garantizará a través de medios electrónicos cuando la naturaleza del documento así lo requiera."

En esta ley se habla de "referencia temporal", sin especificar el tipo. Las posibles referencias temporales que se pueden asociar a un documento electrónico se establecen en el Real Decreto 1671/2009, de 6 de noviembre, por el que se desarrolla parcialmente la LAECSP, hace la siguiente distinción en su artículo 47:

- a) Marca de tiempo: Asignación por medios electrónicos de la fecha y, en su caso, la hora a un documento electrónico. La marca de tiempo será utilizada en todos aquellos casos en los que las normas reguladoras no establezcan la utilización de un sello de tiempo.

- b) Sello de tiempo: Asignación por medios electrónicos de una fecha y hora a un documento electrónico con la intervención de un prestador de servicios de certificación que asegure la exactitud e integridad de la marca de tiempo del documento.

Por tanto, los dos tipos de referencias posibles son marca de tiempo y sello de tiempo, siendo la norma que regula el procedimiento donde residirán los documentos electrónicos la que dicta la conveniencia de la utilización de uno u otro tipo.

AUTORIDAD DE SELLADO DE TIEMPO TSA@

La Autoridad de Sellados de Tiempo (TSA) integrada en la plataforma de Validación y firma electrónica (@firma) es una solución tecnológica que se centra en proporcionar servicios de sellado de tiempo: emisión de sellos de tiempo, validación de sellos de tiempo y resellado.

Los servicios de la TSA están disponibles para todo Organismo o Entidad Pública perteneciente a las diferentes Administraciones Públicas. Desde el Ministerio de Política Territorial y Administración Pública se ofrece la ayuda y el soporte necesario para que los organismos integren estos servicios de sellado de tiempo sincronizados con la hora oficial del Estado, en los sistemas de información de Administración Electrónica. Para ello se ha desarrollado un cliente a integrar dentro de las aplicaciones de aquellos Organismos que deseen dotar de una referencia válida de tiempo.

La plataforma de sellado de tiempo cubre los siguientes objetivos:

- Tras la aprobación de la LAECSP, con la plataforma TS@ se promueven y facilitan servicios cuyo objetivo es el cumplimiento de las obligaciones de las Administraciones para con los ciudadanos en lo referente a garantizar la acreditación a cargo de un tercero de

confianza de la fecha y hora de realización de cualquier operación o transacción por medios electrónicos

- Los servicios son ofrecidos a cualquier organismo o Entidad Pública perteneciente a las diferentes Administraciones Públicas sea cual sea su ámbito.

La posibilidad de emitir válidamente por medios electrónicos los documentos administrativos viene descrita en el Artículo 29 de la LAECSP, el cual en sus apartados 2 y 3 indica que, además de la firma electrónica, deben incluir una referencia temporal cuando la naturaleza del documento así lo requiera. Dicha referencia temporal debe de ser realizada por medios electrónicos a través de cualquier prestador de servicios de sellado de tiempo admitidos por la Administración General del Estado.

La TS@ es una plataforma de sellado de tiempo, sincronizada con la hora legal provista por el Real Observatorio de la Armada, con las funcionalidades de sellado, validación y resellado de sellos de tiempo. Mediante la emisión de un sello de tiempo sobre un documento, se generará una evidencia, que determinará la existencia de ese documento en un instante determinado.

A través de la interfaz de validación, podrán validarse sellos de tiempo emitidos previamente, pudiendo incluir una fecha de manera opcional para saber si en esa fecha dada el sello de tiempo era válido. Si no se indica la fecha se validará con la fecha actual. Mediante la interfaz de resellado podrá volver a sellar, sellos previamente emitidos.

Los protocolos de sellado de tiempo en los cuales se basa la plataforma se encuentran especificados en las siguientes normas:

- RFC 3161 “Internet X.509 Public Key Infrastructure Time Stamp Protocols “, estándar definido por la Internet Engineering Task Force (IETF) para el protocolo Time Stamp.
- IETF RFC 3628 Policy Requirements for Time-Stamping Authorities (TSAs).
- ETSI TS 102 023 Policy requirements for time-stamping authorities.
- XML Timestamping Profile of the 2 OASIS Digital Signature Services (DSS) ver. 1.0.
- ETSI TS 101 861 Time stamping profile.

Es una solución basada en software libre, estándares abiertos y en java: servidor web Apache Tomcat, Sistema Operativo Solaris/Linux, AXIS, JGROUPS, etc.

Desde el punto de vista técnico, el funcionamiento habitual a la hora de utilizar los servicios de sellado de tiempo suele ser el siguiente:

- a) La Administración firma el documento al que pretende adjuntar un sello de tiempo.
- b) La Administración envía a la TS@ dicho documento.
- c) La TS@ recibe el documento, incorpora la fecha y hora, y lo firma con su clave privada, generando de esta manera un certificado o sello de tiempo.

15.5. PAGO ELECTRÓNICO Y NOTIFICACIONES TELEMÁTICAS.

15.5.1. PAGO ELECTRÓNICO

El pago electrónico es un servicio indispensable para que la tramitación completamente electrónica sea posible. En la Administración, muchos servicios llevan asociado el pago de tasas, impuestos o precios públicos, por lo que se hace necesario disponer de servicios de pago de distinto tipo.

El procedimiento más habitual es el de utilización de pasarelas de pago específicas de cada entidad bancaria, o preferiblemente pasarelas de pago desarrolladas por la Administración para la centralización de dicho proceso.

PASARELA DE PAGO DE RED.ES

La Entidad Pública Red.es ofrece el Servicio de Pago Telemático (SPT), que proporciona a los administrados, organismos públicos y entidades financieras un mecanismo común, normalizado y seguro que permite el pago electrónico de conceptos de deuda administrativa (tributos, precios públicos, etc.) con todas las garantías jurídicas, y que soporta los siguientes procesos:

- Pagos en línea y consultas: Para trámites administrativos que suponen el pago individual de tributos y tasas que realizan tanto los ciudadanos como los profesionales que actúan en representación y con autorización de los mismos.
- Pagos por lotes: Para pagos en lotes o remesas, de forma que faciliten las tareas repetitivas de los profesionales que actúan en representación y con autorización de los ciudadanos.
- Administración: Procesos orientados a que los Organismos puedan aprovechar las características del SPT: Consultas de pagos, estadísticas, personalización

Las Administraciones Públicas que pueden optar a diferentes modalidades de prestación del SPT, dependiendo del modo de su utilización: Modalidad web, Modalidad Servicio web con validación de firma por Red.es, modalidad servicio web con validación de firma por la Administración adherida.

Los medios de pago que permite el servicio son tres: Cargo en cuenta, pago por tarjeta de crédito y domiciliación.

Desde el punto de vista tecnológico, como principal característica destaca su diseño modular y escalable, basado en los paradigmas de seguridad (autenticidad, integridad, confidencialidad, disponibilidad, no repudio y flexibilidad)

Tecnología: Integración vía WEB y servicios web, protocolo de acceso seguro HTTPS, estándar de firma electrónica XMLdsig, y soporte de certificados de firma electrónica emitidos por diversos Prestadores de Servicios de Certificación (PSC)

Se puede encontrar más información en la dirección <http://pago.red.es/>.

PASARELA DE PAGOS DEL MINISTERIO DE POLÍTICA TERRITORIAL Y ADMINISTRACIONES PÚBLICAS - AEAT

La pasarela de pagos pretende mejorar la disposición de la Administración del Estado para adoptar el pago telemático en sus trámites.

Objetivo:

- Impulsar el pago electrónico en la Administración General del Estado.
- Facilitar la implantación del pago electrónico en los trámites que lo quieran.
- Aprovechar la experiencia y buenas prácticas de la AEAT, así como su infraestructura de pago.

El proyecto tiene dos modelos de servicio claramente diferenciados. El Organismo colaborador puede solicitar el que más se ajuste a sus necesidades:

- a) Servicio “Mis pagos” centralizado en la web 060. Servicio de pago centralizado. El organismo no necesita implantar nada en su infraestructura. El ciudadano, puede realizar el pago en el servicio centralizado y presentar el justificante correspondiente con el NRC, en el Organismo tramitador.

El pago podrá ser verificado por el Organismo a través de una página Web habilitada para ello o utilizar un modelo de integración con el servicio en el que pueda actualizar su backoffice y redirigir al ciudadano al pago sin perder el contacto con el mismo.

El servicio incorpora, facilidades adicionales para los ciudadanos, como poder planificar pagos con la Administración de tal forma, que tenga un recordatorio de los mismos para iniciar el pago en el momento correspondiente o mantener un histórico de los mismos independientemente del Organismo donde haya realizado el trámite.

- b) Librerías de pago: Servicio en el que se proporcionan unas librerías que se implantan en el Organismo y que son utilizadas por las aplicaciones de gestión que lo requieren. Estas librerías se integran con las aplicaciones, bien como un servicio web o como una librería java propiamente dicha.

La seguridad para la autenticación e integridad de los datos se basa en el uso de firma digital avanzada y comunicación HTTPS entre el Organismo y la AEAT, con certificado de servidor y cliente.

Además, el ciudadano tiene que firmar con su certificado digital los datos del pago que se envían a la Entidad Financiera, cotejándose posteriormente esta firma en el banco con el propietario de la cuenta o la tarjeta. Esto permite garantizar todo el ciclo de pago y mantener informados a todos los actores del resultado del mismo en el instante.

Permite el pago mediante cargo en cuenta o tarjeta, si bien el ciudadano tiene que tener cuenta en el banco que expide la tarjeta.

Permite el pago a terceros, es decir, la persona que firma con certificado digital la petición de pago y está autorizado a una cuenta en el banco, puede pagar por otra persona, que sea la obligada al pago.

La plataforma de firma electrónica utilizada es @Firma, que proporciona la librería de firma del cliente, así como aquellos servicios de seguridad que requiera la aplicación de pago del organismo o la propia pasarela, como puede ser la verificación de que el certificado no está revocado.

El servicio de pago es proporcionado gratuitamente por las Entidades Financieras colaboradoras en función de sus acuerdos de colaboración con la AEAT.

15.5.2. NOTIFICACIONES TELEMÁTICAS

La LAECSP establece que los ciudadanos podrán elegir en todo momento la manera de comunicarse con las Administraciones Públicas, sea o no por medios electrónicos, excepto en aquellos casos en los que de una norma con rango de Ley se establezca o infiera la utilización de un medio no electrónico. La opción de comunicarse por unos u otros medios no vincula al ciudadano, que podrá, en cualquier momento, optar por un medio distinto del inicialmente elegido.

Las Administraciones Públicas utilizarán medios electrónicos en sus comunicaciones con los ciudadanos siempre que así lo hayan solicitado o consentido expresamente. La solicitud y el consentimiento podrán, en todo caso, emitirse y recabarse por medios electrónicos.

Las comunicaciones a través de medios electrónicos serán válidas siempre que exista constancia de la transmisión y recepción, de sus fechas, del contenido íntegro de las comunicaciones y se identifique fidedignamente al remitente y al destinatario de las mismas.

Las Administraciones publicarán, en el correspondiente Diario Oficial y en la propia sede electrónica, aquellos medios electrónicos que los ciudadanos pueden utilizar en cada supuesto en el ejercicio de su derecho a comunicarse con ellas.

Los requisitos de seguridad e integridad de las comunicaciones se establecerán en cada caso de forma apropiada al carácter de los datos objeto de aquellas, de acuerdo con criterios de proporcionalidad, conforme a lo dispuesto en la legislación vigente en materia de protección de datos de carácter personal.

Reglamentariamente, las Administraciones Públicas podrán establecer la obligatoriedad de comunicarse con ellas utilizando sólo medios electrónicos, cuando los interesados se correspondan con personas jurídicas o colectivos de personas físicas que por razón de su capacidad económica o técnica, dedicación profesional u otros motivos acreditados tengan garantizado el acceso y disponibilidad de los medios tecnológicos precisos.

Las Administraciones Públicas utilizarán preferentemente medios electrónicos en sus comunicaciones con otras Administraciones Públicas. Las condiciones que regirán estas comunicaciones se determinarán entre las Administraciones Públicas participantes.

Para que la notificación se practique utilizando algún medio electrónico se requerirá que el interesado haya señalado dicho medio como preferente o haya consentido su utilización, sin perjuicio de lo dispuesto en el artículo 27.6 de la LAECSP. Tanto la indicación de la preferencia en el uso de medios electrónicos como el consentimiento citados anteriormente podrán emitirse y recabarse, en todo caso, por medios electrónicos.

El sistema de notificación permitirá acreditar la fecha y hora en que se produzca la puesta a disposición del interesado del acto objeto de notificación, así como la de acceso a su contenido, momento a partir del cual la notificación se entenderá practicada a todos los efectos legales.

Cuando, existiendo constancia de la puesta a disposición transcurrieran diez días naturales sin que se acceda a su contenido, se entenderá que la notificación ha sido rechazada con los efectos previstos en el artículo 59.4 de la Ley 30/1992 de Régimen Jurídico y del Procedimiento Administrativo Común y normas concordantes, salvo que de oficio o a instancia del destinatario se compruebe la imposibilidad técnica o material del acceso.

Durante la tramitación del procedimiento el interesado podrá requerir al órgano correspondiente que las notificaciones sucesivas no se practiquen por medios electrónicos, utilizándose los demás medios admitidos en el artículo 59 de la Ley 30/1992, de Régimen Jurídico y del Procedimiento Administrativo Común, excepto en los casos previstos en el artículo 27.6 de la LAECSP.

Producirá los efectos propios de la notificación por comparecencia el acceso electrónico por los interesados al contenido de las actuaciones administrativas correspondientes, siempre que quede constancia de dichos acceso.

En respuesta a estas exigencias de la LAECSP, está disponible una plataforma desarrollada y mantenida por la Sociedad Estatal de Correos y Telegrafos, denominada Sistema de Notificaciones Telemáticas seguras. La Administración puede hacer uso de este servicio integrándolo en sus sistemas informáticos a través del módulo SISNOT.

El Servicio de Notificaciones Electrónicas proporciona a cada ciudadano o empresa una Dirección Electrónica Habilitada en la que recibir todas las

notificaciones y comunicaciones de las administraciones públicas. El servicio es gratuito para los ciudadanos y empresas. En un único buzón podrá recibir todas las notificaciones y comunicaciones de la Administración.

Los agentes que intervienen en el Servicio son:

- El Ciudadano o empresa, que tienen el control de su dirección electrónica y que puede solicitar a cualquier Administración que le notifique electrónicamente por este sistema, ya que el ciudadano tiene el derecho a elegir el lugar de notificación.
- El Ministerio de Política Territorial y Administración Pública, responsable de la Dirección Electrónica Habilitada y del servicio
- Correos, el prestador que gestiona la entrega de las notificaciones al interesado
- El emisor, organismo responsable del trámite y competente de emitir la notificación al interesado.

El funcionamiento del servicio consiste en:

- El ciudadano solicita un buzón seguro identificado mediante una Dirección Electrónica Habilitada.
- El ciudadano selecciona, del Catálogo de procedimientos aquellos que para los que quiere ser notificado electrónicamente con total seguridad y confidencialidad.
- El organismo emisor consulta el censo del procedimiento (aquellos ciudadanos que han solicitado la notificación telemática de ese procedimiento).
- El organismo envía la notificación al prestador. El prestador verifica los datos y distribuye las notificaciones en el buzón correspondiente, poniendo ésta a disposición del ciudadano. Al mismo tiempo emite un

aviso a la dirección de correo electrónico que ha facilitado o mediante un mensaje corto a móvil SMS.

- El ciudadano consulta su buzón y acepta o rechaza la notificación telemática, firmando la aceptación o el rechazo de la notificación. La notificación se descarga en el ordenador del interesado.
- El prestador almacena la aceptación, el rechazo firmada por le interesado o vencimiento de plazo firmado por el prestador y entrega esta información de retorno al emisor.

El único requisito para el interesado identificarse a través de un certificado electrónico o DNle.

Para facilitar la integración al servicio, existe un paquete denominado SISNOT, que es un sistema intermedio que gestiona el ciclo de vida de las notificaciones emitidas por aplicaciones cliente y la comunicación con el Servicio de Notificaciones Electrónicas; encargado de hacérselas llegar al ciudadano. También gestiona la actualización del censo de ciudadanos y empresas dados de alta para la notificación telemática según normativa, para lo que se comunica con los sistemas de censo del portal del ciudadano.

SISNOT ofrece un interfaz de servicio web abstrayendo a la aplicación gestora del procedimiento de la labores de comunicación con el SNE.

Se puede encontrar más información en la dirección <https://notificaciones.060.es/>

15.6. REFERENCIAS

- Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común.
- Ley 15/1999, de 13 de diciembre, de Protección de datos de carácter personal
- Ley 53/1999, de 19 de diciembre, de Firma electrónica.
- Ley 34/2002, de 11 de julio, de Servicios de la sociedad de la información y de comercio electrónico.
- Ley 11/2007, de 22 de junio, de Acceso electrónico dos cidadanos a los servicios públicos.
- Ley 37/2007, de 16 de noviembre, sobre Reutilización de la información del sector público.
- Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley 15/1999, de 13 de diciembre, de protección de datos de carácter personal.
- Ley 56/2007, de 28 de diciembre, de Medidas de impulso de la sociedad de la Información.
- Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito da Administración Electrónica.
- Real Decreto 4/2010, de 8 de enero, por el que se regula el Esquema Nacional de Interoperabilidad en el ámbito da Administración Electrónica.
- Decreto 198/2010, de 2 de diciembre, por el que se regula el Desarrollo de la Administración Electrónica en la Xunta de Galicia y en las entidades dependientes.
- Resoluciones de la Secretaría de Estado para la Función Pública por la que se aprueban distintas normas técnicas de interoperabilidad.
- “Manual práctico de supervivencia de la Administración Electrónica”, de Alberto López Tallón, publicado bajo licencia Creative Commons.
- “Anotacións e comentarios ao Decreto de Administración Electrónica da Xunta de Galicia”, editado polo Colexio Profesional de Enxeñaría en

Informática de Galicia coa colaboración da Xunta de Galicia. ISBN 978-84-614-7362-5.

- “Construyendo la identidad digital. Situación actual de la firma electrónica y de las entidades de certificación”, editado polo Colexio Profesional de Enxeñaría en Informática de Galicia. ISBN 978-84-614-6072-4.
- “Las relaciones de la empresa con la Administración Electrónica”, editado polo Colexio Profesional de Enxeñaría en Informática de Galicia. ISBN 978-84-614-9865-9.
- “Empresa, protección de datos y Administración Electrónica”, editado polo Colexio Profesional de Enxeñaría en Informática de Galicia. ISBN 978-84-614-4014-6.

Autor: Jesús Rodríguez Castro

Jefe del Servicio de Informática del Concello de Santiago de
Compostela

Colegiado del CPEIG

16. DESARROLLO DE LA SOCIEDAD DE LA INFORMACIÓN: MARCO DE ACTUACIÓN. EUROPA 2020 AGENDA DIGITAL EUROPEA. PLAN AVANZA 2.

BLOQUE: ADMINISTRACIÓN ELECTRÓNICA Y SOCIEDAD DE LA INFORMACIÓN

TEMA 16. DESARROLLO DE LA SOCIEDAD DE LA INFORMACIÓN: MARCO DE ACTUACIÓN. EUROPA 2020. AGENDA DIGITAL EUROPEA. PLAN AVANZA 2.

16.1.DESARROLLO DE LA SOCIEDAD DE LA INFORMACIÓN. MARCO DE ACTUACIÓN.

16.1.1. EUROPA 2020.

16.1.2. AGENDA DIGITAL EUROPEA.

16.1.3. PLAN AVANZA 2.

16.2.REFERENCIAS

16.1.DESARROLLO DE LA SOCIEDAD DE LA INFORMACIÓN. MARCO DE ACTUACIÓN.

16.1.1. EUROPA 2020.

La Estrategia 2020 es el plan de crecimiento sostenible e inteligente diseñado por la Comisión Europea para la próxima década, y puesto en marcha en marzo de 2010. En él se establecen las líneas de actuación básicas y los objetivos a lograr en los próximos diez años para conseguir un desarrollo integral que vuelva a situar a la Unión Europea en una posición de liderazgo mundial a nivel económico y social. En las siguientes líneas se hace un resumen de las principales medidas, actuaciones y objetivos fijados para la próxima década.

1. Empleo: Aumentar la tasa de empleo de la población activa hasta el 75%. Reforzar la flexibilidad y la seguridad laboral de los trabajadores a través de planes nacionales. Incrementar la colaboración entre las



instituciones privadas del mercado laboral y las instituciones públicas. Asegurar las competencias necesarias para un aprendizaje permanente. Fomentar el movimiento del capital humano. Llevar a cabo una reforma en el sistema de pensiones.

2. Educación: Incrementar la calidad de todos los niveles de educación general de la UE. Integrar e incrementar los programas de movilidad e investigación dentro de la UE. Explorar las formas de promover el espíritu emprendedor, la creatividad y la excelencia. Realizar una evaluación comparativa de los resultados de las universidades y de los sistemas educativos en un contexto general. Reducir el % de abandono escolar al 10%. Consolidar el atractivo internacional de la educación superior europea. Mejorar la entrada de los jóvenes al mercado laboral mediante orientación, asesoramiento y prácticas. Conseguir incrementar el % de población de entre 30 y 34 años que finaliza la enseñanza superior del 31% a por lo menos el 40% en 2020.
3. Innovación: Impulsar los niveles de inversión en I+D en toda la UE. hasta llegar al 3% del PIB de la UE. Utilizar incentivos fiscales que promuevan la inversión en I+D. Mejorar las condiciones de inversión y el acceso a la financiación del sector privado centrándose en las PYMES (promoción del espíritu emprendedor). Poner en marcha cooperaciones de innovación europea entre universidades y empresas. Acelerar la implantación de redes de internet de alta velocidad. Revisar y consolidar el papel de los instrumentos de la UE. destinados a apoyar la innovación. Crear una agenda de investigación europea centrada en los grandes retos del futuro: Transporte, seguridad energética, cambio climático... Crear las condiciones para que la PYME de rápido crecimiento ocupe los mercados emergentes. Utilizar incentivos fiscales para promover los gastos en conocimiento y las inversiones en I+D.

4. Energía e industria: Lograr una Europa que aproveche más eficazmente sus recursos. Reducir las emisiones de carbono en un 20% respecto a los niveles de 1990. Incrementar el uso de las energías renovables. Promover una mayor seguridad energética. Eliminar obstáculos a un mercado único de la energía renovable. Mejorar las redes europeas y transeuropeas. Desarrollar un marco de normas comunes en la promoción de nuevas tecnologías. Modernizar el sector transporte. Utilizar instrumentos reglamentarios y normativos para reducir el consumo de energía, y así, incentivar el ahorro. Eliminar los obstáculos a un mercado único de la energía renovable. Mantener el liderazgo mundial en el campo de las energías verdes. Eliminar las subvenciones a energías que producen un deterioro medioambiental. Desarrollar un enfoque horizontal de la política industrial. Promover la internacionalización de la PYME. Revisar y mejorar la normativa europea con el fin de mejorar la competitividad europea. Desarrollar una política espacial efectiva y líder en el mundo. Reforzar la competitividad del sector turístico europeo. Promover la responsabilidad social de las empresas. Promover el cambio en sectores en crisis.
5. Economía y finanzas: Evitar los proteccionismos nacionales. Llevar a cabo reformas en el sector financiero que mejoren la supervisión, la estabilidad y la rendición de cuentas. Fortalecer el gobierno de las instituciones financieras. Impulsar un saneamiento de las finanzas públicas de los estados que contribuya a un crecimiento sostenido a largo plazo. Buscar una mayor integración e interconexión de los mercados para que la competencia y el acceso de los consumidores estimulen el crecimiento y la innovación. Facilitar y abaratar la ejecución de contratos para las empresas y los consumidores. Hacer realidad un mercado europeo de capital riesgo. Desarrollar una estrategia comercial para Europa centrada en las negociaciones

multilaterales y bilaterales con socios estratégicos. Reducir las cargas administrativas que pesan sobre las empresas y mejorar la calidad de la legislación.

6. Plataforma contra la pobreza: Reducir el número de europeos que viven por debajo de los umbrales de pobreza en un 25%. Promover la cohesión y la inclusión social de los más pobres permitiéndoles vivir con dignidad y haciéndoles partícipes de la vida en sociedad. Promover la responsabilidad colectiva. Garantizar a estas personas el acceso universal a la asistencia sanitaria.

Las prioridades que se establecen en Europa 2020 son las siguientes:

- a) Crecimiento inteligente: Significa mejorar el rendimiento de la UE en materia de: educación (estimular a las personas a aprender, estudiar y actualizar sus conocimientos, investigación e innovación (crear nuevos productos y servicios que generen crecimiento y empleo y ayuden a afrontar los desafíos sociales) y sociedad digital (utilizar las tecnologías de información y la comunicación).
- b) Crecimiento sostenible: Es crecimiento sostenible crear una economía con bajas emisiones de carbono más competitiva, que haga un uso eficiente y sostenible de los recursos, proteger el medio ambiente, reducir las emisiones y evitar la pérdida de biodiversidad, aprovechar el liderazgo europeo en el desarrollo de nuevas tecnologías y métodos de producción ecológicos, introducir redes eléctricas inteligentes y eficaces, aprovechar las redes que ya existen a escala de la UE para dar una ventaja competitiva más a nuestras empresas, sobre todo las pequeñas del sector fabril, mejorar el entorno empresarial, particularmente para las PYME, y ayudar a los consumidores a elegir con conocimiento de causa.

- c) Crecimiento integrador: Es crecimiento integrador: aumentar el nivel de empleo en Europa: más y mejores puestos de trabajo, sobre todo para las mujeres, los jóvenes y los trabajadores de más edad, ayudar a las personas de todas las edades a prever y gestionar el cambio a través de la inversión en las cualificaciones y la formación, modernizar los mercados de trabajo y los sistemas de bienestar, garantizar que los beneficios del crecimiento lleguen a todos los rincones de la UE.
- d) Gobernanza económica: La crisis ha dejado al descubierto en muchos países europeos problemas fundamentales y tendencias insostenibles. También ha puesto de manifiesto hasta qué punto son interdependientes las economías de los países de la UE. Una mayor coordinación de políticas económicas en la UE contribuirá a resolver los problemas y a impulsar el crecimiento y la creación de empleo en el futuro. La gobernanza económica basa en tres elementos principales: Reforzar la agenda económica con una supervisión más estrecha de la UE, salvaguardar la estabilidad de la zona euro, y restauración del sector financiero

Europa ha descubierto nuevos motores del crecimiento y el empleo. A estos ámbitos se destinan siete iniciativas emblemáticas. Dentro de cada iniciativa, tanto la administración europea como las nacionales deben coordinar sus esfuerzos a fin de ayudarse mutuamente. La Comisión presentó la mayoría de estas iniciativas en 2010.

Actuaciones emblemáticas en el área del crecimiento inteligente:

1. Una agenda digital para Europa
2. Unión por la innovación
3. Juventud en movimiento

Actuaciones emblemáticas en el área del crecimiento sostenible:

4. Una Europa que utilice eficazmente los recursos
5. Una política industrial para la era de la mundialización

Actuaciones emblemáticas en el área del crecimiento integrador:

6. Una agenda de nuevas cualificaciones y empleos
7. Plataforma europea contra la pobreza

Con la publicación, el 7 de junio de 2011, de las recomendaciones específicas para cada uno de los 27 países de la UE, la Comisión ha tomado otra medida para ayudar a los Estados miembros a generar crecimiento y empleo y volver a encarrilar así la economía de la Unión. Las recomendaciones se basan en una evaluación exhaustiva (documentos de trabajo) de los planes de los Estados miembros para sanear las finanzas públicas (Programas de Estabilidad o Convergencia) y de las medidas para impulsar el crecimiento y el empleo (Programas Nacionales de Reforma).

16.1.2. LA AGENDA DIGITAL EUROPEA.

La finalidad genérica de la Agenda Digital es obtener los beneficios económicos y sociales sostenibles que pueden derivar de un mercado único digital basado en una internet rápida y ultrarrápida y en unas aplicaciones interoperables.

La crisis ha destruido años de progreso económico y social y dejado al descubierto los puntos débiles estructurales de la economía de Europa. El objetivo principal de Europa debe ser hoy volver a la buena senda. Para conseguir un futuro sostenible, hay que ver más allá del corto plazo.

Enfrentados a una situación de envejecimiento demográfico y competencia mundial, disponemos de tres opciones: trabajar más, trabajar durante más tiempo o trabajar con más inteligencia. Lo más probable es que tengamos que hacer las tres cosas, pero la última es la única que garantizará un incremento del nivel de vida de los europeos. A tal efecto, la Agenda Digital propone medidas que es preciso adoptar urgentemente para poner a Europa en la senda hacia un crecimiento inteligente, sostenible e incluyente. Sus propuestas establecerán el marco para las transformaciones a largo plazo que traerán consigo una sociedad y una economía crecientemente digitales.

La Comisión Europea puso en marcha en marzo de 2010 la estrategia Europa 2020, con el objetivo de salir de la crisis y preparar a la economía de la UE para los retos de la próxima década. Europa 2020 expone una estrategia para conseguir unos niveles elevados de empleo, una economía de baja emisión de carbono, productividad y cohesión social, que debe aplicarse a través de medidas concretas a nivel nacional y de la UE. Esta batalla por el crecimiento y el empleo exige una toma de conciencia en las altas esferas políticas y la movilización en toda Europa de la totalidad de los agentes.

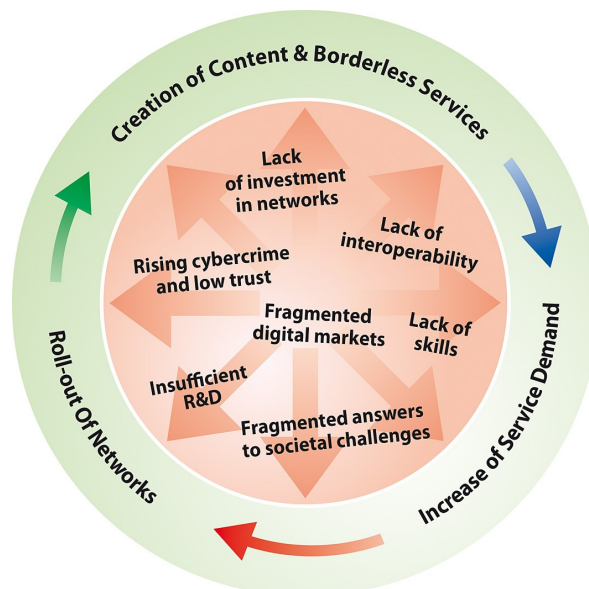
La Agenda Digital para Europa es una de las siete iniciativas emblemáticas de la estrategia Europa 2020, y su propósito es definir la función capacitadora esencial que deberá desempeñar el uso de las tecnologías de la información y la comunicación (TIC) si Europa quiere hacer realidad sus ambiciones para 2020.

El objetivo de esta Agenda es trazar un rumbo que permita maximizar el potencial económico y social de las TIC, y en particular de internet, como soporte esencial de la actividad económica y social: para hacer negocios, trabajar, jugar, comunicarse y expresarse en libertad. Si se consigue llevarla a buen fin, la Agenda fomentará la innovación, el crecimiento económico y la mejora de la vida cotidiana tanto para los ciudadanos como para las empresas. De esta manera, el despliegue generalizado y la

utilización más eficaz de las tecnologías digitales permitirán a Europa afrontar los retos esenciales que tiene planteados y proporcionará a los europeos una mejor calidad de vida manifestada, por ejemplo, en una mejor atención sanitaria, unas soluciones de transporte más seguras y eficientes, un medio ambiente más limpio, nuevas oportunidades en materia de medios de comunicación y un acceso más fácil a los servicios públicos y a los contenidos culturales.

El enorme potencial de las TIC puede movilizarse a través de un ciclo virtuoso de actividad que funcione adecuadamente. Es preciso ofrecer unos contenidos y servicios atractivos en un entorno de internet interoperable y sin fronteras. Con ello se estimula la demanda de velocidades y capacidades más elevadas, lo que a su vez justifica la inversión en redes más rápidas. El despliegue y la adopción de unas redes más rápidas, por su parte, abre el camino hacia unos servicios innovadores que exploten las velocidades más elevadas.

Figura 1: Ciclo virtuoso de la economía digital



Este flujo de actividad puede, en buena medida, autoalimentarse. Exige un entorno empresarial que fomente la inversión y el espíritu emprendedor. Pero, aun cuando el poder de transformación asociado a las TIC sea

evidente, no es menos cierto que para explotarlo hay que hacer frente a retos importantes.

Sobre la base de una consulta con las partes interesadas y de los elementos contenidos tanto en la Declaración de Granada como en la Resolución del Parlamento Europeo, la Comisión ha confeccionado la lista de los siete obstáculos más importantes. Son los situados en el anillo interior de la Figura 1, y se describen brevemente a continuación.

Por sí solos o combinadamente, estos obstáculos socavan gravemente los esfuerzos realizados para explotar las TIC, evidenciando la necesidad de una respuesta política global y unificada a nivel europeo. .

1. Fragmentación de los mercados digitales.

Europa sigue siendo un mosaico de mercados nacionales en línea, y problemas que podrían resolverse perfectamente impiden a los europeos disfrutar de los beneficios de un mercado único digital. Es necesario que los servicios y contenidos comerciales y culturales fluyan a través de las fronteras; a tal efecto, hay que eliminar los obstáculos reglamentarios y facilitar los pagos y la facturación electrónicas, así como la solución de controversias, y suscitar la confianza de los consumidores. Se puede y debe hacer más dentro del marco regulador actual para tejer un mercado único en el sector de las telecomunicaciones.

2. Falta de interoperabilidad

Europa no obtiene aún el máximo beneficio de la interoperabilidad. Los puntos débiles en materia de fijación de normas, contratación pública y coordinación entre autoridades públicas impiden que los servicios y dispositivos digitales que utilizan los europeos trabajen conjuntamente todo lo bien que debieran.

3. Incremento de la ciberdelincuencia y riesgo de escasa confianza en las redes

Europa debe combatir el auge de las nuevas formas de delincuencia (la «ciberdelincuencia») que van desde la explotación infantil al robo de la identidad y los ciberataques, y elaborar mecanismos de respuesta.

4. Ausencia de inversión en redes

Es preciso hacer más para garantizar el despliegue y la adopción de la banda ancha para todos, a velocidades crecientes, a través de tecnologías tanto fijas como inalámbricas.

5. Insuficiencia de los esfuerzos de investigación e innovación

Europa sigue invirtiendo poco, fragmentando sus esfuerzos, infrutilizando la creatividad de las PYME y fracasando en su empeño por transformar la ventaja intelectual de la investigación en la ventaja competitiva de unas innovaciones basadas en el mercado.

6. Carencias en la alfabetización y la capacitación digitales

Europa padece una creciente penuria de cualificación profesional en las TIC y un déficit en la alfabetización digital.

7. Pérdida de oportunidad para afrontar los retos sociales.

Si aprovechara plenamente el potencial de las TIC, Europa podría hacer frente con mucha más eficacia a algunos los retos sociales más agudos: el cambio climático y otras presiones sobre nuestro medio ambiente, el envejecimiento de la población y los costes sanitarios crecientes, el desarrollo de unos servicios públicos más eficientes y la integración de las personas con discapacidad, la digitalización del patrimonio cultural de Europa y su puesta a disposición de las generaciones presentes y futuras, etc

La Agenda Digital para Europa estructura sus acciones clave en torno a la necesidad de abordar sistemáticamente estos siete aspectos

problemáticos, que como iniciativa horizontal abarca las tres dimensiones de crecimiento establecidas en Europa 2020.

La Agenda Digital exigirá un nivel sostenido de compromiso tanto a nivel de la UE como de los Estados miembros (incluido el nivel regional). No podrá tener éxito sin una importante contribución de las demás partes interesadas, incluidos los jóvenes «nativos digitales».

En la Agenda Digital se establecen ocho campos de actuación para dar respuesta a estos problemas, dentro de los cuales se definen apartados más específicos y acciones clave.

1. UN MERCADO ÚNICO DIGITAL DINÁMICO

La creación de contenidos y servicios en línea atractivos y su libre circulación dentro de la UE y a través de sus fronteras resultan fundamentales para estimular el círculo virtuoso de la demanda. La legislación relativa al mercado único en materia de comercio electrónico, facturación electrónica y firma electrónica, las transacciones en el entorno digital siguen siendo demasiado complejas, dadas las incoherencias en la aplicación de la normativa en los Estados miembros. Los consumidores y las empresas siguen enfrentándose a una incertidumbre considerable en relación con sus derechos y su protección jurídica cuando hacen negocios en línea. Europa está lejos de contar con un mercado único de servicios de telecomunicaciones.

Afrontar estos problemas exige actuaciones en los campos que a continuación se enumeran:

- a) Apertura de acceso a los contenidos
- b) Simplificación de las transacciones en línea y transfronterizas
- c) Crear confianza en el mundo digital
- d) Reforzar el mercado único de servicios de telecomunicación.

2. INTEROPERABILIDAD Y NORMAS

Internet constituye el mejor ejemplo del potencial de la interoperabilidad técnica. Su arquitectura abierta aporta dispositivos y aplicaciones interoperables a miles de millones de personas en todo el mundo. Pero para beneficiarse plenamente del despliegue de las TIC, es preciso potenciar aún más la interoperabilidad entre dispositivos, aplicaciones, repositorios de datos, servicios y redes.

Afrontar estos problemas exige actuaciones en los campos que a continuación se enumeran:

- a) Mejorar el establecimiento de normas de TIC
- b) Promover un mejor uso de las normas
- c) Mejorar la interoperabilidad a través de la coordinación.

3. CONFIANZA Y SEGURIDAD

Los usuarios tienen que estar seguros y protegidos cuando se conecten en línea. Al igual que su contrapartida física, la ciberdelincuencia no puede tolerarse. Además, si las nuevas tecnologías no resultan plenamente fiables, será sencillamente imposible que existan algunos de los servicios en línea más innovadores y avanzados, tales como los bancarios o de asistencia sanitaria.

Afrontar estas amenazas y reforzar la seguridad en la sociedad digital es una responsabilidad compartida, tanto de los particulares como de las entidades privadas y públicas, tanto en el hogar como a nivel mundial. Por

ejemplo, para combatir la explotación sexual y la pornografía infantil, pueden constituirse plataformas de alerta a nivel nacional y de la UE, junto con medidas encaminadas a suprimir los contenidos nocivos y evitar su visualización. También resultan esenciales las actividades educativas y las campañas de sensibilización para el público en general. También podría instarse a las industrias a seguir desarrollando y aplicar regímenes de autorregulación, en particular en lo que se refiere a la protección de los menores que utilizan sus servicios.

El derecho a la intimidad y a la protección de los datos personales constituye un derecho fundamental en la UE que es preciso hacer aplicar eficazmente utilizando un amplio abanico de métodos: desde la aplicación generalizada del principio de «privacidad a través del diseño» en las tecnologías de TIC pertinentes, hasta las sanciones disuasorias cuando resulte necesario. El marco de las comunicaciones electrónicas revisado de la UE clarifica las responsabilidades de los operadores de redes y proveedores de servicios, incluyendo su obligación de notificar las violaciones de la seguridad de los datos personales. La revisión del marco general de protección de datos recientemente puesta en marcha incluirá una posible ampliación de la obligación de notificar las violaciones de la seguridad de los datos. La aplicación de la prohibición del correo no solicitado se reforzará utilizando la red de cooperación en materia de protección de los consumidores (CPC).

Una aplicación rápida y efectiva del plan de acción de la UE para la protección de las infraestructuras críticas de información y del Programa de Estocolmo generará una amplia gama de medidas en el ámbito de la seguridad de las redes y de la información, así como en el de la lucha contra la ciberdelincuencia. Por ejemplo, para reaccionar en tiempo real, debería establecerse en Europa una red, amplia y con un buen funcionamiento, de equipos de respuesta a emergencias informáticas (CERT), y también para las instituciones europeas. La cooperación entre los CERT y los organismos policiales y judiciales es algo esencial, y debe

promoverse un sistema de puntos de contacto que ayude a prevenir la ciberdelincuencia y a reaccionar en caso de emergencias tales como los ciberataques. Europa necesita también una estrategia de gestión de identidades, en particular para que los servicios de administración electrónica sean seguros y eficaces.

Por último la cooperación entre los agentes pertinentes debe organizarse a nivel mundial, para que sea efectivamente capaz de luchar contra las amenazas a la seguridad y reducirlas. Esta posibilidad podría encauzarse dentro de los debates sobre la gobernanza de internet. A nivel más operativo, deberían proseguir las acciones sobre seguridad de la información coordinadas internacionalmente y deberían emprenderse acciones conjuntas para luchar contra la delincuencia informática, con el apoyo de una Agencia Europea de Seguridad de las Redes y de la Información (ENISA) renovada.

4. ACCESO RÁPIDO Y ULTRARRÁPIDO A INTERNET

Necesitamos una internet muy rápida para que la economía crezca y genere puestos de trabajo y prosperidad, así como para garantizar que los ciudadanos puedan acceder a los contenidos y servicios que desean.

La economía del futuro será una economía del conocimiento basada en redes cuyo centro será Internet. Europa necesita un acceso a internet rápido y ultrarrápido generalizado y a un precio competitivo. La estrategia Europa 2020 ha subrayado la importancia del despliegue de la banda ancha para fomentar la inclusión social y la competitividad en la UE. Ha reafirmado el objetivo de poner la banda ancha básica a disposición de todos los europeos a más tardar en 2013 y se propone que, para 2020, i) todos los europeos tengan acceso a unas velocidades de internet muy superiores, por encima de los 30 Mbps, y que ii) el 50 % o más de los hogares europeos estén abonados a conexiones de internet por encima de los 100 Mbps.

Para alcanzar estas ambiciosas metas es necesario elaborar una política global, basada en una combinación de tecnologías, que se centre en dos objetivos paralelos: por un lado, garantizar la cobertura universal de la banda ancha (combinando la fija y la inalámbrica) con velocidades de internet que vayan aumentando gradualmente hasta los 30 Mbps y más, y, con el tiempo, fomentar el despliegue y la adopción de las redes de acceso de nueva generación (NGA) en una gran parte del territorio de la UE, para hacer posibles conexiones ultrarrápidas de internet por encima de los 100 Mbps.

Afrontar estos problemas exige actuaciones en los campos que a continuación se enumeran:

- a) Garantizar la cobertura universal de la banda ancha con velocidades crecientes
- b) Fomentar el despliegue de las redes NGA
- c) Una internet abierta y neutral

5. INVESTIGACIÓN E INNOVACIÓN

Europa sigue invirtiendo poco en la investigación y el desarrollo relacionados con las TIC. En comparación con nuestros principales socios comerciales, tales como los Estados Unidos, la I+D sobre TIC en Europa no solo representa una proporción mucho menor del gasto total en I+D (17 % frente a 29 %), sino que, en términos absolutos, supone alrededor del 40 % del gasto de Estados Unidos.

Afrontar estos problemas exige actuaciones en los campos que a continuación se enumeran:

- a) Incrementar los esfuerzos y la eficiencia
- b) Explotar el mercado único para impulsar la innovación en TIC
- c) Iniciativas a favor de la innovación abierta lideradas por la industria

6. FOMENTAR LA ALFABETIZACIÓN, LA CAPACITACIÓN Y LA INCLUSIÓN DIGITALES

Internet se ha convertido en parte integrante de la vida cotidiana de muchos europeos. Sin embargo, 150 millones de europeos –el 30 % aproximadamente– nunca han utilizado todavía internet. Suelen decir que no lo necesitan, o que resulta demasiado caro. Este grupo está compuesto principalmente por las personas de 65 a 74 años, las personas de renta baja, los desempleados y los de nivel cultural más bajo.

En muchos casos, esta situación se debe a falta de capacitación del usuario, por ejemplo alfabetización digital y mediática, no sólo para la empleabilidad, sino también para aprender, crear, participar y abordar con confianza y discernimiento el uso de los medios de comunicación digitales. La accesibilidad y la utilizabilidad constituyen también sendos problemas para los europeos con discapacidad. Salvar esta brecha digital puede ayudar a los miembros de los grupos sociales desfavorecidos a participar más en pie de igualdad en la sociedad digital (incluidos los servicios de interés directo para ellos, por ejemplo en los ámbitos del aprendizaje, la administración pública o la salud en línea) y a salir de su condición desfavorecida incrementando su empleabilidad. La competencia digital es, pues, una de las ocho competencias clave que resultan fundamentales para las personas en una sociedad basada en el conocimiento. También es esencial para que todos sepan cómo garantizar la propia seguridad cuando se está en línea.

Además, las TIC no pueden funcionar con eficacia como sector europeo en crecimiento y como motor de la mejora de la competencia y la productividad en la economía europea si no se dispone de personal

capacitado. Y la economía de la UE padece una penuria de este tipo de personal: Para 2015, Europa podría carecer de la capacitación necesaria para cubrir hasta 700.000 puestos de trabajo en las TI.

Afrontar estos problemas exige actuaciones en los campos que a continuación se enumeran:

- a) Alfabetización y capacitación digitales
- b) Servicios digitales incluyentes

7. BENEFICIOS QUE HACEN POSIBLES LAS TIC PARA LA SOCIEDAD DE LA UE

La sociedad digital debe entenderse como una sociedad que supondrá ventajas para todos. El despliegue de las TIC se está convirtiendo en un elemento crítico para la consecución de objetivos políticos tales como el apoyo a una sociedad que envejece, el cambio climático, la reducción del consumo energético, la mejora de la eficiencia del transporte y de la movilidad, la autonomización de los pacientes y la inclusión de las personas con discapacidad.

Afrontar estos problemas exige actuaciones en los campos que a continuación se enumeran:

- a) Las TIC al servicio del medio ambiente
- b) Atención sanitaria sostenible y apoyo basado en las TIC para una vida digna y autónoma
- c) Promoción de la diversidad cultural y los contenidos creativos
- d) Administración electrónica
- e) Sistemas de transporte inteligentes a favor de un transporte eficiente y una movilidad mejor

8. ASPECTOS INTERNACIONALES DE LA AGENDA DIGITAL

La Agenda Digital europea se propone hacer de Europa un centro neurálgico del crecimiento inteligente, sostenible e incluyente en la escena mundial. Los siete pilares de la Agenda Digital tienen, todos ellos, dimensiones internacionales. El mercado único digital, en particular, necesita de una faceta externa, porque solo a nivel internacional se puede progresar en muchas de las cuestiones políticas. Una interoperabilidad y unas normas reconocidas a escala mundial pueden contribuir a promover una innovación más rápida al disminuir los riesgos y los costes de las nuevas tecnologías. También la lucha contra las crecientes amenazas a la ciberseguridad debe desarrollarse en un contexto internacional. Asimismo, las soluciones reglamentarias europeas, que se basan en la igualdad de oportunidades, la transparencia de los poderes públicos y la gobernanza y la apertura de los mercados a la competencia, están sirviendo de inspiración en otros lugares del mundo. Por último, también es importante comparar los progresos europeos en la Agenda Digital con las mejores prestaciones internacionales.

Por consiguiente, resulta crucial una dimensión internacional en la Agenda Digital a fin de completar las acciones antes mencionadas, sobre todo a la vista de la importancia estratégica de internet. Europa debe seguir desempeñando un papel de liderazgo, en consonancia con la Agenda de Túnez, en la promoción de una gobernanza de internet lo más abierta e incluyente posible. Actualmente internet incluye una amplia gama de dispositivos y aplicaciones que permean todos los aspectos de la vida, con independencia de la geografía, y en el futuro esta tendencia incluso se acentuará. Constituye un instrumento formidable para la libertad de expresión en todo el mundo.

Para fomentar la innovación también a nivel internacional, la Comisión trabajará por conseguir unas condiciones favorables para los bienes y servicios digitales en el comercio exterior, p. ej., crear una asociación más sólida para obtener acceso al mercado y oportunidades de inversión,

reducir las barreras arancelarias y no arancelarias a nivel mundial, mejorar la protección de los derechos de propiedad intelectual y evitar el falseamiento del mercado.

El Acuerdo sobre Tecnologías de la Información (ATI) de 1997 ha producido resultados tangibles a la hora de promover la adopción de la tecnología de la información en Europa y en el mundo. No obstante, hoy en día es preciso actualizar dicho acuerdo para tener en cuenta las últimas novedades, y en especial la convergencia de las tecnologías y los productos.

También será necesario que el progreso tecnológico quede mejor reflejado en los acuerdos comerciales internacionales en lo que se refiere al ámbito de los servicios digitales y la propiedad intelectual.

APLICACIÓN Y GOBERNANZA

El éxito de la Agenda Digital depende de que las diferentes medidas del conjunto se ejecuten de forma precisa y de acuerdo con la estructura de gobernanza prevista en Europa 2020. La Comisión se propone:

1. Instituir un mecanismo de coordinación interno
2. Cooperar estrechamente con los Estados miembros, con el Parlamento Europeo y con todas las partes interesadas.
3. Llevar un seguimiento de los avances de la Agenda Digital mediante la publicación anual, en el mes de mayo, de un cuadro de indicadores.
4. Organizar un amplio debate entre las partes interesadas sobre los avances registrados, según figuren en los cuadros de indicadores digitales, que adoptará la forma de Asamblea Digital anual que se celebrará en junio y reunirá a los Estados miembros, las instituciones de la UE y los representantes de los ciudadanos y del sector, para evaluar los progresos y los desafíos que surjan.

5. La Comisión presentará su informe al Consejo Europeo acerca de los resultados de estas actividades en un Informe de situación anual, como dispone la estructura de gobernanza de Europa 2020.

OBJETIVOS CLAVE EN MATERIA DE RENDIMIENTO

1. Objetivos en materia de banda ancha:

- Banda ancha básica para todos en 2013: cobertura de banda ancha básica para el 100 % de los ciudadanos europeos (base de referencia: en diciembre de 2008 la cobertura DSL total era de un 93 % de la población de la UE).
- Banda ancha rápida para 2020: cobertura de banda ancha de 30 Mbps o superior para el 100 % de los ciudadanos europeos (base de referencia: en enero de 2010 un 23 % de los abonos a la banda ancha alcanzaban al menos los 10 Mbps).
- Banda ancha ultrarrápida para 2020: un 50 % de los hogares europeos deberán contar con abonos por encima de los 100 Mbps (no hay base de referencia).

2. Mercado único digital:

- Promoción del comercio electrónico: un 50 % de la población deberá efectuar compras en línea para 2015. (base de referencia: en 2009, un 37 % de usuarios con edades comprendidas entre los 16 y los 74 años habían efectuado pedidos de bienes o servicios con carácter privado en los 12 meses anteriores).
- Comercio electrónico transfronterizo: un 20% de la población deberá efectuar compras transfronterizas en línea para 2015 (base de referencia: en 2009, un 8 % de usuarios entre los 16 y los 74 años habían efectuado pedidos de bienes o servicios a proveedores de otros países de la UE en los 12 meses anteriores).



- Comercio electrónico para las empresas: un 33 % de las PYME deberán efectuar compras o ventas en línea para 2015 (base de referencia: en 2008, un 24 % y un 12 % de las empresas compró o vendió, respectivamente, de forma electrónica, por un valor igual o superior al 1 % de su volumen total de compras o su facturación).
- Mercado único de los servicios de telecomunicaciones: para 2015 la diferencia entre las tarifas de itinerancia y las nacionales deberá aproximarse a cero (base de referencia: en 2009, el precio medio de un minuto de itinerancia ascendía a 0,38 céntimos (por llamada efectuada), y el precio medio por minuto de todas las llamadas en la UE era de 0,13 céntimos (incluida la itinerancia)).

3. Inclusión digital:

- Aumentar la utilización regular de internet de un 60 % a un 75 % en 2015 y, entre los colectivos desfavorecidos, de un 41 % a un 60 % (la base de referencia son las cifras de 2009).
- Disminuir a la mitad la parte de población que nunca ha usado internet para 2015 (hasta un 15 %) (base de referencia: en 2009, un 30 % de personas con edades comprendidas entre los 16 y los 74 años no había usado nunca internet).

4. Servicios públicos:

- Administración electrónica para 2015: Un 50 % de los ciudadanos utilizan la administración electrónica, y más de la mitad de esa cifra cumplimentan formularios en línea (base de referencia: en 2009, un 38 % de personas con edades comprendidas entre los 16 y los 74 años habían usado la administración electrónica en los 12 meses anteriores, y un 47 % de ellas había cumplimentado formularios en línea).
- Servicios públicos transfronterizos: En 2015 deberán estar disponibles en línea todos los servicios públicos transfronterizos clave contenidos

en una lista que acordarán los Estados miembros en 2011 (no hay base de referencia).

5. Investigación e innovación:

- Fomento de la I+D en las TIC: Duplicación de la inversión pública a 11 000 millones de euros (base de referencia: la cifra nominal de créditos presupuestarios públicos de I+D dedicados a las TIC (CPPID-TIC) ascendía en 2007 a 5 700 millones).

6. Economía con baja emisión de carbono:

- Promoción del alumbrado con bajo consumo de energía: Reducción de al menos un 20 % del consumo de energía en alumbrado para 2020 (no hay base de referencia).

16.1.3. PLAN AVANZA 2.

Avanza es el primer Plan que ha supuesto una verdadera apuesta real del Gobierno y del conjunto de la Sociedad Española por el desarrollo de la Sociedad de la Información (SI) y del Conocimiento.

Avanza ha logrado que el sector de las Telecomunicaciones y de la Sociedad de la Información se convierta, como sector estratégico, en motor e impulso del desarrollo de otros sectores. La SI, como elemento necesario en cualquier actividad económica o industrial, tiene un efecto general y horizontal en el conjunto de la economía y constituye un elemento esencial para vertebrar la recuperación económica.

El sector TIC está adquiriendo en España un volumen de negocio y una presencia de uso y desarrollo de productos y servicios tan importante que permiten situarlo ya como uno de nuestros grandes sectores productivos.

Uno de los principales objetivos del Plan Avanza2 es contribuir a la recuperación económica de nuestro país gracias al uso intensivo y generalizado de las TIC, con una especial atención a los proyectos que compaginen, además, la sostenibilidad y el ahorro energético.

En este contexto, Avanza2 tiene como reto no ya tanto la dinamización de la oferta como el fomento de la demanda, así como en el aprovechamiento del impulso del desarrollo del sector para la consolidación de una industria TIC propia especializada en sectores estratégicos y siempre volcado en la pyme, en la que se centra la mayor parte de los esfuerzos.

Las iniciativas de Avanza2 se agrupan en cinco ejes de actuación:

1. Eje Capacitación: Desde el Plan Avanza 2 se ha abordado esta capacitación desde dos puntos de vista, la persona como ciudadano que forma parte de la sociedad y la persona como trabajador que se integra en una empresa. En la vertiente de la persona como ciudadano, se presta especial atención al uso y la aceptación de las TIC y la utilización de los servicios digitales por parte de los ciudadanos en riesgo de exclusión digital y se fomenta la igualdad de género en la red. Por otro lado, en la vertiente de la persona como trabajador, se observa que el uso general de las TIC en las pequeñas empresas y las microempresas. Dada la importancia que representa este segmento de empresas en el tejido productivo y en la creación de empleo, resulta fundamental impulsar la penetración de las TIC en ellas mediante acciones específicas de capacitación y promoción.

Dentro de este eje, se establecen los siguientes programas:

- a) En la línea de Capacitación Ciudadanía: Capacitación Tecnológica, Género, Mayores, Personas con Discapacidad, Infancia, Otros Colectivos, Equipamiento y conectividad, Inmigrantes.

b) En la línea de Capacitación PYME: Dinamización PYME, Soluciones sectoriales, Formación y Equipamiento y conectividad.

2. Eje Contenidos y Servicios Digitales: Se pretende impulsar a la industria española relacionada con la producción, gestión y distribución de contenidos digitales, destacando que este tipo de industria que no ha dejado de crecer en los últimos años en nuestro país, despertando cada día mayor interés entre creadores, productores, editores, distribuidores, agregadores de contenidos y operadores. Por otro lado se debe tener en cuenta el desarrollo de los servicios que presta la administración. Las ventajas que nos aporta la administración electrónica son un hecho constatado, y por ello, el próximo reto consiste en fomentar el uso de servicios avanzados por parte de la ciudadanía y las empresas.

Dentro de este eje, se establecen los siguientes programas:

- a) En la línea de Contenidos: Contenidos Digitales y Centros del Conocimiento.
 - b) En la línea de Servicios Digitales: Soluciones EELL, Ayuntamiento Digital, Ciudades Digitales, Administración Electrónica de la Administración General del Estado, Educación, Sanidad y Justicia.
3. Eje Desarrollo del Sector TIC: En este eje del Plan Avanza 2 se busca apoyar a empresas que desarrollen nuevos productos, procesos, aplicaciones, contenidos y servicios TIC, promoviendo, como prioridades temáticas básicas, la participación industrial española en la construcción de la Internet del Futuro. Por tanto, fomentar la innovación y la investigación industrial es apostar por la mejora de la competitividad del sector TIC.

Dentro de este eje, se establecen los siguientes programas:

- a) Fomento de Competitividad e Innovación.
 - b) Propiedad Intelectual.
 - c) Software Libre.
 - d) Promoción Tecnológica.
4. Eje Infraestructuras: El objetivo que se pretende alcanzar a través de las medidas contempladas en este apartado es la de disponer de unas infraestructuras de telecomunicaciones adecuadas a las cambiantes necesidades siendo fundamentales para el desarrollo de la sociedad de la información. Su extensión a toda la ciudadanía permite luchar contra la brecha digital y de género, ofrecer servicios electrónicos avanzados a la ciudadanía y las empresas, aumentar la productividad del tejido industrial y generar crecimiento económico.

Dentro de este eje, se establecen los siguientes programas:

- a) Banda Ancha.
 - b) Telecentros.
 - c) Televisión Digital Terrestre.
5. Eje Confianza y Seguridad: Este eje del Plan Avanza 2 centrará sus objetivos y áreas de actuación exclusivamente en el desarrollo de las políticas públicas para la seguridad de la información orientadas a particulares y empresas, contribuyendo al resto de políticas nacionales para la construcción de la confianza desde la cooperación y la coordinación. La misión será la de impulsar la construcción de la confianza a través de políticas públicas proactivas y de carácter preventivo en relación con la seguridad de la información centradas en los particulares y las empresas, especialmente las PYME, promoviendo la participación de todos los agentes implicados.

Dentro de este eje, se establecen los siguientes programas:

- a) Seguridad de la Información.

b) DNI Electrónico.

ESTRATEGIA 2011-2015

El Consejo de Ministros aprobó el 16 de julio de 2010 el acuerdo por el que se aprueba la Estrategia 2011-2015 del Plan Avanza 2. Esta segunda fase da continuidad al Plan Avanza, incorporando las actuaciones en ejecución y actualizando sus objetivos iniciales para adecuarlos a los nuevos retos de la Sociedad en Red.

En el año 2004, el Gobierno era consciente de la importancia de generalizar el uso y el impacto de las nuevas tecnologías en la economía y la sociedad. Por ello surgió de la necesidad de establecer “un plan de convergencia con Europa y entre Comunidades Autónomas y Ciudades Autónomas” en este ámbito, denominado Plan Avanza.

El Plan Avanza, que fue aprobado por el Consejo de Ministros el 4 de noviembre de 2005, ha permitido alcanzar una masa crítica en nuestro país, tanto en términos de mercado como de usuarios, en la aceptación generalizada de las TIC y en la cobertura global de servicios TIC, lo que facilitará enormemente el progreso en los próximos años.

Una vez alcanzados una buena parte de los objetivos planteados y siendo conscientes de la necesidad de seguir avanzando hacia una Sociedad del Conocimiento, comienza una nueva etapa integrada por cinco ejes estratégicos de actuación: Infraestructuras, Confianza y Seguridad, Capacitación Tecnológica, Contenidos y Servicios Digitales y Desarrollo del Sector TIC.

Una de las principales contribuciones del Plan Avanza 2 es coadyuvar al cambio de modelo económico de nuestro país a través de las TIC, ya que la generalización de su uso permite y permitirá un incremento de la

competitividad y la productividad, además de favorecer la igualdad de oportunidades, dinamizando la economía y consolidando un modelo de crecimiento económico sostenible.

La primera fase del Plan Avanza perseguía recuperar el retraso de España respecto de la Unión Europea, especialmente en cobertura y conectividad. La Estrategia 2011-2015 del Plan Avanza 2 pretende situar a España en una posición de liderazgo en el desarrollo y uso de productos y servicios TIC avanzados.

Tras la presentación del Plan Avanza 2 y una vez determinada su estructura, el Consejo de Ministros procedió a aprobar la Estrategia de dicho Plan para el período 2011-2015. Dicha estrategia no está vinculada a unos presupuestos concretos sino que marca unas prioridades que se adoptarán y desarrollarán dentro de los escenarios de consolidación presupuestaria aprobados por el Gobierno.

En el proceso de elaboración de la Estrategia ha de destacarse el consenso que ha suscitado entre las fuerzas políticas. En concreto, el 21 de diciembre de 2009, el Senado aprobó por unanimidad un documento de propuestas que han sido incorporadas íntegramente en la Estrategia 2011-2015 del Plan Avanza 2.

Asimismo, en la elaboración de la Estrategia han colaborado también el sector privado y el conjunto de agentes sociales, políticos e institucionales con el fin de lograr la máxima eficacia y eficiencia de las iniciativas identificadas. Para el Gobierno la elaboración y el desarrollo de un Plan con estas características es una tarea común que requiere de la participación y el esfuerzo de toda la sociedad española.

Asimismo, la Estrategia se enmarca dentro de las iniciativas que se están elaborando en el ámbito europeo. La Comisión Europea aprobó el 19 de

mayo de 2010 una Comunicación sobre la “Agenda Digital Europea”, cuyo objetivo es promover el desarrollo de la Sociedad de la Información y las TIC para la reactivación económica y la creación de empleo en la UE. y un horizonte temporal el año 2015, tomando así el relevo del i2010.

Tomando como punto de partida el Plan Avanza aprobado en el año 2005, así como el marco europeo en el que se encuadran este tipo de iniciativas, se han identificado 34 retos concretos que debe abordar España en el ámbito de las TIC. En este contexto, la Estrategia 2011-2015 del Plan Avanza 2 consiste en centrar sus esfuerzos en la consecución de los siguientes 10 objetivos que facilitarán la superación de los retos definidos:

1. Promover procesos innovadores TIC en las AAPP
2. Extender las TIC en la sanidad y el bienestar social
3. Potenciar la aplicación de las TIC al sistema educativo y formativo
4. Mejorar la capacidad y la extensión de las redes de telecomunicaciones
5. Extender la cultura de la seguridad entre la ciudadanía y las empresas
6. Incrementar el uso avanzado de servicios digitales por la ciudadanía
7. Extender el uso de soluciones TIC de negocio en la empresa
8. Desarrollar las capacidades tecnológicas del sector TIC
9. Fortalecer el sector de contenidos digitales garantizando la mejor protección de la propiedad intelectual en el actual contexto tecnológico y dentro del marco jurídico español y europeo.
10. Desarrollar las TIC verdes.

Para la consecución de los 10 objetivos definidos, se han identificados más de 100 medidas concretas que se deben articular, así como los indicadores de seguimiento que medirán su grado de consecución.

Adicionalmente, se han identificado un conjunto de reformas normativas, necesarias tanto para eliminar barreras existentes a la expansión y uso de las TIC, como para garantizar los derechos de los ciudadanos en la Sociedad de la Información. En este apartado destacan la Ley de Medidas de Impulso de la Sociedad de la Información, y la Ley de Acceso Electrónico de los Ciudadanos a los Servicios Públicos.

Por otro lado, en cuanto al modelo de ejecución para la puesta en marcha de estas medidas, se mantiene el modelo de colaboración con todos los niveles de la Administración Pública, en especial con las Comunidades Autónomas y las entidades locales, así como de las entidades sin fines de lucro y las empresas privadas, iniciado por el Plan Avanza.

La Estrategia 2011-2015 del Plan Avanza 2 consta de un texto base, en el que se destaca el papel de las TIC en la economía y el crecimiento, los logros del Plan Avanza en su primera fase, el Marco Europeo concretado en la Agenda Digital Europea 2010-2015 aprobada durante la Presidencia Española, los principales retos de futuro en el ámbito de la Sociedad de la Información y los 10 objetivos que servirán para conseguir esos retos, y de un anexo en el que se recopilan las más de 100 medidas concretas que deben implementarse.

EVALUACIÓN Y SEGUIMIENTO

Para garantizar el éxito del Plan Avanza es fundamental asegurar la evaluación y seguimiento permanente de las actuaciones que se realicen, valorando así la consecución de objetivos planteados en cada una de las áreas de actuación, a la vez que sirven para orientar la adaptación del Plan a los cambios.

La documentación de evaluación y seguimiento disponible en el sitio web del Plan Avanza es la siguiente:

1. Información Territorial

- Informe Plan Avanza España
- Informes Plan Avanza CC.AA.
- Informes Plan Avanza Provincia

2. Información por Programas.

- Informes Plan Avanza por Programas.

3. Información Indicadores

- Indicador de Convergencia Plan Avanza.
- Indicadores de evolución de la Sociedad de la Información.
- Balance actuaciones SETSI.

4. Información Internacional

- Estudio del Plan Avanza por la OCDE.

Se puede encontrar toda la información necesaria sobre este tema en la dirección <http://www.planavanza.es/>.

16.2. REFERENCIAS

- Comunicación de la Comisión al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones - Una Agenda Digital para Europa, con fecha 28 de agosto de 2010.
- Sitio web Eur-Lex en la dirección <http://eur-lex.europa.eu/>, integrado en el sitio web oficial de la Unión Europea.
- Sitio web de la Comisión Europea dedicado a la Estrategia Europa 2020 en la dirección http://ec.europa.eu/europe2020/index_es.htm
- Sitio web del Ministerio de Industria, Turismo y Comercio dedicado al Plan Avanza2 en la dirección <http://www.planavanza.es/>.

Autor: Jesús Rodríguez Castro

Jefe del Servicio de Informática del Concello de Santiago de
Compostela

Colegiado del CPEIG

17. INICIATIVAS DEL GOBIERNO GALLEGO: OSIMGA, REDE CEMIT, PLAN DE BANDA ANCHAS 2013, AGENDA DIGITAL 2014.GAL, ESTRATEGIA DE IMPULSO AL SECTOR TIC. SISTEMAS DE INFORMACIÓN.

TEMA 17. INICIATIVAS DEL GOBIERNO GALLEGO. OSIMGA. RED CeMIT, PLAN DE BANDA ANCHA 2013. AGENDA DIGITAL 2014.gal. ESTRATEGIA DE IMPULSO DEL SECTOR TIC.

17.1.OSIMGA

17.2.RED CeMIT

17.3.PLAN DE BANDA ANCHA 2013.

17.4. AGENDA DIGITAL 2014.gal

17.5. ESTRATEGIA DE IMPULSO DEL SECTOR TIC

17.6.REFERENCIAS

17.1.OSIMGA

El Observatorio de la Sociedade da Información e a Modernización de Galicia (OSIMGA) es un órgano asesor para la valoración de la evolución de la sociedad de la información, la modernización administrativa y la Administración electrónica en las administraciones públicas de Galicia, y para la participación y colaboración con las distintas administraciones públicas en estas materias.

Creado y regulado por el Decreto 21/2010, de 4 de febrero (DOG, 26/02/2010), el OSIMGA está adscrito a la Secretaría Xeral de Modernización e Innovación Tecnológica de la Xunta de Galicia.

Este decreto le atribuye al observatorio entre sus funciones las de desarrollar o promover estudios y análisis de datos que permitan conocer el nivel de desarrollo, la tendencia y posibles problemáticas que pueden afectar a la extensión de la sociedad de la información en Galicia y la aplicación del modelo de e-Gobierno en las administraciones públicas gallegas. El Osimga elabora informes de situación y de evolución y facilita

datos a otros organismos competentes en la materia, contribuyendo a la definición estratégica de políticas públicas.

Asimismo, el observatorio analiza el estado de desarrollo de la sociedad de la información para toda la ciudadanía y, en especial, en lo que respeta a los colectivos en riesgo de exclusión, promoviendo líneas de actuación que potencien su incorporación y permanencia en condiciones de igualdad efectiva. Entre las observaciones de carácter general cabe destacar que el OSIMGA pondrá en marcha encuestas sobre la sociedad de la información en Galicia y sobre la e-Administración en la Xunta y en las entidades locales.

La web del OSIMGA (<http://www.osimga.org>) es un canal abierto de comunicación y difusión de los datos, informaciones, estudios y otros materiales elaborados por el observatorio. Además suministra una selección de noticias relacionadas con la modernización de la Administración autonómica gallega y la sociedad de la información en Galicia.

Los principales objetivos del observatorio son:

1. Desarrollar o promover recopilaciones, estudios y análisis de datos que permitan conocer con una visión global el nivel de desarrollo, la tendencia y los posibles problemas que afecten a la extensión de la sociedad de la información en Galicia y a la aplicación del modelo de e-Gobierno en las administraciones públicas gallegas.
2. Facilitar análisis comparativos y alineaciones de datos con otros marcos geográficos.
3. Promover el intercambio de experiencias e información entre administraciones, con otros observatorios, organismos o entidades.
4. Impulsar la organización de eventos formativos, reuniones de expertos o grupos de trabajo.

5. Promover y gestionar la elaboración y difusión de publicaciones técnicas, impresas o electrónicas, específicas y monográficas o de publicación periódica.
6. Gestionar y ofrecer periódicamente y, como mínimo, a través de una web específica, información sobre el nivel de desarrollo de la sociedad de la información en Galicia, eventos formativos, noticias de actualidad, o enlaces con otras fuentes de información, observatorios o entidades.
7. Elaborar y presentar públicamente informes que reflejen el estado de situación o la evolución prevista.
8. Facilitar datos a otros organismos y entidades con competencias específicas en la materia.
9. Analizar el estado de desarrollo de la sociedad de la información para toda la ciudadanía y, en especial, en lo que respeta a las mujeres, a las personas con discapacidad, a las personas mayores y a los colectivos con riesgo de exclusión, promoviendo líneas de actuación que potencien su incorporación y permanencia activa en condiciones de igualdad efectiva.
10. Evaluar y servir de elemento para la definición de políticas públicas en materia de sociedad de la información y modernización de la Administración.

DOCUMENTOS Y MEMORIAS

El sistema de indicadores de la sociedad de la información de Galicia es un conjunto de indicadores estadísticos que permite monitorizar, de una manera sintética, rigurosa y transparente, la evolución de la sociedad de la información en Galicia, ofreciendo una visión de conjunto de la situación y de su grado de avance.

Este modelo de indicadores fue elaborado tomando como referencia las recomendaciones establecidas en el código de buenas prácticas de las estadísticas europeas.

El sistema de indicadores ofrece información referente al nivel de equipación y utilización de productos y servicios TIC por parte de la población y las empresas gallegas, realizando además un tratamiento específico del sector gallego de las tecnologías de la información y de las comunicaciones (sector TIC), así como un seguimiento de la Administración electrónica en Galicia.

17.2. RED CeMIT

A Rede de Centros para a Modernización e a Inclusión Tecnolóxica (CeMIT) es una iniciativa puesta en marcha por la Xunta de la Galicia que busca impulsar las TIC y la sociedad de la información en la comunidad gallega. Esta red forma parte de la Agenda Digital 2014.gal, enmarcada en el Plan estratégico Galicia 2010-2014, que tiene como fin conseguir la convergencia tecnológica con Europa en el horizonte del año 2020.

La red CeMIT nace con los objetivos estratégicos de vertebrar territorial y socialmente Galicia, en especial donde la brecha digital se hace más evidente, e impulsar, potenciar y difundir los conocimientos en las tecnologías de la información y la comunicación en tres colectivos principalmente: ciudadanía, profesionales TIC y empleados públicos

Así pues, la nueva Red CeMIT se configura como un importante vehículo para la puesta en práctica de iniciativas orientadas a impulsar el empleo de las TIC con el fin de fomentar la empleabilidad, la competitividad empresarial, la e-Inclusión, el e-Bienestar y el impulso de la e-Administración.

La nueva Rede de Centros para a Modernización e a Inclusión Tecnolóxica de Galicia (Red CeMIT) es una iniciativa impulsada desde la Xunta de Galicia en colaboración con los ayuntamientos gallegos, para potenciar el uso de las TIC y la sociedad de la información en Galicia.

La red se convierte de este modo en un instrumento esencial de soporte a la nueva estrategia en materia de sociedad de la información, definida a través de la Agenda Digital 2014.gal, contribuyendo a vertebrar territorial y socialmente Galicia, impulsar el crecimiento del sector empresarial tradicional, especializar a los profesionales del sector TIC, y potenciar los conocimientos tecnológicos del empleado público.

La red CeMIT ofrece un amplio abanico de servicios que se divide en los siguientes tres grandes bloques:

a) FORMACIÓN

La formación es uno de los servicios principales que ofrecerá la nueva red a ciudadanos, profesionales TIC, empresas, empleados públicos y agentes territoriales a través de dos modalidades:

- Formación presencial: Se impartirá directamente desde los centros de la red a través de métodos que combinan la exposición de conceptos con la demostración de procesos y con la ejecución guiada por parte del grupo, para lo cual se definirán las acciones de formación que se detallan a continuación: Formación en alfabetización digital, formación avanzada de profesionales TIC, formación multimedia y audiovisual, y formación de empleados públicos
- Formación on-line: Les permitirá a los ciudadanos realizar actividades formativas a través de un centro virtual de formación con dos funciones complementarias: tutorización e interacción.

También se contempla la formación mixta basada en el concepto de *blended learning*, es decir, que combina actividades presenciales, síncronas y on-line.

b) ACTIVIDADES DE DIFUSIÓN

La organización de charlas y jornadas de sensibilización y divulgación de las actividades de la red, la captación de usuarios e introducción a temas relacionados con las nuevas tecnologías serán actividades que forman parte de la carta de servicios de la nueva red y que serán planificadas en función de las necesidades y demandas detectadas.

c) AULA ABIERTA

Los centros de la red también se convertirán en “aulas abiertas”, auténticos espacios en los que sus usuarios/as, dentro de un horario establecido, podrán acceder libre y gratuitamente a la utilización de las aulas, para lo cual contarán con el apoyo y asesoramiento de los agentes TIC.

De este modo, las aulas se convierten en verdaderos espacios abiertos en los que cualquier ciudadano puede, sin coste alguno, acercarse a las nuevas tecnologías y hacer uso de ellas de modo personal e independiente.

La estratégica localización de sus instalaciones, al largo de más de 50 comarcas y 89 ayuntamientos, favorece que cualquiera de sus usuarios no deba recorrer grandes distancias para encontrar un Aula CeMIT en la que se impartan alguna de las más de 1.000 actividades formativas previstas. Esta dispersión geográfica permite garantizar la correcta vertebración territorial y social de Galicia, especialmente donde la brecha digital se hace más evidente.

CENTROS DE ALTA ESPECIALIZACIÓN: LA ESCOLA GALEGA DE ADMINISTRACIÓN PÚBLICA Y EL CENTRO DE NOVAS TECNOLOXÍAS DE GALICIA.

La Escola Galega de Administración Pública (EGAP) es un organismo público perteneciente a la Xunta de Galicia, y su finalidad es diseñar e impartir el programa de formación destinado a los empleados públicos de Galicia. Dado que es un instrumento de primer orden para la profesionalización de la Función Pública y tiene el objetivo final de proporcionarle a la sociedad gallega los mejores servicios, constituye un componente indispensable para conseguir los objetivos estratégicos de la red CeMIT

El Centro de Novas Tecnoloxías de Galicia (CNTG) contribuye activamente en la formación y capacitación de los profesionales TIC gallegos a través de cursos especializados y certificaciones tecnológicas de primer nivel. De este modo, el CNTG orienta su actividad hacia los profesionales de los sectores privado y público, ocupados o en busca de empleo, que demanden formación técnica de alto nivel relacionada con el mundo de las nuevas tecnologías. De este modo, constituyen uno de los pilares sobre los que se sustenta la Red CeMIT en lo que respecta a la formación especializada.

17.3. PLAN DE BANDA ANCHA 2013.

El Plan director de telecomunicación de banda ancha busca garantizar que las infraestructuras de telecomunicaciones cuenten con la capacidad necesaria para hacer posible el acceso de todos los gallegos a la sociedad de la información. De hecho, pretende dotar de estrategia, actuaciones y un modelo de gestión en materia de despliegue de infraestructuras de telecomunicaciones a la Comunidad Gallega.

La Xunta de Galicia asume la coordinación de los agentes implicados en la elaboración del plan, asegurando orden, eficiencia y un uso excelente de los recursos. Las autoridades regionales y locales serán las mejor situadas para planificar los proyectos de banda ancha.

La Xunta de Galicia aprobó el 18 de febrero de 2010 el Plan Banda Ancha de Galicia 2010-2013, que define la estrategia a seguir para alcanzar las siguientes metas:

- Reducir el desequilibrio territorial proporcionando acceso a la banda ancha de calidad a toda la población gallega.
- Impulsar la competitividad e innovación en las empresas proporcionando acceso a la banda ancha a los sectores productivos para extraer el máximo aprovechamiento de las nuevas tecnologías.
- Modernizar los servicios públicos proporcionando acceso a la banda ancha a todos los núcleos con puntos de demanda pertenecientes a la Administración.
- Maximizar la cooperación asegurando un despliegue basado en la eficiencia y en la cooperación de todos los agentes implicados.

Por tanto, el Plan Director de Banda Ancha de Galicia es un instrumento esencial y necesario para la definición de las políticas de infraestructuras de Galicia que permitiría, por ejemplo:

- Impulsar una estrategia global, encaminada a situar a Galicia en el núcleo avanzado de la sociedad de la información.
- Garantizar la capacidad de acceso de los gallegos a la sociedad de la información bajo condiciones de homogeneización de calidad de servicio y coste.
- Asegurar la vertebración digital de nuestro territorio, como elemento de compensación de desequilibrios culturales, tecnológicos y socioeconómicos, de inclusión social y de eliminación de la brecha digital.
- Extraer el máximo aprovechamiento de las posibilidades de las nuevas tecnologías como dinamizadoras económicas y generadoras de competitividad e innovación en los diferentes sectores productivos

y como medio para promover la equidad, la sostenibilidad y la calidad de los servicios públicos.

- Impulsar la modernización de la Administración pública autonómica y local, empleando toda la potencialidad que ofrece hoy la tecnología.

ReDe – REGISTRO DE DEMANDANTES

ReDe es una herramienta de consulta que proporciona información sobre la cobertura de banda ancha alcanzada con las actuaciones del Plan Banda Ancha 2010-2013 (PDBL). Gracias a ReDe cualquier ciudadano pode hacer uso de su navegador web habitual para obtener información sobre la cobertura de banda ancha o registrar demandas.

OFICINA TÉCNICA DEL PLAN DE BANDA ANCHA

La oficina técnica es un recurso de la Xunta de Galicia que, dentro del marco del Plan Banda Ancha, pone en marcha distintos servicios para apoyar el desarrollo de las distintas actuaciones del plan:

Los principales objetivos de la oficina técnica son coordinar y tutelar la ejecución del plan y velar por la consecución con éxito de proyectos específicos liderados y ejecutados por un grupo/área y por aquellos proyectos de alcance más amplio, que sean tractores e involucren a más de un área/grupo o a otro tipo de agentes. De este modo, la oficina técnica constituye un punto único de referencia para todos los agentes involucrados en el Plan de Banda Ancha fomentando el avance homogéneo de las distintas actuaciones del plan e incentivando la eficiencia y efectividad de las mismas.

La oficina técnica pone en marcha distintos servicios para apoyar el desarrollo de las distintas actuaciones del Plan de Banda Ancha, agilizando así la consecución de sus objetivos. Dichos servicios se agrupan según su

índole en servicios de gestión, control y seguimiento de las actuaciones del plan, así como, en servicios orientados a la atención del ciudadano en todo lo referente a los proyectos de despliegue de red de banda ancha derivados del Plan de Banda Ancha.

17.4. AGENDA DIGITAL 2014.gal

Galicia se marcó como objetivo, dentro del actual marco establecido por el Plan Estratégico Galicia 2010-2014, el reto de converger con el horizonte europeo para 2020.

De este plan surge la Agenda Digital de Galicia, como apuesta por la definición de una estrategia clara en materia de sociedad de la información que nos permita competir como región en el joven mercado único digital europeo definido por la Agenda Digital para Europa y en la nueva economía del conocimiento, como camino para una recuperación económica sostenible.

Dentro del contexto de la Agenda Digital de Galicia, el último año supuso el arranque para iniciativas básicas en la creación de infraestructuras, como el Plan de Banda Ancha o el Centro de Proceso de Datos Integral, y la apuesta decidida por la Administración electrónica, impulsando el Decreto 198/2010, de 2 de diciembre, por el que se regula el Desarrollo de la Administración Electrónica en la Xunta de Galicia y en las entidades de ella dependientes, desarrollando proyectos para la mejora de servicios públicos digitales y fomentando y divulgando el uso de las TIC, como la red CeMIT o el proyecto Abalar.

La Agenda Digital de Galicia se enfrenta a un importante cambio de enfoque estratégico: su objetivo es pasar de una sociedad que utiliza las TIC a una sociedad gallega que se sirve de las nuevas tecnologías para generar un crecimiento sostenible, para mejorar sus cuotas de

participación en la toma de decisiones y para contribuir a su calidad de vida sobre la base del conocimiento. Para lograrlo, contará con el impulso y la participación activa de todos los agentes implicados en la sociedad de la información.

Este enfoque lo marcó la Comisión Europea, que diseñó una estrategia para ayudarnos a salir fortalecidos de la crisis y a convertir la UE en una economía que disfrute de altos niveles de empleo, de productividad y de cohesión social. Esta es la labor de "Europa 2020: Una estrategia para un crecimiento inteligente, sostenible e integrador" (Bruselas, 3.3.2010 - COM(2010) 2020), que constituye una nueva visión de la economía social de mercado de Europa para el siglo XXI, proponiendo tres prioridades que se refuerzan mutuamente:

- Crecimiento inteligente: desarrollo de una economía basada en el conocimiento y la innovación.
- Crecimiento sostenible: promoción de una economía que haga un uso más eficaz de los recursos, que sea más verde y competitiva.
- Crecimiento integrador: fomento de una economía con alto nivel de empleo que tenga cohesión social y territorial.

En este entorno, Europa 2020 establece siete iniciativas para catalizar los avances en cada uno de los temas fijados como prioritarios. Una de ellas consiste en la definición de la Agenda Digital para Europa (Bruselas, 19.05.2010 COM (2010) 245) que hace de las tecnologías de la información y de la comunicación (TIC) la pieza clave para que Europa consiga sus ambiciones para el 2020.

Algunos de los ejes de actuación en los que se estructura la Agenda Digital para Europa con el objetivo de contribuir al crecimiento económico de Europa son los siguientes:

- Servicios públicos digitales: es necesario el desarrollo de nuevos y mejores servicios públicos digitales, que reactiven la demanda y hagan explícitas las ventajas de la economía digital y el gobierno abierto.
- Uso de internet, seguridad y confianza: Europa necesita una internet más segura, en la que los ciudadanos sean capaces de aprovechar todas las potencialidades a través de una adecuada alfabetización digital, especialmente de los colectivos más desfavorecidos o reticentes a su uso.
- Fortalecer la competitividad del sector TIC europeo: hay que reforzar la competitividad del sector TIC apostando por la investigación, el desarrollo y la innovación mediante programas mejor adaptados a las especiales características de las empresas del sector, especialmente las PYMES.
- Mercado Único Digital: la UE debe crear un verdadero Mercado Único Digital, soporte fundamental de la economía del conocimiento en Europa, y promover de manera activa los mercados europeos existentes de contenidos digitales, mediante soluciones prácticas que impulsen nuevos modelos de negocio.
- Infraestructuras: la UE debe contar con infraestructuras sólidas, más rápidas y eficientes, especialmente con respecto a la banda ancha y las redes de futuro. Es necesario adoptar medidas concretas para superar la brecha digital alcanzando el objetivo del 100% de cobertura de banda ancha básica para todos los ciudadanos en 2013 y promover una amplia penetración de la banda ancha de velocidad ultrarrápida en 2020.

Las políticas deben estar plenamente alineadas con la Agenda Digital Europea para llegar en condiciones excelentes al nuevo período de financiación a partir de 2014. A Agenda Digital impulsará la inclusión de Galicia en el nuevo contexto digital europeo de forma definitiva en el

horizonte 2014. Galicia tiene que ser un país que compita en el joven mercado único digital europeo: Galicia tiene que pensar de forma global.

El Plan Estratégico Galicia 2010-2014 define un nuevo modelo socioeconómico que pretende una modernización para toda Galicia, que nos implique y nos incluya a todos. Las nuevas tecnologías deben servir como catalizadoras de los ejes marcados en el Plan Estratégico, como mecanismo facilitador de la cohesión social, de la calidad de vida de los gallegos, de la generación de empleo de calidad y como impulsor de una Administración austera, eficiente y próxima al ciudadano. Este reto tiene como resultado la Agenda Digital de Galicia, que da respuesta a la estrategia de la Xunta de Galicia en el empleo de las nuevas tecnologías.

A continuación puede verse como se alinea la Agenda Digital de Galicia con el Plan Estratégico Galicia 2010 -2014

		Líneas de transformación					
		L.1. Servicios Públicos digitales	L.2. Admón. eficiente	L.3. Ciudadanía digital	L.4. Impulso al sector de la economía del conocimien to	L.5. Empresa innovadora y economía digital	L.6. Política de telecom.
Ejes de actuación	E.1. Cohesión social, bienestar y calidad de vida						
	E.2. Dinamización económica, crecimiento y empleo						
	E.3. Economía del conocimiento						
	E.4. Sostenibilidad medioambiental y						

	equilibrio territorial						
	E.5. Administración austera, eficiente y cercana al ciudadano						
		Impacto elevado	impacto moderado	impacto bajo			

Además del **Plan Estratégico Galicia 2010-2014**, la nueva Agenda también estará integrada con otros planes estratégicos, como el Plan Gallego de I+D+i, con el Plan de Banda Ancha de Galicia, con planes de competitividad de diferentes sectores estratégicos para Galicia (automoción, madera, textil, construcción naval, energía, piedra y turismo) y con las Agendas Digitales Locales que promueven el desarrollo de la sociedad de la información en un entorno más próximo a la ciudadanía.

Ejes de actuación					
E.1. Cohesión social, bienestar y calidad de vida	E.2. Dinamización económica, crecimiento y empleo	E.3. Economía del conocimiento	E.4. Sostenibilidad medioambiental y equilibrio territorial	E.5. Administración austera, eficiente y cercana al ciudadano	Planes estratégicos sectoriales

ESTRATEGIA

Para alcanzar el salto cualitativo implícito en el reto que se formula Galicia se establecen siete líneas estratégicas dentro de la Agenda Digital de Galicia:

L1. SERVICIOS PÚBLICOS DIGITALES.

Está realizándose un gran esfuerzo para sentar las bases para un desarrollo generalizado de la Administración digital, que en buena lógica, deberá traducirse en una explosión de servicios digitales durante estos próximos años.

La innovación que impulsa esta agenda digital debe proyectarse sobre nuestro sistema de gobernanza. Está demostrado que un uso adecuado de las TIC por parte de las Administraciones tiene la capacidad de transformar las relaciones que se establecen entre los gobiernos y la ciudadanía contribuyendo esa transformación al desarrollo de la sociedad y a un avance de la calidad de vida.

La inclusión de las TIC, para que se realice de forma idónea, lleva consigo aparejado un cambio en el modelo de Administración y en la forma en que se prestan los servicios públicos.

Por todo ello desde la Xunta se puso en marcha el plan e-Gobierno 2013, iniciativa bajo la que se desarrollan todos los planes de modernización y avance de los servicios públicos a través de las TIC.

Objetivos:

- Incluir las TIC en todos los ámbitos de los servicios públicos. Pasar del concepto de Administración “electrónica” al concepto de “e-Gobierno”.
- Adaptar el modelo de Administración para las nuevas posibilidades de gestión a través de las TIC.

- Prestar los servicios públicos transmitiendo seguridad y confianza, asumiendo el reto de la interoperabilidad.
- Facilitar la vida a la ciudadanía mediante la mejora de los servicios prestados en ámbitos como: sanidad, educación, justicia, bienestar, etc.
- Mejorar la competitividad del tejido productivo gallego.
- Garantizar unos servicios públicos homogéneos en todo el territorio mediante la colaboración entre las administraciones públicas.

Enfoque y aspectos clave:

- Desarrollo completo de la Administración electrónica, que implica cambios organizativos, normativos y tecnológicos.
- Colaboración entre todas las AAPP de Galicia. Afrontar el reto de la interoperabilidad y garantizar la homogeneidad en la prestación pública.
- Fomento de la participación ciudadana. Informar de las políticas y colaborar con la ciudadanía en su ejecución, evaluación y diseño de futuras.
- Puesta en marcha de servicios públicos digitales.
- Desarrollo de planes de modernización sectorial.

L2. ADMINISTRACIÓN EFICIENTE.

La Administración pública juega un papel muy importante en el desarrollo de la sociedad de la información en dos áreas fundamentales:

- Como usuaria de las TIC, con el fin de mejorar la calidad de los servicios públicos, modernizar la Administración, ahondar en la transparencia de su actuación, promover la participación ciudadana y garantizar los principios de eficiencia, eficacia, calidad y sostenibilidad.

- Como dinamizador de la sociedad de la información, por medio del planteamiento y ejecución de políticas que promuevan la penetración de las TIC en la sociedad y su acceso a todos los agentes sociales.

En este sentido, es objetivo de esta línea transformar la Administración pública autonómica desde dentro, como usuaria de las TIC, realizando acciones de homogeneización en cuanto a la estrategia tecnológica se refiere y adoptando criterios de economía de escala que permitan la reducción de costes y avance de los servicios prestados.

Existen modelos para mantener y mejorar el papel de las TIC dentro de la organización y, en general, la incorporación de las TIC en la actividad de la Administración mejoran la calidad de vida del ciudadano, proporcionando herramientas eficaces para la reducción de tiempos y costes.

Objetivos:

- Proporcionar servicios de calidad y eficaces a los usuarios alineados con las necesidades y directrices estratégicas.
- Gestión eficiente del gasto: Hacer más y mejor con menos.
- Homogeneizar y consolidar sistemas de gestión TIC, bajo unas directrices operativas y estratégicas unificadas de interoperabilidad.
- Transferencia y compartición del conocimiento TIC en Galicia.

Enfoque y aspectos clave:

- La gestión de los recursos TIC de la Xunta (aplicaciones, datos, tecnología e infraestructura) se considera ámbito de gestión interno y será transparente para los usuarios que consuman estos servicios.
- Política global de ahorro de consumo de energía y residuos derivados de los servicios TIC, denominada sostenibilidad a través de políticas de Green IT.

- Gestión unificada de los activos TIC con el objetivo principal de la consolidación de los servicios mediante su centralización en un único CPD y la estandarización de la plataforma tecnológica.
- Racionalización de los sistemas de información.
- Actividades destinadas al aseguramiento y al control de la calidad de los sistemas.
- Estrategia TIC de consolidación de servicios; evolución de servicios hacia *cloud computing*. La Xunta actuará como proveedor de servicios de *cloud computing* para el resto de las unidades de la Administración.

Se deben tomar medidas de austeridad y racionalidad del gasto TIC a través de dos grandes acciones: la centralización de la función de compras de activos y servicios TIC y la consolidación de contratos en servicios agregados de mayor volumen.

La Xunta de Galicia lanzó una iniciativa para la promoción, difusión y fomento de la utilización de tecnologías basadas en software libre y fuentes abiertas.

L3. CIUDADANÍA DIGITAL.

Galicia quiere ser un país cohesionado con unos ciudadanos y ciudadanas que sean competentes tanto para utilizar contenidos y servicios digitales avanzados como, especialmente, para colaborar activamente en su creación y desarrollo y ponerlos al servicio del bienestar individual y colectivo. Para eso es imprescindible que su ciudadanía tenga las competencias digitales y la motivación necesarias para participar activamente en su desarrollo.

Las personas necesitan aprender continuamente nuevas ideas y capacidades o participar en actividades de formación permanente. De esta

forma, esta capacidad de aprendizaje podrá aplicarse a nuevas tareas, lo que se traducirá en beneficios económicos y sociales.

En esa tarea las TIC abordan un papel doble: por una parte, ser un medio valioso para el aprendizaje permanente a lo largo de la vida y, por otro, ser un área en avance que exige y facilita la mejora constante de las competencias individuales.

Objetivos

- Cohesionar territorial y socialmente Galicia mediante la eliminación de la brecha digital y el impulso de los nativos digitales.
- Incrementar la empleabilidad gracias al desarrollo de las capacidades tecnológicas que derivan del uso de las TIC.
- Mejorar la calidad de vida de los ciudadanos y garantizar su autonomía personal universalizando la cultura digital en nuestra comunidad.

Enfoque y aspectos clave:

- En el ámbito de la ciudadanía digital es preciso evolucionar desde un enfoque tradicional “las TIC por las TIC: el objetivo es introducir las TIC”, al enfoque centrado en el ciudadano: “Quiero estar más capacitado para afrontar todos los retos de la vida, y las TIC me ayudan a estarlo”; y de un enfoque local: “islas de alfabetización digital” a un enfoque global e integrado: “la alfabetización digital es cosa de todos”.
- Apuesta por definir estrategias digitales en el sistema educativo orientadas a crear “nativos digitales”

L4. IMPULSO AL SECTOR DE LA ECONOMÍA DEL CONOCIMIENTO

El Plan Estratégico 2010-2014 y la nueva Agenda Digital de Galicia hacen un reconocimiento de la importancia del sector TIC para contribuir a la dinamización y a aumentar la competitividad de la economía regional,

cualidades que lo convierten no sólo en un sector estratégico, sino en un sector tractor del resto de los sectores estratégicos de Galicia.

Objetivos:

- Consolidar un sector TIC competitivo, innovador y generador de empleo cualificado, capaz de hacer frente a los retos de la nueva economía del conocimiento.
- Construir un sector TIC cohesionado e integrador, que actúe como motor del resto de los sectores estratégicos de Galicia.
- Convertir el sector TIC en un sector fuerte en busca de la excelencia tecnológica, que estimule la creación de una clase emprendedora y creativa.

Enfoque y aspectos clave:

- Posicionamiento del sector de la economía del conocimiento existente en Galicia.
- Capacitación y especialización del capital humano, junto con políticas de personal capaces de atraer personal calificado al sector y fomentar la retención de conocimiento en las empresas.
- Creación y consolidación de empresas de base tecnológica.
- Hacer de Galicia una fuente de conocimiento tecnológico “desde las universidades y para los sectores estratégicos de la región”.
- Especialización de las empresas en segmentos altamente innovadores y con el desarrollo de los mercados en los que actúan.
- Consolidar estructuras eficientes de apoyo a la innovación y refinar los servicios de financiación existentes, orientando los sistemas de ayudas a mejorar la competitividad de las empresas del sector de la economía del conocimiento.
- Alineamiento de la oferta del sector TIC con la demanda del tejido empresarial gallego.

De este modo el sector TIC no sólo se convertirá en un sector estratégico en sí mismo, sino que también actuará como motor de los sectores estratégicos de Galicia impulsando un nuevo modelo productivo basado en la economía del conocimiento.

L5. EMPRESA INNOVADORA Y ECONOMÍA DIGITAL

Las empresas gallegas, independientemente de su tamaño y sector, utilizarán intensiva y extensivamente las TIC para innovar tanto en el desarrollo de productos y servicios que satisfagan plenamente a sus clientes, como en su propia operativa y modelo de negocio, de manera que puedan transformarse optimizando en cada momento sus capacidades competitivas.

ES preciso que las empresas gallegas, especialmente pymes y micropymes, sean capaces de utilizar las TIC para ser más eficientes, aumentar su productividad e innovar. Además, las TIC ofrecen una gran oportunidad para que pequeñas y medianas empresas puedan competir en mercados hasta ahora inaccesibles.

Impulso del sector TIC: El sector TIC de Galicia debe ser uno de los sectores estratégicos de la economía del futuro, y debe convertirse en catalizador de la competitividad del resto de los sectores y de la modernización de la Administración. Este impulso pasa por el alineamiento de los esfuerzos de todos los agentes de este sector —universidades, centros tecnológicos, empresas, etc.— para crear un círculo virtuoso entre oferta y demanda TIC, convirtiendo a este sector en tractor del resto de los sectores estratégicos gracias al uso de las TIC y también en beneficio de la demanda tecnológica.

Las TIC se presentan como la gran oportunidad de las empresas gallegas, sin exclusión por tamaño o sector, de optimizar su competitividad en el mercado y de innovar tanto en el desarrollo de nuevos productos y

servicios, como en su propia operativa, consiguiendo mayores competencias y contribuyendo al crecimiento económico sostenible de la sociedad gallega.

Objetivos:

- Contribuir a la creación de empleo y al crecimiento económico sostenible de Galicia creando un nuevo modelo productivo.
- Hacer más competitivos los sectores estratégicos de Galicia mediante la incorporación de las TIC a sus modelos de negocio (automoción, construcción naval, energía, piedra y rocas ornamentales, textil, madera, turismo).
- Facilitar la incorporación de micropymes y autónomos a la sociedad del conocimiento, reduciendo la brecha digital para converger con España y Europa.

Enfoque y aspectos clave:

Desde hace unos años las empresas gallegas están haciendo frente a una importante transformación tanto interna como en su entorno social y económico. En este contexto tan cambiante su éxito depende de su capacidad para ser competitivas en los mercados globales, y la incorporación de las nuevas tecnologías tiene mucho que decir en este sentido. Se necesita impulsar:

- La incorporación de las TIC como una ventaja competitiva: “las TIC como inversión y no como gasto”.
- Enfoque centrado en las empresas, en sus objetivos y en sus necesidades concretas.
- Enfoque global y coordinado, capaz de integrar la oferta en TIC con las necesidades de las empresas de los diferentes sectores estratégicos de Galicia.
- Además se debe apostar por un enfoque segmentado de las necesidades TIC de las empresas gallegas.

- El nuevo modelo de incorporación de las TIC a las empresas de los sectores estratégicos de Galicia debe entenderse como un proceso constante

L6. POLÍTICAS DE TELECOMUNICACIONES

Las infraestructuras de telecomunicaciones constituyen el canal de acceso de ciudadanos y empresas a los servicios avanzados de la sociedad de la información, y es por ello que resulta necesario disponer de una red de estas infraestructuras moderna y sostenible que garantice el acceso a nuevos servicios y que contribuya así al desarrollo económico y al progreso de nuestro país.

Objetivos:

- Garantizar el acceso a la sociedad de la información la toda la sociedad gallega.
- Mejorar los servicios ofrecidos a la ciudadanía a través de la modernización de los servicios e infraestructuras de telecomunicaciones corporativas soporte de los sistemas y procesos de la Xunta.

Enfoque y aspectos clave:

El primer objetivo se consigue a través de tres líneas de actuación:

- Ejecución de las acciones definidas en el Plan Director de Banda Ancha.
- Transformar el modelo de negocio de Retegal como operador de telecomunicaciones neutro.
- Promover la localización en Galicia de la Agencia Estatal de Radiocomunicaciones e impulsar medidas que faciliten la implantación de operadoras con interés en invertir en el despliegue de infraestructuras en Galicia.

El segundo objetivo de esta línea, el avance de servicios ofrecidos a la ciudadanía, se instrumenta fundamentalmente a través de las siguientes líneas de actuación:

- Mejorar las infraestructuras de las redes corporativas soporte de los sistemas y procesos de la Xunta de Galicia.
- Evolucionar la Red de Investigación de Galicia (RECETGA) desde un modelo de red basado en alquiler de circuitos a un nuevo modelo basado en la adquisición de fibra.
- Crear un Servicio de Comunicación de Emergencias de Galicia.
- Impulsar el hogar digital.

L7. MEDIDAS INSTRUMENTALES DE SEGUIMIENTO Y COOPERACIÓN.

Por último, una séptima línea, que da soporte al desarrollo de las anteriores. En esta línea, la Xunta de Galicia como elemento dinamizador del sector TIC regional pretende establecer una política de austeridad y simplificación de estructuras organizativas, de tal forma que se transforme en una Administración ágil, fiable y segura.

En este sentido, también dentro de esta línea, y para buscar el máximo alineamiento y coordinación, y por lo tanto sinergias y ahorro de costes, adquiere una clara relevancia la necesidad del desarrollo de las necesarias actuaciones de coordinación y liderazgo integrador en el marco de las actuales vías de cooperación en el campo tecnológico con ayuntamientos y diputaciones, trabajando así por consolidar una Agenda Digital Única para Galicia.

El modelo actual de prestación de servicios informáticos y de comunicaciones en la Xunta de Galicia se significa por representar un estricto seguimiento de mecanismos, procedimientos y plazos muy dilatados, tanto para la adquisición de bienes y servicios (Ley de contratos del sector público) como para la contratación de personal (Convocatoria

pública de empleo, procesos de consolidación de puestos, etc.), mecanismos que vienen establecidos por la necesaria aplicación en todos sus términos y requisitos de la normativa que afecta a los organismos públicos, sea cual sea su actividad.

En la presente legislatura, la aparición de la Secretaría General de Modernización e Innovación Tecnológica (SXMIT) constituyó un punto de inflexión en la orientación de las políticas TIC de la Xunta, en el sentido de que suponía la constatación de que estas determinan un instrumento de alto nivel estratégico por su potencial para impulsar la modernización de la Administración pública, así como su capacidad para impulsar y sustentar el desarrollo social y económico de Galicia

Objetivos:

La SXMIT integró una gran cantidad de competencias con el objeto de que se facilitase el desarrollo de una estrategia tecnológica eficaz de la Xunta y se postula como el embrión de un nuevo modelo de gestión de las políticas tecnológicas para la administración autonómica de tal manera que se garantice:

- El alineamiento en el desarrollo de las TIC con las directrices políticas de la Xunta;
- La racionalización de costes;
- La mejora de la eficiencia y la eficacia de la Administración territorial y de las actuaciones que se establezcan;
- Que las TIC consigan transformar los servicios públicos de manera que se conviertan en elemento de dinamización económica y permitan aumentar la competitividad y la innovación en todos los sectores productivos.

Enfoque y aspectos clave:

En esta línea, tal y como se comentó, se establece la necesidad de constituir una nueva entidad de gestión de las TIC de carácter público y adscrita a todos los niveles a la Xunta de Galicia que aglutine las competencias que son responsabilidad de la SXMIT y que concentre los recursos humanos, materiales y presupuestarios asociados a los actuales departamentos TIC dispersos en las consellerías de la Xunta de Galicia.

El Consello de la Xunta de Galicia que tuvo lugar el 21 de julio de 2011 aprobó el plan de puesta en marcha de la Agencia de Modernización Tecnológica de Galicia (AMTEGA) con el objetivo de consolidar un modelo de gestión integrado de las TIC en la Administración autonómica.

La creación de la Agencia permitirá una mayor eficiencia y una reducción de gasto al integrar los servicios tecnológicos de los distintos departamentos de la Xunta bajo una misma dirección. Un total de 558 profesionales de la escala de tecnologías de la información que desempeñan sus funciones en los distintos departamentos de la Xunta.

Este modelo permitirá gestionar las iniciativas y actuaciones que sobre tecnologías de la información se desarrollen en la Xunta de Galicia, así como proporcionar un nuevo modelo de gestión de las TIC para la Administración autonómica con el objeto de gestionar de manera más eficaz y eficiente los recursos globales, y orientarse hacia políticas de optimización y reducción del gasto.

17.5. ESTRATEGIA DE IMPULSO DEL SECTOR TIC

El sector de las tecnologías de la información y de la comunicación está convirtiéndose en una de las áreas productivas claves en el desarrollo económico y social de Galicia, por su condición de acelerador del cambio tecnológico y por su carácter transversal al resto de los sectores. El número

de empresas gallegas del sector TIC en el año 2009 se situaba en 1.542 empresas, lo que supone un 9,8 % más que en 2006.

El sector empresarial de las TIC ocupa una posición estratégica por su capacidad de generación de empleo. El nivel de empleo en el sector TIC se situó en el año 2009 en los 16.327 trabajadores/as, lo que representa el 1,59% de la población ocupada gallega. La evolución de la ocupación en este sector muestra un continuo crecimiento en los últimos años.

El peso de este segmento empresarial también se refleja claramente en su contribución al impulso y desarrollo de la I+D. En el año 2008, el 45,6% de las empresas gallegas del sector disponían de personal con dedicación relacionada con la I+D y un 37,1% realizó proyectos de I+D+i en el último año.

LÍNEA TRANSFORMA TIC

En este entorno, 2014.gal Agenda Digital de Galicia definió una línea de impulso al sector de la economía del conocimiento con el objetivo de convertirlo en un sector que sea capaz de dar soporte a la competitividad de Galicia y que se consolide como un sector de peso en la economía gallega.

2014.gal persigue la consecución de unos objetivos, a través de esta línea:

- Consolidar un hipersector TIC competitivo, innovador y generador de empleo cualificado, que se convierta en sector estratégico para la economía gallega.
- Que ese sector sea cohesionado e integrador. Que actúe también como motor del resto de los sectores estratégicos de Galicia.
- La creación de una clase emprendedora y creativa estimulada por ese hipersector TIC.

- Búsqueda de la excelencia tecnológica.

Las líneas de la Agenda Digital de Galicia, y principalmente las L4 y L5, explican más en detalle los objetivos, enfoque y aspectos clave de este plan de impulso del sector TIC.

MAPA DE CAPACIDADES TECNOLÓGICAS DE GALICIA.

La Xunta de Galicia está poniendo en marcha, como una de las actuaciones dentro de la estrategia de impulso del sector TIC, un programa de demanda temprana de tecnología innovadora.

Este programa promoverá la identificación de soluciones tecnológicas innovadoras que acerquen ventajas competitivas a las administraciones públicas y, por tanto, permitan contar con cada vez mejores servicios públicos que den soporte a las necesidades de los ciudadanos y empresas de Galicia.

Además, a través de este sistema se incentivarán los procesos de innovación en el sector TIC para el desarrollo de soluciones diferenciales y con ventajas competitivas que contribuyan al ánimo del sector en Galicia y a la exportación de nuevos servicios TIC a nuevos mercados fuera de la misma.

Como primera actividad dentro de este programa, y dentro del ámbito socio sanitario, se elaboró el mapa de capacidades tecnológicas de Galicia.

Se trata de un documento vivo, que tiene la intención de recoger el conjunto de las capacidades y conocimientos tecnológicos de los diferentes agentes que desarrollan su actividad en el ámbito sanitario y social de Galicia. Esto incluye tanto entidades gallegas que desarrollan proyectos en este ámbito en Galicia, en el resto del territorio nacional y proyectos

internacionales, como empresas de ámbito nacional y/o internacional que desarrollan proyectos de temática socio sanitaria en el ámbito geográfico concreto de Galicia.

El mapa incluye la experiencia y conocimientos tecnológicos, además de información detallada de numerosos proyectos, de todos los grupos de investigación TIC de Galicia que desarrollan su trabajo en el ámbito mencionado y de diferentes centros tecnológicos gallegos además del sector empresarial.

Este instrumento sirve como punto de partida para conocer las capacidades tecnológicas gallegas en este ámbito y para orientar mejor las actuaciones que a partir de ahora lleven a cabo dentro de este programa para el impulso del sector tecnológico.

LÍNEA EconomiC-IT

En este mundo globalizado, Galicia debe construir una economía inteligente, sostenible e integradora, impulsando la competitividad y mejorando la productividad del tejido empresarial, eliminando las debilidades estructurales existentes, incentivando la innovación y la calidad, apoyando la creación de nuevas empresas y generando un alto nivel de empleo.

AS TIC son la gran oportunidad de las empresas gallegas para hacer frente a esos retos, pues mejoran la eficiencia de las empresas y facilitan la innovación. Con todo, en Galicia el nivel de dotación y uso de las TIC en las micropymes, que conforman la mayor parte del tejido empresarial en Galicia, está lejos de converger con el promedio europeo. Existe una profunda brecha entre las pymes y las micropymes. Estas últimas presentan un preocupante desinterés por la oferta tecnológica, seguramente producido por el desconocimiento.

En este entorno, 2014.gal Agenda Digital de Galicia definió una línea estratégica “Empresa innovadora y Economía Digital” con el objetivo de promover la sociedad de la información en el tejido empresarial gallego.

Con la puesta en marcha de esta línea se promoverá la utilización intensiva y extensiva de las TIC para crear redes de colaboración que les permitan competir con éxito en cualquier sector o mercado y para innovar tanto en el desarrollo de productos como en su propia operativa y modelo de negocio.

Más concretamente, los objetivos estratégicos que persigue la Agenda Digital a través de la definición de esta línea son los siguientes:

- Contribuir a la creación de empleo y al crecimiento económico sostenible de Galicia creando un nuevo modelo productivo.
- Hacer más competitivos los sectores estratégicos de Galicia mediante las incorporaciones de las TIC a sus modelos de negocio (automoción, construcción naval, energía, textil)
- Facilitar la incorporación de las micropymes y autónomos a la sociedad de la información, reduciendo la brecha digital para converger con España y Europa.

El proceso de introducción de las TIC en los sectores productivos debe pasar primeramente por el denominador Plan de demanda anticipada tecnológico-industrial. Este plan permite garantizar la perfecta incorporación de las nuevas tecnologías, ya que está alineada con las necesidades específicas de cada sector.

Además es necesario diseñar actuaciones más y mejor focalizadas apostando por una segmentación de las necesidades TIC en las empresas gallegas.

La figura del tutor tecnológico asociado a la red CeMIT jugará un papel muy importante, ayudando a conocer la situación de las empresas identificando cuáles son sus necesidades concretas.

CENTRO DEMOSTRADOR TIC DE GALICIA

O Centro Demostrador TIC de Galicia es el instrumento operativo enmarcado en el eje de actuación económica-T: “Empresas DIGITAL E INNOVADORA” de la Agenda Digital 2014.gal, y se pone en marcha en Galicia a través de un convenio entre la Secretaría General de Modernización e Innovación Tecnológica, la Consellería de Trabajo y Bienestar y la entidad pública empresarial Red.es.

La misión del Centro es facilitarles a las empresas TIC los medios para acercar su oferta de productos a las empresas de otros sectores productivos, de forma que puedan desarrollar productos adaptados a las necesidades de mercado, con dos objetivos: incrementar la demanda de productos TIC y adaptar esta demanda a las necesidades de innovación de los sectores estratégicos.

Se puede encontrar abundante información sobre los contenidos de este tema en la dirección <http://imit.xunta.es/>

17.6. REFERENCIAS

- Ley 11/2007, de 22 de junio, del Acceso Electrónico de los Ciudadanos a los Servicios Públicos.
- Decreto 198/2010, de 2 de diciembre, por el que se regula el desarrollo de la Administración electrónica en la Xunta de Galicia y en las entidades de ella dependientes.
- iMIT – Iniciativas de Modernización e Innovación Tecnolóxica, de la Xunta de Galicia (<http://www.imit.xunta.es/>).
- Área sobre la Agenda Digital para Europa en el sitio web de la Comisión Europea (http://ec.europa.eu/information_society/digital-agenda/index_en.htm).
- “Anotacións e comentarios ao decreto de Administración electrónica da Xunta de Galicia”, editado por el Colegio Profesional de Ingeniería en Informática de Galicia. ISBN 978-84-614-7362-5.
- “Las relaciones de la empresa con la Administración Electrónica”, editado por el Colegio Profesional de Ingeniería en Informática de Galicia. ISBN 978-84-614-9865-9.

Autor: Jesús Rodríguez Castro

Jefe del Servicio de Informática del Ayuntamiento de Santiago de
Compostela

Colegiado del CPEIG



18. MODELO ENTIDADE- RELACIÓN. MODELO RELACIONAL. NORMALIZACIÓN.

Tema 18. Modelo entidad-relación. Modelo relacional. Normalización

ÍNDICE

<i>18.2.1 Parte Estática del Modelo E/R.....</i>	<i>6</i>
18.2.1.1 Entidad.....	6
18.2.1.2 Relación o Interrelación.....	7
18.2.1.3. Dominio.....	8
18.2.1.4 Atributos.....	8
<i>18.2.2 Parte Dinámica del Modelo E/R.....</i>	<i>9</i>
18.2.2.1 Tipo de correspondencia.....	10
18.2.2.2 Entidades Débiles.....	11
18.2.2.3. Papel o rol.....	13
18.2.2.4 Atributos multivaluados y compuestos.....	14
18.2.2.5 Atributos Derivados.....	15
<i>18.3.1 Cardinalidad.....</i>	<i>15</i>
<i>18.3.2 Jerarquía Subconjunto.....</i>	<i>16</i>
<i>18.3.3 Generalización.....</i>	<i>17</i>
<i>18.3.4 Tipos de relaciones.....</i>	<i>18</i>
<i>18.3.5 Control de redundancias.....</i>	<i>20</i>
<i>18.3.6 Dimensión temporal.....</i>	<i>21</i>
<i>18.4.1 Elementos.....</i>	<i>23</i>
<i>18.4.2 Restricciones.....</i>	<i>25</i>

Se llama datos al conjunto de propiedades que caracterizan un fenómeno, e información al conjunto de valores que pueden tomar estas propiedades junto con las relaciones o dependencias entre las mismas.

Los modelos de datos son herramientas de abstracción que permiten representar la realidad captando las restricciones semánticas que en ella se puedan dar.

Cuando en el mundo real se da información de cualquier suceso u objeto siempre los datos suministrados van acompañados de una semántica o de un significado. De la misma manera estos datos están sujetos a unas

restricciones y nosotros entendemos los datos suministrados sólo si entendemos el dominio y las restricciones de significados que acompañan a la información. Sin embargo, cuando aparecen los ordenadores y las bases de datos se empiezan a informatizar ocurre que se tiende a almacenar datos separando a estos de su interpretación, esto es, de su semántica. Como consecuencia fue necesaria la aparición de los modelos de datos como una herramienta que ayudara a incorporar significado a los datos almacenados.

De esta manera, los modelos de datos proporcionan mecanismos de abstracción que permiten la representación de la parte del mundo real que nos interesa registrar. Esta representación se concibe en dos niveles: el de las estructuras que hacen posible la representación de la información, y el de la información en sí misma.

Esto nos lleva a diferenciar entre lo que se denomina el esquema de la base de datos (descripción específica en términos de un modelo de datos) y la colección de datos en sí misma que es lo que denominamos base de datos.

El primer paso en la representación de un problema del mundo real es la caracterización del mismo, o lo que es lo mismo, la determinación mediante un proceso de simplificación de los datos de interés (de entre todos los que intervienen en el problema) y sus límites (universo del discurso).

Los modelos de datos ofrecen distintos niveles de abstracción que facilitan la representación de los datos:

1. Clasificación. Es la acción de crear una categoría a partir de las características comunes a un conjunto de ejemplares. Por ejemplo, a partir de los elementos Pedro, Juan y Cristina podemos crear la categoría profesor de instituto.

Su proceso inverso es la particularización.

2. Agregación. Es la capacidad de considerar un objeto en base a los elementos que lo constituyen. Por ejemplo, podemos crear la clase coche a partir de las clases volante, ruedas, motor y carrocería.

Su proceso inverso es la desagregación.

3. Generalización. Es similar a la clasificación, pero creando una categoría a partir de las características comunes a un conjunto de otras categorías. Por ejemplo, a partir de las categorías profesor de matemáticas, profesor de física y profesor de informática, podemos crear la categoría profesor de instituto.

Su proceso inverso es la especialización.

Según el nivel de abstracción que apliquemos, podemos hablar de tres tipos de modelos de datos:

- **Modelo conceptual.** Describe los tipos o clases de objetos desde un punto de vista estructural. Para cada uno de estos tipos de objetos describe sus propiedades y el dominio y restricciones de cada una, así como las relaciones entre ellos. (Modelo Entidad/Relación).
- **Modelo lógico.** Representa el problema bajo las restricciones específicas del tipo de Sistema Gestor de Base de Datos (SGBD) que se aplique en cada caso específico. (Modelo Relacional para el caso de los SGBD Relacionales).
- **Modelo físico.** Representa el problema desde el punto de vista de su implementación en el sistema de tratamiento utilizado y los métodos y mecanismos que se van a usar en su almacenamiento.

Un modelo de datos define las reglas mediante las cuales se han de estructurar los datos del mundo real.



La representación de un mundo real mediante un determinado modelo da lugar a un esquema, el cual describe las categorías existentes. Sin embargo, la realidad contempla además de los aspectos estáticos, los aspectos dinámicos. Por tanto las propiedades del mundo real son de dos tipos:

- **Estáticas** relativamente invariantes en el tiempo, que es lo que se suele conocer como estructuras. Este tipo de propiedades está compuesto por:

- o Elementos permitidos como: los objetos (entidades, relaciones, registros, ...), asociaciones entre objetos, propiedades de los objetos y asociaciones (atributos, elementos de datos, ...), dominios (conjuntos de valores que pueden tomar las propiedades).

- o Elementos no permitidos o restricciones, puesto que no todos los valores, cambios de valor o estructuras están permitidos en el mundo real. Cada modelo tiene por sí mismo limitaciones en cuanto a las estructuras que permite:

- Las restricciones impuestas por el modelo se conocen como restricciones inherentes

- Las restricciones que permiten capturar la semántica del universo de discurso que se quiere modelar y verificar la corrección de los datos almacenados en la base de datos. Estas últimas restricciones se conocen como restricciones de integridad o semánticas.

- Las restricciones de integridad son impuestas por el usuario, mientras que las restricciones inherentes al modelo son impuestas directamente por el modelo.

- **Dinámicas** Son las operaciones que se aplican a los datos o valores almacenados en las estructuras, los cuales varían a lo largo del tiempo

al aplicarles dichas operaciones. La aplicación de cualquier operación sobre los valores de los elementos, debe dejar a estos con un estado válido, es decir los valores de los elementos deben pertenecer a alguna de las categorías definidas en el esquema y deben cumplir las restricciones de integridad.

La componente estática de un modelo de datos se define a través del lenguaje de definición de datos (DDL) y la componente dinámica se define a través del lenguaje de manipulación de datos (DML), constituyendo ambas componentes el lenguaje de datos. También se puede mencionar el lenguaje de control de datos (DCL) que añade una capa de seguridad.

18.2.- MODELO ENTIDAD - RELACIÓN (E-R)

Propuesto por Peter Chen en dos artículos (1976 y 1977). Es un modelo muy extendido que ha experimentado una serie de ampliaciones a lo largo de los años.

El modelo se apoya en dos conceptos, el concepto de entidad y el concepto de relación. Este modelo de datos permite representar casi cualquier restricción del diseño de datos.

El modelo E/R percibe el mundo real como una serie de objetos relacionados entre sí y pretende representarlos gráficamente mediante un mecanismo de abstracción. Este mecanismo de abstracción está basado en una serie de símbolos, reglas y métodos que permitirán representar los datos de interés del mundo real, ofreciendo al diseñador una herramienta para aislar al modelo de consideraciones relativas a la máquina y a los usuarios.

Tal y como veíamos en los apartados anteriores distinguiremos entre la estática del modelo y la dinámica del mismo



18.2.1 Parte Estática del Modelo E/R

Chen distingue en el modelo E/R los siguientes elementos: Entidad, Relación, Atributo y Dominio

18.2.1.1 Entidad

Una entidad es un objeto real o abstracto de interés en una organización y acerca del cual se puede y se quiere obtener una determinada información; personas, cosas, lugares, etc., son ejemplos de entidades

La estructura genérica que describe un conjunto de entidades aplicando la abstracción se denomina tipo de entidad, mientras que entidad se refiere a cada una de las ocurrencias o ejemplares de ese tipo de entidad. Así pues, asociado al concepto de entidad surge el concepto de ocurrencia de entidad. Una ocurrencia de entidad es una realización concreta de una entidad. De esta manera, Hospital es un tipo de entidad mientras que “CHOU” es una ocurrencia o ejemplar.

Una entidad debe cumplir las siguientes reglas:

- Debe tener existencia propia (veremos que hay un tipo de entidades que en puro rigor no cumple esta restricción como son las entidades débiles)
- Cada ocurrencia de un tipo de entidad tiene que poder distinguirse de los demás
- Todas las ocurrencias de un mismo tipo de entidad deben tener las mismas propiedades o atributos

Una entidad se representa gráficamente en el modelo E/R mediante un rectángulo y en el interior del mismo se escribe en mayúsculas el nombre del tipo de entidad.

ENTIDA

D

Existen dos tipos de entidades:

- **Regulares:** sus ejemplares tienen existencia por sí mismos, p.ej. LIBRO.
- **Débiles** en las que la existencia de un ejemplar depende de que exista un cierto ejemplar de otro tipo de entidad. Se verán en el apartado 2.2.2

18.2.1.2 Relación o Interrelación

Una interrelación es una asociación entre entidades y se caracterizará por unas determinadas restricciones que determinarán las entidades que pueden o no participar de dicha relación.

La interrelación se representa gráficamente por un rombo etiquetado con el nombre de la interrelación en mayúsculas unido mediante arcos a las relaciones que vincula.

Asociado al concepto de interrelación surge el concepto de ocurrencia de interrelación.

Una ocurrencia de interrelación es la asociación concreta de ocurrencias de entidad de diferentes entidades. Por ejemplo, si tenemos las entidades MEDICO y HOSPITAL, y la interrelación “trabaja en”, una ocurrencia de interrelación será: MARTA GARCÍA trabaja en el CHOU.

Una interrelación queda caracterizada por tres propiedades:

- **Nombre:** las interrelaciones deben tener un nombre que las identifique unívocamente.

- Grado: número de tipos de entidad sobre las que se realiza la asociación. La interrelación del ejemplo anterior será binaria, es decir, su grado sería dos.
- Tipo de Correspondencia: Número máximo de ocurrencias de cada tipo de entidad que pueden intervenir en una ocurrencia del tipo de interrelación.

Las relaciones pueden tener atributos propios.

18.2.1.3. Dominio

Representa el conjunto de valores posibles de una determinada propiedad o atributo de un tipo de entidad o de un tipo de interrelación. En términos de abstracción, es una especialización de un conjunto. Con lo que se puede decir que el dominio es un conjunto de valores homogéneos con un nombre.

Se representa por un círculo pequeño acompañado de su nombre en minúsculas.

Es importante resaltar en este punto que los dominios tienen existencia propia y es el que realmente captura una semántica del mundo real. Lo que ha ocurrido muy a menudo es que se tiende a confundir dominio con atributo.

18.2.1.4 Atributos

Es cada una de las posibles propiedades o características de un tipo de entidad o tipo de interrelación. Los atributos toman valor en un dominio por lo que un atributo es una determinada interpretación de un dominio y varios atributos pueden tomar valores en el mismo dominio. Por ejemplo, si tenemos el atributo COLOR el dominio sobre el que se define podría ser: (NARANJA, BLANCO, AZUL y NEGRO).

Se puede representa gráficamente de 2 formas:



- a) Por un círculo pequeño unido por un arco al tipo de entidad y acompañado del nombre del atributo.
- b) Encerrando en un ovalo el nombre del atributo unido por un arco al tipo de entidad.

En función de las características del atributo respecto de la entidad se distinguen dos tipos de atributos:

- **Atributo identificador clave:** distingue de manera única una ocurrencia de entidad del resto de ocurrencias de entidad. Normalmente, el atributo identificador es único, pero puede haber casos en los que haya varios atributos identificadores, por lo que denominaremos a cada uno de ellos **atributo identificador candidato**. Elegiremos uno como identificador clave y el resto serán atributos identificadores. Se representa gráficamente:

- **Atributo descriptor:** caracteriza una ocurrencia de entidad pero no la distingue del resto de ocurrencias de entidad.

Una relación puede tener atributos al igual que las entidades.

18.2.2 Parte Dinámica del Modelo E/R

Decíamos que el interés de los modelos de datos es captar tanta semántica como sea posible del mundo real. Con lo que hemos visto hasta el momento comprobamos que se permite establecer cualquier número de relaciones diferentes entre tipos de entidad pero no podemos establecer restricciones del tipo:

- Un médico sólo trabaja en un hospital

- En un hospital trabajan n médicos
- Todos los socios del videoclub han alquilado al menos una película

A continuación se analiza en detalle todos los aspectos de las relaciones que nos permitirán captar toda la semántica deseada.

18.2.2.1 Tipo de correspondencia

Se denomina tipo de correspondencia al tipo de asociación que se establece entre las entidades relacionadas. Concretamente, se puede definir el tipo de correspondencia como el número máximo de ocurrencias de una entidad asociada a una ocurrencia de otra o de la misma entidad a través de una relación.

Para una relación binaria, es decir, de grado dos, entre las entidades A y B, existen tres tipos posibles de correspondencias:

- **Correspondencia 1:1** Una ocurrencia de la entidad A se asocia como máximo con una ocurrencia de la entidad B y viceversa, como se puede observar en la figura

Un ejemplo de este tipo de correspondencia puede ser que un cliente tiene una única cuenta bancaria en una sucursal determinada y una cuenta determinada de una sucursal pertenece a un único cliente.

- **Correspondencia 1:N** Una ocurrencia de la entidad A se asocia con un número indeterminado de ocurrencias de la entidad B, pero una ocurrencia de la entidad B se asocia como máximo con una ocurrencia de la entidad A. Si fuera al revés la correspondencia sería N:1.

Un exemplo de este tipo de correspondencia pode ser que una persoa vive en unha cidade e en unha cidade viven moitas persoas.

- **Correspondencia N:M** Una ocorrencia da entidade A se asocia con un número indeterminado de ocorrencias da entidade B e viceversa.

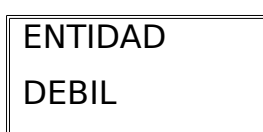
Un exemplo de este tipo de cardinalidade pode ser que un proveedor suministra varios produtos e cada produto pode ser suministrado por varios provedores.

18.2.2.2 Entidades Débiles

El concepto de entidade débil está directamente relacionado con as restricións de tipo semántico do modelo E/R e, máis concretamente, con a denominada restricción de existencia.

Esta restricción establece o feito de que a existencia de unha entidade non ten sentido sen a existencia de outra, é dicir, unha entidade ten dependencia de existencia de outra cando sen a primeira a segunda carecería de sentido.

Esto conlleva que a desaparición das ocorrencias da entidade da cal depende a súa existencia leve a desaparición das ocorrencias da entidade débil que dependan delas. Por exemplo, un exemplar da entidade EDICIÓN non existiría se non hubiera un exemplar correspondente na entidade LIBRO. As entidades débiles se representan gráficamente por dous rectángulos concéntricos e no interior o nome da entidade.



Hay dos tipos de dependencias de las entidades débiles respecto a las entidades regulares:

Dependencia en existencia los ejemplares de la entidad débil no pueden existir si desaparece el ejemplar de la entidad regular con el que están relacionados, pero la entidad débil puede ser identificada sin necesidad de identificar la entidad fuerte relacionada, es decir, la entidad débil tiene un atributo identificador clave.

En el ejemplo es evidente que si desaparece un empleado de la base de datos la existencia de sus familiares carece de sentido, es decir, la entidad FAMILIAR tiene dependencia de existencia respecto de la entidad EMPLEADO. Sin embargo, cada una de las ocurrencias de la entidad familiar puede identificarse por sí misma.

Por identificación la entidad débil no tiene sentido en sí misma y no puede ser identificada sin la entidad fuerte relacionada, es decir no tiene un atributo identificador clave sino tan sólo un descriptor discriminador y necesita el atributo clave de la entidad fuerte para poder identificar de manera única sus ocurrencias de entidad.

En el ejemplo, el atributo identificador clave será Cod_Libro (como clave de la entidad fuerte LIBRO) más ID como discriminador de la entidad EJEMPLAR.

Como conclusión al concepto de entidad débil conviene resaltar las circunstancias siguientes:

1. La dependencia en existencia no implica una dependencia en identificación, hecho que si sucede en el caso inverso pues una entidad que depende de otra por su Atributo Clave no tendrá sentido sin la existencia de esta última.
2. En una interrelación con cardinalidad N:M nunca habrá entidades débiles. La razón es que la supuesta ocurrencia de la entidad débil que se tuviera que borrar podría estar asociada a más de una ocurrencia de la supuesta entidad fuerte, lo que implicaría la imposibilidad de su borrado, hecho éste en clara contraposición con la definición de entidad débil.

18.2.2.3. Papel o rol

Es la función que cada una de las entidades realiza en una interrelación concreta. Gráficamente se representa indicando el nombre del rol en la línea que une las entidades con las relaciones.

Los roles juegan un papel especialmente importante en relaciones reflexivas donde es necesario conocer los dos roles que el mismo tipo de entidad juega en una determinada relación.

La razón está en que estamos asociando entre sí ocurrencias de una misma entidad de forma que cada una de ellas tiene un significado diferente. En el ejemplo, una ocurrencia de PERSONAS hará papel de 'padre' y la otra papel de 'hijo'.

18.2.2.4 Atributos multivaluados y compuestos

Un último tipo de restricciones que se deben tener en cuenta a la hora de realizar el diseño conceptual de una base de datos con el Modelo E/R son las que afectan a la tipología de los diferentes atributos. Desde este punto de vista podemos definir dos tipos diferentes de atributos respecto a los manejados hasta el momento, que son los siguientes:

Atributos multivaluados. Son aquellos atributos que para una misma ocurrencia de la entidad toman más de un valor. Por, ejemplo si cada cliente puede tener más de un teléfono y es de interés guardar todos sus posibles valores, el atributo teléfono sería multivaluado. Se representa etiquetando su arco con un valor de cardinalidad N.

Atributos Compuestos. Son aquellos que agrupan en sí mismos, por afinidad o por forma de uso, más de un atributo. Por ejemplo el atributo "dirección" engloba los atributos calle, numero, ciudad, provincia y código postal.

Se representa especificando sus atributos componentes rodeando al mismo y enlazándolos al símbolo del atributo compuesto mediante arcos.

18.2.2.5 Atributos Derivados

Son aquellos que pueden calcularse a partir de otros. Por ejemplo, si tenemos la entidad PERSONA con los atributos DNI, Nombre, Fecha_Nacimiento y Edad, el último atributo (Edad) puede obtenerse a partir de otro atributo (la fecha de nacimiento) y es, por lo tanto, redundante. Este tipo de atributos deben eliminarse del esquema.

18.3.- MODELO ENTIDAD RELACIÓN EXTENDIDO

El Modelo E/R con el paso del tiempo ha sufrido una serie de modificaciones tanto en su simbolismo gráfico, como en la ampliación de sus elementos.

18.3.1 Cardinalidad

Este primer concepto en cierto modo estaba tratado de forma implícita en el Modelo E/R original. Sin embargo, ha sido posteriormente cuando se le ha dado cierta relevancia e incluso una forma de representación.

El concepto cardinalidad, también denominado “clase de pertenencia”, permite especificar si todas las ocurrencias de una entidad participan o no en la interrelación establecida con otra(s) entidad(es):

- Si toda ocurrencia de la entidad A debe estar asociada con al menos una ocurrencia de la entidad B a la que está asociada por una determinada interrelación, se dice que la clase de pertenencia es obligatoria, es decir, la cardinalidad mínima es 1.



- Por el contrario, si no toda ocurrencia de la entidad A necesita estar asociada con alguna ocurrencia de la entidad B asociada, se dice que la clase de pertenencia es opcional, es decir, la cardinalidad mínima es 0.

Podemos definir la **Cardinalidad de un tipo de Entidad** como el número mínimo y máximo de ocurrencias de un tipo de entidad que pueden estar relacionadas con una ocurrencia del otro tipo de entidad que participan en el tipo de interrelación.

Su representación gráfica es una etiqueta del tipo (0,1), (1,1), (0,n) ó (1,n) según corresponda, al lado de las entidades asociadas por la relación tal como se puede observar en el siguiente ejemplo, donde el primer elemento de la tupla es la cardinalidad mínima, y el segundo elemento de la tupla es la cardinalidad máxima, que coincide con el tipo de correspondencia

Ejemplo: 'Un libro puede estar escrito por ninguno, uno o varios autores. Un autor escribe al menos un libro y puede escribir varios.'

18.3.2 Jerarquía Subconjunto

La descomposición de tipos de entidad en varios subtipos es una necesidad muy habitual en el modelado conceptual. En el mundo real se pueden identificar varias jerarquías de entidades. La interrelación que se establece entre un supertipo y sus subtipos corresponde a la noción de "ES-UN" (IS-A) o más exactamente "es un tipo de".

Para su representación se utiliza un triángulo invertido, con la base paralela al rectángulo que representa el supertipo.

El concepto jerarquía Subconjunto establece que una entidad A es un subconjunto de otra entidad B cuando toda ocurrencia de la primera

también es una ocurrencia de la segunda, y lo contrario no tiene por qué ser cierto.

Por tanto, tendremos una jerarquía subconjunto cuando cada ocurrencia de una entidad genérica pueda ser también una ocurrencia de otras entidades que, potencialmente, son subconjuntos no disjuntos (solapados). Es decir, en las entidades subconjunto pueden aparecer ocurrencias repetidas.

Características:

- Toda ocurrencia de un subtipo es una ocurrencia del supertipo, las cardinalidades serán siempre (1,1) en el supertipo y (0,1) o (1,1) en los subtipos.
- Todo atributo del supertipo pasa a ser un atributo de los subtipos.

La entidad subconjunto puede tener atributos, además de tener los atributos de la entidad genérica, pero siempre las entidades subconjunto se encuentran identificadas por la clave de la entidad genérica. Además todos los atributos comunes de las entidades subconjunto deberían aparecer en la entidad genérica para evitar repetir los atributos en cada una de las entidades subconjunto.

18.3.3 Generalización

El concepto de jerarquía de generalización o generalización establece que una entidad genérica X es una generalización de otras entidades especializadas si cada ocurrencia de la primera es una ocurrencia y solamente una de las otras entidades. A veces este concepto se conoce también como jerarquía de especialización.

Se tendrá una jerarquía de generalización cuando la entidad genérica se divida en una serie de entidades en función del valor que tome un determinado atributo de la entidad genérica.

La generalización tiene dos restricciones semánticas asociadas:

- **Totalidad** si todo ejemplar del supertipo tiene que pertenecer a algún subtipo. El caso contrario se llama **Parcialidad**.
- **Solapamiento** si un mismo ejemplar del supertipo puede pertenecer a más de un subtipo. El caso contrario se llama **Exclusividad**.

Pueden existir interrelaciones de cada una de las cuatro combinaciones posibles, y se representarían de la siguiente forma:

TOTAL SIN SOLAPAMIENTO	PARCIAL SIN SOLAPAMIENTO
Tanto un hombre como una mujer son persona.	Tanto un artículo como un libro son documentos.
Una persona no puede ser a la vez hombre y mujer.	Un mismo documento no puede ser a la vez un artículo y un libro.
Toda persona tiene que ser un hombre o una mujer.	Puede haber documentos que no sean ni artículos ni libros.
TOTAL CON SOLAPAMIENTO	PARCIAL CON SOLAPAMIENTO
Tanto un empleado como un estudiante son personas.	Tanto un docente como un investigador son empleados.
Una misma persona puede ser estudiante a la vez que empleado.	Un mismo empleado puede ser docente a la vez que investigador.
Toda persona en nuestra BD tiene que ser un estudiante y/o empleado.	

18.3.4 Tipos de relaciones

A. RELACIONES REFLEXIVAS Son interrelaciones en las que interviene un único tipo de entidad (unarias).

Ejemplo: Un trabajador puede ser jefe de ningún trabajador o puede serlo de varios trabajadores,

mientras que un trabajador sólo es dirigido por ninguno o un trabajador

B. INTERRELACIONES CON RESTRICCIONES DE EXCLUSIVIDAD. Dos interrelaciones que implican a un mismo tipo de entidad participan de una restricción de exclusividad si los ejemplares de esa entidad pueden participar de una u otra interrelación, pero no de ambas.

Se ha recogido en el esquema que en una determinada biblioteca los artículos están publicados en revistas o aparecen en recopilaciones, pero no en ambos

C. INTERRELACIONES CON RESTRICCIONES DE EXCLUSIÓN. Dos interrelaciones entre los mismos dos tipos de entidad son exclusivas si un ejemplar del primer tipo de entidad y otro ejemplar del segundo tipo de entidad sólo pueden estar relacionados por una de las dos interrelaciones, nunca por ambas simultáneamente.

Un profesor no puede recibir e impartir el mismo curso, aunque al contrario que en la restricción anterior puede impartirlo o recibirlo.

D. INTERRELACIONES CON RESTRICCIONES DE INCLUSIVIDAD. Son dos interrelaciones que implican a un mismo tipo de entidad, en las que los ejemplares de la entidad tienen que haber participado de una interrelación con una cardinalidad determinada para poder participar de la otra.

Para que un profesor pueda impartir un curso, tiene que haber recibido el curso un mínimo de 3 veces.

E. INTERRELACIONES CON RESTRICCIONES DE INCLUSIÓN. Son aquellas que se establecen entre los mismos dos tipos de entidad y que restringen una interrelación entre dos ejemplares de cada una de las entidades a la vinculación de esos dos mismos ejemplares a través de la otra interrelación.

Todo ejemplar de profesor que esté unido a un ejemplar de curso mediante la interrelación imparte tiene necesariamente que estar unido al mismo ejemplar de curso mediante la interrelación recibe.

F. AGREGACIÓN. Es un tipo especial de interrelación que permite representar tipos de entidad compuestos que se forman a partir de otros más simples. Existen dos clases de agregaciones

Compuesto/Componente El supertipo de entidad se obtiene por la unión de los subtipos. Se representa de la siguiente forma

Miembro/Colección: El supertipo de entidad es una colección de elementos de un mismo subtipo. Se representa como:

18.3.5 Control de redundancias

En el modelo E/R es necesario evitar las redundancias para no tener problemas de inconsistencias de la representación. Un elemento de un esquema es redundante si puede ser eliminado sin pérdida de semántica.

Existen dos formas principales de redundancia:



- En los atributos (atributos derivados o calculados): Aunque son redundantes, no dan lugar a inconsistencias siempre que en el esquema se indique su condición de derivados y la fórmula mediante la que han de ser calculados.
- En las interrelaciones (también llamadas interrelaciones derivadas): Una interrelación es redundante si su eliminación no implica pérdida de semántica porque existe la posibilidad de realizar la misma asociación de ejemplares por medio de otras interrelaciones. Para ello es condición necesaria pero no suficiente que forme parte de un ciclo.

La existencia de un ciclo no implica la existencia de interrelaciones redundantes.

Para que una interrelación pueda ser eliminada por redundante se tiene que cumplir:

- Que exista un ciclo.
- Que las interrelaciones que componen el ciclo sean equivalentes semánticamente,
- Que después de eliminar la interrelación se puedan seguir asociando los ejemplares de las dos entidades que estaban interrelacionadas
- Que la interrelación no tenga atributos o que éstos puedan ser transferidos a otro elemento del esquema a fin de no perder su semántica.

18.3.6 Dimensión temporal

Es necesario establecer un método semántico y gráfico que recoja de algún modo, en el esquema conceptual, el transcurso del tiempo y su influencia en la forma en que cambian los datos. Existen varias aproximaciones:

- La más simple la constituyen los atributos de tipo fecha asociados a algunas entidades o interrelaciones:



- o Para sucesos instantáneos, es decir, sin duración, bastará con un sólo atributo de este tipo.
 - o Para poder almacenar hechos que transcurren en un intervalo de tiempo determinado necesitaremos una fecha_inicio y una fecha_fin.
 - o En las bases de datos históricas, en las que una interrelación entre dos ejemplares concretos se pueda repetir en el tiempo, el atributo fecha será multivaluado.
- Cuando es necesario representar la evolución de un tipo de entidad a lo largo del tiempo se utiliza un atributo de estado, que indicará en qué estado concreto se encuentra la entidad.

En muchos casos lleva asociado otro atributo, que es la fecha en la que se ha producido el cambio de estado o el intervalo de tiempo en que ha permanecido en dicho estado.

18.4.- MODELO RELACIONAL

Es un modelo lógico de datos, desarrollado por Codd, que introdujo la teoría matemática de las relaciones en el campo de las BD y supuso un importante paso en la investigación de los SGBD. El documento de Codd propone un modelo de datos basado en la “Teoría de las Relaciones”, donde los datos se estructuran lógicamente en forma de relaciones -tablas-, siendo un objetivo fundamental del modelo mantener la independencia de esta estructura lógica respecto al modo de almacenamiento y a otras características de tipo físico (independencia de ordenación, indexación y de los caminos de acceso).

Este nuevo modelo de datos perseguía los siguientes objetivos:



- Independencia lógica: añadir, eliminar o modificar cualquier elemento de la BD no debe repercutir en los programas y/o usuarios que accedan a vistas de los mismos.
- Independencia física: el modo en que se almacenan los datos no debe influir en su manipulación lógica y, por tanto, los usuarios que acceden a esos datos no han de modificar sus programas por cambios en el almacenamiento físico.
- Flexibilidad: poder ofrecer a cada usuario los datos de la forma más adecuada a su aplicación.
- Uniformidad: Las estructuras lógicas de los datos presentan un aspecto uniforme (tablas), lo que facilita la concepción y manipulación de la BD por parte de los usuarios.
- Sencillez: Las características anteriores, así como unos lenguajes de usuario muy sencillos, producen como resultado que el modelo de datos relacional sea fácil de comprender y utilizar por parte del usuario final.

18.4.1 Elementos

El modelo relacional introduce su propia terminología para denominar los objetos y elementos utilizados:

1. **Relación.** Es el elemento central del modelo relacional. Son matrices bidimensionales (tablas) caracterizadas por un nombre, un conjunto de atributos (dimensión vertical de la tabla = columnas) y un conjunto de tuplas (dimensión horizontal = filas).

Cada tupla está formada por el conjunto de valores que toma cada uno de los atributos para un elemento de la relación.

En las relaciones podemos hablar de dos componentes:



- Intensión es la parte definitoria y estática de la relación. Define la estructura abstracta de datos y las restricciones de integridad de la misma. Es lo que llamaremos *esquema de relación*.
- Extensión es el conjunto de tuplas que satisfacen el esquema de relación en un instante dado y se encuentran almacenadas en la base de datos. Varía con el transcurso del tiempo.

Al número de tuplas de una relación en un instante dado se le denomina **cardinalidad** de la relación, y normalmente varía con el transcurso del tiempo. Al número de columnas o atributos se le denomina **grado** de la relación.

2. **Dominio**. Es el conjunto definido, finito y homogéneo de los valores atómicos posibles de un determinado atributo.

Cada atributo está ligado a un determinado dominio y representa el uso de un dominio para una determinada relación.

Los dominios pueden estar definidos por intención (conjunto definido mediante una serie de reglas abstractas) o por extensión (conjunto finito de valores posibles).

3. **Claves de una relación**. Una clave es una(s) columna(s) cuyos valores identifican una única fila de una tabla. Hay varias clases de claves

- *Clave candidata* Cada uno de los conjuntos mínimos de atributos que identifiquen sin ambigüedad y de forma única cada una de las tuplas de una relación.



- *Clave primaria o principal* De entre todas las claves candidatas de una relación, en la definición del esquema se deberá especificar cuál de ellas se considera como identificador primario. Al resto de las claves candidatas se les denominará *claves alternativas*.
- *Claves foráneas o claves ajenas* son el conjunto de atributos de una relación que se corresponden con la clave primaria de otra relación del modelo. Proporcionan al modelo relacional los mecanismos adecuados para representar las (inter)relaciones existentes entre los objetos del problema.
 - o Puede referenciar la clave primaria de la misma tabla (relaciones reflexivas)
 - o Debe tener siempre un valor correspondiente en la tabla donde es clave primaria
 - o Debe estar formada por toda la clave primaria y no solo una parte de ella
 - o Puede tener nulos
 - o Puede tener valores duplicados
 - o Una tabla puede contener múltiples claves foráneas, donde cada una representa la relación con otra tabla

18.4.2 Restricciones

En el modelo relacional existen restricciones, es decir, estructuras u ocurrencias no permitidas, siendo preciso distinguir entre restricciones inherentes (propias del modelo) y restricciones semánticas (de usuario).

Restricciones inherentes

- i.1. No se define ningún orden en los elementos que forman una relación, ni en el sentido horizontal (tuplas) ni en el vertical (atributos). El orden es siempre irrelevante.
- i.2. En toda relación es obligatoria la existencia de la clave primaria, y por tanto no puede haber dos tuplas iguales.
- i.3. Cada atributo de una tupla sólo puede tomar un único valor del dominio sobre el cual está definido.
- i.4. Regla de integridad de clave o entidad: ninguno de los atributos que forman parte de una clave primaria de una relación puede tomar un valor nulo para ninguna tupla de esa relación.

Restricciones semánticas

- 1. Declaración de Clave primaria (PRIMARY KEY): Permite declarar un atributo o un conjunto de atributos como clave primaria de una relación, por lo que sus valores no se podrán repetir ni admitirán nulos.
- 2. Unicidad (UNIQUE): indica que los valores de un atributo (o conjunto) no pueden repetirse en una relación. Esta restricción permite definir claves candidatas.
- 3. Obligatoriedad (NOT NULL) , indica que un atributo (o conjunto) no admite nulos
- 4. Integridad referencial (restricción de clave ajena): permiten que las claves foráneas de una relación referencien una tupla válida de la relación padre. El usuario puede especificar, en la definición del esquema relacional, las operaciones que deben llevarse a cabo cuando se produce el borrado o modificación de una tupla en la relación padre. Las posibilidades son:



- Borrado/modificación en cascada (CASCADE). El borrado o modificación de una tupla en la relación padre, provoca el borrado o modificación de todas las tuplas relacionadas en la relación hija.
- Borrado / modificación restringido (NO ACTION). Si existen tuplas relacionadas en la relación hija, no se permite el borrado o modificación de las tuplas de la relación padre.
- Borrado / modificación con puesta a nulos (SET NULL). Pone a nulo los valores de todos los atributos que conforman la clave ajena en la relación hija. Sólo está permitido cuando esos valores se puedan poner a nulo.
- Borrado / modificación con puesta a un valor por defecto (SET DEFAULT). Similar al anterior, pero los atributos que conforman la clave ajena en la relación hija se ponen a un valor especificado previamente en la definición del esquema.

5. Restricciones de rechazo. En la definición del esquema relacional pueden imponerse otra serie de restricciones que garanticen la integridad del modelo, y por tanto, de la información almacenada en la base de datos. Estas restricciones deben ser verificadas en toda operación de actualización para que el nuevo estado constituya una ocurrencia válida del esquema; en caso de que la operación intente violar la condición se impide que la operación se lleve a cabo, como son:

- Restricciones de verificación (CHECK). Especifican condiciones que deben cumplir los valores de determinados atributos de una relación, como pueden ser los atributos de existencia obligatoria (NOT NULL).
- Aserciones (ASSERTION). Permiten especificar condiciones entre los elementos de distintas relaciones del esquema.

- Disparadores (TRIGGER). Permiten especificar condiciones y acciones que se lleven a cabo cuando se efectúe una acción determinada sobre alguna relación del esquema

18.5.- NORMALIZACIÓN DE RELACIONES.

Al estudiar la estructura del modelo relacional, se deduce que la información de nuestra base de datos puede representarse por medio de un conjunto de objetos (relaciones y dominios) y de un conjunto de reglas de integridad.

En el modelo relacional, como en los demás modelos de datos, el diseño de una base de datos se puede abordar de dos formas distintas:

- Obteniendo el esquema relacional directamente a partir de la observación de nuestro universo del discurso, de forma que plasmemos nuestra percepción del mismo en un conjunto de esquemas de relación, los cuales contendrán los atributos y las restricciones de integridad que representan los objetos y reglas que hemos podido captar en nuestro análisis del mundo real.
- Realizando el proceso de diseño en dos fases, en la primera se lleva a cabo el diseño conceptual, por ejemplo en el modelo E/R, obteniéndose el correspondiente esquema conceptual; en la segunda, éste se transforma en un esquema relacional siguiendo unas determinadas reglas de transformación.

Estas relaciones que resultan de la observación del mundo real o de la transformación al modelo relacional del esquema E/R elaborado en la etapa de modelado conceptual, pueden presentar algunos problemas, derivados de fallos en la percepción del universo del discurso, en el diseño del esquema E/R, o en el paso al modelo relacional;

Entre estos problemas cabe destacar los siguientes:

- Incapacidad para almacenar ciertos hechos.
- Redundancias y, por tanto, posibilidad de inconsistencias,
- Ambigüedades.
- Pérdida de información (aparición de tuplas repetidas).
- Pérdida de dependencias funcionales, es decir, de ciertas restricciones de integridad que dan lugar a interdependencias entre los datos.
- Existencia de valores nulos.
- Aparición, en la base de datos, de estados que no son válidos en el mundo real (anomalías de inserción, borrado y modificación).

En definitiva, el esquema relacional debe ser siempre analizado para comprobar que no presenta los problemas anteriormente citados, evitando la pérdida de información y la aparición de estados que no son válidos en el mundo real.

Para evitar que se puedan dar estos problemas, existen una serie de reglas o formas normales. Estas formas normales serán aplicadas normalmente a bases de datos ya implantadas en forma de relaciones (tablas), lo que nos permitirá pasar a otras relaciones (tablas) que no den los problemas anteriormente descritos.

Existen seis formas normales. Las tres primeras en la mayor parte de los casos son suficientes para normalizar los esquemas de relación.

1. Primera Forma Normal (1FN).

Se dice que una relación está en 1FN cuando cada atributo sólo toma un valor del dominio simple subyacente. Es decir, cada atributo tiene asociado un dominio del cual sólo toma un valor en cada tupla.

Es una restricción inherente al modelo relacional, por lo que su cumplimiento es obligatorio y afecta al número de valores que pueden tomar los atributos de una relación.

2. Segunda Forma Normal (2FN).

Se dice que una relación está en 2FN si:

- Está en 1FN.
- Cada atributo no principal de la relación tiene dependencia funcional completa respecto de la clave primaria de esa relación, esto es, el valor de los atributos no principales de la relación viene determinado por el valor de todos los atributos de la clave.

Por ejemplo, la relación:

Matrícula (dni, asignatura, nombre, apellidos, curso, nota, aula, lugar)

No está en 2FN, puesto que nombre y apellidos dependen únicamente de dni y no del valor de asignatura. Igualmente, curso depende únicamente de asignatura, y no del valor de dni.

Para pasar a 2FN se descompone la relación en otras tres, de la forma:

Matrícula2 (dni, asignatura, nota, aula, lugar)

Alumno (dni, nombre, apellidos)

Materia (asignatura, curso)

3. Tercera Forma Normal (3FN).

Una relación R satisface la tercera forma normal (3FN), si y sólo si está en 2FN, y, cada atributo no principal (atributo que no forma parte de la clave) de la relación no depende funcionalmente de otros atributos no principales

de esa relación. Es decir, no pueden existir dependencias entre los atributos que no forman parte de la clave primaria de la relación R.

Si se considera, como es lógico, que cada aula se encuentra ubicada físicamente en un único lugar, se puede observar que la relación Matricula2, la cual se encuentra en 2FN, sigue presentando problemas debidos a que existe una dependencia entre los atributos aula y lugar (no se encuentra, por tanto, en 3FN),

Para eliminar los problemas que ocasiona en la relación Matricula2 la existencia de esta dependencia funcional, esta relación debe descomponerse en dos relaciones, quedando el esquema de la forma:

Matrícula3 (dni, asignatura, nota, aula)

Ubicación (aula, lugar)

Alumno (dni, nombre, apellidos)

Materia (asignatura, curso)

4. Forma Normal de Boyce-Codd (FNBC).

Es una redefinición más estricta de la 3FN, ya que ésta presentaba ciertos problemas en relaciones con varias claves candidatas compuestas que se solapaban. Por ello en 1974, Boyce y Codd definieron la llamada forma normal que lleva su nombre (FNBC). Se basa en el concepto de determinante funcional.

Se llama determinante funcional a un atributo o a un conjunto de atributos de una relación R del cual depende funcionalmente de forma completa algún otro atributo de la misma relación.

Una relación R satisface la forma normal de Boyce-Codd (FNBC) si, y sólo si se encuentra en 1 FN, y cada determinante funcional es una clave candidata de la relación R, esto es, ningún atributo facilita información de otro atributo que no es clave candidata.

Por exemplo, en el esquema:

Matrícula4 (dni, asignatura, apellidos, nombre, nota, aula)

Ubicación (aula, lugar)

Materia (asignatura, curso)

(donde *asignatura*, *apellidos*, *nombre* es una clave candidata y *dni*, *asignatura* es otra clave candidata de la relación Matrícula4).

En este caso, el esquema está en 3FN pero no está en FNBC, puesto que *dni* es un determinante funcional (*apellidos* y *nombre* dependen de *dni*) y no es clave candidata de la relación. Para poner el esquema en FNBC hay que descomponer Matrícula4 en 2 relaciones, de tal forma que queda un esquema similar al obtenido en el apartado anterior:

Matrícula3 (dni, asignatura, nota, aula)

Alumno (dni, nombre, apellidos)

Ubicación (aula, lugar)

Materia (asignatura, curso)

5. Cuarta Forma Normal (4FN)

Está basada en la eliminación de las dependencias multivaluadas. Se dice que en una relación existe una dependencia multivaluada ($\alpha \twoheadrightarrow \beta$), si los valores de un conjunto de atributos β depende únicamente del valor que tome otro conjunto de atributos α , de forma independiente al resto de atributos de la relación.

Por ejemplo, si tenemos una relación para un concesionario con todos los modelos de coches que se vende, con su color y equipamiento respectivo:

Concesionario (modelo, color, equipamiento)

y sabemos que puede vender dos modelos, *utilitario* y *berlina*. Si el modelo utilitario se puede vender en color azul o verde con dos tipos de equipamiento (base o normal) y el modelo berlina se puede vender en color plata o azul con equipamientos normal o lujo.

En este caso, si sabemos que el modelo es utilitario, sabemos los posibles valores para el color y el equipamiento, y por tanto existen dos dependencias multivaluadas: modelo $\rightarrow \rightarrow$ color y modelo $\rightarrow \rightarrow$ equipamiento, y la relación se encuentra en 4 FN pero no en FNBC

Para poner el esquema en 4FN se debe descomponer la relación en otras dos de la forma:

Concesionario1 (modelo, color)

Concesionario 2 (modelo, equipamiento)

6. Quinta Forma Normal (5FN).

Está basada en la eliminación de las dependencias de reunión. Se dice que existe una dependencia de reunión si la relación puede ser construida en base a la reunión natural de las proyecciones de esa relación sobre los atributos que la forman.

Una relación está en 5FN si y sólo si toda dependencia de reunión en esa relación está implicada por las claves candidatas entre sí, y no por cualquier otro atributo de esa relación.

Por ejemplo, en la relación: **Docencia (dni, asignatura, aula)**

que define las aulas que se asignan a cada asignatura y los alumnos matriculados en la misma (cada alumno matriculado en una asignatura recibe clase en todas las aulas asignadas a la misma), existe dependencia de reunión entre los atributos dni, asignatura y aula.

Para eliminar las dependencias de reunión y ponerlo en 5FN, se descompone la relación en otras tres:

Docencia1 (dni, asignatura)

Docencia2 (asignatura, aula)

Docencia3 (dni, aula)



18.6.- TRADUCCIÓN DE ESQUEMAS E/R A ESQUEMAS RELACIONALES.

1. Aplicar la 1 FN a los objetos que forman parte del esquema, esto es:
 - Eliminar los atributos multivaluados. Se transforman en entidades débiles dependientes en existencia de la entidad de la cual formaban parte, con relación uno a muchos si el atributo es un identificador alternativo o muchos a muchos en caso contrario.
2. Los tipos de entidad se transforman a relaciones en el esquema relacional.
3. Los tipos de interrelación binarias uno a uno se transforman en general en dos tablas mediante propagación de la clave, esto es, se añade a una de las tablas como clave foránea el identificador principal de la otra tabla con la que está relacionado.

Dependiendo de las cardinalidades mínimas de cada tipo de entidad, tenemos:

- *Cardinalidad mínima uno en ambos casos:* propagación de la clave hacia cualquiera de los dos lados.
- *Cardinalidad mínima uno en ambos casos y dependencia en identificación, con el mismo identificador principal en ambos tipos de relaciones:* se transforman ambos tipos de entidad en una única tabla.
- *Sólo uno de los dos tipos de entidades tiene cardinalidad mínima cero:* se convierte cada tipo de entidad en una tabla y se propaga la clave hacia el lado de cardinalidad mínima cero.
- *Cardinalidad mínima cero en ambos casos:* se puede hacer una tabla nueva (tres tablas), para evitar la existencia de demasiados valores nulos en las tablas.

4. Los tipos de interrelación binarias uno a muchos se transforman en general en dos tablas mediante propagación de la clave hacia el lado muchos. Existe un caso especial:
 - Cardinalidad mínima cero en la entidad del lado uno (0,1): para evitar la presencia de demasiados valores nulos, se generan tres tablas, una por cada tipo de entidad y otra con los identificadores de ambas entidades y los atributos (si los hay) de la interrelación. La clave principal será el identificador principal del tipo de entidad con cardinalidad máxima n. El identificador principal del otro tipo de entidad será clave foránea en esta tabla.
5. Los tipos de interrelación binarias muchos a muchos se transforman siempre en tres tablas mediante propagación de la clave hacia el lado muchos; una por cada tipo de entidad y otra con los identificadores de ambas entidades y los atributos (si los hay) de la interrelación. La clave principal de esta tabla estará compuesta por los identificadores principales de ambos tipos de entidades.
6. Los tipos de interrelación en los que intervienen más de dos tipos de entidad, se transforman de la misma forma que los tipos de interrelación binarias muchos a muchos.
7. Los tipos de interrelación reflexivas se transforman:
 - En interrelaciones reflexivas del tipo N:M, se transforman de la misma forma que los tipos de interrelación binarias muchos a muchos, es decir, se genera una tabla para el tipo de entidad y otra para el tipo de interrelación.
 - En interrelaciones reflexivas del tipo 1 :N, se puede proceder de dos formas: se genera una única tabla para el tipo de entidad añadiendo como clave foránea el identificador principal de la misma; o se crean dos tablas, una para el tipo de entidad y otra

para el tipo de interrelación con el identificador principal de la entidad duplicado (en un caso es la clave principal y en otro la clave foránea de la otra tabla).

8. Los atributos de las interrelaciones, cuando hay propagación de la clave, también se propagan.
9. Las relaciones jerárquicas de generalización - especialización se pueden transformar de tres formas:
 - Transformando el tipo de entidad padre en una relación y colgando de ella los atributos comunes y no comunes de todos los tipos de entidad hijo.
 - Crear una relación para el tipo de entidad padre, con los atributos comunes, y otra relación para cada uno de los tipos de entidad hijo.
 - Crear una relación para cada uno de los tipos de entidad hijo y poniendo en cada una de ellas todos los atributos comunes del tipo de entidad padre. Sólo sirve en caso de jerarquía total.
10. Las dependencias en identificación y en existencia, para evitar la existencia de valores nulos en la clave foránea de la relación proveniente del tipo de entidad débil, al transformarse deben obligar al borrado y actualización en cascada (CASCADE).

18.7.- BIBLIOGRAFÍA

- The Entity/Relationship Model: Toward a unified view of data. CACM, 1,1. 1976
- The Entity/Relationship Model: A basis for the enterprise view of data. AFIPS Conference Proceedings, Vol 46. 1977

- Introducción a los sistemas de bases de datos. C.J. Date. Pearson Educación, 2001.
- Fundamentos de Sistemas de Bases de Datos. Ramez A. Elmasri & Shamkant B. Navathe. Addison-Wesley, 2002 [3ª edición].

Autor: Francisco Javier Rodríguez Martínez

Subdirector de Sistemas Escola Superior Enxeñaría Informática Ourense

Colegiado del CPEIG



19. SISTEMAS DE GESTIÓN DE BASES DE DATOS. BASES DE DATOS XML NATIVAS. MONITORES TRANSACCIONALES.

Tema 19: Sistemas de gestión de bases de datos. Bases de datos XML nativas. Monitores transaccionales.

ÍNDICE

19.1 Sistemas de Gestión de Bases de Datos (SGBD).....	3
19.1.1 <i>Introducción.....</i>	3
19.1.2 <i>SGBD objetivo y características.....</i>	4
19.1.3 <i>Evolución.....</i>	7
19.1.3.1 <i>Arquitectura en 2 capas.....</i>	7
19.1.3.2 <i>Arquitectura en 3 capas.....</i>	8
19.1.4 <i>Modelo de referencia ANSI.....</i>	9
19.1.4.1 <i>Objetivos y beneficio.....</i>	10
19.1.4.2 <i>Niveles de descripción de Datos.....</i>	11
19.1.4.3 <i>Entorno.....</i>	13
19.1.4.4 <i>Componentes de un SGBD.....</i>	13
19.1.4.5 <i>Modelos de Datos.....</i>	14
19.1.5 <i>Estructura General de un SGBD.....</i>	16
19.1.6 <i>SGBD Relacionales (SGBD-R).....</i>	18
19.1.6.1 <i>Características de los SGBD-R.....</i>	18
19.1.6.1.1 <i>Estructuras de datos: Relaciones y Claves.....</i>	18
19.1.6.1.2 <i>Operadores asociados.....</i>	19
19.1.6.1.3 <i>Aspectos Semánticos.....</i>	20
19.2 Bases de Datos XML Nativas.....	22
19.2.1 <i>Bases de datos XML.....</i>	22



19.2.1.1 Bases de datos habilitadas para XML.....	22
19.2.2 Bases de datos XML nativas.....	23
19.3 Monitores transaccionales.....	24
19.3.1 Ventajas de los monitores transaccionales.....	24
19.3.2 Arquitecturas.....	25
19.3.2.1 Modelo de un Proceso por Cliente.....	25
19.3.2.2 Modelo de Proceso Único.....	25
19.3.2.3 Modelo de muchos Servidores, un Router.....	25
19.3.2.4 Modelo de muchos Servidores, muchos Routers.....	26
19.4 Bibliografía.....	26

19.1 SISTEMAS DE GESTIÓN DE BASES DE DATOS (SGBD)

19.1.1 Introducción

Para que una base de datos funcione correctamente precisa de un software que gestione todas sus operaciones y que además proporcione una interfaz de comunicación para los usuarios facilitando el acceso a los datos contenidos en ella. Este tipo de software son los denominados *Sistemas de Gestión de Bases de Datos* o *S.G.B.D.*

Según una definición formal, un Sistema de Gestión de Bases de Datos, *“es un conjunto coordinado de programas, procedimientos, lenguajes, etc... que suministra, tanto a los usuarios no informáticos, como a los analistas programadores, o al administrador, los medios necesarios para describir y manipular los datos integrados en la base, manteniendo su integridad, confidencialidad y seguridad”*.

Este grupo definido de software encargado de ofrecer soporte a las bases de datos aporta una serie de facilidades para el manejo de las bases de datos. Estas facilidades se traducen en una serie de Lenguajes que permiten operar contra las distintas bases de datos que soporta el SGBD, siendo los principales:

- **Lenguaje de Definición de Datos o DDL** (Data Definition Language): permite definir los esquemas conceptuales de una base de datos.
- **Lenguaje de Manipulación de Datos o DML** (Data Manipulation Language): suministra operaciones para la realización de consultas y actualizaciones de la información contenida en las bases de datos.
- **Lenguaje de Control de Datos o DCL** (Data Control Language): permite administrar y controlar el acceso a los datos existentes en una base de datos.

Desde los años 70, el grupo ANSI/X3/SPARC es el encargado de ocuparse de la normalización de los SGBD, publicando en 1975 un informe

provisional en donde propone una arquitectura de 3 capas para los SGBD que posteriormente se revisaría y detallaría en 1977. Sin embargo, hasta 1985 no se presentó el *Modelo de Referencia* para la estandarización de los SGBD (Modelo ANSI).

19.1.2 SGBD objetivo y características

Para un sistema gestor de bases de datos su objetivo principal es el de ofrecer un entorno idóneo para la extracción, manipulación almacenamiento de la información de las bases de datos. Los SGBD realizan una gestión centralizada de todas las peticiones de acceso funcionando de interfaz entre los usuarios y la base de datos. También es el gestor de la estructura física de los datos y de su almacenamiento, por lo que en definitiva, libera a los usuarios de conocer la organización física exacta de los datos, así como de crear los algoritmos de almacenamiento, actualización o consulta de la información contenida en la base de datos.

No todos los SGBD son iguales ni tienen las mismas funcionalidades, puesto que dependen de cada producto y del modelo de base de datos que gestionen. Independientemente de esto, existen una serie de características que se podrían identificar como comunes a todos ellos, las cuales fueron definidas por Codd y revisadas con posterioridad, a medida que las nuevas necesidades se fueron integrando. Las características necesarias para que un SGBD pueda cubrir las necesidades de un usuario son:

- Con el fin de simplificar el mantenimiento de las aplicaciones que hacen uso de las bases de datos, un SGBD ha de mantener la independencia entre las soluciones software y la estructura de la base de datos. Esta independencia no es completa pero cada vez se aproximan más a esta exigencia.
- En la medida de lo posible, no debe existir redundancia de datos, es decir, estos no deben de estar almacenados varias veces. Con esto se consigue asegurar la coherencia de los datos.
- Un SGBD ofrece las herramientas necesarias a un usuario para:
 - o Almacenar datos.

- o Acceder a la información.
- o Actualizar los datos.

Estas herramientas han de proporcionar estos servicios de tal manera que resulte transparente al usuario.

- Permite el acceso de múltiples usuarios a la misma base de datos y en el mismo momento. Cuando esto se produce, si alguno de los usuarios está realizando operaciones de actualización de los datos, el SGBD ha de asegurarse de realizar una correcta gestión de la concurrencia evitando la corrupción de los datos o que estos se vuelvan inconsistentes. Para realizar esta gestión el SGBD hace un correcto uso de los bloqueos de las bases de datos.
- Ofrece a los usuarios un catálogo al cual pueden acceder donde se almacenan de una manera centralizada, las descripciones de los datos. Este servicio es el que permite la eliminación y detección de las redundancias de datos y se denomina *diccionario de datos*.
- Realiza las transacciones garantizando que las actualizaciones correspondientes a una transacción se realizaran, o en caso de que no sean posible realizar alguna, ninguna tendrá efecto. Esto se debe a que durante una transacción, se producen acciones que cambian el contenido de la base de dato. Si por algún motivo la transacción falla, entonces al base de datos pasa a un estado de inconsistencia, puesto que no todos los cambios de la transacción se produjeron, obligando al SGBD a deshacer los cambios para que la base de datos vuelva a un estado consistente.
- Garantiza la recuperación de las bases de datos. Si ocurre algún problema que provoque que la información se vea afectada, un fallo de hardware o software que hagan abortar al SGBD, o que un usuario interrumpa una operación antes de que se finalice la transacción, el SGBD debe proporcionar los mecanismos necesarios para solventar este tipo de situaciones y recuperar la base de datos a un estado consistente.

- Proporciona seguridad a las bases de datos, es decir, restringe mediante diferentes niveles, que el acceso a las bases de datos sólo lo realizaran usuarios autorizados, protegiendo las bases de accesos no autorizados, ya sean accidentales o no.
- Un SGBD garantiza la integridad de las bases de datos. Aporta un conjunto de reglas que la base de datos no puede violar consiguiendo así la validez y consistencia de los datos.
- Proporciona herramientas para la administración de las bases de datos. Este conjunto de herramientas permiten una serie de funcionalidades:
 - o Importación y extracción de datos
 - o Monitorización del funcionamiento y obtención de datos estadísticos sobre el uso de las bases de datos.
 - o Reorganización de índices
 - o Optimización del espacio liberado para su reutilización.
- Mantiene una disponibilidad continua, garantizando que en todo momento las bases de datos están accesibles. Proporciona que las tareas de administración, gestión y mantenimiento se puedan llevar a cabo sin interrumpir el correcto funcionamiento de las bases de datos.
- Todo SGBD se integra con un gestor de comunicaciones, software encargado de gestionar el acceso de los usuarios que realicen la conexión con la máquina que sirve de soporte al SGBD de una manera remota a través de una red de datos. El gestor de comunicaciones no forma parte de un SGBD pero si es preciso que el SGBD se integre con él.
- Posee un DDL, Lenguaje de Definición de Datos para la creación y modificación de las bases de datos.

- Posee un DML, Lenguaje de Manipulación de Datos para la inserción, manipulación y consulta de la información contenida en las bases de datos.
- Posee un DCL, Lenguaje de Control de Datos para controlar el acceso a la información de las bases de datos.
- Garantiza la escalabilidad y elevada capacidad de proceso, es decir, es capaz de aprovechar los recursos de la máquina disponibles, aumentando su capacidad de procesamiento a medida que disponga de recurso.
- Es capaz de almacenar enormes cantidades de datos sin que el usuario perciba una degradación en el rendimiento del sistema.

19.1.3 Evolución

En los primeros inicios de la informática los datos formaban parte de los programas, integrados como constantes. Posteriormente, con la aparición de los ficheros como colección de datos homogénea, se empieza a diferenciar la estructura lógica que representa el punto de vista del usuario y la estructura física de los datos.

Esta diferenciación se hace más evidente con la aparición en los sistemas operativos de subsistemas de gestión de datos, pero no resulta suficiente para romper la dependencia entre los datos y los programas y viceversa, y de ambos con respecto a la máquina.

Para limar estas dependencias existentes entre los datos y las aplicaciones, se comienzan a utilizar arquitecturas que diferencian la estructura lógica de los datos, representación de los datos orientados hacia el problema, de la estructura física, representación orientada hacia la máquina. Esta diferenciación funciona a través de una transformación o mapping que hace las tareas de conversión entre una estructura y otra.

19.1.3.1 Arquitectura en 2 capas

Con la aparición de los primeros SGBD en los años 60, los sistemas pasan de una orientación centrada en el proceso a una orientación enfocada hacia las bases de datos.

Esto produce que los datos y las relaciones entre los mismos se ubiquen en la bases de datos, consiguiendo aislarlos de las aplicaciones. Esta evolución provoca un cambio en las tendencias de las estructuras de datos haciendo que la estructura lógica sea más flexible y sencilla, mientras que la estructura física se vuelva más compleja con el fin de mejorar el rendimiento.

Los primeros SGBD facilitan en gran medida la descripción y el almacenamiento de las relaciones permitidas caracterizando al mismo tiempo los distintos modelos de datos: jerárquico, red, relacional.

La arquitectura seguida por estos SGBD estaba definida en dos niveles:

- *Estructura Global*, con la características lógicas y físicas: Esquema
- *Vistas Lógicas Externas* de los usuarios: Subesquemas

19.1.3.2 Arquitectura en 3 capas

La organización ANSI (American National Standards Institute) publica en el año 1975 un informe que resultaría clave para el desarrollo de los SGBD. En este informe se indica la necesidad de evolucionar los SGBD con el fin de conseguir una total independencia entre los datos y las aplicaciones. Para tal propósito propone un modelo arquitectónico en 3 capas y define a su vez el modelo conceptual para conseguirlo.

En este informe la estructura global del modelo de 2 niveles se divide dando lugar a dos estructuras, en una se quedan los aspectos lógicos y el esquema conceptual, mientras que en la otra se queda con los aspectos físico o esquema interno.

Mediante esta definición, los SGBD que siguen esta normativa muestran internamente los tres niveles perfectamente diferenciados:

- **Nivel Interno o Físico:** representa el nivel más bajo de abstracción y en este nivel es donde se describe en detalle la estructura física de la base de datos, dispositivos de almacenamiento físico, estrategias de acceso, índices, etc. Para ello interactúa con el sistema operativo y con el gestor de ficheros. En definitiva el esquema interno especifica que datos son

almacenados y cómo, además de describir la estructura de la base de datos en forma de modelo conceptual de almacenamiento.

- **Nivel Conceptual:** se corresponde con el nivel intermedio de abstracción y describe los datos que son almacenados en la base de datos y las relaciones existentes entre ellos. También describe la base de datos según su estructura de diseño. En este nivel la base de datos resulta una colección de registros lógicos sin descriptores de almacenamiento. Mediante este nivel se consigue el aislamiento de la representación de la información de los requerimientos de la máquina y de las exigencias de los usuarios.
- **Nivel Externo o Lógico:** supone el de mayor grado de abstracción y contiene las vistas externas de la base de datos asociadas a un esquema externo. Proporciona a cada tipo de usuario únicamente la parte del esquema que resulta relevante para él y para la cual tiene acceso. Cada base de datos puede tener tantas vistas como necesite.

Con esta arquitectura se pretende conseguir que el esquema conceptual sea una descripción estable e independiente del nivel superior y del inferior, es decir, independiente tanto de las vistas como del almacenamiento de los datos. Con la consecución de esta independencia las bases de datos se convierten en sistema más flexibles y adaptables.

19.1.4 Modelo de referencia ANSI

En el año 1985 se publica un estudio en el cual se presenta un modelo para la estandarización de los SGBD. Este estudio, *“Modelo de Referencia para la estandarización de los Sistemas Gestores de Bases de Datos”*, fue presentado por el Database Architecture Framework Task Group, miembro del ANSI/X3/SPARC Database System Study Group.

Este Modelo de Referencia no supone un estándar sino que supone simplemente un marco conceptual para la simplificación del trabajo de estandarización de los distintos elementos y sus relaciones dentro de un SGBD.

Parte de la arquitectura de tres niveles propuesta por ANSI sobre la cual se realizan una serie de revisiones y simplificaciones, además de describir las interacciones de un SGBD.

Los datos dentro del Modelo de Referencia pasan por los tres niveles descritos por la arquitectura, pero estos niveles ahora se encuentran separados y aislados por un conjunto de interfaces que les proporciona completa independencia entre sí.

19.1.4.1 **Objetivos y beneficio**

El Modelo de Referencia se desarrolla con los siguientes propósitos:

- Crear una herramienta que guíe el desarrollo y coordinación para el proceso de estandarización en el área de los SGBD.
- Aportar las descripciones de las distintas interacciones de un SGBD con el resto de componentes de los sistemas de información.
- Proporcionar un marco común de descripción de los SGBD con el fin de facilitar los procesos de formación.
- Clasificar los distintos productos según sus características y funcionalidades.
- Ofrecer un punto de ayuda a los usuarios en los procesos de análisis, cambio e implantación de SGBD.

Siguiendo estos propósitos generales, el Modelo de Referencia pretende garantizar o aportar los siguientes beneficios una vez estandarizados los SGBD:

- La portabilidad de las aplicaciones
- Mejoras en la productividad y procesos de aprendizaje.
- Simplificación los procesos de evaluación y selección de los SGBD.
- Ofrecer la posibilidad de intercambiar datos entre distintos SGBD.

19.1.4.2 Niveles de descripción de Datos

Los datos dentro del Modelo de Referencia pasan por los tres niveles descritos por la arquitectura, pero estos niveles ahora se encuentran separados y aislados por un conjunto de interfaces que les proporciona completa independencia entre sí.

Debido a la existencia de los tres niveles independientes, esquema conceptual, externo e interno, se generan dentro del modelo de referencia 3 tipos de funciones de administración:

1. *Administración de Empresa:* encargado del diseño del esquema conceptual.
2. *Administración de la Base de Datos:* especifica el esquema interno de tal manera que se adapta lo mejor posible al esquema conceptual ya almacenado en forma de metadatos.
3. *Administración de Aplicaciones:* construye los esquemas externos partiendo del esquema conceptual y gestiona los distintos programas de aplicación que utilizan las bases de datos.

Dentro de esta estructura lógica de tres tipos de esquemas se diferencian dos fases o secciones:

- **Definición:** es realizada por funciones de programa y sus correspondientes interfaces, los cuales producen los metadatos que se almacenan en el diccionario de datos que es el núcleo de la arquitectura.

La base de datos comienza con la creación del esquema conceptual por parte del administrador de la empresa. Este rol fue llamado así por ANSI y refleja lo que hoy se conoce como diseñador de la base de datos. Ese esquema es procesado mediante el procesador del esquema conceptual, convirtiéndolo en metadatos.

A través de la interfaz se posibilita a los otros dos administradores, administrador de la base de datos y el de aplicaciones, el acceso al esquema conceptual con el cual construyen sus respectivos esquemas, internos y externos mediante sus interfaces y sus procesadores que

almacenan la información correspondiente a estos esquemas en los metadatos.

Las etapas más significativas de la fase de Definición son:

- o Especificación del esquema conceptual mediante el lenguaje de definición.
 - o Compilación del esquema conceptual por parte del procesador de del esquema conceptual.
 - o Almacenamiento del esquema conceptual en el diccionario de datos.
 - o Procesado del esquema conceptual para la creación de los esquemas internos y externos por parte de sus respectivos procesadores.
 - o Control y almacenado de los esquemas internos y externos en la base de datos por parte de sus procesadores.
- **Manipulación:** es realizada por acciones del usuario. Una vez definida la base de datos el usuario puede realizar funciones de manipulación de los datos (inserción, borrado, modificación) mediante el lenguaje de manipulación de datos.

El proceso de manipulación por parte de un usuario consta de los siguientes puntos o pasos dentro de un SGBD.

- o Para la realización de operaciones sobre la base de datos un usuario hace uso de su interfaz, generalmente una aplicación, para enviar una petición.
- o Esta petición es transformada por el transformador externo/conceptual el cual hace uso de los metadatos para obtener el esquema correspondiente.
- o El resultado se envía al transformador interno que genera el esquema interno haciendo uso también de los metadatos.

- o Des esquema interno se traslada al transformador interno de almacenamiento mediante el cual se accede a los datos utilizando para ello los metadatos.
- o Una vez obtenidos los datos, estos sufren el proceso inverso para presentarlos al usuario en un formato adecuado.

19.1.4.3 **Entorno**

Un SGBD no resulta un sistema aislado, es decir, se encuentra situado dentro de un entorno. Por eso en la descripción de un SGBD se requiere de la especificación de sus interfaces y de los componentes o subsistemas que interaccionan con él. En un entorno de un SGBD se puede encontrar los siguientes elementos:

- Programas de aplicación y procesadores de lenguaje de aplicación.
- Sistemas de diccionario de datos.
- Sistemas operativos.
- Sistemas de gestión de ficheros.
- Sistemas distribuidos y protocolos.
- Herramientas de gestión.

19.1.4.4 **Componentes de un SGBD**

En el Modelo de Referencia de ANSI uno de los enfoques para estudiar los Sistemas Gestores de Base de Datos es el de los componentes. Éste enfoque consiste en separar el SGBD en distintas partes y, al poseer diversas interfaces de comunicación, posibilitar el ensamblado de un SGBD con partes procedentes de distintos suministradores, con el fin de conseguir la compatibilidad entre los módulos y una compatibilidad en el mercado. En este punto el Modelo de Referencia revisa la compleja arquitectura ANSI/SPARC, que posee un elevado número de interfaces, simplificándola y realizando el proceso de análisis para la recogida de los requisitos sin llegar nunca a la implementación.

El objetivo del Modelo de Referencia ANSI/X3 es describir las interrelaciones del SGBD, pero no indicar nada acerca de su instrumentación.

El Modelo de Referencia define los componentes que ha de tener todo SGBD. Los componentes propuestos son:

- **Sistema de Control de Transformación de Datos (SCTD).** Es el núcleo del SGBD y proporciona una serie de operadores para la descripción y manipulación de los datos. Está basado en un modelo de Datos con la capacidad de soportar a su vez la descripción y manipulación de otros modelos de datos.
- **Interfaz de lenguaje de datos (LD)** que posibilita a los usuarios y a los procesadores especificar sus peticiones para la recuperación de los datos.
- **Interfaz de lenguaje de datos interno (LD-i)** que permite el uso de los servicios de los procesadores que soportan el funcionamiento de los SGBD, en especial los del SO.

Adicionalmente, en el entorno del SGBD destacan las herramientas de gestión de datos (HGD), que son componentes de soporte lógico, como los lenguajes de cuarta generación (L4G), soporte para ayuda a la decisión, facilidades para realizar el ajuste (tuning), utilidades para el volcado de ficheros, sistemas de diccionario de datos, etc.

19.1.4.5 **Modelos de Datos**

Un Modelo de Datos resulta una abstracción del Universo del Discurso, es decir un *“Conjunto de conceptos, reglas y convenciones que permiten describir los datos de una parcela del mundo real (Universo del Discurso)”*.

El Modelo de Datos se considera también una herramienta intelectual que sirve de apoyo a la hora de diseñar una base de datos, ya que en un proceso de diseño de una base de datos lo que se pretende es crear una modelización de un problema presente en el mundo real.

El Modelo de Datos ha de recoger las propiedades existentes dentro del Universo del Discurso y se pueden dividir en dos tipos:

- *Estáticas:* Invariantes en el tiempo y conforman la Componente Estática del Modelo de Datos que es el conjunto de reglas que permiten la generación de la estructura las cuales se definen mediante el lenguaje de definición de datos.
 - o Conjunto de objetos, entidades y sus atributos.
 - o Conjunto de asociaciones entre objetos, interrelaciones.
 - o Conjunto de restricciones, inherentes u opcionales.
- *Dinámicas:* Varían con el tiempo y se corresponden con la Componente Dinámica del Modelo de Datos. Supone el conjunto de operadores aplicables sobre la estructura y se definen mediante el lenguaje de manipulación de datos.

Entre los Modelos de Datos convencionales instrumentados en los SGBD se establecen tres grupos ordenados cronológicamente:

- **Modelo Jerárquico.** Responde a una estructura arborescente a varios niveles. Cada nivel de la jerarquía está compuesto de uno o varios grupos de datos (nodos), de cada uno de los cuales pueden depender otros nodos que dando unidos por ramas. Los nodos y las ramas determinan una relación del tipo 1:n. La forma de recuperar los datos es recorriendo los distintos niveles según el camino definido por la sucesión de nodos en el árbol. Este modelo asume que ciertos datos son más importantes que otros.
- **Modelo en Red.** Es bastante más flexible que el jerárquico, pues permite establecer múltiples conexiones, combinando varias jerarquías arborescentes. Se obtienen relaciones n:m. Estas relaciones permiten al usuario acceder a un dato sin tener que recorrer todas las jerarquías.
- **Modelo Relacional.** Propuesto teóricamente por Codd en 1970. Es reconocida su superioridad frente a los anteriores. Basado en el álgebra y cálculo relacional, hace posible el proceso de conjuntos de datos y no simples registros como en el caso de sus antecesores. Básicamente se caracteriza, en cuanto a su

estructura, por disponer de los datos organizados en tablas (relaciones) de filas similares (tuplas) cada una con un conjunto de campos (atributos) en columnas. No existen vinculaciones entre tablas visibles para el usuario, y además se cumplen ciertas restricciones.

En todos ellos los objetos que permiten son:

- Entidades
- Atributos
- Dominios
- Interrelaciones

Sin embargo los tres tipos de modelos se diferencian básicamente en el modo de representación de las relaciones entre entidades y en la manera de acceder a la base de datos.

19.1.5 Estructura General de un SGBD

Los principales módulos del SGBD son:

- **El compilador del DDL.** Chequea la sintaxis de las sentencias del DDL y actualiza las tablas del diccionario de datos o catálogo que contienen los metadatos.
- **El precompilador del DML.** Convierte las sentencias del DML embebidas en el lenguaje anfitrión, en sentencias listas para su procesamiento por parte del compilador de lenguaje anfitrión y además extrae dichas sentencias DML para que puedan ser procesadas de forma independiente por el compilador del DML.
- **El compilador del DML.** Chequea la sintaxis de las sentencias del DML y se las pasa al procesador de consultas.
- **El procesador de consultas.** Realiza la transformación de las consultas en un conjunto de instrucciones de bajo nivel que se dirigen al gestor de la base de datos.

- **El gestor de la base de datos.** Sirve de interfaz para los programas de aplicación y las consultas de los usuarios. El gestor de la base de datos acepta consultas y examina los esquemas externo y conceptual para determinar qué registros se requieren para satisfacer la petición. Entonces el gestor de la base de datos realiza una llamada al gestor de ficheros para ejecutar la petición.

Los principales componentes del gestor de la base de datos son los siguientes:

- o *El gestor de transacciones.* Realiza el procesamiento de las transacciones.
- o *El gestor de buffers.* Transfiere los datos entre memoria principal y los dispositivos de almacenamiento secundario.
- o *El gestor de ficheros.* Gestiona los ficheros en disco en donde se almacena la base de datos. Este gestor establece y mantiene la lista de estructuras e índices definidos en el esquema interno. Para acceder a los datos pasa la petición a los métodos de acceso del sistema operativo que se encargan de leer o escribir en los ficheros físicos que almacenan la información de la base de datos.

En el esquema propuesto se reflejan distintos bloques en los que se indican:

- Tipos de usuarios que pueden acceder al SGBD
- Métodos utilizados por los usuarios para acceder a la información.
- SGBD que se divide en:
 - o El primer subsistema es el encargado de recibir las peticiones y dirigirlas al gestor de la base de datos o al diccionario de datos.
 - o El segundo es el gestor de la base de datos, que posee un gestor de transacciones, un gestor de buffer y el gestor de ficheros.

- o La base de datos con sus índices y el diccionario de datos.

19.1.6 SGBD Relacionales (SGBD-R)

Los Sistemas Gestores de Base de Datos Relacionales están basados en el **Modelo Relacional** el cual intenta representar el Universo del Discurso mediante el álgebra relacional y sus principales características son:

Basado en un modelo matemático con un conjunto de reglas y algoritmos establecidos, permitiendo que se desarrollen lenguajes de acceso y manipulación muy potentes y fiables.

La estructuración de los datos se realiza mediante relaciones que son modeladas utilizando tablas bidimensionales que representan las entidades como sus relaciones.

Estable reglas de integridad que posibilitan la incorporación de aspectos semánticos y el traslado de restricciones o comportamientos de los datos al esquema conceptual, que de otra forma, no se podrían modelar sólo con las tablas.

19.1.6.1 Características de los SGBD-R

Sus tres principales características son las estructuras de datos, los operadores asociados y los aspectos semánticos.

19.1.6.1.1 Estructuras de datos: Relaciones y Claves

Elementos:

- *Relación*: subconjunto de un producto cartesiano entre conjuntos de atributos que en el modelo relacional se muestra como una tabla con m fila y n columnas.
- *Atributo*: representan las columnas de una tabla y se corresponden con las propiedades de las entidades. Estos atributos se encuentran limitados por un dominio que especifica el rango de valores que pueden tomar pudiendo ser compartido por varios atributos.

- *Dominio*: rango de valores que un atributo puede adoptar. Este rango es dependiente del tipo de atributo y los valores del dominio han de ser homogéneos.
- *Tuplas*: nombre que se le asocia a cada una de las filas de una tabla que se corresponden con cada una de las ocurrencias de la relación que se representa en la tabla. Su orden no es relevante.
- *Cardinalidad de la relación*: número de tuplas de una relación.
- *Grado de la relación*: número de atributos de una relación.

Dentro de los elementos que conforman la estructura de datos los más importantes son las relaciones, cuyas características más importantes son:

- Todas las tuplas de una relación están formadas por el mismo número, tipo de atributos y en el mismo orden.
- El orden de las tuplas carece de relevancia.
- En cada atributo de una tupla sólo puede aparecer un valor que además ha de pertenecer al dominio correspondiente.
- No pueden existir dos tuplas iguales en la misma relación. Esto provoca que exista uno o varios atributos que sirvan para distinguir unas tuplas de otras denominados *claves candidatas*.

Alguna de estas claves candidatas son seleccionadas por el administrador o diseñador de la base de datos para la identificación de tuplas, entonces la clave se denomina *clave primaria* y no puede adoptar nunca el valor nulo. El resto de claves candidatas que no son seleccionadas como primarias se denominan *claves alternativas o secundarias*.

Además una relación puede incluir dentro de sus atributos la clave primaria de otra relación, pasando ésta a ser *clave foránea* de la primera relación.

19.1.6.1.2

Operadores asociados

El álgebra con la que se mueve el modelo relacional está formada por un conjunto de operadores asociados y es completa, es decir, garantiza

matemáticamente que con ella se puede realizar cualquier acceso a la base de datos.

Los operadores utilizan las relaciones del modelo como operandos. Los operadores más importantes se muestran a continuación:

- **Unión.** La unión de dos relaciones “A” y “B” produce el conjunto de tuplas formado por las tuplas de “A” y las tuplas de “B”. Solo es aplicable a relaciones con el mismo grado y con los mismos atributos.
- **Diferencia.** La diferencia entre dos relaciones “A” y “B” es el conjunto de tuplas de la relación A que no están en “B”. Solo es aplicable a relaciones con el mismo grado y con los mismos atributos.
- **Producto Cartesiano.** El producto cartesiano de dos relaciones “A” de grado m y “B” de grado n, está formado por el conjunto de todas las posibles tuplas de m+n atributos con los m primeros valores de “A” y los n restantes de “B”.
- **Proyección.** Considerando “x” un subconjunto de atributos de la relación “A”, la *proyección* del atributo “x” sobre la relación “A” es la relación formada por los atributos de “A” correspondientes con los del subconjunto “x”.
- **Selección.** Si “F” resulta una fórmula que está compuesta por operadores lógicos, aritméticos y de comparación y los operandos se corresponden con valores de los atributos de una relación “A”, entonces la selección de “F” sobre “A” es el conjunto resultante formado por las tuplas de “A” que cumplen la condición establecida por “F”.

Partiendo de este conjunto de operadores se pueden generar otros derivados como la intersección, el cociente o la unión natural.

19.1.6.1.3

Aspectos Semánticos

Cuando una característica del entorno o del universo del discurso no se puede modelar mediante la definición de una relación, ésta ha de definirse

mediante un nivel de descripción superior pasando a formar parte de los aspectos semánticos. Estos aspectos, desde un punto de vista práctico, son restricciones que se añaden a las propias del modelo relacional y que su propósito es el de garantizar la integridad y validez de los datos. A su vez también aportan un mayor grado de información al esquema lógico de datos.

Dentro de este conjunto de restricciones se pueden identificar dos grupos:

- *Restricciones de Usuario.* Son restricciones que se aplican a los valores pertenecientes al dominio de los atributos, como por ejemplo en un atributo fecha limitar los meses a 12 y los días a 31.
- *Integridad Referencial.* Las restricciones pertenecientes a la integridad referencial se ocupan del mantenimiento de las referencias existentes entre las propias relaciones.

Para mantener la integridad referencial, cuando se realiza alguna tarea de borrado o modificación de las tuplas se ha de realizar alguna de las siguientes acciones.

- o Impedir la operación, para asegurarse que una vez establecida la relación entre dos tuplas de distintas tablas no se puede deshacer.
- o Transmitir en cascada, es decir si se borra o modifica una tupla, todas aquellas que hace referencia a ella se han también de borrar o modificar.
- o Poner a nulo, mantener la integridad asignando el valor nulo al atributo que realiza las tareas de clave foránea.
- o Establecer valor por omisión o lanzar un procedimiento de usuario que lo establezca.

19.2 BASES DE DATOS XML NATIVAS

La mayoría de las aplicaciones tradicionales de negocio y de las aplicaciones basadas en Internet dependen de bases de datos, ya que en ellas se almacena información crucial para el buen funcionamiento de las mismas. También se sabe que XML es el presente y futuro de la administración de datos, pues este lenguaje ha permitido romper barreras y crear una manera estándar de procesar la información.

Pues bien, la aplicación de XML también ha afectado al mundo de las bases de datos, dando lugar a un nuevo enfoque y creando una nueva generación de bases de datos denominadas bases de datos XML y bases de datos XML nativas.

Las bases de datos nativas son totalmente distintas a las bases de datos tradicionales puesto que a pesar de que pueden soportar XML lo siguen realizando de una manera relacional.

Por el contrario, las bases de datos XML brindan una nueva capacidad sobre las relacionales, y es el hecho de que permiten obtener los resultados de las consultas directamente en XML.

19.2.1 Bases de datos XML

En el conjunto de bases de datos que hacen uso del XML es posible caracterizar tres tipos de archivos XML:

- **Centrados en datos:** constan de muchos elementos de datos de pequeño tamaño y tienen una estructura regular y bien definida. Se usa como mecanismo de intercambio o para mostrar datos.
- **Centrados en documentos:** están formados por pocos elementos y con estructura impredecible en tamaño y contenido. Se enfocan a sistemas documentales y de gestión de contenidos.
- **Híbridos:** mezcla partes de los dos tipos anteriores.

19.2.1.1 Bases de datos habilitadas para XML

Desglosan un documento XML en su correspondiente modelo relacional o

entre el contenido XML y las tablas en el SGBD-R. Las bases de datos relacionales habilitadas para XML son buenas para cierto tipo de contenido de documentos XML centrado en los datos, el cual tiene una estructura fija y se ajusta bien a tablas relacionales y no tiene información jerárquica.

19.2.2 *Bases de datos XML nativas*

Según el DBXml Group, *“Las bases de datos XML nativas son BD que almacenan XML usando un formato que permite un procesamiento más rápido”*.

Son bases de datos especialmente diseñadas para almacenar documentos XML y por tanto son bases de datos centradas en documentos que definen un modelo lógico para el documento XML. Respetan la estructura del documento, permiten hacer consultas sobre dicha estructura y recuperan el documento tal y como fue insertado originalmente.

Sus características principales son las siguientes:

- No tienen ningún modelo de almacenamiento físico subyacente concreto
- Almacenamiento de documentos en colecciones.
- Validación de documentos.
- Soportan uno o más lenguajes de consulta entre ellos XML.
- Permiten la creación de índices para acelerar consultas realizadas frecuentemente.
- Crean un identificador único para cada documento XML.
- Tienen una gran variedad de estrategias para actualizar y borrar documentos.

19.3 MONITORES TRANSACCIONALES

Los monitores transaccionales son aplicaciones de control que realizan tareas de monitorización de las transferencias de datos que se producen dentro de una organización. Su intención es la de controlar las transacciones que se producen en los terminales, ya sean locales o remotos. Su objetivo es el garantizar que un proceso de transacción se produce de manera correcta y en el caso de no ser así, lanzar los procedimientos necesarios para solventar el problema y mantener la integridad del sistema.

Un monitor transaccional en cierto modo rompe la ejecución de las aplicaciones en transacciones para asegurarse que todas las bases de datos se actualizan mediante una única transacción.

Esta capacidad que garantiza la unicidad de una transacción resulta muy útil en sistemas de gestión de reservas y en cualquier tipo de sistema en el que ocurra un elevado número de transacciones.

Recibe peticiones de consulta o de procesado procedentes de los clientes para ejecutarlas en uno o varios servidores de bases de datos. El monitor transaccional encola estas peticiones y las prioriza para posteriormente volcarlas sobre los sistemas de gestión de datos.

Una de las ventajas que aportan los monitores transaccionales es que una vez que una transacción es aceptada por el monitor, éste asume la responsabilidad de llevarla a cabo, liberando a su vez al cliente y posibilitando que este continúe con su procesamiento.

19.3.1 *Ventajas de los monitores transaccionales*

- Ofrecen la capacidad de actualización de múltiples bases de datos en una sola conexión, estableciendo un pool de conexiones.
- Permiten que sea posible mantener estable un sistema con conectividad a múltiples fuentes de datos y de distintos tipos archivos planos, XML, datos no relacionales, mainframes, etc.
- Proporcionan mecanismos para priorizar las transacciones.

- ### 19.3.2 Arquitecturas

19.3.2.1 *Modelo de un Proceso por Cliente*

- Supone un elevado consumo de memoria.

19.3.2.2 *Modelo de Proceso Único*

- Se utiliza en entornos cliente-servidor
- El proceso servidor es un proceso multihilo, lo que ofrece bajo coste en el intercambio de hilos.
- No ofrece protección entre aplicaciones
- No recomendable para bases de datos distribuidas o paralelas.

19.3.2.3 Modelo de muchos Servidores, un Router

- Procesos servidores independientes para cada aplicación
- Los procesos servidores son multihilo
- Válido para bases de datos paralelas y distribuidas.

19.3.2.4 Modelo de muchos Servidores, muchos Routers

Utiliza múltiples procesos de comunicación con los clientes.

- Los clientes se comunican con los routers que redireccionan las peticiones hacia los servidores apropiados.
- Se utiliza un control y supervisión de procesos.

19.4 BIBLIOGRAFÍA

- Codd, E.F. "A Relational Model of Data for Large Shared Data Banks". In: Communications of the ACM 13 (6): 377-387, 1970.
- DAFTG of the ANSI/X3/SPARC Database System Study Group, "Reference Model for DBMS Standardization". Sigmod Record, Vol.15, No.1, March 1986)
- de Miguel y M. Piattini. "Fundamentos y Modelos de Bases de Datos". Ed. RA-MA. 1999. ISBN 978-84-78-97361-3
- M. Piattini, E. Marcos, C. Calero y B. Vela. "Tecnología y Diseño de Bases de Datos". Ed. RA-MA 2006. ISBN 978-847-897733-8
- Nguyen Viet Cuong, "XML Native Database Systems Review of Sedna, Ozone, NeoCoreXMS". 2006.
- Jim Gray, "Transaction Processing: Concepts and Techniques". Ed. Morgan Kaufman, 1992. ISBN 15 586 0190 2

Autor: Francisco Javier Rodríguez Martínez

Subdirector de Sistemas Escola Superior Enxeñaría Informática Ourense

Colegiado del CPEIG

20. SQL. LENGUAJE DE DEFINICIÓN DE DATOS (DDL). LENGUAJE DE MANIPULACIÓN DE DATOS (DML) Y DCL.

Tema 20 SQL. Lenguajes de definición de datos (DDL). Lenguajes de manipulación de datos (DML) y DCL.

ÍNDICE

20.1.1 Partes del lenguaje SQL.....	2
20.1.2 Modos de trabajo con SQL.....	4
20.2.1 Objetos de la Base de Datos.....	7
20.2.2 Gestión de tablas.....	9
20.2.3 Gestión de vistas.....	16
20.2.4 Gestión de índices.....	17
20.3.1 Inserción de valores en una tabla.....	19
20.3.2 Borrado de valores de una tabla.....	20
20.3.3 Modificación de valores de una tabla.....	20
20.3.4 Consulta de datos.....	21
20.3.5 Consultas sobre múltiples tablas.....	27
20.3.6 Subconsultas.....	30
20.3.7 Operaciones con consultas.....	32
20.4.1 Seguridad.....	33
20.4.2 Transacciones.....	36

20.1.- SQL

EL SQL (Structured Query Language) es un lenguaje estandarizado de peticiones (query) a bases de datos relacionales. Es el lenguaje de manipulación de bases de datos relacionales más extendido, habiéndose convertido en un estándar de facto.

Permite realizar consultas utilizando los recursos del álgebra relacional combinados con el cálculo relacional de tuplas.

SQL sea un lenguaje declarativo en lo que lo importante es definir qué se desea hacer, por encima de cómo hacerlo. Con este lenguaje se pretendía que las instrucciones se pudieran escribir como si fueran órdenes

humanas; es decir, utilizar un lenguaje lo más natural posible. De ahí que se le considere un lenguaje de cuarta generación.

La base teórica de SQL es bastante fuerte. Las operaciones funcionan en términos de conjuntos y no de registros individuales. Además no incluye ninguna especificación de localización de los datos o ruta de acceso dejando esta tarea al intérprete del lenguaje.

La primera definición del modelo relacional de bases de datos fue publicada por Codd en 1970. El trabajo de Codd fue inmediatamente desarrollado por empresas y universidades. El SQL fue desarrollado en el centro de investigación de IBM bajo el nombre SEQUEL (Structured English Query Language) en 1974 y 1975. La versión SEQUEL/2 cambió de nombre a SQL por motivos legales. IBM comenzó a trabajar en una implementación de SEQLTL/2 (SQL) llamada System R que estuvo operativa en 1977.

En 1986 se publicó el estándar ANSI del lenguaje que, posteriormente fue adoptado por ISO en 1987, lo que convierte a SQL en estándar mundial como lenguaje de bases de datos relacionales.

En 1989 aparece el estándar ISO (y ANSI) llamado SQL89 o SQL1. En 1992 aparece la nueva versión estándar de SQL (a día de hoy sigue siendo la más conocida) llamada SQL92. En 1999 se aprueba un nuevo SQL estándar que incorpora mejoras que incluyen triggers, procedimientos, funciones,... y otras características de las bases de datos objeto-relacionales; dicho estándar se conoce como SQL99.

El último estándar es el del año 2008 (SQL2008). ISO/IEC 9075-1:2008

20.1.1 Partes del lenguaje SQL

Podemos considerar dos fases en la vida de la base de datos: la etapa de preparación y puesta en marcha y la etapa de explotación. Esta última es el objetivo final de todo el sistema y las tareas de preparación se realizarán antes de entrar en esa fase de utilidad para la organización.

El lenguaje SQL se compone de un conjunto de instrucciones al igual que cualquier lenguaje tradicional. Debido a la existencia de las dos fases antes descritas se suelen agrupar estas instrucciones en tres “sublenguajes” que en particular en bases de datos relacionales son los siguientes:

- **Lenguaje de Definición de Datos, DDL** (Data Description Language): Es el lenguaje utilizado para la creación y mantenimiento de la estructura de la base de datos. Se utiliza para definir y modificar los esquemas de las relaciones, crear o destruir índices y eliminar relaciones. Permite también la definición de vistas y permisos de acceso para los usuarios. Es el lenguaje que utiliza el administrador de las bases de datos para realizar sus tareas.
- **Lenguaje de Manipulación de datos, DML** (Data Manipulation Language). Incluye todas las instrucciones para realizar consultas a las bases de datos, insertar, modificar o eliminar datos. Éste es el que utilizan los usuarios finales en la fase de explotación de la base de datos. A la parte del DML que permite realizar consultas sobre los datos de la BD se le llama DQL (Data Query Language), pero es una parte del DML.
- **Lenguaje de Control de Datos, DCL** (Data Control Language). Existen una serie de tareas relacionadas con las bases de datos que no están incluidas en ninguno de los dos grupos antes descritos ya que no son propiamente de descripción ni de manipulación de datos. Mediante este lenguaje se establecen las restricciones adicionales necesarias para controlar la privacidad y la integridad de la información almacenada en la base de datos.

Además, los lenguajes comerciales, y SQL en particular, incluyen otras facilidades como son control de principio y final de las operaciones o el bloqueo de datos mientras dura una consulta.

20.1.2 Modos de trabajo con SQL

Los modos en que el lenguaje SQL actúa sobre una base de datos son los siguientes.

- Modo interactivo: El usuario de la base de datos establece un diálogo con el Sistema Gestor de Base de Datos (SGBD) a través del intérprete de SQL. De esta forma puede realizar operaciones interactivamente sobre la base de datos introduciendo cualquier sentencia SQL y sin restricción en el orden de éstas.

Las sentencias SQL así introducidas son traducidas por el intérprete de SQL que producirá la solicitud correspondiente para el gestor de la base de datos que la gestionará y generará una respuesta para el usuario.

- Desde un programa: El usuario ejecuta una aplicación sobre el sistema operativo. La aplicación puede ser de dos tipos:
 - o Programa escrito íntegramente en SQL o mejor en extensiones de éste que incluyen las estructuras de programación habituales (bucles y selección). Un ejemplo de esto es PL/SQL de Oracle que es un lenguaje procedural que permite desarrollar programas que acceden a la base de datos vía SQL. Estos programas o módulos de sentencias SQL son en realidad guiones que el intérprete SQL va siguiendo.
 - o Programa escrito en un lenguaje convencional de programación con partes escritas en SQL. Esto es lo que se llama SQL embebido y al lenguaje que contiene el texto SQL se le llama lenguaje anfitrión (host). En este caso las instrucciones del lenguaje de programación se ejecutan por el procedimiento habitual mientras que las sentencias SQL se le pasan a un módulo especial de ejecución del SGBD. Una implementación de SQL embebido establece las relaciones que deben mantener los objetos de la base de datos con los objetos del programa

anfitrión y restricciones de funcionamiento. Este modo de trabajo admite dos variantes:

- SQL estático: el programa no admite cambios durante la ejecución. Este es el método utilizado en la mayoría de las aplicaciones.
- SQL dinámico: si durante la ejecución se debe modificar algún parámetro se tiene que utilizar SQL dinámico. Esto resulta menos eficiente que un programa SQL estático y utiliza técnicas dinámicas de manejo de variables, lo que dificulta la tarea de programación.

20.2.- LENGUAJE DE DEFINICIÓN DE DATOS (DDL)

Los datos en bases de datos relacionales se almacenan en tablas. Una tabla se compone de filas y columnas o registros y campos correspondientes a entidades y atributos de una relación. A todas las estructuras lógicas de datos se les llama de una forma genérica objetos de las bases de datos.

Normalmente en un SGBD existen varios usuarios que deberán disponer en primer lugar de acceso al sistema operativo de la máquina. Cada usuario para el SGBD estará identificado por un nombre, una palabra clave y unas propiedades. Todo ello es fijado y administrado por el administrador de la base de datos (ABD) que es un usuario especial con derechos sobre todos los objetos.

Lo normal es que las estructuras de datos que van a ser compartidas sean creadas por el administrador pero esto no es un requisito imprescindible dado que puede haber usuarios para los que sea de interés mantener sus propias bases de datos que compartirán con parte o toda la organización.

El creador o propietario de una tabla puede permitir el acceso a su tabla a otros usuarios del sistema pero puede que le interese también permitir el acceso a una parte de la tabla. Para estos casos se creará una vista (view).

En una vista se seleccionan algunos atributos o algunas tuplas de la tabla y se permite que usuarios seleccionados las puedan manejar.

La búsqueda de un registro en una tabla es una búsqueda secuencial. Una forma de agilizar la búsqueda consiste en ordenar los registros según algún criterio y preguntar por los registros según ese orden. Si existe una tabla en la que se anota el valor característico de cada registro y su dirección, la búsqueda se llama indexada y esta tabla auxiliar se llama índice.

En un sistema multiusuario cada usuario tiene un conjunto de objetos que le pertenecen de diferentes tipos como tablas, índices o vistas. A este conjunto se le suele llamar esquema.

Todos los objetos citados hasta ahora deben crearse y configurarse antes de pasar al uso de la base de datos. Estas tareas se realizan con DDL.

Cada objeto de una base de datos tiene un nombre que sirve para localizarlo a lo largo de su vida. Estos nombres tienen un ámbito donde son reconocidos. Cada nombre debe ser único en su ámbito. Los objetos que pertenecen a un esquema (tablas, índices, etc.) tienen ese esquema como ámbito máximo. Por ello un nombre de tabla, por ejemplo, puede repetirse en distintos esquemas de usuarios diferentes pero no dentro del mismo esquema.

Además de estas normas básicas las diferentes implementaciones tienen sus propias reglas sobre ámbitos.

Resumiendo, con un DDL se puede hacer:

- Gestión de tablas
- Gestión de vistas
- Gestión de índices

20.2.1 Objetos de la Base de Datos

Según los estándares, una base de datos es un conjunto de objetos pensados para gestionar datos. Estos objetos están contenidos en esquemas. Un **esquema** representa la estructura de la base de datos. Los elementos que incluye un esquema son tablas, dominios, vistas, restricciones, disparadores y otros constructores.

En el estándar SQL existe el concepto de **catálogo** que sirve para almacenar esquemas. Así el nombre completo de un objeto vendría dado por:

catálogo.esquema.objeto

Si no se indica el catálogo se toma el catálogo por defecto. Si no se indica el esquema se entiende que el objeto está en el esquema actual.

Tipos de datos y dominios

Un dominio es un conjunto del cual toma sus valores una columna o atributo de una relación. Según este concepto los tipos de datos predefinidos son dominios.

Algunos de los tipos de datos predefinidos en el estándar son:

- Integer (4 Bytes) y SmallInt (2 Bytes)
- Decimal (precisión, (escala)). Representa un decimal de coma fija. Si se omite la escala se supone 0.
- Float. Representa un decimal de coma variable.
- Char (n) Cadena de caracteres de longitud fija (de n caracteres).
- Varchar (n) Cadena de caracteres de longitud variable (de máximo n caracteres).
- Date (fecha), Time (hora), TimeStamp (fecha y hora).

- Boolean, bit
- CLOB. Representa textos de gran longitud.
- BLOB. Representa binarios de gran longitud.

Definición de dominios

Una definición de dominios es un tipo de datos especializado que se puede utilizar en la definición de columnas. Su sintaxis es la siguiente.

CREATE DOMAIN nombre dominio tipo de datos

[DEFAULT valor defecto]

[definición de restricciones de dominio] ;

Donde:

- tipo de datos: uno de los proporcionados por SQL
- valor defecto: Especifica el valor por omisión para columnas definidas de este dominio. Será asignado a cada columna con dicho dominio, si no tiene ya su propia cláusula DEFAULT
- definición de restricciones de dominio: implica una restricción que se aplica a toda columna definida sobre el dominio. Se define con la cláusula

[CONSTRAINT nombre_restricción] CHECK (expresión condicional)

Ejemplo: Enumeración de posibles valores de los colores para un dominio particular

CREATE DOMAIN Color VARCHAR(8) DEFAULT 'sinColor'

CONSTRAINT color_valido

CHECK (VALUE IN ('rojo', 'amarillo', 'azul', 'verde', 'sinColor')

) ;

20.2.2 Gestión de tablas

Una tabla es un objeto de la base de datos que almacena datos.

Para describir una tabla se utiliza la sentencia CREATE, especificando el nombre y las características de la tabla.

Las características básicas que debe de tener una tabla son:

- Definición de los atributos o columnas
- Restricciones de integridad

Para definir una columna habrá que decir el nombre y tipo de datos que se van a almacenar en ese campo de la tabla

Restricciones de integridad

Se denomina restricción de integridad a una propiedad que debe cumplirse para mantener en las tablas los criterios de diseño.

Las restricciones tienen un nombre para poder ser manipuladas posteriormente y pueden afectar a una tabla entera o a una columna o atributo (restricciones de tabla o restricciones de columna).

La restricción de tabla es alguna característica de mantenimiento de la integridad que se asocia a la tabla al crearla. Esta restricción se aplicará a los valores que contenga la tabla, luego supondrá una validación de los datos al introducirlos o modificarlos.

Las restricciones de columnas indican ciertas características que deben asociarse a la columna que se está describiendo.

En SQL las restricciones de integridad se fijan mediante una sentencia CONSTRAINT.

La sintaxis de restricciones para tablas es la siguiente:

[CONSTRAINT nombre_restricción] (

```

[UNIQUE | PRIMARY KEY (atrib1[,atrib2]...) ]
[FOREIGN KEY (atrib1 [,atrib2]...)
    REFERENCES tabla(atrib1[,atrib2]...)
    [ON UPDATE [CASCADE | NO ACTION | RESTRICT |
SET          NULL | SET DEFAULT]
    [ON DELETE [CASCADE | NO ACTION | RESTRICT |
SET          NULL | SET DEFAULT] ]
[CHECK condición]
)

```

La sintaxis de restricciones para atributos es la siguiente:

```

[CONSTRAINT nombre_restricción] (
    [NOT NULL]
    [UNIQUE | PRIMARY KEY]
    REFERENCES tabla(atrib1[,atrib2]...)
    [ON UPDATE [CASCADE | NO ACTION | RESTRICT |
SET          NULL | SET DEFAULT]
    [ON DELETE [CASCADE | NO ACTION | RESTRICT |
SET          NULL | SET DEFAULT] ]
    [CHECK condicion]
)

```

Las restricciones que se pueden establecer son:

- **NOT NULL:** se aplica a un campo e indica que no puede contener valores nulos.
- **UNIQUE:** la(s) columna(s) NO puede contener valores duplicados. Debe declararse como NOT NULL y NO pueden formar parte de la clave primaria.

- **PRIMARY KEY:** denota la(s) columna(s) que son clave principal de la tabla. Tienen valor único y no nulo.
- **CHECK:** se puede aplicar a un atributo o a toda la tabla. Indica una condición que debe satisfacer cada atributo o cada fila de la tabla antes de ser insertada borrada o actualizada.
- **FOREING KEY / REFERENCES:** cuando entre dos tablas se establece una relación las tuplas de una se relacionan con las de la otra mediante ciertos campos clave en cada tabla. La tabla de la que parte la relación se llama tabla primaria y la otra se llama tabla secundaria.

Se llama **clave ajena** (foreign key) al conjunto de atributos de la tabla secundaria que es clave principal en la tabla primaria. Esta última debe ser clave principal o única.

Una relación mantiene la integridad referencial si cumple las siguientes dos condiciones:

- o Toda tupla de la tabla hija está asociada con una tupla de la tabla padre.
- o Si una tupla de la tabla hija no cumple lo anterior, el valor que tiene la columna de la clave ajena es nulo.

La restricción de integridad referencial debe establecerse en la tabla hija. Se usan ciertos parámetros para fijarla

- o **FOREING KEY:** indica que columna o columnas constituyen la clave ajena en una restricción de integridad referencial. Se aplica en la restricción de tabla.
- o **REFERENCES:** especifica la tabla padre. Si no indica a qué clave primaria o única se refiere la clave ajena se entiende que la clave referenciada es la clave primaria de la tabla indicada.

Las siguientes opciones hacen que el gestor mantenga la integridad referencial

- a) ON [DELETE | UPDATE] CASCADE: Borra o actualiza el registro en la tabla padre y automáticamente borra o actualiza los registros coincidentes en la tabla hija. Sin esta cláusula no se permite borrar o actualizar un registro principal que tenga registros secundarios asociados.
- b) ON [DELETE | UPDATE] RESTRICT: No se puede borrar o actualizar un registro en la tabla padre mientras no se borre o actualice el registro secundario asociado en la tabla hija.
- c) ON [DELETE | UPDATE] SET NULL: Borra o actualiza el registro en la tabla padre y establece en NULL la o las columnas de clave foránea en la tabla hija.
- d) ON [DELETE | UPDATE] NO ACTION: Significa ninguna acción en el sentido de que un intento de borrar o actualizar un valor de clave primaria no será permitido si en la tabla referenciada hay un valor de clave foránea relacionado.
- e) ON [DELETE | UPDATE] SET DEFAULT: Borra o actualiza el registro en la tabla padre y establece el valor por defecto de la o las columnas de clave foránea en la tabla hija.

1) Creación de una tabla

La sintaxis básica de la instrucción es la siguiente.

```
CREATE TABLE nombretabla (  
    atributo1 tipo1 [restricciones de atributo]  
    [,atributo2 tipo2 [NOT NULL] [UNIQUE] [DEFAULT valor]  
    [Restricciones De Tabla])
```

La creación de una tabla engloba las definiciones de atributos y/o restricciones:

- a) **La DEFINICIÓN DE ATRIBUTOS** se realiza dando el nombre del atributo (se ajusta a las mismas reglas que los nombres de tablas) y su tipo. Opcionalmente se puede indicar unas restricciones de atributos:
 - a. Not null: restricción de valor no nulo.
 - b. Definiciones de restricciones de clave primaria, valor UNIQUE, clave ajena.
 - c. Definición de restricciones generales con la cláusula check.
- b) **La DEFINICIÓN DE RESTRICCIONES DE INTEGRIDAD / SEMÁNTICAS:** Permiten al diseñador restringir el rango de valores de una tabla. Las restricciones pueden ser de columna si afectan a una sola columna, o de tabla si afectan a una o más columnas, tal como se vio en el apartado anterior.

Ejemplo:

```
CREATE TABLE DPTO(  
    DEPTNO    INTEGER(4),  
    DNAME     VARCHAR(14) NOT NULL,  
    LOC       VARCHAR(13) DEFAULT "OURENSE",  
    PRIMARY KEY (DEPTNO)  
)
```

CREATE TABLE EMP (
EMPNO	INTEGER (4) NOT NULL ,
ENAME	VARCHAR(10),
JOB	VARCHAR(9),
MGR	INTEGER(4),

```
HIREDATE    DATE,  
SAL         DECIMAL(7,2),  
COMM        DECIMAL(7,2),  
DEPTNO      INTEGER(4);  
  
CONSTRAINT pk_empl PRIMARY KEY (EMPNO),  
FOREIGN KEY (DEPTNO) REFERENCES DEPT (DEPTNO)  
                ON UPDATE CASCADE ON DELETE RESTRICT,  
CHECK SAL > 600,04  
)
```

2) Modificación de una tabla

Para modificar una tabla ya creada se utiliza el comando ALTER TABLE con el que pueden especificarse nuevas columnas, nuevas restricciones (ADD) o bien modificarse una columna (MODIFY). La sintaxis es:

```
ALTER TABLE table (  
    [ADD (col1|restric1) (,col2|restric2)...)]  
    [ALTER (col1 tipo1(,col2 tipo2)...)]  
    [DROP CONSTRAINT restricción]  
    [DROP COLUMN columna [CASCADE | RESTRICT] ]  
)
```

- Al añadir una columna a una tabla ya existente hay que tener en cuenta que **NO** está permitido NOT NULL en la definición de una nueva columna, y si se desea introducir un valor para la columna, en cada fila existente, hay que especificarlo con la cláusula DEFAULT al añadir la columna.
- Sólo se puede cambiar el tipo o disminuir el tamaño de una columna si tiene valores nulos en todas las columnas.

- Sólo se pueden borrar restricciones que tengan nombre.
- Al eliminar una columna de una tabla podemos indicar la opción:
 - o CASCADE: elimina la columna y toda restricción o vista que le hace referencia.
 - o RESTRICT: sólo elimina la columna si ninguna vista ni restricción le referencia.

Por ejemplo, la sentencia:

```
ALTER TABLE EMP (  
    ADD ADDRESS VARCHAR(12) DEFAULT "Unknow";  
    ALTER ENAME VARCHAR(30)  
)
```

Modifica la longitud del atributo ENAME y añade el campo ADDRESS.

3) Destrucción de una tabla

La sintaxis para eliminar una tabla es:

DROP TABLE nombre_de_tabla [CASCADE | RESTRICT]

Para ejecutar esta instrucción se deben tener suficientes privilegios en el sistema o ser el propietario de la tabla.

El parámetro opcional :

- RESTRICT: Destruye la tabla sólo si no se le hace referencia desde ninguna otra tabla (clave ajena), ni es tabla base de una vista.
- CASCADE: Elimina la tabla junto con las restricciones y vistas que la referencian.

Después de la ejecución de la sentencia DROP cualquier referencia a la tabla dará un error. La tabla se borrará independientemente de que contenga datos o no.

20.2.3 Gestión de vistas

Una vista es una tabla virtual, es decir, una tabla que no existe físicamente en la base de datos pero aparece al usuario como si existiera. Las vistas no tienen datos almacenados propios, distinguibles y físicamente almacenados. En su lugar, el sistema almacena la definición de la vista (es decir, las reglas para acceder a las tablas base físicamente almacenadas para materializar la vista).

Las vistas tienen varias utilidades:

- Mostrar a los usuarios los datos que les interesan.
- Proteger los datos.
- Reestructurar datos que pueden estar distribuidos en diferentes soportes de manera que aparezcan como una tabla.
- Crear interfaces para aplicaciones que esperan una estructura de tablas distinta a la de creación. Mediante las vistas las aplicaciones se independizan de la estructuración real de los datos.

Creación de una vista

Se usa la sentencia CREATE VIEW cuya sintaxis es:

```
CREATE [OR REPLACE] VIEW nombre_de_vista [lista_de_campos]
```

AS consulta

Cuando se ejecuta una sentencia de creación de vista se realiza una consulta que selecciona tuplas y atributos de una o varias tablas. Ejemplo: si se le quiere dar una lista de empleados a la empresa de seguridad que controla el acceso al edificio, se utilizará una vista sobre la tabla original:

```
CREATE VIEW EMP_SECURITY  
AS  SELECT EMPNO, ENAME  
    FROM EMP
```

Por defecto, la vista toma los nombres de los atributos seleccionados desde las tablas base, siempre que ningún atributo sea el resultado de una operación aritmética o función de agregado. Si se desea cambiar los nombres de los atributos se utiliza la lista_de_campos.

Modificación de la estructura de una vista

La estructura de una vista no puede ser modificada como tal. Lo que se puede hacer es utilizar una sentencia de creación con la cláusula OR REPLACE que sustituirá una vista por otras.

El comando de SQL ALTER VIEW se utiliza para recompilar una vista, Esto se debe hacer cuando se han modificado las tablas bases de la vista para actualizar la vista sobre las nuevas estructuras. Su sintaxis es:

ALTER VIEW vista COMPILE

Después de esta instrucción toda referencia a la vista desde otro objeto se destruye.

Destrucción de una vista

La instrucción DROP VIEW permite eliminar una vista que haya sido creada anteriormente

DROP VIEW view

20.2.4 Gestión de índices

En una base de datos un índice es un medio de acceder a los registros de una forma más rápida que con el simple recorrido secuencial de una tabla. El índice es un objeto de la base de datos que contendrá una entrada para cada valor de las columnas indexadas, con la dirección del registro donde debe buscarse ese valor.

Uno de los usos más comunes de los índices es el mantenimiento de una tabla ordenada por distintos criterios.

Sólo es recomendable crear índices para aquellos campos que tengan muchas búsquedas pues el índice ocupa espacio y tiene que actualizarse cada vez que se borra, actualiza o inserta un elemento en una tabla.

Creación de un índice

La instrucción para crear un índice es CREATE INDEX

```
CREATE INDEX nombre índice  
ON nombre_tabla (campo{, campo})  
[NOSORT]
```

Se especifica el nombre de la tabla sobre la que se crea el índice, así como el campo o campos sobre el que se indexa. Es posible crear índices concatenados, que se forman con más de una columna. Se emplea en caso de columnas que siempre se consultan juntas.

La opción NOSORT que aparece en algunos sistemas SQL hace que se ahorre tiempo y espacio en la creación de un índice haciendo que si la tabla se ha llenado con registros que están físicamente ordenados con el mismo criterio que el índice se pueda evitar la ordenación que se produce al crear el índice.

```
CREATE INDEX IND_EMPRE ON EMPRESA (Abre_emp)
```

Eliminar un índice

Para destruir un índice se utiliza la cláusula DROP INDEX

```
DROP INDEX índice
```

20.3.- LENGUAJE DE MANIPULACIÓN DE DATOS (DML)

Se llaman manipulaciones a aquellas operaciones sobre una base de datos que no afectan a la estructura de ésta sino a su contenido. Estas

operaciones se realizan con DML (Data Manipulation Language). Las manipulaciones posibles sobre una base de datos son las siguientes:

- Insertar valores en tuplas (INSERT)
- Eliminar una tupla (DELETE)
- Actualizar el valor de un campo en una o varias tuplas (UPDATE)
- Consultar o listar todos o algunos campos de un grupo de tuplas (SELECT)

Las operaciones de manipulación se pueden hacer tanto en tablas como en vistas ya que éstas no son sino tablas lógicas.

20.3.1 Inserción de valores en una tabla

Para insertar una fila o tupla en una tabla ya creada se utiliza el comando INSERT cuya sintaxis es:

```
INSERT INTO nombre_tabla [columna (,columna)*]  
VALUES (valor (,valor)*)}
```

Si no se especifican nombres de columnas, los valores insertados deben corresponder en cantidad y tipo de datos con los atributos de la tabla y tienen que estar en el mismo orden con el que se creó la tabla.

Se pueden especificar unas columnas y otras no, teniendo en cuenta que las columnas no especificadas tomarán el valor por defecto, si se definió, o NULL.

```
INSERT INTO DEPT (DEPTNO, DNAME, LOC)  
VALUES (90, 'CONTABILIDAD', 'OURENSE')
```

Para insertar varias tuplas con una sola instrucción se puede utilizar una subconsulta que devuelva tuplas de estructura compatible con la de la tabla:

INSERT INTO nombre_tabla [columna (,columna)*]
consulta

20.3.2 Borrado de valores de una tabla

Para borrar una fila se utiliza el comando DELETE cuya sintaxis es la siguiente:

```
DELETE FROM nombre_tabla  
      [WHERE condición]
```

Con esta instrucción se borran todas las tuplas que cumplan la condición WHERE. Si no se incluye ésta se borran todos los elementos de la tabla. Por ejemplo, para borrar el departamento “CONTABILIDAD”:

```
DELETE FROM DEPT WHERE DNAME = “CONTABILIDAD”
```

20.3.3 Modificación de valores de una tabla

Para modificar los valores de determinadas tuplas de una tabla se utiliza la sentencia UPDATE con la siguiente sintaxis:

```
UPDATE nombre_tabla  
      SET columna1=valor1{,columna2=valor2}*}  
      [WHERE condición]
```

Con la cláusula SET se especifica las columnas a modificar con sus nuevos valores y con la cláusula WHERE se seleccionan las filas a actualizar. Si no hay WHERE, se aplica la modificación a todas las filas. Por ejemplo, si se quiere conceder a todo empleado del departamento de Informática un aumento salarial del 18%.

```
UPDATE EMP  
      SET SAL = SAL*1.18  
      WHERE DEPTNO IN (SELECT DEPTNO  
                        FROM DEPT  
                        WHERE DNAME='INFORMATICA')
```

20.3.4 Consulta de datos

Una consulta sirve para extraer los datos almacenados en una base de datos. La consulta en SQL consta de tres partes:

- Cláusula SELECT: para indicar qué atributos se desean consultar
- Cláusula FROM: indica sobre qué relación o relaciones se quiere hacer la consulta
- Cláusula WHERE: indica las condiciones que deben cumplir las tuplas para ser seleccionadas

Su sintaxis abreviada es la siguiente:

```
SELECT * | {[DISTINCT] columna | expresión [[AS] alias], ...}  
      FROM tablas  
      [WHERE condiciones_where]  
      [GROUP BY columnas_group]  
      [HAVING condiciones_having]  
      [ORDER BY columnas_orden]
```

El efecto de una consulta como ésta es el siguiente:

- Se realiza el producto cartesiano de las relaciones citadas en la cláusula FROM
- Se aplica el operador selección del álgebra relacional para seleccionar aquellas tuplas del producto cartesiano que hagan verdadero el predicado WHERE
- Se proyecta el resultado obtenido sobre los atributos especificados en SELECT

Selección de atributos

La consulta más sencilla es seleccionar todas las tuplas de una tabla. Por ejemplo, seleccionar todos los datos de todos los empleados.

```
SELECT EMPNO, ENAME, JOB, MGR, HIREDATE, SAL, COMM, DEPTNO  
FROM EMP
```

Se utiliza el asterisco (*) como comodín para seleccionar todos los campos. La sentencia anterior es equivalente a:

```
SELECT * FROM EMP;
```

Se pueden seleccionar columnas individuales: "Lista todos los salarios"

```
SELECT SAL FROM EMP
```

En una tabla, algunas columnas tendrán valores repetidos. Si solo se quieren mostrar los valores diferentes de una columna en una tabla hay que usar la palabra clave **DISTINCT** antepuesta al nombre de la columna

```
SELECT DISTINCT SAL FROM EMP
```

Se puede cambiar el nombre que se le da a la cabecera de la columna en el resultado de la instrucción SELECT. Para ello se utiliza un alias con el comando AS después del nombre de la columna.

```
SELECT SAL AS Salario FROM EMP
```

Orden

Por defecto SQL no ordena los resultados, para ordenarlos, se utiliza la cláusula ORDER BY:

```
ORDER BY campo1 [ASC|DESC], campo2 [ASC|DESC], ...
```

El modo de ordenación se indica para cada campo:

- ASC ordena ascendente
- DESC ordena descendente

Consulta con expresiones

También se pueden realizar consultas en las que se evalúe una expresión.

Por ejemplo, si se dispone de una tabla con el salario bruto anual de los empleados de una empresa, es posible consultar su sueldo neto mensual. Suponiendo que se paguen 14 pagas anuales y que se conozca el tipo de IRPF la instrucción para realizar esta consulta sería:

```
SELECT ENAME, (SAL/14)(1-IRPF/100) FROM EMP
```

Condiciones para restringir la consulta

Para restringir las tuplas que se obtienen, se pueden imponer condiciones. Para ello se usa la cláusula WHERE que admite los siguientes operadores

Operadores Relacionales (comparación): >, >=, <, <=, =, <>: Estos operadores se utilizan para comparar datos.

Operadores lógicos: AND, OR, NOT: Se utilizan para unir condiciones.

```
SELECT * FROM EMP
      WHERE DEPTNO = 99
      AND SAL > 1250;
```

Además, las condiciones unidas por AND, OR y NOT admiten paréntesis. Si no se ponen paréntesis la prioridad, de mayor a menor, es NOT, AND y OR.

Consulta de pertenencia a un rango

Se puede comprobar si una expresión entra o no dentro de un rango marcado. Se utiliza el operador BETWEEN. La sintaxis es:

expresión[NOT] BETWEEN expresión [AND expresión]

```
SELECT * FROM EMP
      WHERE EMPNO BETWEEN 9 AND 54
```

Consultas de pertenencias a una lista

Con el operador IN se comprueba si un elemento pertenece a una lista de valores. La sintaxis de la condición es:

elemento[NOT] IN lista_expresiones | subconsulta
Ejemplo:

```
SELECT * FROM EMP
      WHERE ENAME IN('Pepe Martínez' y 'Josefa Martín')
```

Selecciona de la tabla de empleados los datos de 'Pepe Martínez' y 'Josefa Martín'.

Consulta con patrones

Con la utilización del operador LIKE se puede buscar una cadena de caracteres dentro de otra. La sintaxis es la siguiente:

<cadena>[NOT] LIKE <cadena>

Es una comparación de igualdad pero admite comodines:

- %: se puede sustituir por cualquier número de caracteres (0 o más).
- Los SGBDR también admiten sustituir un único carácter.

Ejemplo: Para seleccionar aquellos elementos de la tabla ALUMNO cuyo campo Nombre empiece por la cadena "Ma"

```
SELECT * FROM EMP WHERE ENAME LIKE 'Ma%'
```

Funciones de agregación

Existen funciones que permiten calcular, desde una sentencia SQL, sumas, medias aritméticas, etc. de datos. Muchas de estas funciones aceptan el parámetro DISTINCT|ALL. Si toma el valor ALL (valor por defecto) indica que deben considerarse todas las apariciones aunque sean repetidas y si es DISTINCT deben ignorarse las repeticiones. Algunas de las más importantes funciones son:

- AVG (Atributo): media aritmética de los valores de atributo.
- MIN (Atributo): valor mínimo de los valores de atributo.
- MAX (Atributo): valor máximo de los valores de atributo.
- SUM (Atributo): suma los valores de atributo.
- COUNT (Atributo): cuenta el número de filas donde atributo no es nulo.
- COUNT (*): cuenta el número de filas incluyendo aquellas con nulos.
- LCASE (Atributo): transforma Atributo a mayúsculas.
- UCASE (Atributo): transforma Atributo a minúsculas.
- MID (Atributo, m [, n]): devuelve una porción de Atributo comenzando en el carácter m y con n caracteres de longitud.
- LEN (Atributo): devuelve la longitud de Atributo.

```
SELECT AVG (SAL) FROM EMP  
SELECT COUNT (*) FROM EMP
```

Consulta con agrupamiento de filas

Las funciones de agregación se suelen utilizar combinadas con la cláusula de agrupamiento GROUP BY, que agrupa el resultado por una serie de atributos.

Una instrucción SELECT con este parámetro devuelve grupos de tuplas en lugar de tuplas individuales. Como resultado de la consulta aparecerá un resumen de la información por cada grupo en lugar de todas las filas.

Por ejemplo para listar los números de departamento y la suma de los salarios de cada uno de ellos se utilizaría:

```
SELECT DEPTNO, SUM(SAL)
FROM EMP
GROUP BY DEPTNO
```

La expresión de un GROUP BY puede contener referencias a cualquier campo de las tablas nombradas en FROM. Sin embargo la lista de expresiones que siguen al SELECT no puede contener más que:

- Constantes
- Funciones de grupo (AVG, MAX, MIN, COUNT, SUM)
- Expresiones idénticas a las de la cláusula GROUP BY
- Expresiones que devuelvan el mismo valor para todas las tuplas que formen parte de un grupo.

No se pueden seleccionar atributos que no se puedan agrupar por los atributos indicados en el GROUP BY.

Si en una consulta aparece una cláusula WHERE y una GROUP BY primero se seleccionarán las tuplas que cumplan la condición del WHERE y después se aplica el agrupamiento.

Restricciones en los agrupamientos

Cuando se selecciona un conjunto de atributos agrupados por uno o más atributos, se pueden imponer condiciones a los grupos (es decir, condiciones a los atributos que se están seleccionando). Es la cláusula

HAVING, que sería el equivalente a la cláusula WHERE pero aplicada a los grupos. Por ejemplo,

“Lista la suma de los sueldos agrupada por departamentos, pero sólo aquellos en los que la suma sea mayor que 7.000”

```
SELECT SUM(SAL), DEPTNO
      FROM EMP
      GROUP BY DEPTNO
      HAVING SUM(SAL)>7.000
```

20.3.5 Consultas sobre múltiples tablas.

Es más que habitual necesitar en una consulta datos que se encuentran distribuidos en varias tablas. Las bases de datos relacionales se basan en que los datos se distribuyen en tablas que se pueden relacionar mediante un campo.

Para realizar consultas a más de una tabla, basta con indicar en la cláusula FROM las tablas separadas por comas y añadir las condiciones necesarias en la cláusula WHERE.

```
SELECT ENAME, DNAME
      FROM EMP, DEPT
```

Este ejemplo realiza el producto cartesiano de la tabla EMP y DEPT y devolvería para cada registro de la tabla EMP, todos los registros de la tabla DEPT.

Si se quiere hacer correctamente, asociando nombre de trabajador con el departamento en el que trabaja, se utiliza un criterio de comparación por la clave ajena, por ejemplo:

```
SELECT ENAME, DNAME
      FROM EMP, DEPT
      WHERE EMP.DEPTNO = DEPT.DEPTNO
```

Los nombres de los atributos, en caso de que las tablas tengan atributos con el mismo nombre, irán precedidos por el nombre de la tabla y un punto, como en EMP.DEPTNO. Si no existe confusión posible pueden indicarse sin el nombre de la tabla, como por ejemplo DNAME, que sólo existe en la tabla DEPT.

Para evitar repetir continuamente el nombre de las tablas, se puede especificar un alias, añadiendo al nombre de la tabla en la cláusula from el alias.

A partir de la versión SQL 1999 se ideó una nueva sintaxis para consultar varias tablas. La razón fue separar las condiciones de asociación respecto de las condiciones de selección de registros. La sintaxis completa es:

```
SELECT      tabla1.column1,      tbl1.column2,...      tabla2.column1,
tabla2.column2,...
FROM tabla1
      [CROSS JOIN tabla2] |
      [NATURAL JOIN tabla2] |
      [JOIN tabla2 USING (columna)] |
      [JOIN tabla2 ON (tabla1.columa=tabla2.columna)] |
      [LEFT|RIGHT|FULL      OUTER      JOIN      tabla2      ON
(tbl1.colum=tbl2.column)]
```

- **CROSS JOIN.** Realiza un producto cruzado entre las tablas indicadas. Eso significa que cada tupla de la primera tabla se combina con cada tupla de la segunda tabla. Es decir si la primera tabla tiene 10 filas y la segunda otras 10, como resultado se obtienen 100 filas, resultado de combinar todas entre sí.

```
SELECT ENAME, DNAME
      FROM EMP CROSS JOIN DEPT
```

- **NATURAL JOIN.** Establece una relación de igualdad entre las tablas a través de los campos que tengan el mismo nombre en ambas tablas:

```
SELECT ENAME, DNAME  
FROM EMP NATURAL JOIN DEPT
```

En ese ejemplo se obtienen la lista de los empleados y los nombres de los departamentos a los que pertenecen a través de los campos que tengan el mismo nombre en ambas tablas. Hay que asegurarse de que sólo son las claves principales y secundarias de las tablas relacionadas, las columnas en las que el nombre coincide, de otro modo fallaría la asociación y la consulta no funcionaría.

- **JOIN USING.** Permite establecer relaciones indicando qué columna (o columnas) común a las dos tablas hay que utilizar. Las columnas deben de tener exactamente el mismo nombre en ambas tablas:

```
SELECT ENAME, DNAME  
FROM EMP JOIN DEPT USING (DEPTNO)
```

- **JOIN ON** Permite establecer relaciones cuya condición se establece manualmente, lo cual es útil para asociaciones cuyos campos en las tablas no tienen el mismo nombre:

```
SELECT ENAME, DNAME  
FROM EMP e JOIN DEPT d ON (e.DEPTNO=d.DEPTNO)
```

- **OUTER JOIN** Utilizando las formas vistas hasta ahora de relacionar tablas sólo aparecen en el resultado de la consulta filas presentes en las tablas relacionadas. Es decir en la consulta anterior sólo aparecen empleados relacionados con la tabla de departamentos. Si hay empleados que no están en departamentos, éstos no aparecen (y si hay departamentos que no están en la tabla de empleados, tampoco salen).

- Para solventar esto, se utilizan relaciones laterales o externas (outer join):
 - o `tabla1 LEFT OUTER JOIN tabla2 ON`. Obtiene los datos de la tabla1 estén o no relacionados con datos de la tabla 2.
 - o `tabla1 RIGHT OUTER JOIN tabla2 ON`. Obtiene los datos de la tabla2 estén o no relacionados con datos de la tabla 1.
 - o `tabla1 FULL OUTER JOIN tabla2 ON`. Obtiene los registros no relacionados de ambas tablas.

20.3.6 Subconsultas

Son sentencias SELECT que se encuentra anidadas dentro de otras SELECT. Estas sentencias se escriben entre paréntesis para advertir al gestor que se deben de ejecutar primero. Permite solucionar consultas que requieren para funcionar el resultado previo de otra consulta.

```
SELECT ENAME
FROM EMP
WHERE SAL >= (SELECT AVG(SAL) FROM EMP)
```

Da como resultado el listado de los empleados que superan la media de sueldo. Primero se realiza la operación del SELECT de la cláusula Where y seguidamente se ejecuta el SELECT del principio.

Una subconsulta que utilice los valores `>`, `<`, `>=`, ... tiene que devolver un único valor, de otro modo ocurre un error. Además tienen que tener el mismo tipo de columna para relacionar la subconsulta con la consulta que la utiliza (no puede ocurrir que la subconsulta tenga dos columnas y ese resultado se compare usando una sola columna en la consulta general).

La cláusula (NOT) EXISTS

La cláusula EXISTS (o NOT EXISTS) comprueba si una subconsulta devuelve algún valor (EXISTS) o no devuelve ninguno (NOT EXISTS). Por ejemplo:

“Lista los departamentos que no hayan contratado a nadie el 28 de diciembre de 2010”

```
SELECT D.DNAME
      FROM DEPT D
     WHERE NOT EXISTS
           (SELECT * FROM EMP E
            WHERE E.DEPTNO=D.DEPTNO
            AND HIREDATE ='28/12/2010')
```

La consulta de primer nivel busca en la tabla de departamentos los nombres y, para cada fila, comprueba —mediante la subconsulta— que para ese número de departamento no existan empleados que hayan sido contratados el 28 de diciembre de 2010.

Consulta con cuantificadores

Se denominan cualificadores a ciertos predicados que permiten utilizar subconsultas que devuelven varias filas en la columna correspondiente a un atributo.

Por ejemplo si se quiere mostrar el sueldo y nombre de los empleados cuyo sueldo supera al de cualquier empleado del departamento de ventas. La subconsulta necesaria para ese resultado mostraría todos los sueldos del departamento de ventas. Pero no podremos utilizar un operador de comparación directamente ya que esa subconsulta devuelve más de una fila. La solución a esto es utilizar los cuantificadores entre el operador y la consulta, que permiten el uso de subconsultas de varias filas.

La sintaxis de uso dentro de condiciones es la siguiente:

expresión operador_relacional cuantificador {lista_exps | subconsulta}

Los cuantificadores son:

- **ANY o SOME:** La comparación con un ANY (o SOME , equivalente) es verdadera si lo es para algún valor de los obtenidos con una subconsulta.
- **ALL.** En este caso la comparación es verdadera si lo es con todos los valores devueltos por la consulta subordinada y falsa en caso contrario. Por ejemplo: para saber el empleado con el sueldo más alto de toda la empresa.

```
SELECT ENAME  
FROM EMP  
WHERE SAL > = ALL(SELECT SAL FROM EMP)
```

20.3.7 Operaciones con consultas

Existen ciertos operadores que permiten combinar los conjuntos de tuplas que se obtiene de dos consultas SELECT y obtener un nuevo conjunto de tuplas. Estas operaciones corresponden con operadores del álgebra relacional y son los siguientes:

- UNION y UNION ALL realizan la unión de las tuplas obtenidas por dos consultas que se especifican como operandos. UNION no incluye las tuplas repetidas mientras que UNION ALL sí las incluye. UNION corresponde a la unión de relaciones del álgebra relacional.

Para ello ambas instrucciones tienen que utilizar el mismo número y tipo de columnas

```
SELECT nombre FROM empleados
```

UNION

```
SELECT nombre FROM visitantes
```

Esto crea una tabla que incluye los nombres de los empleados y visitantes

- INTERSECT permite unir dos consultas SELECT de modo que el resultado serán las filas que estén presentes en ambas consultas. Equivale al operador intersección del álgebra relacional.

```
SELECT tipo,modelo FROM productos  
WHERE chip="QWER-21"
```

INTERSECT

```
SELECT tipo,modelo FROM productos  
WHERE chip="WDFV-23"
```

- MINUS combina dos consultas SELECT de forma que aparecerán los registros del primer SELECT que no estén presentes en el segundo. Corresponde a la diferencia del álgebra relacional.

```
SELECT tipo,modelo FROM productos  
WHERE chip="QWER-21"
```

MINUS

```
SELECT tipo,modelo FROM productos  
WHERE chip="WDFV-23"
```

Las dos consultas sobre las que se aplique cualquiera de estos operadores deben devolver tuplas con la misma estructura.

20.4.- DCL. LENGUAJE DE CONTROL DE DATOS

Con el nombre de lenguaje de control de datos (DCL Data Control Language) se hace referencia a la parte del lenguaje SQL que se ocupa de los apartados de seguridad y de la integridad en el procesamiento concurrente.

20.4.1 Seguridad

El lenguaje SQL supone un nivel general de seguridad del software gestor de la base de datos y sus sentencias se utilizan para especificar restricciones de seguridad. El esquema de seguridad SQL se basa en tres conceptos:

- Los usuarios son los actores de la base de datos. Cada vez que el gestor de la base de datos recupera, inserta, suprime o actualiza datos, lo hace a cuenta de algún usuario.
- Los objetos de la base de datos son los elementos a los cuales se puede aplicar la protección de seguridad SQL. La seguridad se aplica generalmente a tablas, vistas y columnas
- Los privilegios son las acciones que un usuario tiene permitido efectuar para un determinado objeto de la base de datos.

La creación y eliminación de usuarios en SQL no es estándar, dependiendo de cada producto comercial. Sin embargo, la concesión y revocación de privilegios si es estándar y está recogida en las sentencias GRANT y REVOKE.

Concesión de privilegios: GRANT

La sentencia GRANT se utiliza para conceder privilegios de seguridad sobre objetos de la base de datos a usuarios específicos. Normalmente la sentencia GRANT es utilizada por el propietario de la tabla o vista para proporcionar a otros usuarios acceso a los datos. La sentencia GRANT incluye una lista específica de los privilegios a conceder, el nombre del objeto al cual se aplican los privilegios y la lista de usuarios a los cuales se conceden los privilegios. La sintaxis es la siguiente:

```
GRANT listaPrivilegios  
ON listaObjetos  
TO listaUsuarios  
[WITH GRANT OPTION]
```

- ListaPrivilegios: Se conceden todos (ALL) o un subconjunto de privilegios (separados por comas) que permiten borrar, insertar,

consultar, actualizar o modificar (DELETE, INSERT, SELECT, UPDATE, ALTER) una tabla, vista o un conjunto de ellas.

- ListaObjetos: Objetos a los que se le aplican los privilegios.
- ListaUsuarios: Se conceden a todos los usuarios (PUBLIC) o a una lista de usuarios.
- WITH GRANT OPTION: Indica que aquellos usuarios a los que se ha concedido estos privilegios pueden a su vez concederlos (nunca más de los que se tienen actualmente) a otros usuarios por medio de sentencias GRANT.

Por norma general los privilegios de acceso se aplican sobre todas las columnas en la tabla o vista, pero también se puede especificar una lista de columnas con el privilegio UPDATE.

GRANT UPDATE (SAL) ON EMP TO grupoNominas

Sólo el propietario de un objeto puede conceder los privilegios del mismo. El propietario es siempre el creador del mismo.

Las operaciones con el esquema de la base de datos (CREATE, DROP, etc.) sólo pueden ser realizadas por el propietario del esquema.

Revocación de privilegios: REVOKE

Los privilegios que se han concedido con la sentencia GRANT pueden ser retirados con la sentencia REVOKE. La sentencia REVOKE tiene una estructura que se asemeja estrechamente a la sentencia GRANT, especificando un conjunto específico de privilegios a ser revocados, para un objeto de la base de datos específico, para uno o más usuarios. Una sentencia REVOKE puede retirar todos o parte de los privilegios que previamente se han concedido a un usuario. Es necesario especificar que

un usuario sólo puede retirar los privilegios que él mismo ha concedido a otro usuario.

REVOKE ListaPrivilegios

ON ListaObjetos

FROM ListaUsuarios

La utilización de vistas combinada con una definición de usuarios y concesión juiciosa de privilegios constituye el mecanismo de seguridad que el administrador de la base de datos SQL utiliza para llevar a cabo las políticas de seguridad del sistema.

20.4.2 Transacciones

Se entiende por transacción el efecto producido por un grupo de instrucciones DML ejecutadas una tras otra, es decir, una transacción es un conjunto de acciones que o bien se realizan todas, o bien no se realiza ninguna.

En SQL una transacción comienza implícitamente en la primera instrucción que altera el estado de la información almacenada en la base de datos. Para preservar las propiedades ACID (Atomic, Consistent, Isolate, Durable) de una transacción, SQL dispone de dos sentencias que permiten que los cambios realizados por una transacción queden reflejados permanentemente en la base de datos (comprometer)

- COMMIT [WORK]. Termina la transacción actual grabando permanentemente las modificaciones.
- ROLLBACK [WORK]. Obliga al sistema a volver al estado anterior al inicio de la transacción.

También es posible que cada entorno de programación y/o SGBD disponga de elementos adicionales para el control de concurrencia que puedan ser utilizados por el usuario, como por ejemplo bloqueos.

Desde el momento en que a una base de datos pueden acceder diferentes usuarios al mismo tiempo, en cada instante podremos tener distintas transacciones que manipulen la base de datos a la vez.

Las transacciones especifican un nivel de aislamiento que define el grado en que se debe aislar una transacción de las modificaciones de recursos o datos realizadas por otras transacciones. En teoría, toda transacción debe estar completamente aislada de otras transacciones, pero en la realidad, por razones prácticas, esto puede no ser cierto siempre. Los niveles de aislamiento se describen en cuanto a los efectos secundarios de la simultaneidad que se permiten, como las lecturas desfasadas o ficticias.

El estándar SQL define cuatro niveles de aislamiento transaccional en función de tres eventos que son permitidos o no dependiendo del nivel de aislamiento. Estos eventos son:

- *Lectura sucia*. Las sentencias SELECT son ejecutadas sin realizar bloqueos, pero podría usarse una versión anterior de un registro. Por lo tanto, las lecturas no son consistentes al usar este nivel de aislamiento.
- *Lectura no repetible*. Una transacción vuelve a leer datos que previamente había leído y encuentra que han sido modificados o eliminados por una transacción cursada.
- *Lectura fantasma*. Una transacción vuelve a ejecutar una consulta, devolviendo un conjunto de registros que satisfacen una condición de búsqueda y encuentra que otros registros que satisfacen la condición han sido insertados por otra transacción cursada.

Los niveles de aislamiento SQL se definen en base a si permiten cada uno de los eventos definidos anteriormente.

Niveles de aislamiento:

Nivel de aislamiento	Comportamiento			
	Permitido	Lect. Sucia	Lect. No Repetible	Lect. Fantasma
Lectura confirmada	no	SI	SI	SI
Lectura confirmada		NO	SI	SI
Lectura repetible		NO	NO	SI
Serializable		NO	NO	NO

La sentencia para controlar el nivel de aislamiento en SQL es:

```
SET TRANSACTION ISOLATION LEVEL {READ UNCOMMITTED |READ
COMMITTED| REPEATABLE READ|SERIALIZABLE }
```

- **READ UNCOMMITTED.** Especifica que las instrucciones pueden leer filas que han sido modificadas por otras transacciones pero todavía no se han confirmado.
- **READ COMMITTED.** Especifica que las instrucciones no pueden leer datos que hayan sido modificados.
- **REPEATABLE READ.** Especifica que las instrucciones no pueden leer datos que han sido modificados pero aún no confirmados por otras transacciones y que ninguna otra transacción puede modificar los datos leídos por la transacción actual hasta que ésta finalice.
- **SERIALIZABLE.** Especifica que las instrucciones no pueden leer datos que hayan sido modificados, pero aún no confirmados, por otras transacciones. Ninguna otra transacción puede modificar los datos

leídos por la transacción actual hasta que la transacción actual finalice.

20.5.- BIBLIOGRAFÍA

- Connolly & Begg. (2005). Sistemas de bases de datos. Un enfoque práctico para diseño, implementación y gestión. Pearson Addison Wesley. Madrid.
- Kroenke. (2002). Procesamiento de Bases de Datos. Fundamentos, Diseño e Implementación. Octava Edición. Pearson. Prentice Hall.
- Piattiani, Esparza Marcos, Calero Coral & Vela Belen.(2007). Tecnología y diseño de Bases de Datos. AlfaOmega Ra-Ma. México.
- Silberschatz, Korth & Sudarshan. (2006). Fundamentos de Base de Datos. Mc Graw Hil. Quinta Edición. España.
- ANSI SQL: ISO/IEC 9075-1:2008

Autor: Francisco Javier Rodriguez Martínez

Subdirector de Sistemas Escola Superior Enxeñaría Informática Ourense

Colegiado del CPEIG

**21. SISTEMAS CRM (CUSTOMER
RELATIONSHIP MANAGEMENT)
Y ERP (ENTERPRISE
RESOURCE PLANNING).
LA INFORMATIZACIÓN DE LOS
PROCEDIMIENTOS. BPM
(BUSINESS PROCESS
MANAGEMENT). SISTEMAS DE
GESTIÓN DOCUMENTAL.
GESTIÓN DEL CONOCIMIENTO.**

Tema 21: CRM. ERP. BPM. Sistemas de Gestión Documental. Gestión del Conocimiento.

ÍNDICE

21.1. CRM.....	3
21.1.1. Definición de CRM (Customer Relationship Management).....	3
21.1.2. Principios de CRM.....	5
21.1.3. Historia de CRM.....	7
21.1.4. Proceso de Formación CRM.....	9
21.1.5. Evaluación del CRM	11
21.1.6. Consideraciones sobre la implementación de un CRM.....	12
21.2. ERP.....	13
21.2.1. Definición de ERP (Enterprise Resource Planning).....	13
21.2.2. Objetivos de la implantación de un ERP.....	15
21.2.3. Arquitectura de un ERP.....	15
Características de la arquitectura de un ERP.....	16
Modelo Cliente-Servidor.....	16
Flexibilidad.....	17
Modularidad.....	17
Integración.....	17
Seguridad.....	17
Interfaz de Usuario.....	18
Simulación.....	18
Trazabilidad.....	19
Intercambio electrónico de datos.....	19
21.2.4. Principales Módulos de un ERP.....	20
Ventas y Distribución (Logística).....	20
Producción y Fabricación.....	21
Contabilidad y Finanzas.....	21
Mantenimiento y Gestión de Proyectos.....	22
Recursos Humanos.....	22
21.2.5. Implantación.....	23
Problemas en la Implantación.....	24
Análisis Económico.....	25
21.3. BPM.....	26
21.3.1. Definición de BPM.....	26
21.3.2. Estructura del BPM.....	26
21.3.3. Objetivos de la aplicación.....	27
21.3.4. BPM y Workflow.....	27
21.3.5. BI x BPM.....	28
21.4. Sistemas de Gestión Documental.....	30
21.4.1. Definición de Sistemas de Gestión Documental.....	30
21.4.2. Funciones de la Gestión documental.....	32
21.4.3. Ciclo de Vida de los Documentos.....	32
21.4.4. Beneficios de la Gestión Documental.....	33
21.5. Gestión del Conocimiento.....	35
21.5.1. Definición de Gestión del Conocimiento.....	35

21.5.2. Cuestiones sobre gestión del conocimiento.....	36
21.6. Bibliografía.....	39

21.1. CRM

21.1.1. Definición de CRM (Customer Relationship Management)

Antes de comenzar a examinar los fundamentos conceptuales de CRM, es necesario definir que es CRM. Una estrecha perspectiva de la gestión de relaciones con los clientes es el marketing de bases de datos, haciendo hincapié en los aspectos promocionales del marketing vinculados a los esfuerzos de base de datos.

Otro estrecho y relevante punto de vista es considerar CRM sólo como la retención de clientes en el que se utiliza una variedad de tácticas de marketing para conseguir a los clientes o mantenerse en contacto con ellos después de que la venta se haya realizado.

Se puede definir el marketing relacional como *"un esfuerzo integrado para identificar, mantener y construir una red entre los consumidores particulares y fortalecer continuamente la red para el beneficio mutuo de ambas partes, a través de contactos interactivos, individualizados y de valor añadido en un período de tiempo"*.

El tema central de todos los CRM y las perspectivas de marketing de relaciones es que se centra en las relaciones de cooperación y de colaboración entre la empresa y sus clientes, e incluso con otros posibles actores de marketing.

CRM se basa en la premisa de que, al tener una mejor comprensión de las necesidades de los clientes y de sus deseos, podremos mantenerlos por más tiempo y venderles más.

Se han realizado una serie de un análisis estadísticos de los datos de satisfacción de clientes que abarcan los resultados de más de 20.000 encuestas a clientes realizadas en 40 países.

Las conclusiones de este estudio fueron:

- i. Un cliente totalmente satisfecho contribuye 2,6 veces más a los ingresos de la empresa que un cliente poco satisfecho.
- ii. Un cliente totalmente satisfecho contribuye con un 17 veces más ingresos que un cliente algo insatisfecho.
- iii. Un cliente totalmente insatisfecho reduce los ingresos en una tasa igual a 1,8 veces lo que un cliente totalmente satisfecho contribuye a una empresa.
- iv. El reducir la deserción de clientes (por lo menos en un 5%) se traducirá en aumento de los beneficios en un 25% a 85%, dependiendo del tipo de industria de que se trate.

Un aspecto importante del CRM es la selección de los clientes. Como varios estudios han demostrado, no todos los clientes son igual de rentables (de hecho, en algunos casos el 80% de las ventas vienen a través de un 20% de los clientes). La empresa por lo tanto, debe ser selectiva y adaptar sus programas y esfuerzos de marketing a la segmentación y selección de los clientes apropiados.

En algunos casos, podría incluso llevarse a cabo la "*subcontratación de algunos clientes*" para que la empresa emplee mejor sus recursos en aquellos clientes que pueden servir mejor y crear valor mutuo. Sin embargo, el objetivo de una empresa no es menguar su base de clientes, sino identificar los programas apropiados para los clientes, los métodos que sean rentables y crear valor para la empresa y el cliente. Por lo tanto, el CRM se define como:

"Una estrategia integral y un proceso de adquisición, retención y asociación con los clientes selectivos para crear un valor superior tanto para la empresa como para el cliente."

Como está implícito en la definición anterior, con el propósito de CRM es mejorar la productividad del marketing. La productividad del marketing se logra mediante una eficiencia cada vez mayor en la comercialización y por la mejora de la eficacia del marketing.

En CRM, la eficiencia del marketing se logra gracias a los procesos de cooperación y colaboración lo que permitirá reducir los costes de transacción y los costes generales de desarrollo para la empresa. Dos importantes procesos de CRM son el desarrollo proactivo del negocio del cliente y la construcción de relaciones con la mayoría de los clientes importantes. Estas situaciones conducen a la creación de un valor superior.

El concepto básico es que el cliente no es alguien fuera de la organización sino que es una parte de la organización.

21.1.2. Principios de CRM

Diferenciar a los clientes:

- No todos los clientes son iguales.
- Es importante reconocer y premiar a los mejores clientes.
- Cada cliente se vuelve particularmente importante.
- Para el mismo producto o servicio no todos los clientes pueden ser tratados por igual y el CRM de saber distinguir entre un cliente de alto valor y un cliente de bajo valor.

Para diferenciar a los clientes es necesario que el CRM entienda a los clientes en los siguientes aspectos:

- Sensibilidad, gustos, preferencias y personalidades.

- Estilo de vida y edad.
- Nivel de cultura y educación.
- Características físicas y psicológicas.

Hay que diferenciar los distintos tipos de situaciones:

- i. Clientes de bajo valor que requieren una gran inversión.
- ii. Clientes de bajo valor con potencial de convertirse en clientes con alto valor en un futuro próximo.
- iii. Clientes de alto valor que requieren de servicios de alto valor.
- iv. Clientes de alto valor que requieren de servicios de bajo valor.

Mantener los clientes existentes:

Establecer una clasificación de los clientes entre, *muy satisfechos* y *muy decepcionado* ayuda a la organización a mejorar los niveles de satisfacción de los clientes y los resultados que se ofrecen. A medida que el nivel de satisfacción de cada cliente mejorar, también mejorará la permanencia de los clientes con la empresa.

- *Maximizar el valor de tiempo:* Si se consigue identificar circunstancias como la etapa de la vida o el evento que ha desencadenado la necesidad en el cliente, los vendedores pueden maximizar la probabilidad de realizar una venta.
- *Aumentar la lealtad:* Los clientes leales son más rentables. Hay que innovar y satisfacer las necesidades de sus clientes, para que permanezcan como vinculados a la empresa.

21.1.3. Historia de CRM

Mirando hacia atrás en la historia de una instantánea de marketing, podemos ver la siguiente evolución y clara progresión:

- 1960: la era del marketing masivo.
- 1970: comienzo de la segmentación, campañas de correo directo y telemarketing.
- 1980: expansión del marketing Niche (localizar un pequeño segmento del mercado y crear un producto o servicio para ese segmento).
- 1990: marketing Relacional. La explosión de los centros de telemarketing. Desarrollo de las relaciones con los clientes. Reconocimiento del verdadero valor de la lealtad.

El desarrollo de la relación con el cliente tiene antecedentes históricos que se remontan a la era industrial, del mismo modo que los artesanos a menudo desarrollaban productos a medida para cada cliente. Esta interacción directa condujo a la vinculación relacional entre el productor y el consumidor.

En la era industrial, con la producción masiva y la llegada de los intermediarios no había interacciones frecuentes entre los productores y los consumidores. En los últimos años sin embargo, varios factores han contribuido al rápido desarrollo y evolución de CRM. Estos incluyen:

- El creciente proceso de des-intermediación en muchas industrias debido a la aparición de novedosas tecnologías informáticas que permiten a los productores interactuar directamente con los clientes finales. Por ejemplo, en muchas industrias, tales como aerolíneas,

software del hogar e incluso de consumo, el proceso de intermediación está cambiando rápidamente la naturaleza del marketing y volviendo el marketing relacional mucho más popular.

- Los avances en la tecnología de la información, redes y tecnologías de fabricación han ayudado a las empresas a ponerse a la par de la competencia. Como resultado la calidad del producto y el coste ya no son importantes ventajas competitivas.
- El crecimiento de la economía de servicios. Dado que los servicios suelen ser producidos y entregados en la misma institución, se minimiza el papel de los intermediarios.
- Otra fuerza impulsora de la adopción de CRM ha sido el movimiento de calidad total. Cuando las empresas adoptaron el TQM se hizo necesaria la participación de clientes y proveedores en la ejecución del programa a todos los niveles de la cadena de valor. Esto necesita una estrecha relación de trabajo con los clientes.
- Las expectativas de los clientes están cambiando casi a diario. Los clientes ahora eligen la forma de comunicarse con las empresas a través de diversos canales disponibles. También hoy en día los consumidores esperan un alto grado de personalización.
- Importancia del tiempo real. Los canales interactivos como el correo electrónico, cajeros automáticos y centros de llamadas se deben sincronizar con las actividades del cliente. La velocidad del cambio de los negocios, requieren flexibilidad y una rápida adopción de las tecnologías.
- En la actual era de la competencia, los comerciantes se ven obligados a estar más preocupados por la retención de clientes y fidelización de clientes.

- Como varias investigaciones han descubierto retener a los clientes es menos costoso y es, de hecho, una ventaja competitiva sostenible mayor que la adquisición de otros nuevos.
- Es más ventajoso desarrollar relaciones más estrechas con unos pocos proveedores que desarrollar más proveedores con relaciones más impersonales.
- Además los vendedores se preocupan de mantener al cliente durante un largo periodo en lugar de por una venta esporádica.
- La globalización de los mercados mundiales hace que sea necesaria la gestión de cuentas globales para los clientes.

21.1.4. *Proceso de Formación CRM*

En el proceso de formación, las tres áreas de decisión más importantes son:

- La definición del propósito que se tiene para (u objetivos) usar un CRM.
- La elección de las partes (o parejas de los clientes) para los programas de CRM apropiados.
- El desarrollo de programas (o esquemas relacionales de actividad) para la participación de relación con el cliente.

Propósito de CRM

El objetivo general de CRM es mejorar la productividad del marketing y mejorar el valor para los partes que participan en la relación. Al perseguir y conseguir los objetivos operacionales, tales como la reducción de los costes de distribución, la racionalización del procesamiento de pedidos, la gestión de inventario, la reducción del coste de adquisición de clientes y la retención de clientes, las empresas podrían lograr una mayor eficiencia de marketing.

Se puede mejorar la efectividad del marketing con:

- Una cuidadosa selección de los clientes para sus distintos programas.
- La individualización y la personalización de la oferta de mercado para anticipar y satisfacer las necesidades emergentes de los clientes.
- La construcción de la lealtad y el compromiso del cliente.
- La asociación para entrar en nuevos mercados y desarrollar nuevos productos.
- La redefinición del campo de juego competitivo para la empresa.

De este modo, indicando los objetivos y definiendo el propósito del CRM en una empresa, ayuda a aclarar la naturaleza de los programas de CRM y las actividades que debe llevarse a cabo por los socios.

La definición del propósito también ayudará en la identificación de los socios adecuados, relacionando las expectativas y capacidades necesarias para cumplir con las metas comunes. Además, la definición del propósito ayudará a evaluar el desempeño del CRM mediante la comparación de los resultados obtenidos con los objetivos. Estos objetivos pueden ser especificados como objetivos financieros, objetivos de marketing, objetivos estratégicos, objetivos operativos, y los objetivos generales.

Partes de la relación

En la fase inicial, una empresa tiene que decidir qué tipo de clientes, de clientes específicos o de grupos de clientes serán el foco de sus actividades de CRM.

Programas CRM

Una revisión cuidadosa de la literatura y la observación de las prácticas empresariales sugieren que hay tres tipos de programas de CRM:

- Marketing continuo
- Marketing uno a uno
- Programas de asociación.

Estas adoptan diferentes formas dependiendo de si están destinados a los consumidores finales, a consumidores-distribuidores o clientes empresa-a-empresa.

21.1.5. *Evaluación del CRM*

Sin las medidas de rendimiento adecuados para evaluar los esfuerzos de CRM es difícil para tomar decisiones objetivas respecto a la continuación, modificación, mejora o finalización de los programas de CRM.

Si la relación con los clientes es tratada como un activo intangible de la empresa, su valoración económica puede ser evaluada utilizando los flujos de efectivo futuros.

Otra de las medidas globales que utilizan las empresas para supervisar el rendimiento de CRM es la medición de la satisfacción de la relación con el cliente.

Mediante la medición de satisfacción de la relación, se podría estimar la tendencia de inclinación de cualquiera de las partes de continuar o terminar la relación. Esta tendencia también podría ser estimada indirectamente mediante la medición de la lealtad del cliente.

21.1.6. Consideraciones sobre la implementación de un CRM

Uno de los aspectos más interesantes del desarrollo de CRM es la multitud de interfaces de cliente que tiene una empresa para gestionar actualmente. Hasta hace poco, la interfaz directa de la empresa con los clientes era principalmente a través del personal de ventas o agentes de servicio.

En el entorno actual la mayoría de las empresas interactúan con sus clientes a través de una gran variedad de canales, incluyendo personal de ventas, personal de servicio, centros de atención telefónica, páginas de Internet, cuentas en redes sociales, departamentos de marketing, etc. Para grandes clientes también se incluyen funciones cruzadas, esto es, equipos que pueden incluir al personal de varios departamentos funcionales. Aunque cada una de estas unidades puede funcionar de manera independiente, comparten información acerca de clientes individuales y sus interacciones con la empresa en tiempo real. Por ejemplo, un cliente que acaba de realizar un pedido a través Internet y, posteriormente, llama al centro de llamadas para la verificación de pedidos, espera que el personal del centro de llamadas conozca los detalles de la historia de su orden.

Por lo tanto, CRM eficaz requiere de un sistema de información de primera línea que comparta información relevante de los clientes entre todos los departamentos funcionales. Las bases de datos y las herramientas de minería de datos son muy valiosos tanto para los sistemas de CRM.

Sin embargo, el desafío consiste en desarrollar una plataforma CRM integrada que recoja los datos de entrada correspondientes a cada interfaz de cliente y al mismo tiempo ofrezca la información adecuada acerca de la estrategia precisa para ganar la lealtad de dicho cliente. Por ejemplo, si el personal del centro de llamadas no puede identificar o

diferenciar un cliente de alto valor, entonces sería una tremenda pérdida de oportunidad para la compañía.

21.2.ERP

21.2.1. Definición de ERP (Enterprise Resource Planning)

Actualmente, en la sociedad de la información, el activo más importante para una empresa es la información. Los procesos o sistemas que se emplee en cada empresa y cómo se trabaje con esa información, es lo que distinguirá a unas empresas de otras y hará que las empresas consigan o no beneficios. Por lo tanto, es obvio, que es fundamental para una empresa el tener unos sistemas de tratamiento de información actualizados y modernos que ayuden en los procesos de negocio, a reducir tiempos, a disminuir costes, etc.

En las Pymes, se suelen usar distintos sistemas software para automatizar distintas tareas y funciones por separado. Aunque esto no se considera realmente eficiente. Para resolver los problemas que pueden existir por la mala comunicación de los distintos sistemas, surgen los Sistemas de Gestión Empresarial o ERP (Enterprise Resource Planning), que se puede definir como *un paquete de software que integra toda la gestión de la empresa* (financiera, de producción, logística, comercial y de recursos humanos). Los ERP están diseñados para modelar y automatizar la mayoría de los procesos básicos de la empresa, desde la gestión financiera hasta la producción en un único sistema de información.

Los ERP son **sistemas transaccionales**, es decir, están diseñados para trabajar con procesos de la empresa, soportarlos, procesar los datos y obtener de ellos información específica.

Un ERP permite gestionar de manera eficiente e integrada la información de la empresa, permitiendo la comunicación de las diferentes áreas del negocio mediante procesos electrónicos. La función principal de un ERP es estandarizar y organizar los datos internos y procesos de la empresa, convirtiéndolos en información útil para el proceso de toma de decisiones. Con todo, es necesario tener en cuenta que aunque estos sistemas apoyan el proceso de toma de decisiones, la decisión final es de los administradores que son los que tienen la responsabilidad final de hacer lo más adecuado para la empresa en cada momento.

Algunas de las principales características de un ERP son:

- Integrables
- Interfaces con otras aplicaciones
- Modulares
- Multiplataforma
- Optimizan las operaciones de las empresas, permitiéndoles evaluar, implementar y gestionar más fácilmente su negocio
- Sistemas abiertos
- Universales

Los sistemas ERP actualmente ya se usan en todo tipo de empresas, ya sean grandes o de pequeño tamaño, sin embargo, al principio los sistemas ERP sólo se usaban en grandes empresas con múltiples fábricas y socios alrededor del mundo. En estas grandes empresas los sistemas ERP empleaban diferentes lenguajes, tipos de moneda y soportaban operaciones tanto centralizadas, como descentralizadas o multi-sitio.

Un sistema ERP es un tipo de software que permite compañía integrar los procesos de negocio de una empresa, acceder a la información en tiempo real y producir y compartir datos.

21.2.2. Objetivos de la implantación de un ERP

Al decidir implantar un ERP, se suele hacer con alguno o varios de los siguientes objetivos:

- Conseguir un alto grado de integración de datos.
- Conseguir acceso a información precisa y confiable. El tener toda la información centralizada bajo un mismo sistema garantiza que los datos serán correctos.
- Optimización de los procesos empresariales. Un proceso empresarial es una actividad que ofrece una serie de salidas con cierto valor añadido a partir de unas entradas. Al implantar un ERP se pretende mejorar estos procesos disminuyendo los costes de los mismos y aumentando la productividad.
- Posibilidad de compartir información entre todos los componentes de la organización. Con un ERP la información está disponible para todos y se elimina la redundancia de los datos.
- Supresión de datos y operaciones innecesarias. Al tener la información compartida, las operaciones como la búsqueda de datos a través de los diferentes sistemas dejan de ser necesarias.
- Reducción de tiempos y costes de los procesos.

21.2.3. Arquitectura de un ERP

Generalmente la arquitectura de los ERP suelen coincidir en los siguientes aspectos:

- Base de datos común que favorece la coherencia de datos y la integración de los datos generados.
- Arquitectura modular. Cada módulo se centra en un proceso diferente de la empresa como recursos humanos, ventas, producción, etc.

- Interconexión de módulos.

Los ERP al ser modulares permiten que la implantación del sistema se realice por etapas, de tal forma que el impacto en la organización es menor, de cada a una transacción con respecto al sistema anterior. Generalmente al implantar un ERP se empieza por el departamento financiero y poco a poco se van integrando los otros departamentos.

La arquitectura básica de un ERP se compone de:

- Aplicaciones técnicas.
- Arquitectura para dar soporte al resto de módulos.
- Herramientas de administración para todo el sistema.

Cada proveedor de un sistema ERP define el nivel de modularidad de su producto, no existiendo un estándar global. De hecho cada proveedor en función de su política comercial o técnica decide qué módulos desarrolla y cómo los va a integrar.

Características de la arquitectura de un ERP

Modelo Cliente-Servidor

Los ERP siguen un modelo cliente-servidor, donde dicho servidor almacena los datos de los que hacen uso los distintos programas.

El servidor debe permitir:

- Autorización de privilegios de cada cliente.
- Autenticación de la identidad del cliente.
- Privacidad y seguridad de los datos.
- Protección de los recursos de red.

Flexibilidad

El software del ERP debe ser flexible y:

- Incorporar un sistema de configuración.
- Permitir adaptarse a las necesidades de la empresa.

Modularidad

Un ERP se divide en una serie de módulos que se caracterizan por:

- Presentan una interfaz común.
- Cada módulo implementa la funcionalidad de un área en concreto.
- Los módulos deben ser fácilmente integrables entre si.
- Facilidad en el aprendizaje y reducción del coste. Al tratarse de sistemas modulares y manejarse estos de forma similar, la formación del personal es más rápida.

Integración

En un ERP se tiene una base de datos común que garantiza la integridad de los datos y elimina la redundancia. De esta forma la empresa se ve como un único sistema donde la información que se actualice en un punto, quedará actualizada para el resto de dicho sistema.

Seguridad

De cara a un sistema ERP podemos considerar dos tipos de seguridad:

1. Privilegios de acceso a la aplicación: los usuario ejecutarán únicamente aquellas aplicaciones que sean imprescindibles para su trabajo y ninguna más.
2. Privilegios de acceso a datos: estarán gestionados por los SGBD o directamente por la aplicación. Un SGBD tiene como objetivo

garantizar que los datos que contiene sólo estén disponibles para las personas autorizadas.

Para garantizar la seguridad se utilizan algunas o varias de estas técnicas:

- Identificación de usuario. Al identificar al usuario se obtiene la lista de recursos del sistema a los que dicho usuario tiene acceso además de qué operaciones puede realizar sobre dichos recursos.
- Determinación de accesos permitidos.
 - o Lista de autorizaciones que identifican los datos accesibles y las operaciones posibles sobre los mismos.
 - o Establecimiento de distintos niveles de autorización, de tal forma que todos los usuarios de un grupo o nivel podrán realizar las mismas operaciones.

Interfaz de Usuario

La interfaz permite la comunicación entre el usuario y el sistema. Existen dos tipos de interfaces de usuario.

- Interfaz gráfica. La interfaz gráfica ofrece un acceso homogéneo a todos los módulos del sistema.
- Interfaz por consola (basada en comandos). La interacción se basa en una serie de órdenes que se transmiten entre el usuario y el sistema mediante un teclado.

Simulación

Mediante la simulación se puede saber cuales serán las consecuencias de una decisión, lo cual es de gran valor para saber si se debe o no adoptar esa decisión.

La simulación se suele emplear en:

- *Planificación financiera:* se pueden obtener los gráficos de los efectos de los planes de producción. Se pueden realizar informes sobre la previsión de stock o hasta qué punto se cubren costes.
- *Costes de actividad:* se pueden calcular las consecuencias de un posible cambio en el sistema.
- *Planificación de las necesidades materiales:* se pueden simular flujos de bienes para decidir qué artículos se deben fabricar, cuales adquirir, etc.
- *Plan de producción:* se pueden obtener distintos planes de producción de distintos productos para evaluar la viabilidad de los mismos.
- *Planificación de las necesidades de capacidades:* se pueden simular las consecuencias de retrasos, trabajar con prioridades, inclusión de trabajo atrasado en un momento puntual, etc.

Trazabilidad

En un sistema, se trata de poder determinar qué componentes participan en la elaboración de los productos finales y seguir el procesos de forma recursiva, determinando el origen de las materias primas, centros de trabajo y operarios que han participado en el proceso.

En caso de un producto defectuoso, la trazabilidad permite detectar el punto donde se ha producido el error y depurar responsabilidades.

Intercambio electrónico de datos

El EDI permite establecer comunicación entre los socios de forma electrónica, enviándose pedidos, facturas, etc. De esta forma se simplifica enormemente el hecho de gestionar múltiples instalaciones de una misma empresa.

21.2.4. Principales Módulos de un ERP

Los ERP se componen de una serie de módulos que se corresponden con las distintas áreas funcionales de la empresa. El tipo, funcionalidad y extensión de los módulos de los distintos ERP son distintos, aunque generalmente todos los ERP contienen los módulos básicos para el funcionamiento y gestión de la empresa.

De forma general los módulos cumplen con las siguientes características:

- Integración con el resto de los módulos.
- Implantación en el departamento donde se necesite.
- Autonomía propia.

Aunque la implantación de un ERP puede realizarse de forma modular, la implantación de un conjunto de módulos incrementa de forma notable el éxito de un ERP empresarial.

A continuación se comentarán las características de los principales módulos presentes en un ERP.

- Ventas y Distribución (Logística)

Este módulo permite llevar a cabo las actividades de venta y distribución de los productos. Mediante las funciones de ese módulo se puede:

- Información sobre las cuentas de los clientes
- Información sobre los pedidos y su estado
- Información sobre las facturas pendientes
- Control de calidad
- Administración de ventas
- Gestión de sistemas de transporte
- Control de calidad

- Gestión de compras
- ...

Producción y Fabricación

Los ERP implementan módulos de producción y fabricación que permiten emplear distintos métodos o estrategias de producción en diferentes ambientes, como son:

- Just In Time
- Bajo stock
- Contra pedido
- Proyectados
- Procesos

Dentro del módulo de producción, se permiten las siguientes funcionalidades:

- Planificar la producción
- Gestión de las órdenes de producción
- Gestión de costes
- Análisis de la producción
- Control de la producción

Contabilidad y Finanzas

Se trata de un módulo muy importante, que ofrece gran cantidad de informes sobre la situación económica de la empresa.

Este módulo se encarga, entre otras, de operaciones relacionadas con:

- *Gestión de Cuentas*: se puede realizar un control completo tanto de los pagos como de los cobros pendientes, la gestión de caja y abonos.
- *Costes de actividad*: se puede realizar un control de gastos de cada actividad.

- *Contabilidad general*: se pueden realizar todas las operaciones que de otra forma deberían realizarse manualmente, así como los cierres de fin de mes y anual.
- *Costes de recursos*: se pueden tratar los gastos generales directos mejorando estimación de los costes.
- *Tesorería*: se pueden realizar todas operaciones básicas de pagos y cobros.
- *Gestión de Nóminas*: se pueden automatizar todas las tareas relacionadas con las nóminas. Cálculo de impuestos, pagos a la Seguridad Social, horas extra, etc.
- *Gestión de contratos*: incluyen todas las actividades relacionadas con:
 - o Auditoria de contratos.
 - o Definición de contratos.
 - o Confección de informes.
 - o Calculo de costes actuales y proyectados
 - o Progreso de la facturación.

Mantenimiento y Gestión de Proyectos

Este módulo ayuda a optimizar la producción y en la mayoría de los casos se incluye en el módulo de logística. En este módulo se incluyen:

- Gestión del mantenimiento y servicios
- Seguimiento y control de proyectos.

Recursos Humanos

En este módulo se integran las herramientas para obtener un conocimiento del entorno económico y administrativo del personal. Las acciones que se realizan habitualmente con este módulo son las relacionadas con:

- Estadísticas de personal
- Generación de Nóminas

- Planificación de turnos y gestión de tiempos
- Perfiles profesionales de los trabajadores
- Formación y desarrollo

21.2.5. *Implantación*

La implantación de un sistema ERP suele ser compleja y costosa por la cantidad de recursos que engloba y sus requisitos a nivel técnico y organizativo.

La implantación de un sistema ERP puede significar importantes cambios en los procesos internos, que pueden tener repercusión tanto en la estructura organizativa como en las actividades y los puestos de trabajo de la empresa. Por esto, para reducir los problemas derivados de la implantación es fundamental que la formación de los empleados de la organización sea muy buena ya que se van a convertir en los usuarios del sistema, además estos deben participar activamente en todo el proceso de implantación y adaptación de la herramienta.

La implantación de un ERP se inicia con un análisis técnico y funcional, y con una evaluación de las restricciones económicas y temporales que pueden influir en la ejecución del proyecto. En un primer momento se deben analizar los distintos ERP disponibles en el mercado e identificar cual se ajusta más a las necesidades de la empresa.

Por tanto, en esta primera etapa de la implantación hay que definir:

- Qué módulos se van a implantar (Alcance funcional)
- Qué departamentos y procesos se verán afectados (Alcance organizativo)
- Viabilidad del proyecto considerando:

- o Presupuesto disponible
- o Integración con otras plataformas y sistemas
- o Calendario de implantación

Factores de éxito

Para tener éxito en la implantación del ERP es necesario considerar una serie de factores determinantes, como son:

- Tener una clara definición de los objetivos
- La empresa debe estar comprometida e informada del cambio en todos los departamentos y jerarquía de la empresa
- Realizar una planificación realista de la implantación a todos los niveles
- Formación y soporte a los usuarios
- Buena documentación del sistema
 - o Técnica
 - o Procedimientos
 - o Usuario

Una vez implantado el ERP el trabajo no finaliza, sino que debe considerarse también el mantenimiento, actualización, cambios en el entorno legal, aparición de nuevos estándares, incorporación de nuevos módulos, etc.

Problemas en la Implantación

Un sistema ERP ofrece muchas ventajas a una empresa, pero siempre teniendo en cuenta el esfuerzo necesario y los requisitos para su implantación, no solo a nivel económico sino técnico y de personal.

Una implantación de ERP puede fallar, los principales motivos por los que esto sucede suelen ser algunos de los siguientes:

- Insuficiente formación de los usuarios
- Poca vinculación de todas las áreas de la empresa con el proyecto
- La información es inexacta o incompleta al iniciar la implantación del nuevo sistema
- Cambio en la administración de la empresa mientras se está produciendo la implantación
- Mala elección de una herramienta ERP

Análisis Económico

Uno de los aspectos de mayor influencia a la hora de implantar un ERP es el económico. Dentro del análisis económico es necesario tener en cuenta:

- Equipamiento hardware y software necesario: identificar el hardware y software mínimo para la implantación del sistema, tanto a nivel de cliente como de servidor.
- Licencias del ERP: algunos sistemas de ERP son software libre y otras soluciones son propietarias, es necesario considerar el coste de estas licencias y el tipo de tarifa que se vaya a aplicar, por número de usuarios, intervalo temporal, etc.
- Formación del personal y consultoría externa para la implantación.
- Gastos de mantenimiento del sistema ERP.
- Costes de los servicios de telecomunicaciones.

21.3. BPM

21.3.1. Definición de BPM

El Business Process Management o BPM surgió en Estados Unidos y empezó siendo usado principalmente por empresas interesadas en nuevas herramientas para la implementación y el control de estrategias. BPM apareció a partir del auge que tuvo la integración de los ERP en las grandes empresas privadas.

El propósito de BPM es controlar cómo todos los recursos de la empresa, físicos, humanos, financieros y tecnológicos, participan y se integran en las acciones operacionales que llevan hacia las metas organizacionales a partir de la definición de prioridades.

BPM permite realizar una gestión global de los procesos incluyendo su definición, análisis, ejecución, seguimiento y administración; además da soporte para la interacción entre personas y distintas herramientas informáticas.

La meta de un sistema BPM es tener un registro de los procesos corporativos y mejorar tanto la productividad como la eficiencia. Las herramientas BPM por lo tanto, son aplicaciones que evalúan, analizan y optimizan la gestión de los procesos y por lo tanto, la gestión global del negocio.

21.3.2. Estructura del BPM

Un sistema BPM debe dar soporte a las actividades básicas de la gestión de una empresa, como son:

- Definir una estrategia para guiar el rendimiento.
- Traducir esta estrategia en indicadores, objetivos y metas.
- Guiar el progreso en relación con las metas.

- Seleccionar e implantar acciones correctivas.

Los sistemas BPM ayudan a la empresa a realizar un mejor control de sus propios procesos, a modificarlos cuando es necesario y a realizar las tareas importantes con mayor eficiencia. Este tipo de sistemas permite al usuario tener un mayor control sobre la automatización de procesos.

21.3.3. Objetivos de la aplicación

El objetivo de un sistema BPM no es rehacer sistemas heredados, sino automatizar flujos de trabajo, para que se realicen de forma más rápida y simple.

Otro aspecto relacionado directamente con el BPM es la necesidad de reducir el ciclo de integración. La mayoría de las empresas ya tienen sus sistemas montados, con mayor o menor nivel de complejidad. Las herramientas BPM extraen de los sistemas existentes las actividades que forman parte de los procesos, además de complementar y supervisar dichas aplicaciones instaladas.

Después de haber sido identificadas, estas actividades son almacenadas en un repositorio de procesos, así, cuando la empresa decide cambiar o elaborar un nuevo proceso, el BPM analiza su repositorio y emplea un modelo existente, lo cual elimina la necesidad de una personalización extrema de las aplicaciones, lo que repercute en el tiempo de trabajo y costes.

21.3.4. BPM y Workflow

El BPM surge a partir de los sistemas de Workflow, que aparecieron a final de la década de los 80. Este tipo de herramienta consiste en un conjunto de soluciones software donde se incluyen todos los procesos que se necesitan para administrar el rendimiento de la empresa, las metodologías que guían a algunos procesos y los indicadores empleados para evaluar el rendimiento, teniendo en cuenta los objetivos operacionales y estratégicos. A pesar del hecho de que el origen de BPM lo podemos encontrar en workflow, su intención no es la de sustituir a otros programas software.

Los sistemas de workflow tenían su base en la automatización del flujo de trabajo, por su parte el BPM permite que los usuarios reciban las tareas que tienen que realizar junto con sus instrucciones en sus sistemas personales. Además BPM permite realizar representaciones gráficas de todos los tipos de trámites, flujos y posibles desvíos, incluyendo separación de documentos, flujos alternativos, etc.

Las herramientas de Workflow tendían a usar cada una su propia notación gráfica, sin embargo las herramientas BPM, gracias a la notación definida por la Business Process Management Iniciativa, suele emplear una notación común, lo que simplifica mucho los procesos de formación de los usuarios.

Los sistemas de Workflow no incorporaban las operaciones que se realizaban en sistemas externos a ellos, sin embargo, gracias a la evolución en las tecnologías de integración de sistemas, el BPM permite realizar, además de lo que hacían los sistemas Workflow, una transferencia de datos entre sistemas para que se puedan desempeñar tareas automáticamente en sistemas externos y obtener los resultados de dichas acciones.

21.3.5. BI x BPM

Aunque BPM no es una herramienta estrictamente estratégica, como las soluciones de Business Intelligence (BI), cuyo propósito es la ayuda en la toma de decisiones, BPM puede coordinarse perfectamente con este tipo de herramientas e incluso suplir algunas de sus carencias. A pesar de todo es importante tener en cuenta que son dos tipos de herramientas distintas con propósitos diferentes.

BPM se orienta al ajuste de la operación y de las decisiones estratégicas de una empresa. Las herramientas de BI por su parte, al menos las tradicionales, se orientan más a realizar un seguimiento de lo que ya ha sucedido en la empresa. Estas soluciones de BPM trabajan con una visión más amplia de la empresa que el BI, que se orienta a un ámbito departamental.

BPM tiene un enfoque hacia la oportunidad y es proactivo, además de incorporar y analizar información y alertas en tiempo real; por su parte BI es reactivo y opera con informaciones históricas de la empresa.

BPM se centra en el control de las actividades que han sido identificadas para un proceso, las cuales generarán datos e informaciones que deben ser estudiados y consolidados como indicadores, que es lo que emplean las herramientas de BI, junto con otros datos, para producir informes de apoyo a la toma de decisiones.

Las soluciones BI se orientan a analizar el rendimiento y actuación actual y pasado de la empresa, mientras que el BPM se orienta hacia la evaluación de la situación actual y futuro, siendo por tanto, herramientas complementarias .

Por lo tanto, queda claro que BI y BPM son conceptos distintos y complementarios.

21.4. SISTEMAS DE GESTIÓN DOCUMENTAL

21.4.1. Definición de Sistemas de Gestión Documental

Un sistema de gestión documental se define como un conjunto de elementos y relaciones entre ellos, que tiene el propósito de normalizar, controlar y coordinar todas las actividades y procesos que afectan en cualquier medida a los documentos generados en el transcurso de la actividad de una organización. Las operaciones más habituales que se realizan sobre estos documentos, abarcan todo su ciclo de vida, desde su creación hasta su almacenamiento y puesta a disposición de los usuarios.

Además, un sistema de gestión documental tiene que satisfacer lo siguiente:

- Conservar los atributos básicos de los documentos, que les confieren su valor informativo, legal y probatorio.
 - o Originalidad
 - o Autenticidad
 - o Integridad
 - o Veracidad
- Mantener la organización de los documentos integrados en un contexto. Esto implica conservar una interrelación con los otros documentos que surgen de la misma función, actividad, que son producidos por el mismo departamento u organismo, que forman parte de la misma serie, etc.

Software de gestión documental

El software de gestión documental abarca todos aquellos programas software diseñados para gestionar grandes cantidades de documentos. En

estos documentos no necesariamente debe existir organización dentro de sus contenidos, de hecho, lo más común es que el contenido de estos documentos no guarde una organización clara.

Existen diversos métodos que usados en combinación con las bibliotecas de documentos y una serie de índices, permiten un acceso rápido a la información almacenada en dichos documentos, los cuales, habitualmente se encuentran comprimidos y suelen almacenar, además del texto plano, otros contenidos multimedia como imágenes, videos, etc.

Entre los objetivos que se persiguen a la hora de implantar un sistemas de gestión documental cabe mencionar:

- Resaltar la importancia que tienen los documentos dentro de cualquier tipo de organización, pública o privada.
- Facilitar la recuperación de información de forma rápida, exacta y efectiva.
- Analizar la producción documental, para evitar documentos innecesarios o que no merece la pena almacenar pasado cierto tiempo.
- Conseguir que los archivos sean útiles y significativos como unidades de información no sólo dentro de la empresa sino también externamente.

Antes de montar un sistema de gestión documental es necesario realizar una serie de consideraciones previas que podemos agrupar en las siguientes categorías:

- Administrativas: se centra todo lo que puede influir en la administración de la empresa.
- Económicas: se refiere a la evaluación del ahorro que genera la gestión de documentos.

Para la implantación de este tipo de sistema, es necesario también realizar un diagnóstico y una evaluación de los requisitos tanto técnicos como administrativos.

21.4.2. Funciones de la Gestión documental

Las principales funciones de la gestión documental son:

- Almacenamiento
- Captura
- Conservación
- Consulta
- Creación
- Difusión
- Eliminación
- Ingreso
- Uso

21.4.3. Ciclo de Vida de los Documentos

El ciclo de vida de un documento abarca todas las fases por las que un documento pasas, desde que se crea hasta que se archiva o elimina.

Los documentos pueden tener distintos valores que son:

- *Valor Primario (Administrativo)*: su propósito es dejar constancia de una actividad.
- o Valor fiscal o contable: acreditar el cumplimiento de las obligaciones contables o tributarias.
- o Valor legal o jurídico: su finalidad es, entre otras, servir de prueba ante la ley.

- *Valor Secundario:*
 - o Valor Informativo: su propósito es servir de base para la reconstrucción de cualquier actividad realizada.
 - o Valor Histórico: sirve de fuente para la investigación histórica.

Las distintas fases que atraviesa un documento son:

- Archivo de Oficina (Documentación Activa): fase en la cual los documentos son creados o recibidos por algún departamento, sobre los cuales se puede realizar una serie de operaciones de edición.
- Archivo General (Documentación semiactiva): en esta etapa la principal función es la consulta de la documentación y la actividad que recibe este tipo de documentación es menor que en el Archivo de Oficina.
- Archivo Histórico (Documentación Inactiva): en esta etapa la documentación sólo tiene utilidad como fuente de información histórica. Las consultas que recibe son menores.

21.4.4. Beneficios de la Gestión Documental

Si se realiza una buena gestión de los documentos, esto repercute en la empresa con una serie de beneficios, como son:

- Obtener información precisa de las actividades de la empresa que sirva de apoyo para actividades futuras, toma de decisiones, etc.
- Facilitar la realización de las actividades de la empresa.
- Documentar las políticas y el proceso de toma de decisiones.
- Garantizar la continuidad de la empresa en caso de fallo masivo en los sistemas, catástrofe, etc.
- Cumplir con los requisitos legales que existen con algún tipo de ficheros de datos.

- Almacenamiento de evidencias de las actividades relacionadas con la empresa y entidades externas.
- Mantener un histórico de la evolución de la entidad.
- Centralizar el almacenamiento de documentos.
- Facilitar la prestación de servicios a los usuarios de la empresa.

21.5. GESTIÓN DEL CONOCIMIENTO

21.5.1. Definición de Gestión del Conocimiento

No existe una definición universalmente aceptada de la gestión del conocimiento. Sin embargo, existen numerosas definiciones de diversos expertos.

En general, la gestión del conocimiento es la conversión del conocimiento tácito en conocimiento explícito y su intercambio dentro de la organización. La gestión del conocimiento es el proceso mediante el cual las organizaciones generan valor de sus activos intelectuales. Definidos de esta manera, se hace evidente que la gestión del conocimiento tiene que ver con el proceso de identificación, adquisición, distribución y mantenimiento de los conocimientos que son esenciales para la organización.

Si se considera la gestión del conocimiento en un contexto más amplio, entonces existen múltiples definiciones, sin embargo, todas ellas apuntan a la misma idea, aunque cada una se centre en un aspecto particular de la gestión del conocimiento .

- Una definición orientada a los resultados puede afirmar que la gestión del conocimiento es "tener el conocimiento adecuado en el lugar correcto, en el momento adecuado y en el formato correcto".
- Una definición orientada al proceso puede afirmar que la gestión del conocimiento consiste en "la gestión sistemática de los procesos por los cuales el conocimiento se identifica, se crea, se une, se comparte y se aplica".
- Una definición orientada a la tecnología puede presentar una fórmula de gestión del conocimiento como "Business Intelligence + motores de búsqueda + agentes inteligentes".

21.5.2. Cuestiones sobre gestión del conocimiento

Existen dos aspectos principales en la gestión del conocimiento, que son la *gestión de la información* y la *gestión de las personas*. Visto desde esta perspectiva, la gestión del conocimiento es, por un lado, la información y, por otro, la gente.

La mayoría de empresarios y directivos están familiarizados con el manejo de información a largo plazo. Este término se asocia con la gestión del conocimiento en relación con los objetos, que son identificados y controlados por los sistemas de información.

La práctica de la gestión de la información fue ampliamente aceptada cuando los ejecutivos se dieron cuenta de que la información era un recurso importante, que debía ser manejado correctamente, para que las empresas puedan mejorar su competitividad.

Como consecuencia del crecimiento de la práctica de la gestión de la información, los conceptos de "*análisis de la información*" y "*planificación de la información*", se han desarrollado, proporcionando herramientas adicionales para los profesionales.

En la vertiente teórica la gestión de la información ha evolucionado convirtiéndose en gestión del conocimiento.

En la práctica, la gestión del conocimiento implica, entre otros, la identificación y mapeo de los activos intelectuales de una organización. Esto significa, básicamente, la identificación de quién sabe qué dentro de la empresa.

Cuando se mira desde esta perspectiva, la gestión del conocimiento puede ser considerado como un proceso de realización de una auditoría de los activos intelectuales. Sin embargo, la gestión del conocimiento va más allá

de este nivel de la cartografía y también implica la creación de conocimiento para obtener ventajas competitivas y la conversión de grandes cantidades de datos de la organización en información de fácil acceso.

Se ha demostrado una y otra vez que cuando el conocimiento se gestiona bien, hay una reducción significativa en el tiempo necesario para completar las tareas y la duplicación innecesaria se evita.

Como ya comentamos, un aspecto de la gestión del conocimiento es la gestión de personas. Básicamente, se trata de la gestión del conocimiento tácito que reside dentro de las cabezas de las personas. En la práctica implica la gestión del conocimiento que existe junto a los procesos organizativos que implica una serie compleja de capacidades dinámicas, know-how y otras capacidades relacionadas con el conocimiento.

Con el fin de gestionar de forma eficaz a las personas que poseen el conocimiento tácito que se desea, es esencial tener en cuenta su diversidad cultural y los valores sociales, actitudes, aspiraciones y gustos. Si esto se puede hacer con éxito, puede conducir a la creación de nuevos conocimientos que de otra manera no se puede lograr mediante la gestión de información por sí sola.

A pesar de la importancia de los dos aspectos de la gestión del conocimiento, la cual está bien reconocida por muchas organizaciones, el verdadero potencial de la gestión del conocimiento todavía queda por alcanzarse. De hecho, no todas las organizaciones con algún sistema de gestión del conocimiento son conscientes de que tienen estos sistemas.

La mayoría de las organizaciones tienen algún tipo de sistema para la gestión del conocimiento explícito, ya sea simple o compleja, aunque, no necesariamente se refieran a él como un sistema de gestión del

conocimiento. Por otro lado, la gestión del conocimiento tácito no es común y la tecnología actual basada en la gestión del conocimiento no se ha desarrollado de forma plenamente eficaz para la extracción de conocimiento tácito. Aunque el conocimiento tácito es la base de conocimiento organizacional, es algo tan personal que es difícil de formalizar y comunicar.

Ambos aspectos de la gestión del conocimiento presentan dos cuestiones inmediatas:

- Hacer que el conocimiento de la organización sea más productivo.
- Producir beneficios significativamente mayores que los previstos.

La gestión del conocimiento ofrece una excelente oportunidad para adoptar estrategias de negocio que antes eran imposibles. Por ejemplo, se puede abrir la puerta a la creación de una red casi ilimitada que mejore las relaciones con clientes y proveedores. En la mejora de relaciones con los clientes, la gestión del conocimiento hace posible el descubrimiento de nuevos problemas y oportunidades a través del uso óptimo de los activos de conocimiento, tales como el contrato de venta, los registros, los datos demográficos de los clientes, etc. Es precisamente de esta manera la gestión del conocimiento se puede complementar y mejorar el impacto de otras iniciativas de la organización como la gestión de la calidad total, el proceso de reingeniería de negocios, y el aprendizaje organizacional.

Es evidente a partir de esta discusión que las iniciativas de gestión del conocimiento se pueden aplicar en una variedad de ámbitos para lograr resultados superiores en casi cualquier tipo de organización. Y es posible alcanzar estos resultados, independientemente del nivel de disponibilidad tecnológica o el sector del mercado en cuestión.

21.6. BIBLIOGRAFÍA

1. Business Process Management: Concepts, Languages, Architectures. Mathias Weske.
2. Harvard Business Review on Customer Relationship Management.
3. Customer Relationship Management. Roger Baran, Christopher Zerres y Michael Zerres.
4. ERP: Making It Happen. Thomas F. Wallace y Michael H. Kremzar.
5. Introduction to Knowledge Management. Filemon A. Uriarte Jr.

Autor: Francisco Javier Rodríguez Martínez

Subdirector de Sistemas Escola Superior Enxeñaría Informática Ourense

Colegiado del CPEIG

**22. DATAWAREHOUSE. DATA
MARTS. ARQUITECTURA.
ANÁLISIS MULTIDIMENSIONAL
Y ARQUITECTURAS OLAP.
ROLAP/MOLAP/HOLAP.
MINERÍA DE DATOS.
GENERACIÓN DE INFORMES A
LA DIRECCIÓN.**

Tema 22: Datawarehouse. Data Marts. Arquitectura. Análisis multidimensional y arquitecturas OLAP. ROLAP/MOLAP/HOLAP. Minería de datos. Generación de informes para la dirección.

ÍNDICE

22.1 Datawarehouse.....	3
22.1.1 Estructura Multidimensional.....	3
22.1.2 Características de un Datawarehouse.....	4
22.1.3 Los Metadatos.....	6
22.1.4 Elementos que componen un Datawarehouse.....	6
22.1.5 Ventajas principales de un Datawarehouse.....	9
22.2 Data Marts.....	10
22.4 Análisis multidimensional y arquitecturas OLAP.....	13
22.4.1 Análisis Multidimensional y OLAP.....	13
22.4.2 Sistemas OLAP.....	16
22.4.3 OLAP como sistema de información ejecutiva.....	16
22.4.4 Operadores OLAP.....	17
22.5 ROLAP, MOLAP Y HOLAP.....	19
22.5.1 ROLAP.....	19
22.5.1.1 Ventajas de los sistemas ROLAP.....	19
22.5.1.2 Desventajas de los sistema ROLAP.....	20
22.5.2 MOLAP.....	20
22.5.2.1 Ventajas de los sistemas ROLAP.....	20
22.5.2.2 Desventajas de los sistema ROLAP.....	21
22.5.3 HOLAP.....	21

22.5.3.1 Particionamiento vertical.....	21
22.5.3.2 Particionamiento horizontal.....	21
22.6 Minería de Datos.....	22
22.6.1 <i>Características principales.....</i>	22
22.6.2 <i>Técnicas principales.....</i>	23
22.6.3 <i>Algoritmos empleados.....</i>	24
22.8 Generación de informes a la dirección.....	26
22.9 Bibliografía.....	29

22.1 DATAWAREHOUSE

22.1.1 Estructura Multidimensional

La estructura multidimensional de bases de datos es una variante del modelo relacional, la cual hace uso de estructuras multidimensionales en las cuales mantiene la información organizada y en las que es capaz de expresar a su vez las relaciones entre los datos contenidos en ellas. Estas estructuras multidimensionales son visualizadas como cubos de datos que a su vez pueden contener otros cubos de datos, considerando cada una de las caras de los cubos como una dimensión de los datos.

Las celdas que conforman la estructura multidimensional contienen información agregada que se relaciona con los elementos a lo largo de cada una de sus dimensiones. Es decir, una única celda puede llegar a contener las ventas totales de un determinado artículo en una zona geográfica específica para un tipo de venta concreto en un período determinado (ventas del procesador XMX-01, en Galicia, a través del portal web, en el mes de abril).

El principal aporte que ofrece esta estructuración multidimensional es que supone un modelo compacto y fácilmente comprensible, lo cual permite la manipulación y visualización de elementos de datos que poseen un elevado número de interrelaciones.

Debido a todo esto las estructuras multidimensionales han pasado a formar parte de las estructuras de bases de datos más utilizadas, llegando a convertirse en las estructuras más importantes para las bases de datos analíticas que soportan las aplicaciones que llevan a cabo *procesamiento analítico en línea, OLAP*, en donde es vital obtener una respuesta rápida al realizarse una serie de consultas de elevada complejidad.

Generalmente una organización o entidad almacena su datos en bases de datos diseñadas para introducir y almacenar datos mediante el proceso OLTP (On-Line Transaction Process, Proceso de Transacciones On-Line). Este proceso realiza de una manera idónea las tareas de inserción, modificación o borrado de registros, pero resulta ineficiente a la hora de realizar consultas complejas. Los Datawarehouse surgen como solución a los

problemas que plantea el realizar análisis de datos sobre una base de datos OLTP.

El término *Datawarehouse* o almacén de datos representa un conjunto o compendio de datos atendiendo a una temática, no volátil, integrado, de tiempo variable, que es utilizado para aportar mayor información y en menor tiempo al proceso de toma de decisiones en el ámbito de la gerencia empresarial.

Desde un punto de vista más concreto un *Datawarehouse* es una base de datos de carácter corporativo. Esta base de datos se caracteriza por la integración y depuración de información procedente de una o múltiples fuentes de datos, con el fin de procesarla y así ofrecer la posibilidad de analizarla desde un mayor número de perspectivas y a una mayor velocidad de respuesta sobre las posibles consultas que sobre ella se realicen.

La ventaja principal que aporta un *Datawarehouse* tiene su origen en las estructuras o modelos en los que organiza y almacena la información, los principales son:

- Modelo de tablas en estrella.
- Modelo de tablas en copo de nieve.
- Cubos relacionales.

Debido a esto, la persistencia de la información de un *Datawarehouse* es homogénea y fiable, aportando a su vez la posibilidad de realizar consultas y de tratar la información de una manera jerárquica.

22.1.2 Características de un Datawarehouse

Los aspectos por los cuales se caracteriza un *Datawarehouse* son los siguientes:

- **Temático:** orientado sobre la información que resulta relevante para la organización. El proceso de desarrollo del *Datawarehouse*, se lleva a cabo con el fin de realizar de una manera eficiente las consultas sobre la información que ofrece mayor interés a las

actividades esenciales de la entidad, compras, ventas, producción, etc. En ningún momento se tienen en cuenta otro tipo de procesos como gestión o facturación.

Los datos son organizados en temas, facilitando así su acceso y entendimiento por parte de los usuarios. De esta forma también se ven beneficiadas las consultas, puesto que toda la información referente a una temática se encontrará agrupada.

- **Integrado:** es capaz de incorporar en una sola solución integral datos recopilados de diversos sistemas operacionales y fuentes de información, las cuales pueden ser de carácter interno a la organización como externo. Además permite que esas fuentes de información externa contengan los datos en distintos formatos. La estructura en la cual se realiza la integración de los datos ha de ser consistente, para lo cual se deben eliminar las inconsistencias que existen entre los distintos sistemas operacionales.
- **Histórico:** la variable temporal forma parte de la información implícita contenida en un Datawarehouse. En contraposición con los sistemas operacionales, los cuales siempre son reflejo del estado de la actividad en el momento presente, es decir no reflejan la temporalidad de la información, un Datawarehouse proporciona la capacidad de analizar tendencias que se produzcan a lo largo de una etapa y compararlos con otros anteriores. En definitiva, almacena los datos como si realizara fotos que se corresponden con los distintos momentos o períodos de tiempo.
- **No volátil:** el repositorio de información contenida dentro de un Datawarehouse sólo existe para ser consultada, no para modificar su contenido, lo cual proporciona a esta información carácter permanente. Esto significa que cuando se realiza una actualización del Datawarehouse, únicamente se incorporan los últimos valores

que tomaron las variables contenidas en él, pero no se realiza ningún tipo de acción que altere los valores ya existentes.

22.1.3 Los Metadatos

Otro valor añadido que aporta un Datawarehouse son los metadatos, datos que describen a otros datos. Estos metadatos aportan nueva información sobre los valores existentes en el Datawarehouse, mejorando la descripción de los datos y aportando nuevo conocimiento permitiendo, por ejemplo, conocer la procedencia de la información, su grado de fiabilidad, su periodicidad de refresco o incluso el algoritmo utilizado para calcularla.

Los metadatos, además de ampliar información permiten al Datawarehouse realizar una serie de procesos que simplifican y posibilitan obtener la información de una manera automática desde los sistemas operacionales a los sistemas informacionales.

Los objetivos principales que siguen los metadatos son:

- **Ofrecer soporte al usuario final:** gracias a su propio lenguaje de negocio, facilitan el acceso al Datawarehouse indicando qué información está contenida y el significado que esta aporta. También pueden ser utilizados por otras herramientas para construir informes, consultas, etc.
- **Ofrecer soporte técnico:** suponen un gran punto de apoyo para los técnicos que gestionan el Datawarehouse ya que son de gran ayuda en aspectos de auditoría, en la gestión de la información histórica, en la propia administración del Datawarehouse, etc.

22.1.4 Elementos que componen un Datawarehouse

Los elementos más importantes que conforman un Datawarehouse son:

1. **Fuentes de datos:** las fuentes de datos forman parte del Datawarehouse desde el principio, puesto que son el origen de los datos que contendrá. Las fuentes de datos pueden pertenecer a

diversos ámbitos tanto dentro como fuera de la organización, desde sistemas operacionales propios a fuentes externas.

2. **ETL (Extracción, transformación y carga):** representa la parte del sistema que realiza el proceso de construcción del Datawarehouse. Para ello hace uso de las fuentes de datos desde las cuales extrae la información para luego procesarlas y almacenarlas.
 - o *Extracción:* recuperación de la información procedente de las distintas fuentes de datos.
 - o *Transformación:* proceso mediante el cual se realizan tareas de filtrado, limpieza, depuración, homogeneización y agrupación de la información.
 - o *Carga:* este proceso se encarga de la organización y la actualización de los datos y de los metadatos del Datawarehouse.
3. **Servidor de datos:** componente que realiza las labores de gestión del Datawarehouse. Para llevar a cabo estas tareas suele hacer uso de los recursos ofrecidos por el sistema operativo y por el gestor de base de datos.

Para el almacenamiento de los datos se pueden diferenciar dos posibilidades en función del tipo de bases de datos y gestor de la misma empleados:

- o Bases de datos relacionales y un sistema gestor de base de datos relacional o SGBDR.
- o Bases de datos multidimensionales, con un gestor de base de datos multidimensional o SGBDM.

Ha de ofrecer:

- o Servicio de mantenimiento.

- o Servicio de distribución para poder exportar los datos hacia otros servidores de bases de datos descentralizadas y a otros sistemas de soporte de decisiones.
 - o Servicio de seguridad, archivo, backup, recuperación, etc.
4. **Herramientas de acceso:** estas herramientas aportan técnicas para la captura de datos de una manera rápida para poder ser analizados desde distintos puntos de vista. También realizan tareas de transformación de los datos en información útil para el usuario. Este tipo de herramientas se denominan business intelligence tools y se sitúan a nivel conceptual sobre el Datawarehouse. alguna de estas herramientas son:
- o Consultas SQL.
 - o Herramientas MDA, Multidimensional Analysis.
 - o Herramientas OLAP, On-Line Analytical Processing.
 - o Herramientas ROLAP, Relational On-Line Analytical Processing.
 - o Herramientas MOLAP, Multidimensional On-Line Analytical Processing.
 - o Herramientas HOLAP, Hybrid On-Line Analytical Processing.
 - o Herramientas de Minería de Datos.
5. **Repositorio/Metadatos:** el repositorio ayuda a los usuarios a saber qué es lo que hay almacenado en el Datawarehouse y como pueden acceder a lo que quieren. Además realiza diversas funcionalidades como:
- o Catalogar y describir la información disponible.
 - o Especificar el propósito de la información.
 - o Reflejar las relaciones de los datos.

- o Indicar el propietario de la información.
- o Relacionar las estructuras técnicas de datos con la información de negocio
- o Especificar las relaciones entre los datos operacionales y las reglas de transformación.
- o Limitar la validez de la información.

22.1.5 Ventajas principales de un Datawarehouse

Las aportaciones más importantes que ofrece un Datawarehouse son las siguientes:

- Facilita la implantación de sistemas de gestión integral de la relación con el cliente desde el núcleo de una organización.
- Posibilita la utilización de técnicas de modelización y análisis estadístico para la búsqueda de relaciones ocultas entre los datos almacenados, lo cual ofrece un valor añadido al sistema de gestión de la información.
- Ofrece una herramienta de apoyo a la toma de decisiones en cualquier área funcional, gracias la información integrada y global que proporciona.
- Aporta la capacidad de aprendizaje sobre los datos pasados para la predicción de posibles situaciones futuras.

22.2

DATA MARTS

La solución a los problemas relacionados con el análisis de datos sobre una base de datos OLTP son solucionados con la creación de los datawarehouse (base de datos independiente orientada a consultas). Sin embargo, cuando los datawarehouse aumentan su tamaño se vuelven cada vez más complejos lo que provoca un decrecimiento en el rendimiento de las consultas, dejando de ser útil el modelo centralizado. Como respuesta a esta bajada de rendimiento surgen los Data Marts, que son almacenes de datos que se especializan por áreas o temáticas como pueden ser ventas o compras.

Los Data Marts suelen recibir la información desde el datawarehouse, almacén de datos centralizado, y pueden estar ubicados en máquinas distintas, en otras BBDD, redes, etc. También pueden integrar la información desde distintas fuentes. Según estos dos modelos de extracción de la información, existen dos tipos de Data Mart:

- *Data Mart dependiente*, cuyos datos vienen proporcionados desde un datawarehouse. En la ilustración 9 se puede observar el funcionamiento de un Data Mart con un datawarehouse.
- *Data Mart independiente*, donde los datos son extraídos de diversas fuentes de información de los sistemas operacionales.

Un Data Mart representa una pequeña porción de un datawarehouse, con lo que soporta un número de usuarios más reducido, con lo cual se pueden optimizar para realizar el proceso de recuperación de la información de una manera más rápida.

Un Data Mart en realidad es una base de datos específica de un departamento o sección, dedicada únicamente a los datos relevantes que se producen en ese ámbito. Debido a esta especialización disponen de una estructura óptima de datos adaptada al análisis de la información desde todas las perspectivas que afecten a los procesos de ese ámbito.

Para la creación de un Data Mart es necesario encontrar la estructura

montada sobre un sistema OLTP como un datawarehouse, o por el contrario, puede sostenerse sobre un sistema OLAP. Por ello se pueden establecer dos tipos de Data Marts:

- **Data Mart OLTP:** son Data Marts basados en un datawarehouse, pero es habitual que incorporen mejoras para ofrecer un mayor rendimiento adaptando las necesidades de cada área al Data Mart.

En este tipo de Data Marts las estructuras más comunes son:

- o *Tablas report*, que son tablas de hechos reducidas que agregan las dimensiones oportunas.
 - o *Vistas materializadas*, que se construyen con la misma estructura que las tablas report para explotar la reescritura de las consultas. Este tipo de estructura es dependiente del SGBD.
- **Data Mart OLAP:** se basan en cubos OLAP que se generan en función de los requisitos de cada área, agregando las dimensiones y los indicadores necesarios de cada cubo relacional. Los modos de creación, explotación y mantenimiento de este tipo de estructura es muy dependiente de la herramienta que se utilice para su manejo.

Los Data Marts gracias a este tipo de estructuras óptimas para el análisis ofrecen una serie de ventajas como:

- Elevada rapidez de consulta de la información.
- Reducido conjunto de datos.
- La información se valida directamente.
- Realizar fácilmente históricos de los datos.
- Posibilidad de Consultas SQL y MDX sencillas.

22.3

22.4 ANÁLISIS MULTIDIMENSIONAL Y ARQUITECTURAS OLAP.

La primera aparición del término OLAP (On-Line Analytical Processing) fue publicada en 1993 por Edgar F. Codd. Sin embargo, en 1970 ya existían productos que realizaban consultas OLAP. Codd definió OLAP como un tipo de procesamiento de datos caracterizado por permitir el análisis multidimensional.

22.4.1 *Análisis Multidimensional y OLAP*

La multidimensionalidad desde el punto de vista de un proceso analítico en línea consiste en transformar los datos procedentes desde varias fuentes, tablas de una base de datos, archivos,... y convertirlos en una estructura donde estos estén agrupados en dimensiones separadas y heterogéneas. Estas estructuras se denominan *cubos*.

Las dimensiones constituyen las perspectivas de alto nivel de los datos que representan la información más importante de un negocio. Estas dimensiones en una solución OLAP tienden a ser invariantes.

El análisis multidimensional se fundamenta en modelar la información en dimensiones, hechos y medidas.

- **Medidas:** es un tipo de dato que contiene información que utilizan los usuarios en sus consultas con las que son capaces de medir el grado de rendimiento de un proceso.
- **Dimensiones:** entidades o colección de entidades que se encuentran relacionadas y que son usadas para determinar o identificar el contexto de las medidas.

El tipo y el número de dimensiones para cada una de las medidas del modelo es un proceso que ha de realizarse cuidadosamente, puesto que al definir las dimensiones, el añadir, eliminar o cambiar propiedades particulares de las dimensiones candidatas varía el contexto y también el significado de la medida candidata.

Una dimensión tiene componentes denominados *miembros* (dimensión Tiempo, miembro trimestre) y entre los miembros pueden existir jerarquías (un mes puede considerarse dentro de un trimestre).

Las dimensiones contienen:

- o Entidades de dimensión.
- o Atributos de dimensión.
- o Jerarquías de dimensión.
- o Niveles de agregación.

Para referenciar a las dimensiones se utilizan las *llaves de dimensión*.

- **Hechos:** identifican la existencia de valores específicos de una o más medidas para una combinación concreta de dimensiones. Mediante un hecho se puede representar desde un objeto de negocio hasta una transacción e incluso un evento utilizado por los usuarios.

Los hechos contienen:

- o Un identificador para cada hecho.
- o Llaves de dimensión, que lo enlazan con las dimensiones.
- o Medidas.
- o Tipos de atributos normalmente derivados de otros datos del modelo.

Una característica fundamental y muy importante de este modelo es que tiene la capacidad de representarse de manera vectorial. Los hechos se sitúan de manera lógica en una celda, la cual se encuentra en la intersección de ciertas coordenadas según el modelo (x, y, z,...), donde

además cada una de las coordenadas que se encuentran en las celdas representan una dimensión.

La utilización de la correspondencia entre los elementos del modelo, es decir, los hechos y las coordenadas, y los de la base de datos, la tabla de hechos y dimensiones, es fundamental para poder llevar a cabo el análisis multidimensional en una base de datos. En una base de datos se pueden implementar los hechos y las dimensiones en una tabla y debido a esto es posible utilizar el lenguaje SQL para la definición de un modelo multidimensional en una base de datos relacional. A pesar de esto, fue necesario realizar una serie de extensiones del modelo relacional para poder dar soporte a las funcionalidades y necesidades propias del análisis multidimensional. Estas funcionalidades son:

1. Declaración de Dimensiones y Jerarquías. El modelo relacional no incorporaba ni trataba con anterioridad estos conceptos.
2. Acceso más rápido a los datos. Para añadir esta mejora se utilizaron métodos de generación de índices para datos espaciales desde el punto de vista multidimensional.
3. Cálculo de valores previamente agrupados para la optimización de consultas.
4. Definición de operaciones de navegación en las dimensiones y de agrupación de medidas como:
 - o Slice-and-dice:
 - o Drill-down
 - o Roll-up
 - o Pivot
 - o Drill-across
 - o Drill-through

Partiendo de las primeras propuestas, el modelo multidimensional no precisa de un almacenaje previo en una base de datos multidimensional, sino que propone que el acceso a la información puede hacerse directamente a múltiples fuentes, bases de datos (ya sean relacionales o

multidimensionales), hojas de cálculo, archivos e incluso permite que los datos puedan proceder directamente de los usuarios finales.

A pesar de estas primeras ideas, se ha determinado a través de la experiencia de que el análisis OLAP tiene un mejor desempeño si la fuente de datos es única y aún mejor si esa fuente de información es a su vez una base de datos multidimensional, como por ejemplo un Datawarehouse.

22.4.2 *Sistemas OLAP*

Los sistemas OLAP son un conjunto de métodos que permiten consultar la información contenida en los datos de diversas maneras. Esta versatilidad y multiplicidad de opciones de visualización viene producida por la clasificación de los datos en diferentes dimensiones que pueden ser visualizadas unas con otras combinándolas para obtener diferentes análisis de la información.

La información de un modelo OLAP es vista como un cubo, los cuales son determinados por categorías descriptivas o dimensiones y valores cuantitativos, las medidas. Este modelo de datos multidimensional simplifica mucho las tareas que el usuario puede realizar sobre los datos, consultas complejas, filtrar en subconjuntos,...

22.4.3 OLAP como sistema de información ejecutiva

Como clasificación de los sistemas OLAP se pueden considerar dentro del grupo de aplicaciones o sistemas de información para ejecutivos (EIS), que se emplean para proporcionar al nivel estratégico información que resulte relevante a la hora de tomar decisiones.

Si comparamos los sistemas OLAP con el resto de EIS podemos afirmar que las herramientas OLAP ofrecen una opción mucho más general, es decir son más genéricas:

- Funcionan sobre un sistema de información como los datawarehouse.
- Permiten la creación de agregaciones y combinaciones de los datos de muchas maneras posibilitando realizar análisis más estratégicos de datos.

- Posee operadores para realizar tareas específicas (Drill, Roll, Slice-and-Dice,...).
- El resultado puede ser expresado de manera matricial o híbrida.

22.4.4 Operadores OLAP

Estas herramientas de las soluciones OLAP permiten al usuario tener una visión multidimensional de la información para cada una de las actividades de análisis. Con los operadores se realizan consultas simplemente seleccionando atributos del esquema multidimensional sin tener que tener conocimiento de es la estructura interna en la que se almacenan los datos, puesto que la propia herramienta OLAP se encarga de generar la consulta y enviarla al sistema de gestión de consultas.

Una consulta consiste en la obtención de medidas sobre los hechos parametrizadas por los atributos de las dimensiones y limitadas por las condiciones impuestas sobre las dimensiones. Las herramientas OLAP ofrecen una serie de nuevos operadores que refinan esas consultas. Los operadores son los ya mencionados anteriormente en el punto (Análisis multidimensional y OLAP).

- **Drill o disgregación:** posibilita introducir un nuevo criterio de agrupación en el análisis, disgregando los grupos actuales. Actúa sobre el operador original *informa* con lo cual no es necesario crear o realizar un nuevo informe. Existen varias variantes:
 - o *Drill-down*, permite visualizar los datos del nivel inferior de la dimensión actual dentro de una jerarquía definida. Muestra los datos detallados que en conjunto determinan el valor.
 - o *Drill-across*, visualiza la información contenida en otro modelo multidimensional, sin detallar ni consolidar la información cambia el modelo multidimensional que se está consultando. Para realizar esta operación ambos modelos han de tener una dimensión común.
 - o *Drill-through*, similar a drill-dow consulta la información del nivel inferior a la dimensión actual. Sin embargo drill-throug

navega por fuera del modelo multidimensional estableciendo un enlace entre este y el sistema fuente, sobre el cual consulta los datos del nivel detallado directamente. Para poder utilizar este operador se debe establecer acceso al sistema fuente desde el sistema OLAP.

- **Roll o agregación:** permite que se elimine un criterio de agrupación en el análisis, agregando los grupos actuales. Actúa sobre el informe ya creado y no es preciso realizar uno nuevo. Variantes:
 - o *Roll-up*, también conocido como drill-up se encarga de pasar al nivel superior de la jerarquía de la dimensión actual. Para ello consolida los datos del nivel actual y muestra el valor consolidado que corresponde con el nivel superior de la dimensión.
 - o *Roll-across*, funciona de una manera parecida al *Roll-up* salvo que no se realiza sobre jerarquías de una dimensión, sino que elimina un criterio de análisis eliminando de la consulta una dimensión.
- **Slice-and-dice:** permite seleccionar y proyectar datos en el informe. Selecciona la información de un miembro de una dimensión, se trabaja con un subconjunto de los datos para un valor determinado de un nivel en una dimensión. Con frecuencia este operador es empleado sobre un eje temporal para poder analizar tendencias y encontrar patrones.
- **Pivot:** con este operador se permite cambiar la orientación de las dimensiones en un informe. Selecciona el orden de visualización

de las dimensiones con el fin de analizar los datos desde distintas perspectivas.

22.5 ROLAP, MOLAP Y HOLAP

22.5.1 ROLAP

Es un tipo de organización de la información a nivel físico que se implementa sobre tecnología relacional, pero incorpora de algunas facilidades que incrementan su rendimiento.

ROLAP (Relational On-Line Analytic Processing) posee las virtudes de un sistema gestor de bases de datos relacional sobre el cual se le incorporan una serie de herramientas y extensiones para poder ser utilizado como un datawarehouse o almacén de datos. Las principales características de los sistemas ROLAP son:

- Almacena los datos en una base de datos relacional.
- Utilización de índices de mapas de bits.
- Utilización de índices de join.
- Técnicas de particionamiento de datos.
- Optimizadores de consultas.
- Extensiones de SQL (drill, roll, etc).

22.5.1.1 Ventajas de los sistemas ROLAP

- Utilización completa de la integridad y seguridad que ofrecen las bases de datos relacionales.
- Es escalable para volúmenes grandes.
- Los datos pueden ser compartidos con otras aplicaciones que utilicen el lenguaje SQL.
- Datos y estructuras más dinámicas.

22.5.1.2 Desventajas de los sistema ROLAP

- Las consultas resultan más lentas.
- Su construcción suele resultar costosa.
- Los índices no se mantienen de manera automática.
- Los cálculos se encuentran limitados por las funciones de la base de datos.

22.5.2 *MOLAP*

La función principal de los sistemas MOLAP (Multidimensional On-Line Analytic Processing) es la de almacenar físicamente los datos en estas estructuras específicas de tipo multidimensional haciendo coincidir la representación interna de los datos con la representación que las capas superiores dan a la información.

Poseen estructuras específicas para el almacenamiento de la información, aportando también técnicas para la compactación de los datos lo cual mejora el rendimiento del almacén de datos.

Las características más importantes de los sistemas MOLAP son:

- Incorporan tecnología optimizada para la realización de las consultas y del análisis, la cual está fundamentada en el modelo multidimensional.
- Tiene un motor especializado.
- Construye los datos y los almacena en estructuras multidimensionales.

22.5.2.1 Ventajas de los sistemas ROLAP

- Mayor rendimiento a la hora de ejecutar las consultas.
- Poco tiempo de cálculos realizados en el momento.
- Puede realizar la escritura de manera directa en la base de datos.
- Ofrece la posibilidad de implementar cálculos más sofisticados.

22.5.2.2 **Desventajas de los sistema ROLAP**

- El tamaño viene limitado por la arquitectura del cubo.
- Sólo es capaz de gestionar los datos si estos se encuentran almacenado en un cubo.
- Procesos de mantenimiento y de copias de seguridad limitados.
- No explota la capacidad de paralelismo que ofrecen las bases de datos.
- Introduce redundancia de datos.

22.5.3 **HOLAP**

Este tipo de sistemas HOLAP (Hybrid On-Line Analytic Processing) están considerados como sistemas híbridos entre los ROLAP y los MOLAP, puesto que incorpora características de ambos. Para ello utiliza un motor relacional para almacenar parte de los datos en una base de datos de tipo relacional y utiliza una base de datos multidimensional para otra parte de la información.

22.5.3.1 **Particionamiento vertical**

En este modo, HOLAP mejora la velocidad de las consultas almacenando las agregaciones en un sistema MOLAP, mientras que para optimizar el tiempo, los datos son detallados en un sistema ROLAP.

22.5.3.2 **Particionamiento horizontal**

Un sistema HOLAP en modo de particionamiento horizontal almacena parte de los datos, normalmente los más recientes particionados por una de las dimensiones (dimensión tiempo por ejemplo) en modo MOLAP, con lo que consigue un aumento en la velocidad de respuesta de las consultas. Por otra parte mantiene en un sistema ROLAP los datos más antiguos. También este modo permite que los cubos se almacenen unos en sistemas MOLAP y otros en sistemas ROLAP.

22.6 MINERÍA DE DATOS

El concepto de Data Mining o Minería de datos viene determinado por el método de extracción de la información contenida en los datos. La minería de datos obtiene información contenida en los datos, pero de una forma indirecta, puesto que esta se encuentra implícita en los datos y no se puede acceder a ella directamente.

La minería de datos *prepara, sondea y explora* el conjunto de datos con el fin de conseguir información que de algún modo se encuentra oculta. Esta ocultación de la información se debe a que normalmente para un experto lo que resulta relevante es la información contenida en las relaciones, fluctuaciones y dependencias de los datos, no los datos en sí. Esta información es por lo general desconocida, lo cual ofrece un valor muy importante, puesto que puede resultar de gran utilidad a los procesos de una organización.

Está formada por un conjunto de técnicas dirigidas a la obtención del conocimiento procesable oculto en las bases de datos. Estas técnicas fundamentan su base en la inteligencia artificial y en el análisis estadístico para generar modelos con el fin de poder abordar la solución a problemas de predicción, clasificación y segmentación.

La minería de datos es un proceso que invierte la dinámica del método científico puesto que en este, primero se formulan las hipótesis y luego se desarrolla un experimento para la obtención de los datos que las confirmen o refuten, obteniendo así nuevo conocimiento. En la minería de datos se recaba una colección de datos con la intención de que de estos surjan hipótesis. Se espera que de los propios datos describan o indiquen como son para poder validar las hipótesis aparecidas con los datos mismos. Es por este motivo que la minería de datos ha de realizarse con un enfoque exploratorio y no confirmador

22.6.1 Características principales

Las principales características que determinan un sistema de minería de datos son:

- Trabaja con la información contenida en lo más oculto de las bases de datos o almacenes de datos analizando información almacenada durante años.
- Suelen ser soluciones con una arquitectura cliente-servidor.
- Poseen gran variedad de herramientas para la extracción de la información.
- Las herramientas son fácilmente combinables entre sí.
- Son los usuarios finales los que hacen uso de las herramientas para indagar en el conjunto de datos y obtener respuestas rápidas.
- Es habitual hacer uso de un procesamiento paralelo que acelere el proceso debido a la existencia de una gran cantidad de datos.
- Produce cinco tipos de información:
 - o Asociaciones
 - o Secuencias
 - o Clasificaciones
 - o Agrupamientos
 - o Pronósticos.

22.6.2 *Técnicas principales*

Las técnicas más importantes que se utilizan para llevar a cabo este proceso son:

- *Redes Neuronales*: es una técnica que proviene de la inteligencia artificial para la detección de categorías comunes en los datos ya que es capaz de detectar y aprender complejos patrones y características de los datos.

Un punto fuerte de las redes neuronales es que son capaces de trabajar con conjuntos incompletos de datos e incluso con algunos

paradójicos que en función del problema pueden ser ventajosos o resultar un inconveniente.

- *Árboles de Decisión*: esta técnica se representa en forma de árbol siendo cada nodo una decisión, los cuales generan una serie de reglas mediante las cuales clasifican los datos.

Son sencillos de utilizar, admiten tanto atributos discretos como continuos y tratan bien tanto los atributos no significativos como los valores faltantes. Además son fácilmente interpretables.

- *Algoritmos Genéticos*: son técnicas que imitan la evolución de las especies mediante la generación de mutaciones, la reproducción y selección. Aportan herramientas para integrar en la construcción y entrenamiento de otras estructuras como por ejemplo las redes neuronales. Están basados en el principio de supervivencia de los más aptos.
- *Clustering (Agrupamiento)*: técnica que agrupa datos dentro de una serie de clases, que pueden ser predefinidas o no, siguiendo los criterios de distancia o similitud de modo que los datos contenidos dentro de una clase son similares entre sí y distintos con los contenidos en las otras clases. Es un método muy flexible y es fácilmente combinable con otras técnicas de minería de datos.
- *Aprendizaje Automático*: técnica procedente de la inteligencia artificial en la que se trata de inferir conocimiento partiendo del resultado obtenido mediante alguna de las otras técnicas anteriormente mencionadas.

22.6.3 Algoritmos empleados

Los algoritmos utilizados en la minería de datos se pueden clasificar en:

- **Supervisados**
 - o Predicen el valor de un atributo de un conjunto de datos una vez conocidos otros atributos.

- o Partiendo de los datos cuyos atributos son conocidos, se inducen nuevas relaciones entre atributos.
- o Constan de dos fases:
 - *Entrenamiento*, en la cual se construye un modelo usando un subconjunto de datos conocidos.
 - *Prueba*, se prueba el modelo con el resto de los datos.

- **No Supervisados**

- o Se utilizan cuando una aplicación no se encuentra lo suficientemente madura o no tiene las capacidades necesarias para realizar una solución predictiva.
- o Descubren patrones y tendencias en los datos.
- o Con el descubrimiento de la información se pueden llevar a cabo acciones que reporten en un beneficio.

22.7

22.8 GENERACIÓN DE INFORMES A LA DIRECCIÓN

Los aplicaciones para la generación de informes a la dirección o *Sistemas de Información para Ejecutivos (EIS)*, son herramientas software que se basan en sistemas de apoyo a las decisiones (DSS Decision Support System) proporcionando a la gerencia de una organización acceso fácil y sencillo a la información que resulta clave para el éxito de su compañía, ya sea interna o externa.

El objetivo principal de este tipo de aplicaciones es poner a disposición de los ejecutivos una serie de herramientas que muestren el abanico completo del estado de los indicadores de negocio que le interesan en tiempo real, ofreciendo a su vez la capacidad de un análisis detallado de aquellos que no se estén consiguiendo las expectativas o las planificaciones establecidas a priori.

Este tipo de sistemas se pueden definir como soluciones para mostrar informes y listados (query & reporting) de los distintas áreas de negocio de una forma consolidada facilitando una monitorización completa y real de una organización.

Ofrecen además un acceso rápido y efectivo a la información compartida, para lo cual hacen uso de interfaces gráficas muy visuales e intuitivas. Incorporan también incluyen alertas e informes basados en excepción, así como históricos y análisis de tendencias.

Mediante estos sistemas el seguimiento del comportamiento de una organización o de un área de negocio se hace de una manera fácil y comparable a través del tiempo.

Dentro de estos sistemas, lo más común es encontrar los términos de Informes (Reports), Cuadro de Mando (Dashboard) y Cuadro de Mando Integral (Balanced ScoreCard).

Informes

Los informes son la herramienta más común de transmitir toda la información obtenida de un sistema de business intelligence. Un informe se puede describir como un documento, o conjunto de documentos, que

contiene datos utilizados para su estudio y análisis por parte de la dirección. Pueden estar compuestos desde una simple tabla de datos o un vista más compleja con datos agregados, con datos transformados mediante la aplicación de fórmulas o con sistemas de navegación interactiva a través de los datos (habitualmente ampliando la vista de cada fila en la tabla).

La característica principal de un informe es que no ofrece al lector del mismo ningún tipo de conclusión o visión predefinida de los datos. Aunque un informe incluya datos analíticos, datos agregados, datos calculados o algún gráfico es el propio lector el que debe extraer conclusiones o determinar las próximas acciones en base a los datos presentados en el informe.

Dashboard

Un cuadro de mando es una interfaz de carácter visual que ofrece en cada momento diferentes vistas o perspectivas de las diferentes métricas o indicadores (también denominados KPI Key Performance Indicators) que se hayan considerado como relevantes para un proceso de negocio o los objetivos de una empresa. Un KPI es un indicador de la ejecución y el rendimiento de una tarea o actividad diaria que se considera fundamental desde el punto de vista de la dirección para su seguimiento. La idea que subyace a un KPI es que no es una métrica simple del negocio, sino que está diseñado de forma que describe y alerta sobre distintas circunstancias permitiendo detectar e intervenir en aquellas situaciones que así lo requieran.

Un dashboard presenta tres características diferenciadoras:

Muestra los datos de forma gráfica. Esto proporciona una visión mucha más centrada en los indicadores de rendimiento, en las posibles comparaciones entre datos y aquellos datos que sean una excepción o que identifiquen una anomalía.

Sólo muestran aquellos datos que son necesarios para un determinado objetivo empresarial.

Además, incluye conclusiones predefinidas que son relevantes para los objetivos del cuadro de mando y que ayudan al lector a realizar su propio análisis.

Cuadro de Mando Integral

Un cuadro de mando integral (Balanced Scorecard) es una representación visual de la estrategia de la empresa. El cuadro de mando integral permite de una forma sencilla presentar los indicadores o métricas críticas para el negocio y contrastarlas con la estrategia de negocio que se pretende para la organización.

El cuadro de mando integral ha de mostrarse de una forma visual y ser la referencia a cualquier persona de la organización para ver:

El rendimiento de las iniciativas específicas a distintas unidades de negocio o desde un punto de vista global a toda la compañía.

Los objetivos individuales referenciados al contexto global de la compañía mediante una representación visual.

Los cuadros de mando integral se diseñan siempre con el fin de aumentar la productividad de toda la organización, porque indica en tiempo real como se está comportando un empleado, un equipo, un departamento o toda la empresa, de acuerdo a los objetivos definidos en el plan estratégico. Esto lo convierte en un sistema de gestión estratégica de la empresa que permite:

Formular estrategias consistentes y que estas sean transparentes a toda la organización.

Comunicar las estrategias definidas por la dirección a través de toda la organización.

Coordinar los objetivos de las diversas unidades organizacionales (equipos, departamentos, secciones, etc.) de acuerdo al mismo plan estratégico.

Conectar los objetivos de cada unidad organizacional con la planificación financiera y presupuestaria de la organización.

Medir de un modo sistemático la realización, proponiendo acciones correctivas oportunas por parte de la dirección o por cada uno de las unidades organizacionales implicadas.

22.9 BIBLIOGRAFÍA

- *"Building the Data Warehouse"*. Inmon, W.H.
- *"Sistemas de Información Para la Toma de Decisiones"*. Cohen K. Daniel, Ed. Mc Graw Hill, 1996.
- *"OLAP Solutions: Building Multidimensional Information Systems"*. Erik Thomsen. Ed. Wiley, 2002. ISBN: 04 714 0030 0
- *"State of the Art: Data Mining"*. S. R. Hedberg, K. Watterson y C. D. Krivda. Publicado en BYTE (10-95)
- *"MOLAP, ROLAP, Overlap"*. Jeff Stamen. Publicado en BYTE (8-96)
- *State of the Art: Data Warehouses*. Autor: J. L. Weldon, A. Simon y M. Hurwicz. Publicado en BYTE (1-97)
- *"Introducción a la Minería de Datos"*. José Hernández Orallo, M. José Ramírez Quintana, César Ferri Ramírez. Ed. Pearson, 2004. ISBN: 84 205 4091 9.

Autor: Francisco Javier Rodríguez Martínez

Subdirector de Sistemas Escola Superior Enxeñaría Informática Ourense
Colegiado del CPEIG

23. SISTEMAS DE GESTIÓN DE CONTENIDOS. E-LEARNING. ACCESIBILIDAD Y USABILIDAD. W3C.

ÍNDICE

23.1 SISTEMAS DE GESTIÓN DE CONTENIDOS

23.1.1 Introducción a los Sistemas de Gestión de Contenidos.

Los sistemas de gestión de contenidos, en adelante SGC (CMS en inglés), son un tipo especial de software orientado a la creación, administración y distribución de contenidos digitales. Los SGC proporcionan una estructura o framework para dar soporte a tareas básicas y complejas de gestión de contenido. Están principalmente orientados para servir como marco de publicación de contenidos en la red a través de web. El éxito de este tipo de sistemas radica fundamentalmente en la facilidad de uso, estableciendo mecanismos sencillos para la creación de contenidos, su actualización, su administración y categorización, y su publicación. Proporcionar facilidad en el manejo de contenidos implica otorgar un mayor dinamismo en el flujo de la información.

Una de sus principales características es que permiten separar el contenido de la presentación, cuestión que proporciona versatilidad a la hora de realizar cambios en el diseño. Además, aportan herramientas que permiten descentralizar la publicación de contenidos en la Web.

Un aspecto clave en la gestión de contenidos es la categorización de la información. La capacidad de establecer mecanismos que permitan localizar la información útil es otra de las características propias de los sistemas de gestión de contenidos. Esta capacidad se basa en el uso de metadatos que sirven para proporcionar información añadida a los contenidos publicados, y que son utilizados por los buscadores y clasificadores de información.

23.1.2 Funcionalidad de los SGC

La funcionalidad general ofrecida por los SGC puede agruparse en cinco bloques

fundamentalmente:

- Creación de contenido : Se realiza de forma sencilla. Los CMS aportan herramientas para que los creadores sin conocimientos técnicos en páginas web pueden concentrarse en el contenido. La forma habitual consiste en proporcionar un editor de texto WYSIWYG, en el que el usuario ve el resultado final mientras escribe. El uso de este tipo de editores es muy sencillo. El acceso a los mismos es muy cómodo, ya que sólo se requiere para ello un equipo con acceso a Internet y un navegador web.
- Gestión de contenido : Todo el contenido creado se almacena en la base de datos que utiliza el sistema. En la propia base de datos es en donde también se guardan datos relacionados con la estructura de la web o los usuarios autorizados.
- Gestión de usuarios: La mayoría de los SGC presentan una gestión de usuarios en la que cada uno cuenta con diferentes permisos para gestionar el contenido. Dependiendo de los permisos de usuarios, se



pueden encontrar distintos roles que van desde el administrador general de la plataforma, hasta el usuario final que consulta la información.

- **Publicación de contenido** : Una vez creado el contenido, los SGC proporcionan diferentes mecanismos para proceder a su publicación. Se le puede asignar una fecha de publicación o bien se puede publicar directamente. En la publicación del contenido, el aspecto que tendrá viene marcado por el patrón marcado para la sección donde se encuentre la información, que habitualmente se corresponde con un conjunto de estilos predefinidos. Esta separación entre contenido y forma representa una característica muy importante de los SGC dado que permite que se pueda modificar el estilo de un portal web sin necesidad de modificar el contenido.
- **Presentación de contenido**: Los SGC gestionan automáticamente la accesibilidad del web, proporcionando mecanismos de adaptación a las necesidades de cada usuario y además son perfectamente compatibles con la mayoría de los navegadores web existentes. El sistema se encarga de gestionar otros aspectos como los menús de navegación, añadiendo enlaces de forma automática. También gestionan todos los módulos, internos o externos, que sean incorporados al sistema.

Dentro del ciclo de actividades que se corresponde con la funcionalidad de los CMS, es necesario definir un conjunto de roles o usuarios a los que se asocian una serie de tareas:

1. **Autor**: Que puede ser cualquier miembro usuario del sistema que desee publicar contenido.
2. **Publicador**: que revisa esa información y autoriza su publicación en tiempo y forma adecuadas.
3. **Administrador del Sistema**: desempeña funciones técnicas que consisten en optimizar el rendimiento y arquitectura del sistema. Pueden además proponer las plantillas de diseño y los sistemas de categorización más

adecuados, de acuerdo con los proveedores de información y de mantener el sistema en constante mejora y actualización.

La definición de roles o usuarios es dependiente de la plataforma final que se puede escoger como SGC, y van desde los presentados anteriormente hasta una definición de grano fino, donde se especifican roles intermedios y se diversifican más las tareas. El sistema de gestión de contenidos controla y ayuda a manejar cada paso de este proceso, incluyendo las labores técnicas de publicar los documentos a uno o más sitios.

23.1.3 Arquitectura general de los Sistemas de Gestión de Contenidos.

La arquitectura de estos sistemas es modular, proporcionando un marco de desarrollo que facilita la implementación de nuevas funcionalidades. En este sentido, los SGC incorporan una gran variedad de módulos que permiten extender el funcionamiento del sistema. Existen módulos para gestión integral de un sitio Web, para la gestión de páginas generadas dinámicamente, y otros módulos que posibilitan la personalización del sistema por parte del usuario.

Los SGC, a nivel de software, pueden definirse como un framework que habitualmente consta de dos partes diferenciadas:

- **Backend o parte administrativa:** A través del backend pueden controlarse todos los aspectos relativos a la configuración del framework, la administración del contenido (creación, categorización, edición, publicación, eliminación), la personalización del entorno de consulta (frontend), actualización y configuración de nuevas funcionalidades.
- **Frontend o parte pública:** A través del frontend se pueden consultar los contenidos publicados, acceder a las funcionalidades proporcionadas

para los usuarios configuradas desde el backend, y también sirve para recolectar ciertos datos de entrada.

La separación del sistema en frontend y backend es un tipo de abstracción que ayuda a mantener las dos principales partes del SGC separadas. Dentro de la arquitectura de SGC se contempla la existencia de una o varias bases de datos, responsables fundamentalmente de la persistencia del contenido publicado a través del CMS y de todos los datos relativos a la configuración del sistema.

El flujo básico es que gestor responde a las solicitudes de páginas que se plantean desde los lectores, recuperándolas la base de datos, componiendo las plantillas definidas y devolviendo al servidor web el contenido final que este ofrece al lector.

Los SGC, al ser aplicaciones web, se ejecutan en el servidor web donde estén alojados. Dependiendo de las tecnologías utilizadas para el desarrollo del SGC, la complejidad del servicio web que soporta la plataforma será mayor. El acceso a los SGC se realiza a través de los navegadores web. Cuando un usuario realiza una petición de una página, el gestor de contenidos es el encargado de interactuar con el servidor para generar una página dinámica, con un formato definido, y cuyo contenido se extrae de la base de datos.

23..4 Categorías

En cuanto a la categorización de los SGC, no existe una clasificación estricta, sino más bien, categorizaciones en función de determinadas características propias de los sistemas. Así pues, podemos clasificarlos en función del lenguaje de programación en el que se desarrollen, según su licencia (código abierto o software privativo), e incluso por su funcionalidad (Blogs, Wikis, Foros, ...)

23.1.5 Criterios de valoración

A la hora de proceder a la implantación de un SGC, es necesario tener en cuenta una serie de criterios que nos servirán para establecer, en función de la situación, cuál es el SGC más adecuado. Estos criterios son los siguientes:

- **Código abierto o código propietario:** En el caso de los SGC de tipo privativo, es decir, los comercializados por empresas bajo licencias restrictivas, no se permite el acceso al código fuente por parte de terceros. Sin embargo con los SGC de código fuente abierto, esta limitación no existe, dado que los desarrolladores sí que permiten el acceso libre y la modificación del código. Esta característica es muy importante puesto que el poder disponer del código fuente proporciona el poder modificar el producto, aportándole nuevas funcionalidades o incluso corrigiendo posibles errores. Esta es una faceta muy importante relacionada con la evolución del producto. Otra ventaja de los SGC de código libre es el coste, puesto que este tipo de gestores de contenido son gratuitos, sin ningún coste de licencias. En el caso de los SGC comerciales, el coste puede llegar a ser muy elevado, sobre todo para un particular. Además de todo esto, alrededor de los gestores de contenido de código libre suelen existir comunidades de usuarios que comentan sus experiencias con el uso de estos sistemas, aportan novedades y desarrollan nuevas funcionalidades.
- **Arquitectura técnica:** El SGC tiene que ser fiable, robusto y adaptable a futuras necesidades. Para ello, es preciso tener en cuenta cuál es la arquitectura del sistema, que tecnologías se han utilizado, y analizar el diseño de la plataforma, con el objetivo de poder emprender ampliaciones en las funcionalidades ofrecidas en caso de ser necesario. También es conveniente que permita separar contenido, presentación y estructura, de acuerdo con los estándares establecidos para el web. Para ello, es altamente recomendable decantarse por el uso de sistemas que



hagan uso de motores de plantillas, así como uso de definiciones de estilos basadas en hojas de estilo (CSS).

- **Grado de desarrollo:** Es muy importante que la herramienta seleccionada tenga un grado de madurez adecuado para poder desarrollar la funcionalidad requerida, y que se disponga de módulos o componentes para poderle añadir funcionalidad.
- **Soporte, posición en el mercado y opiniones:** La herramienta tiene que tener soporte tanto por los creadores como por los desarrolladores. Es fundamental que una herramienta que sea conocida por muchos usuarios y expertos, este hecho puede ayudar a posibles usuarios a decidirse por el SGC en cuestión. Habitualmente las grandes comunidades de usuarios y desarrolladores se encuentran alrededor de los SGC libres, proporcionando un marco ideal para el rápido desarrollo de estos sistemas así como de su mantenimiento.
- **Usabilidad:** Partiendo de la premisa de que existen diferentes roles con diferenciación clara de tareas, debemos de tener en cuenta que determinados perfiles de usuarios no tienen por qué tener conocimientos técnicos. Ello implica que el SGC tiene que ser fácil de aprender y utilizar.
- **Accesibilidad:** Tenemos que tener en cuenta que en el momento en que trabajamos con SGC, el sistema debe estar preparado para el uso por parte de la mayor cantidad de usuarios posible. Por tanto, es siempre recomendable que el portal web cumpla un estándar de accesibilidad.
- **Velocidad de descarga:** Es importante que las páginas solicitadas por los usuarios se carguen rápido. La naturaleza de las páginas dinámicas y la separación de estructura, presentación y contenido contribuyen a que las páginas sean más ligeras.

23.1.6 JOOMLA!

23.1.6.1 Introducción

Joomla! Es uno de los SGC con mayor impacto y distribución. Esto ha sido proporcionado por el hecho de ser un sistema de código abierto, desarrollado en uno de los lenguajes mayoritarios para Internet como es PHP. Está recogido bajo licencia GPL y actualmente cuenta con una de las mayores comunidades de usuarios y desarrolladores. Este administrador de contenidos puede trabajar en Internet o intranets y requiere de una base de datos MySQL, así como de un servidor web, preferiblemente HTTP Apache.

23.1.6.2 Arquitectura

En cuanto a su diseño, desde el punto de vista de desarrollo, Joomla! está programado en PHP bajo un patrón Modelo-Vista-Controlador, integrando un motor de plantillas, y permitiendo separar totalmente la capa de presentación de la lógica de los datos. Esta modularidad proporciona una gran facilidad para extender el sistema. Las funcionalidades en Joomla! se añaden a nivel de módulos o componentes. Estos módulos o componentes son partes del sistema que se implementan de forma independiente, bajo el patrón MVC, y se integran perfectamente dentro del SGC principal. Existen repositorios libre de la comunidad de usuarios y desarrolladores donde se pueden encontrar cientos de módulos gratuitos para extender las funcionalidades de Joomla!. Sin embargo, esta cuota también representa un modelo de negocio para muchas empresas que proporcionan sus productos en forma de módulos para Joomla!. Así pues, el diseño patronizado mediante MVC y el uso de tecnologías maduras como PHP y MySQL hace que resulte relativamente sencillo ampliar las funcionalidades de este SGC a partir de la implementación propia de módulos que satisfagan alguna funcionalidad concreta.

El SGC Joomla presenta una arquitectura en tres niveles: nivel de extensiones, nivel de aplicación y de desarrollo.

El nivel superior, de extensiones, se compone de extensiones del marco de desarrollo de Joomla y de sus aplicaciones. En esta capa se sitúan los módulos, componentes y plantillas (templates). El nivel del medio, de aplicación, consiste en una serie de aplicaciones que extienden del core para dar soporte a los módulos y componentes. Implementa también las aplicaciones necesarias para la administración (backend) así como la arquitectura principal del frontend. El nivel inferior, correspondiente al de desarrollo, consta del conjunto de clases PHP que lo forman, las bibliotecas que son utilizadas por el marco de desarrollo o se instalan para uso por los desarrolladores y finalmente los plugins, que extienden la funcionalidad.

Algunas características básicas que se incluyen en Joomla! son: sistema adaptado para mejorar el rendimiento web, versiones imprimibles de páginas y generación directa en pdf, módulos de flash con noticias, integración con blogs y foros, módulos nativos para la gestión de encuestas, calendarios, búsqueda en el sitio web e internacionalización del lenguaje. El nombre de Joomla! proviene de una pronunciación fonética para anglófonos de la palabra swahili jumla, que significa "todos juntos" o "como un todo". Fue escogido como una reflexión del compromiso del grupo de desarrolladores y la comunidad del proyecto.

23.1.6.3 Comunidad de desarrollo

La comunidad de Joomla, para el desarrollo de sus múltiples frentes, usa diferentes formas de comunicación como son el uso de salas de chat a través de IRC, participación en foros especializados, listas de correo, "wikis" y blogs. La gestión de administración principal del proyecto esta delegada al grupo principal, conocido como "Core Team". Este grupo de desarrolladores representa la columna vertebral del proyecto, ya que son los encargados de guiar a Joomla! dentro del movimiento de código abierto. Este grupo esta compuesto por diferentes perfiles, con variadas experiencias y totalmente multidisciplinar. Lleva activo desde el año 2005, aproximadamente con el nacimiento oficial de Joomla!. Su responsabilidad principal radica en la

organización con respecto Joomla en su estructura funcional como organización y no únicamente en la programación del sistema de gestión de contenidos.

Además del grupo principal o Core Team, existen también otros grupos que se han creado para enriquecer el conocimiento que la comunidad Joomla proporciona. Cada uno de los grupos se especializa en un aspecto específico de Joomla! que es importante para la expansión y desarrollo. El Core Team no puede estar en cada discusión de estos temas, por ello existe una estructura jerarquizada en donde un responsable de cada grupo de desarrollo se encarga de comunicarse de forma directa con el Grupo Principal.

Además del trabajo de la comunidad de usuarios y desarrolladores, existe una organización que proporciona soporte para muchos aspectos del proyecto. Se trata de la Open Source Matters Inc (OSM), que es una organización sin ánimo de lucro de origen estadounidense. El objetivo fundamental de esta organización es dar soporte a la parte legal y financiera del proyecto de código abierto Joomla. Recientemente la OSM se ha incorporado como una organización sin ánimo de lucro de Nueva York, proporcionando una garantía de continuidad para el proyecto y actividades futuras, proporcionando el soporte necesario para que las comunidades de usuarios y desarrolladores puedan seguir participando.

23.1.6.4 Principales características

Las principales características que han hecho de Joomla uno de los mejores SGC del momento son las siguientes:

- **Usabilidad de su interfaz:** Esta característica se hace principalmente notoria en la interfaz de administración. El objetivo fundamental es que cualquier persona sin conocimientos técnicos pueda tener control del sistema, para acortar la curva de aprendizaje de las tareas administrativas.



- **Gestión de contenido:** El sistema presenta una estructura jerárquica para gestionar el contenido basada en agrupaciones de artículos (la unidad fundamental de contenido) que se organizan en secciones y categorías. Permite crear menús y submenús, subir imágenes y ficheros, así como syndicar de forma nativa noticias mediante RSS.
- **Gestión de usuarios:** Existen dos tipos de usuarios básicos: los usuarios invitados, que son aquellos que acceden al portal navegando, que no poseen ninguna cuenta en el sistema y que habitualmente están capacitados para consultar los artículos, y los usuarios registrados que son aquellos que disponen de una cuenta (nombre de usuario/contraseña) para autenticarse en el sitio y acceder a funcionalidades específicas. Dentro de los usuarios registrados existen distintos roles cada uno con una serie de privilegios. La gestión de las cuentas y permisos de los usuarios en Joomla! puede hacerse de forma nativa, o bien haciendo uso de un sistema externo como LDAP.
- **Personalizable:** Gracias a la combinación del uso de estándares, y al diseño desacoplado proporcionado por el patrón MVC, la presentación del contenido se puede personalizar de forma muy sencilla. La apariencia del front-end es perfectamente modificable gracias al uso de plantillas. Las plantillas pueden modificarse de manera sencilla permitiendo que se adapten a las necesidades del sistema.
- **Extensibilidad:** Como ya se ha comentado con anterioridad, una de las principales características que definen a este software es la modularidad de la plataforma, que permite el desarrollo e integración de una gran cantidad de módulos y componentes que permiten extender las funcionalidades del sistema. La facilidad en el desarrollo de estas piezas software ha proporcionado que actualmente exista un gran número de extensiones y módulos existentes, programados por la comunidad de usuarios, que aumentan las posibilidades de la aplicación con nuevas características y que se integran fácilmente en el sistema. Como ejemplo de extensiones disponibles, se citan gestores de documentos, galerías de

imágenes multimedia, motores de comercio y venta electrónica, calendarios, etc.

- **Multiplataforma:** Debido a la utilización de tecnologías libres estandarizadas, este SGC puede correr sobre cualquier sistema operativo, ya sea GNU/Linux, en Windows o en Mac OSX. Los únicos requisitos son disponer en la máquina de un servidor web, y de una base de datos MySQL.

23.1.7 WORDPRESS

23.1.7.1 Introducción

La popularidad creciente de los blogs o bitácoras como medio popular para difundir contenido, ha tenido también cabida dentro del desarrollo de los Sistemas de Gestión de Contenidos. WordPress es un SGC enfocado precisamente a la creación de blogs, especialmente orientado a ofrecer comodidad para la ardua tarea de mantener los sitios web periódicamente actualizados.

Wordpress está desarrollado en PHP y MySQL, bajo licencia GPL, lo que también implica que es software libre y por tanto su código es modificable y adaptable. En este sentido, comparte muchas de las ventajas que esta filosofía otorga a otros SGC como Joomla!.

El fundador del proyecto de Wordpress es Matt Mullenweg. WordPress fue creado a partir del desaparecido b2/cafelog y actualmente es el SGC más popular orientado a la creación de blogs. Las causas de su enorme crecimiento están relacionadas con su licencia libre, la facilidad de uso y las características que proporcionan en general los sistemas de gestión de contenido.

Al igual que la mayoría de los SGC más populares, Wordpress está implementado bajo un patrón MVC. Sumado a esto, al proporcionarse como producto libre, se posibilita la labor de la enorme comunidad de desarrolladores para revisiones e implementación de módulos que añadan nuevas

funcionalidades. Éste es otro de los factores que ha proporcionado su creciente expansión.

Como ocurre con Joomla!, sumado al trabajo de la comunidad libre de desarrolladores, el liderazgo del proyecto recae sobre una entidad llamada Automattic.

23.1.7.2 Características

Algunas características básicas que definen Wordpress son las siguientes:

- Proporciona un sistema de publicación web basado en entradas ordenadas por fecha.
- La estructura y diseño visual del sitio depende de un sistema de plantillas, que es independiente del contenido en sí. Separación de la capa de presentación.
- Se apuesta decididamente por las recomendaciones del W3C, pero es dependiente siempre de la plantilla a usar.
- La gestión y ejecución corre a cargo del sistema de administración con los plugins y los widgets que usan las plantillas.
- Como en otros SGC, existe una jerarquía de usuarios/roles, y Wordpress permite múltiples autores o usuarios.
- Aunque el sistema está orientado a configurar un único blog o bitácora por sistema instalado, permite múltiples blogs o bitácoras.
- Dispone de múltiples herramientas para organizar el contenido (artículos) en categorías.
- Dispone de componentes visuales para la edición de los artículos (componentes WYSIWYG "What You See Is What You Get")
- Permite comentarios y herramientas de comunicación entre blogs.

- Dispone de funcionalidades necesarias para la sindicación de contenidos en los principales formatos estándar.(RSS 2.0 y ATOM 1.0).
- Subida y gestión de adjuntos y archivos multimedia.
- Sistema de búsqueda integrada dentro de la plataforma.

23.1.8 DRUPAL

23.1.8.1 Introducción

Otro de los más conocidos en el mundo de los SGC es Drupal. Drupal es un sistema de gestión de contenido, similar en cuanto su arquitectura y orientación a Joomla!. Es un sistema modular multipropósito y muy configurable. Permite gestionar y publicar artículos, imágenes, u otros archivos. Su diseño modular permite integrar una gran cantidad de servicios diferentes como foros, encuestas, votaciones, blogs y administración de usuarios y permisos.

Drupal es un sistema dinámico. Esto implica que, como el todos los anteriores, el contenido se almacena de forma persistente en una base de datos, y las páginas que se demandan desde el front-end de consulta son generadas dinámicamente. El sistema se encarga de acceder al contenido de la base de datos y montar la página que suministrará al servidor web.

Es un programa libre, con licencia GNU/GPL, escrito en PHP bajo un patrón de diseño MVC, lo que de nuevo facilita su modificación y adaptabilidad, potenciando el trabajo de la extensa comunidad de usuarios.

Algunas características propias de Drupal a nivel de desarrollo son la calidad de su código y de las páginas generadas. Hace especial hincapié en el respeto de los estándares de la web, y un énfasis particular en la usabilidad y consistencia de todo el sistema.

El diseño de Drupal lo hace especialmente idóneo para construir y gestionar comunidades en Internet. Sin embargo, gracias a sus características de flexibilidad y adaptabilidad, así como la gran cantidad de módulos adicionales disponibles, convierte a Drupal en un SGC de propósito general, capaz de adecuarse a muchos tipos diferentes de sitio web.

23.1.8.2 Características

Sus características principales son las siguientes:

- **Extensibilidad:** Gracias a la extensa comunidad de usuarios y desarrolladores, dispone de una gran cantidad de módulos con distintas funcionalidades: foro, galería, encuestas, boletín de noticias, correo electrónico, chat, etc.
- **Código abierto:** Al estar disponible el código fuente bajo los términos de la licencia GNU/GPL, es posible extender o adaptar Drupal según las necesidades.
- **Personalización:** La capa de presentación está perfectamente aislada del resto del sistema, haciendo la apariencia totalmente configurable en función de las preferencias de los usuarios.
- **Gestión de usuarios:** Como todo SGC, dispone de una jerarquía de usuarios/roles y de un sistema interno para gestionarlos y permitir la autenticación. Ésta última puede hacerse bien de forma local o utilizando un sistema de autenticación externo.
- **Gestión de contenidos:** Proporciona un sistema de control de versiones, que permite seguir y auditar todas las actualizaciones del contenido. Dispone de un sistema de temas o plantillas que permite separar el contenido del sitio de la presentación. También cuenta con la posibilidad de exportar el contenido en formato RDF/RSS para ser utilizado por otros sitios web.

- **Multiplataforma:** Puede funcionar con cualquier servidor web (Apache, Microsoft IIS) y en sistemas como Linux, Windows, Solaris, BSD y Mac OS X. Al estar implementado en PHP es portable.

23.2 E-LEARNING

23.2.1 Introducción

En los últimos años han aparecido sistemas informáticos orientados a la enseñanza y aunque el objetivo de todos ellos es muy similar, los medios mediante los cuales llegan a dicho objetivo varían en gran medida. El involucrar a las nuevas tecnologías en el ámbito de la enseñanza, introduciendo las mismas como herramienta fundamental del proceso de aprendizaje, ha desembocado en la aparición de un nuevo término conocido como eLearning. Las tecnologías asociadas se engloban en un conjunto de sistemas que tratan de proporcionar los medios y mecanismos adecuados para facilitar los procesos de aprendizaje en prácticamente todas las áreas de conocimiento. Sin embargo, muchos de estos sistemas, mal identificados como “sistemas de eLearning”, únicamente se centran en la gestión y clasificación de documentos para ponerlos a disposición de alumnos y docentes, como es el caso de los Sistemas de Gestión de Contenidos, o de los Sistemas de Gestión Documental. Aunque ciertamente facilitan la tarea de búsqueda y organización de información, este tipo de sistemas no realizan ningún tipo de seguimiento del proceso de aprendizaje de los alumnos.

La idea de eLearning, y en consecuencia, los sistemas de eLearning, pretenden precisamente abarcar esa fase del proceso de aprendizaje, proporcionando los mecanismos necesarios para realizar el seguimiento del proceso de forma íntegra.

23.2.2 Concepto

El concepto de eLearning se define de muchas formas diferentes, fundamentalmente debido a que los actores que de él hacen uso son muy diversos, cada cual con su idiosincrasia y su ámbito de aplicación.

A nivel general, se puede definir el eLearning como la educación a distancia completamente virtualizada a través de las nuevas posibilidades tecnológicas que hay disponibles, como las nuevas redes de comunicación, y fundamentalmente la red de red, Internet. Fundamentalmente se utilizan para ello herramientas o aplicaciones de hipertexto, que proporcionan la ventaja de ser totalmente portables y accesibles desde cualquier plataforma. La idea es que este tipo de sistemas den soporte a los procesos de enseñanza-aprendizaje. Este tipo de sistemas pueden englobarse como un subgrupo de los Sistemas de Gestión de Contenidos, entendiendo estos últimos como una generalización, y asumiendo los sistemas de eLearning como una especialización de los SGC para un propósito específico con funcionalidades propias.

Algunos teóricos dividen el eLearning en tres ramas diferentes:

- computer aid instruction (CAI)
- computer-managed instruction (CMI)
- computer supporter learning resources (CSLR)

El primer término abarca la porción de productos de eLearning que proporcionan enseñanza como tutoriales, simulaciones y ejercicios. El segundo término se refiere a los productos de eLearning que tienen funciones de evaluación, seguimiento y guía de estudio. Finalmente, el tercer término cubre los aspectos del eLearning que dan soporte al desempeño, la comunicación y el almacenamiento. Esta clasificación se refiere sólo a partes del conjunto total representado por el eLearning.

23.2.3 Plataformas de e-Learning

En la práctica, para llevar a cabo un programa de formación basado en eLearning, se hace uso de plataformas o sistemas de software que permitan la comunicación e interacción entre profesores, alumnos y contenidos. Se tienen principalmente dos tipos de plataformas:

- LMS (Learning Management Systems), utilizados para impartir y dar seguimiento administrativo a los cursos en línea.
- LCMS (Learning Content Management Systems), empleados para la gestión de los contenidos digitales. Siguen el concepto básico de los CMS, que es la administración de contenidos, pero enfocados al ámbito educativo.

A veces la diferenciación entre ambas es sólo funcional y en lugar de constituir dos herramientas software diferentes se ofrecen en una misma aplicación, que en España se conoce por el nombre de Plataforma Tecnológica o de Teledocencia.

Entre las herramientas más utilizadas para los ambientes o sistemas eLearning están, como ya se ha dicho anteriormente, los Sistemas de Administración de Aprendizaje o LMS, también ampliamente conocidos como plataformas de aprendizaje. Un LMS es un software basado en un servidor web que provee módulos para los procesos administrativos y de seguimiento que se requieren para un sistema de enseñanza, simplificando el control de estas tareas. Los módulos administrativos permiten, por ejemplo, configurar cursos, matricular alumnos, registrar profesores, asignar cursos a un alumno, llevar informes de progreso y calificaciones. También facilitan el aprendizaje distribuido y colaborativo a partir de actividades y contenidos pre-elaborados,

de forma síncrona o asíncrona, utilizando los servicios de comunicación de Internet como el correo, los foros, las videoconferencias o el chat.

El alumno interactúa con la plataforma a través de una interfaz web que le permite seguir las lecciones del curso, realizar las actividades programadas, comunicarse con el profesor y con otros alumnos, así como dar seguimiento a su propio progreso con datos estadísticos y calificaciones. La complejidad y las capacidades de las plataformas varían de un sistema a otro, pero en general todas cuentan con funciones básicas como las que se han mencionado. Entre las plataformas comerciales más comunes se encuentran Blackboard y WebCT, mientras que las más reconocidas por parte del software libre son Moodle y Claroline.

23.2.4 Ventajas

El eLearning permite superar algunas de las barreras existentes en los sistemas de enseñanza asistida por ordenador. Algunas de ellas son:

- Elimina las distancias y favorece la movilidad de los alumnos.
- Aumenta el número de destinatarios que pueden seguir un curso simultáneamente.
- Permite flexibilidad horaria.
- Permite alternar diversos métodos de enseñanza.
- Favorece la interacción entre alumnos. Está demostrado que la no presencia física minimiza la timidez y favorece el establecimiento de comunicación entre los alumnos, especialmente en la adolescencia.
- Anonimato.

- Seguimiento y tutoría del progreso del alumno a través de los canales de comunicación establecidos.
- Posibilidad de escoger entre gran variedad de materiales, cursos y especialidades.
- Minimiza los costes de formación continua en la empresa.
- Favorece la convivencia familiar para alumnos con responsabilidades familiares a su cargo.

Además de por las ventajas enumeradas, intervienen otros factores que favorecen la implantación de sistemas eLearning:

- **Factores económicos:** Se alcanza una mejor relación coste-beneficio en la producción y desarrollo aprovechando la reutilización de componentes tecnológicos y materiales de aprendizaje. Es un factor interesante a la hora de aumentar los niveles de formación en países en desarrollo, con un alto ritmo de crecimiento económico y con grandes necesidades de trabajadores cualificados.
- **Alta disponibilidad de recursos digitales:** Las grandes empresas multinacionales necesitan distribuir materiales de aprendizaje a sitios geográficamente dispersos, para que estén disponibles en cualquier momento desde cualquier lugar. La existencia de un gran número de recursos digitales libres y gratuitos en Internet (imágenes, clips de audio y vídeo, animaciones, etc.) favorecen su reutilización y aprovechamiento por parte de las grandes empresas (o terceros, como puede ser una empresa especializada en la creación de cursos o implantación de sistemas de eLearning) para la creación de cursos a través de sistemas eLearning.
- **Penetración social:** La alta penetración en la sociedad de las nuevas tecnologías en general y de Internet en particular, favorece la aceptación de nuevas vías de información y de comunicación.



- **Ayudas estatales:** Los programas de subvenciones por parte del Estado, las Comunidades Autónomas y el Fondo Social Europeo, han incentivado la creación y desarrollo de un sector empresarial dedicado a la formación on-line. Estas subvenciones han hecho posible la aparición de programas como los de Formación Continua de trabajadores, que contribuyen a la adaptación de los trabajadores a las más nuevas tecnologías.

23.2.5 Inconvenientes

Algunos inconvenientes en el empleo de sistemas de eLearning son:

- **Preparación del estudiante:** Es necesario un esfuerzo para asegurar que los estudiantes tienen las habilidades y conocimientos técnicos, así como el acceso al hardware y software necesarios para completar satisfactoriamente el curso basado en las TICs. Tanto la gestión del tiempo y las habilidades metacognitivas están relacionadas con las actitudes y la motivación del estudiante.
- **Personal dedicado:** Al igual que los estudiantes, los profesores deben tener habilidades técnicas, conocimiento y acceso al hardware y software, necesarios en este caso, para facilitar el diseño y desarrollo del curso basado en las TICs. Y deben tener un excelente manejo del tiempo y la motivación para proporcionar asistencia y llevar el seguimiento del estudiante. No obstante algunos autores diferencian rol del profesor, encargado de la selección de contenidos, seguimiento y asistencia al alumno, del rol del técnico encargado del diseño y creación del curso eLearning a partir de los contenidos, objetivos y metodologías, estableciendo de esta forma la necesidad de diferentes perfiles.
- **Gestión de la información:** A pesar de que se posean unas habilidades técnicas y un manejo del tiempo excepcionales, tanto los profesores

como los alumnos requieren de interfaces que reduzcan las cuestiones logísticas y técnicas. El uso de boletines y listas de distribución pueden ayudar a manejar la sobrecarga de información.

- **Equidad:** No todos los usuarios cuentan con las mismas facilidades de acceso a Internet. La tecnología incrementa las diferencias entre los que tienen y los que no tienen tales posibilidades.
- **Ancho de banda:** Este es uno de los mayores inconvenientes desde hace una década y que está desapareciendo rápidamente con la llegada de líneas de banda ancha. Actualmente, en Europa, el ancho de banda es aceptable y permite transmitir con buenos resultados audio y vídeo sincronizados sin los indeseables “saltos” de antaño.

23.2.6 Estandarización

Uno de los principales problemas de los sistemas de eLearning siempre ha sido reutilización de los contenidos, de forma que estos puedan ser utilizados en sistemas diferentes, debido a que la mayoría de los sistemas definían sus propios formatos de almacenamiento y procesamiento de los contenidos educativos, así como la forma de acceder y manejarlos. Esta falta de acuerdo se debe en gran medida a la descoordinación en el desarrollo de estándares para eLearning en la década pasada.

Hoy en día existen multitud de sistemas destinados a la enseñanza, ya sean meros gestores de contenidos, gestores del proceso de aprendizaje o sistemas más completos capaces de dar soporte a procesos administrativos, ofrecer herramientas de autoría y edición de cursos, etc. Sin embargo, a pesar de la variedad existente, su heterogeneidad dificulta la compatibilidad entre ellos. No todos son de código abierto, algunos usan formatos propietarios y generalmente no es posible reutilizar contenidos y estructuras de aprendizaje entre ellos.

Estas incompatibilidades, ya sean totales o parciales, repercuten negativamente en el coste asociado a la implantación de un sistema de eLearning, puesto que en el mejor de los casos, una vez superado el tiempo de aprendizaje de las distintas aplicaciones del sistema, sería necesaria la readaptación de material ya existente para otros sistemas, o en el peor de los casos, crear dicho material desde cero. Una especificación sobre aprendizaje virtual asegura que el nuevo material siga funcionando exactamente igual independientemente de la plataforma que se utilice, siempre que dichas plataformas cumplan la misma especificación.

23.2.7 Plataforma Moodle

23.2.7.1 Introducción

Moodle es un acrónimo de Module Object-Oriented Dynamic Learning Environment. Consiste en una plataforma que proporciona de forma integral mecanismos para la gestión de cursos. Moodle integra además las herramientas necesarias para crear y gestionar comunidades virtuales orientadas al aprendizaje online. Por tanto, podemos categorizar a Moodle como una plataforma tecnológica de tipo LMS (Learning Management System).

Originalmente Moodle fue creado por Martin Dougiamas. Basó el diseño de la plataforma partiendo de que el conocimiento se construye en la mente del estudiante en lugar de ser transmitido sin cambios a partir de libros. Existe también una importante apuesta por el modelo de aprendizaje colaborativo. El propósito es construir un ambiente centrado en el estudiante que le proporcione capacidad para generar ese conocimiento, basado en las habilidades y conocimientos propios de los tutores o profesores, en lugar de simplemente publicar y transmitir la información que se considera que los estudiantes deben conocer.

En conclusión, Moodle es un paquete de software para la creación de cursos y sitios web basados en internet, orientado a dar soporte a un marco de

educación constructivista. El sistema es multiplataforma y está registrado bajo licencia GNU/GPL.

En cuanto a la arquitectura de la plataforma, Moodle es una aplicación web que se ejecuta en servidores que soportan PHP y haciendo uso de base de datos para la persistencia de la información. Esa base de datos es única, y desde la versión 1.7 Moodle cuenta con una capa de abstracción que le permite seleccionar entre diversos motores de bases de datos, siendo MySQL y PostgreSQL las más utilizadas.

23.2.7.2 Principales características

Moodle, como sistema englobado dentro de los gestores de contenido, y a su vez como sistema específico de eLearning, tiene las siguientes características:

- Promueve una pedagogía constructivista social fundamentada en el trabajo colaborativo, la realización de actividades y debates.
- Su arquitectura y herramientas son apropiadas para clases en línea, además de servir como complemento del aprendizaje presencial.
- Tiene una interfaz de navegador de tecnología sencilla, ligera, y compatible.
- Para su puesta en producción, únicamente es necesaria una plataforma que soporte PHP y la disponibilidad de una base de datos. Gracias a su capa de abstracción, Moodle soporta los principales sistemas gestores de bases de datos.
- Es una plataforma segura. Todos los formularios son revisados y las cookies cifradas.

- Es adaptable y extensible. La mayoría de las áreas de introducción de texto pueden ser editadas usando el editor HTML, tan sencillo como cualquier editor de texto.

23.3 ACCESIBILIDAD Y USABILIDAD

23.3.1 Accesibilidad como calidad de los sistemas

La accesibilidad es una calidad de los sistemas informáticos vinculada al campo de la interacción entre humanos y ordenadores. Fundamentalmente se centra en la capacidad de acceso al uso de la aplicación o sistema informático que es objetivo por parte del usuario. En el campo concreto de las tecnologías web, accesibilidad hace referencia a la capacidad de acceso a la Web y a sus contenidos por todas las personas. La accesibilidad pretende facilitar el acceso a cualquier tipo de usuario independientemente de la discapacidad (física, intelectual o técnica) que presenten. También está relacionado con aquellas dificultades que se derivan del contexto de uso ya sean tecnológicas o ambientales. Esta calidad está íntimamente relacionada con la usabilidad de los sistemas.

A la hora de diseñar contenidos, hay que tener en cuenta los factores de accesibilidad que permitirán que cualquier tipo de usuario pueda acceder en condiciones de igualdad a la información almacenada. Existen mecanismos y estándares actualmente que trabajan sobre ello, y las tecnologías proporcionadas por la mayoría de los SGC permiten estructurar nuestros contenidos teniendo en cuenta este tipo de facetas. Un caso concreto se da con los sitios que tienen un código XHTML semánticamente correcto, permitiendo proporcionar un texto equivalente alternativo a las imágenes y a los enlaces. Esto supone que los usuarios ciegos puedan utilizar lectores de pantalla o líneas Braille para acceder a los contenidos. Lo mismo ocurre cuando

cuando los vídeos disponen de subtítulos; usuarios con dificultades auditivas podrán entenderlos perfectamente.

Los sistemas de gestión de contenido actuales permiten además cierta personalización de las características del sitio. Factores como el tamaño de letra o las proporciones de la interfaz comienzan a ser ya personalizables por cada tipo de usuario, proporcionando ayuda para que los usuarios con problemas visuales puedan leerlos sin dificultad.

23.3.2 Limitaciones en la accesibilidad

Existen fundamentalmente cuatro tipos de limitaciones en la accesibilidad de los sitios Web:

- Visuales: Abarcando un amplio abanico de patologías y de distintos grados de deficiencia visual, que pueden ir desde la baja visión a la ceguera total, además de problemas para distinguir colores.
- Motrices: Dificultad o la imposibilidad de usar las manos, incluidos temblores, lentitud muscular, debido a enfermedades como el Parkinson, distrofia muscular, parálisis cerebral o amputaciones.
- Auditivas: Sordera o deficiencias auditivas.
- Cognitivas: Dificultades de aprendizaje o discapacidades cognitivas que afecten a la memoria, la atención, las habilidades lógicas, etc.

23.3.3 Promoviendo la accesibilidad

La tarea de promover la accesibilidad en el entorno web corre a cargo del grupo de trabajo Web Accessibility Initiative (WAI), que depende directamente

del World Wide Web Consortium. En 1999 el WAI publicó la versión 1.0 de sus pautas de accesibilidad Web (WCAG). Con el paso del tiempo se han convertido en un referente internacionalmente aceptado hasta que en diciembre del 2008 las WCAG 2.0 fueron aprobadas como recomendación oficial.

Estas pautas se dividen en tres bloques orientadas específicamente para cada uno de los principales perfiles que forman parte de un proyecto de desarrollo web:

- **Pautas de Accesibilidad al Contenido en la Web (WCAG):** Están dirigidas a los profesionales del diseño y desarrollo web y proporcionan información y recomendaciones acerca de cómo hacer que los contenidos del sitio Web sean accesibles.
- **Pautas de Accesibilidad para Herramientas de Autor (ATAG):** Están dirigidas a los desarrolladores del software que usan los webmásters, con el objetivo de proporcionar un mejor soporte para la construcción de sitios accesibles.
- **Pautas de Accesibilidad para Agentes de Usuario (UAAG):** Están dirigidas a los desarrolladores de Agentes de usuario (navegadores y similares), para que estos programas faciliten a todos los usuarios el acceso a los sitios Web.

23.3.4 Usabilidad

La usabilidad es otro atributo vinculado a los sistemas software, particularmente importante en el campo de la interacción hombre-computador. Actualmente la usabilidad está reconocida como un importante atributo de calidad del software. Actualmente no llega con fabricar sistemas con alto rendimiento y fiabilidad, sino que el objetivo es crear sistemas que sean cómodos y manejables, adaptados para los usuarios finales. En el marco de la

usabilidad se ha generado un importante centro de servicios en el que empresas especializadas desarrollan sus actividades fundamentalmente orientadas a la asesoría en estos campos.

En los proyectos de desarrollo de software en general, y en los orientados a la distribución y gestión de contenidos en particular, el concepto de usabilidad es de importancia capital. A la hora de distribuir contenido a través de la red, el portal está abierto a todo tipo de usuarios. Esta faceta comparte importancia con el concepto anterior de accesibilidad. Pero además, la usabilidad permite incrementar el atractivo, desarrollando sistemas sencillos e intuitivos que permiten un fácil manejo y rápido aprendizaje.

Desde un enfoque del diseño y evaluación de aplicaciones software, hablamos de usabilidad software como un conjunto de fundamentos teóricos y metodológicos que aseguran el cumplimiento de los niveles de usabilidad requeridos.

23.4 W3C

El World Wide Web Consortium, abreviado W3C, es el máximo organismo a nivel mundial que se encarga de gestionar y publicar las recomendaciones y estándares asociados al World Wide Web. Es decir, el objetivo de este consorcio es estandarizar los protocolos y las tecnologías utilizadas para construir la web, de manera que el contenido este disponible para la mayor parte posible de la población del mundo. Las principales actividades a las que se dedica son, a la coordinación de los diferentes grupos de trabajo en el ámbito de la generación de:

- Especificaciones y estándares: sobre tecnologías asociadas al WWW.

- Directrices: y recomendaciones de desarrollo para buenas prácticas.
- Herramientas: que permitan validar la aceptación y cumplimiento de los estándares y recomendaciones propuestas.

Está dirigida por Tim Berners-Lee, responsable del grupo de investigación que desarrolló la URL, el protocolo HTTP (HyperText Transfer Protocol, Protocolo de Transferencia de HiperTexto), así como también del lenguaje de etiquetado HTML (Lenguaje de Marcado de HiperTexto) que son las principales tecnologías sobre las que se basa la Web.

Se creó en 1994 en el MIT, actual sede central del consorcio. El consorcio está formado por una gran diversidad de miembros y entidades cada una de las cuales colabora en los ámbitos en los que el W3C ejerce su función. Actualmente está integrado por tres tipos de figuras principales:

- Miembros adscritos del W3C: garantizan la fortaleza y el sentido del Consorcio a través de la inversión y la participación activa en las Actividades del W3C. El W3C cuenta con más de 400 organizaciones Miembro provenientes de más de 40 países, con intereses muy variados. Entre los Miembros del W3C se incluyen proveedores de productos de tecnología y servicios, proveedores de contenido, usuarios corporativos, laboratorios de investigación, organismos de estandarización y administraciones, que trabajan conjuntamente para alcanzar un acuerdo sobre la dirección que debe tomar la Web.
- Equipo W3C (W3C Team): El Equipo del W3C incluye a más de sesenta investigadores e ingenieros de todo el mundo que dirigen las actividades técnicas del W3C y gestionan las operaciones del Consorcio. La mayoría de los componentes del Equipo del W3C trabajan en una de las tres



instituciones que albergan al W3C: El MIT/CSAIL, en los Estados Unidos; el ERCIM, las oficinas centrales en Francia; y la Universidad de Keio, en Japón. Están coordinados por el Director Tim Berners-Lee, el Director de Operaciones Steve Bratt, y un Equipo de Dirección, los trabajadores del W3C:

- Se mantienen informados sobre las nuevas tecnologías, las fluctuaciones del mercado y las actividades de organizaciones relacionadas, con intención de orientar al W3C adecuadamente.
- Organizan las Actividades del W3C para, así, cumplir el mayor número de objetivos dentro de unos límites prácticos (tales como los recursos disponibles).
- Promueven la cooperación entre los Miembros, a la vez que buscan su diversidad, incentivan la innovación, y facilitan su activa participación.
- Divulgan los resultados del W3C a los Miembros y a la prensa, y promueven su aceptación en la comunidad Web; vea la lista de presentaciones públicas realizadas por el Equipo.
- Oficinas W3C (W3C Offices): El objetivo de las Oficinas del W3C es trabajar con las comunidades regionales para potenciar la adopción de las recomendaciones del W3C entre los desarrolladores, los creadores de aplicaciones, y los difusores de estándares, así como fomentar la inclusión de las organizaciones más importantes en la creación de futuras recomendaciones a través de su adscripción al Consorcio.

23.5 BIBLIOGRAFÍA

- ***“SILVERSTRIPE: THE COMPLETE GUIDE TO CMS DEVELOPMENT”.***
INGO SCHOMMER Y STEVEN BROSCHART. ED. WILEY, 2009. ISBN:
04 7068183 1.
- *“WordPress, The best Content Management System (CMS) Guide by Heinz Duthel”.* Heinz Duthel. Ed. IAC Society, 2010.
- *“The Official Joomla! Book”.* Jennifer Marriott, Elin Waring. Ed. Addison-Wesley Professional, 2010. ISBN: 03 217 0421 5.
- *“Using Drupal”.* Angela Byron, Addison Berry, Nathan Haug, Jeff Eaton, James Walker, Jeff Robbins. Ed. O'Reilly Media, 2008. ISBN: 05 965 1580 4.
- *“e-Learning and the Science of Instruction: Proven Guidelines for Consumers and Designers of Multimedia Learning”.* Ruth C. Clark, Richard E. Mayer. Ed. Pfeiffer, 2007. ISBN: 07 879 8683 6
- *“World Wide Web Consortium”.* www.w3c.es, www.w3c.org.

Autor: Francisco Javier Rodríguez Martínez

Subdirector de Sistemas Escola Superior Enxeñaría Informática Ourense

Colegiado del CPEIG

**24. MOTORES DE BUSQUEDA.
HERRAMIENTAS
COLABORATIVAS. CORREO
ELECTRÓNICO. LISTAS DE
DISTRIBUCIÓN. GRUPOS DE
NOTICIAS DE RED (NNTP).
FOROS DE DISCUSIÓN. CHAT.
SISTEMAS DE
VIDEOCONFERENCIA.
MENSAJERÍA INSTANTÁNEA.**

Tema 24: Motores de búsqueda. Herramientas colaborativas. Correo electrónico. Listas de distribución. Grupos de noticias de red (NNTP). Foros de discusión. Chat. Sistemas de videoconferencia. Mensajería instantánea.

ÍNDICE

24.1.1 Spiders.....	3
24.1.2 Directorios.....	4
24.1.3 Sistemas mixtos (directorio y motor de búsqueda).....	4
24.1.4 Metabuscadores.....	5
24.1.5 Multibuscadores.....	5
24.2.1 Características.....	9
24.2.1 Groupware.....	10
24.2.2 Workflows.....	11
24.3.1 Elementos del servicio de correo electrónico.....	12
24.3.2 Dirección de correo electrónico.....	15
24.3.3 Proceso de envío de mensajes.....	15

24.1 MOTORES DE BÚSQUEDA

En los inicios, internet comenzaba ofrecer una gran cantidad de información, que difícilmente podía ser catalogada y referenciada. Esto suponía un impedimento a la hora de realizar búsquedas de información relativas a temáticas concretas, provocando una alta ineficiencia a nivel general en el uso de internet y el acceso a la red para la búsqueda y/o divulgación de la información. Como solución para este problema surgieron los motores búsqueda.

Los motores de búsqueda, también conocidos como buscadores, son sistemas software que se encargan de localizar sitios web relacionados con un determinado conjunto de términos clave que se le suministran. En esencia, son un sistema informático que consulta los ficheros de las web que se encuentran almacenadas en los servidores web. Para realizar esta tarea, habitualmente utilizan una pieza de software específicamente diseñado para analizar la red en busca de webs y obtener información que permita clasificarlas mediante términos clave o bien utilizando árboles jerárquicos por temas.

La solución ofrecida por los motores de búsqueda no es total, sino parcial. Esto es debido a que en realidad no buscan en Internet cada vez que realizamos una consulta. La búsqueda la realizan en una base de datos en la cuál almacenan referencias de las páginas accesibles junto con datos concretos, metainformación, que sirve para catalogarlas. Esta información habitualmente se recoge a través de un programa (habitualmente robot) que es el que se encarga de realizar visitas periódicas por todo el contenido disponible del web. No existe unicidad en los criterios de selección para la agregar nuevas páginas a las base de datos de los motores de búsqueda. El resultado es que cada base de datos contiene información de muy diversa calidad, especificando sus propios criterios de selección, y

consecuentemente, estableciendo categorizaciones y resultados diferentes para cada búsqueda en función del motor de búsqueda con el que estemos trabajando.

A nivel general, se pueden distinguir cinco tipos básicos de motores de búsqueda, diferenciados entre sí fundamentalmente por el tipo de información que albergan, o los mecanismos que utilizan para realizar la referenciación de las páginas que ofrecen. Estos cinco tipos son los spiders, directorios, sistemas mixtos, metabuscadores y multibuscadores.

24.1.1 Spiders

Los Spiders, también conocidos como arañas web o crawlers, son programas que revisan las páginas web de forma metódica y automática. Habitualmente realizan copias de las páginas web visitadas para un procesamiento posterior que consiste en indexar dichas páginas en función de su contenido, determinado por conjuntos de términos clave, para proporcionar un sistema de búsqueda posterior más optimizado.

El funcionamiento es simple. La araña se inicia con una lista de URLs o páginas a visitar. A medida que va consultando las páginas, va añadiendo todos los hipervínculos que se encuentran en dichas páginas a una lista de URLs que visitará de forma recurrente en función de unas reglas establecidas. Las visitas se realizan de forma periódica, por tanto, es posible que en determinadas ocasiones el contenido no aparezca totalmente actualizado. El orden en que se muestran los resultados de la consulta está determinado por diversos factores que dependen de cada buscador en particular,.

La gran mayoría de los buscadores que se utilizan habitualmente entran dentro de la categoría de Spiders. Son sistemas costosos, que hacen uso intensivo de una gran cantidad de recursos.

Algunos ejemplos de “Spiders” son Google, Bing o Hotbot

24.1.2 Directorios

Los directorios son un tipo de motores de búsqueda con un funcionamiento totalmente distinto de los “Spiders”. Los directorios son simplemente listas categorizadas de recursos, que se estructuran jerárquicamente. Esta estructura se organiza en forma de árbol, permitiendo visualizar los contenidos con diferente grado de granularidad, desde los más generales a los más específicos.

En realidad estos motores no disponen de ningún software específico que analice los contenidos web, sino que realiza las clasificaciones y categorizaciones del material en función de un conjunto de criterios seleccionados de forma manual. Esto implica que la tecnología en la que se basan sea barata y sencilla, sin embargo el coste operacional es alto, ya que siempre se requiere de intervención humana.

Algunos ejemplos de directorios son Yahoo! y Open Directory Project

24.1.3 Sistemas mixtos (directorio y motor de búsqueda)

Los sistemas mixtos combinan características de directorios y motores de búsqueda. Disponen habitualmente de alguna pieza software de tipo “Spider” para realizar el análisis de la web, y además permiten añadir y presentar páginas clasificadas en catálogos según su contenido.

La combinación de estas características representa la tendencia actual en los buscadores más importantes.

24.1.4 Metabuscadores

Los metabuscadores son un tipo de motores de búsqueda que centran sus resultados en búsquedas que realizan sobre otros buscadores. Esto significa que obtienen inicialmente un conjunto de resultados de otro buscador, y a continuación refinan esos resultados presentando una selección propia.

Una de las principales ventajas de los metabuscadores es que amplían el ámbito de las búsquedas que realiza el usuario. Proporciona una gran cantidad de resultados combinados en función de los criterios particulares de cada metabuscador. En muchas ocasiones estos criterios de ordenación no resultan del todo claros.

Por otro lado, el problema principal es que los metabuscadores no distinguen entre las diferentes sintaxis de los buscadores, limitando la especificidad con la que los metabuscadores pueden trabajar para localizar información. Además, al realizar las búsquedas en diferentes fuentes (buscadores), la obtención de resultados suele demorarse mucho más que al utilizar otro tipo de motor de búsqueda.

Algunos ejemplos de metabuscadores son Metacrawler, Ixquick, Dogpile o Metabuscador

24.1.5 Multibuscadores

Los multibuscadores son un tipo de motores de búsqueda similares a los metabuscadores, pero con una diferencia notable; mientras que los metabuscadores no distinguen las diferentes sintaxis de los buscadores que utilizan para la obtención de resultados, los multibuscadores sí lo hacen. Esto implica que puedan lanzar varias búsquedas en motores seleccionados respetando el formato original de los buscadores.

Los multibuscadores son útiles para realizar búsquedas en diferentes buscadores al mismo tiempo. Su operativa difiere de los buscadores normales, dado que no disponen de componentes software que analicen y almacenen contenido, sino que lo único que contienen es un registro de buscadores y los criterios de adecuación de las expresiones de búsqueda asociadas a cada buscador. Los multibuscadores no almacenan información de páginas relativas a contenido. Simplemente realizan la consulta adecuada a cada buscador dentro de su registro, y realizan un filtrado de los enlaces repetidos, y aplican además criterios de selección como la relevancia de cada enlace en los diferentes buscadores, para generar finalmente una lista de resultados. Un ejemplo de multibuscador es iniciodirecto.com.

24.2 HERRAMIENTAS COLABORATIVAS

Las herramientas colaborativas son aquellas que proporcionan los medios adecuados para que los usuarios finales puedan interactuar entre sí y alcanzar metas comunes. Son aplicables a cualquier campo de desarrollo. Habitualmente se las conoce como sistemas colaborativos o Groupwares. Estos sistemas dan un mayor énfasis a la utilización de ordenadores para la interacción de las personas. Se basan en la adopción de un espacio de trabajo virtual y compartido denominado Workplace, definido como un

sistema que proporciona procesamiento de información y actividades comunicativas.

Existen diversas maneras para clasificar los sistemas colaborativos, pero dentro de este área se suele utilizar una clasificación básica que permite entender las interacciones principales entre personas, conocida como matriz de espacio y tiempo. Esta matriz nos permite entender las interacciones principales entre los distintos tipos de taxonomías mediante las cuáles se puede clasificar un sistema colaborativo, con respecto al tiempo y espacio.

El trabajo colaborativo en cuanto a tiempo, puede ser sincrónico o asíncrono:

- **Sincrónico:** los individuos que hacen uso de los sistemas o herramientas colaborativas lo hacen al mismo tiempo.
- **Asincrónico:** Los individuos que trabajan lo hacen en distintos instantes de tiempo.

En cuanto al espacio, el trabajo en grupo se divide en dos tipos: en el mismo espacio de trabajo o en espacios distintos. Cuando se habla de mismo espacio de trabajo, hace referencia al mismo lugar físico donde el grupo de personas trabaja, lo cual a su vez puede darse en el mismo momento del tiempo o en momentos distintos. De la misma manera los integrantes pueden trabajar en distintos lugares físicos al mismo o distinto tiempo.

Según esta clasificación, observamos que el trabajo colaborativo tiene cuatro alternativas de reuniones, las cuales vendrían de una mezcla entre los tiempos y espacios posibles de colaboración.

Mismo tiempo

Diferentes tiempos

Mismo lugar	Interacción sincrónica cara a cara	Interacción asíncrona
Diferentes lugares	Interacción sincrónica distribuida	Interacción asíncrona distribuida.

Estas cuatro categorías nos muestran una gama de colaboración posible en la taxonomía espacio tiempo:

- Colaboración sincrónica cara a cara: Se da cuando las personas están trabajando al mismo tiempo y en el mismo lugar. Este tipo de colaboración se produce usualmente en una sala de reuniones, pudiendo estar trabajando en un presupuesto entre varias personas o en el proceso de enseñanza y aprendizaje dentro de una sala de clases.
- La interacción asíncrona se refiere a los procesos que ocurren en un mismo lugar pero en distintos instantes. Esto puede realizarse a través de un fichero en una oficina o universidad.
- En la interacción sincrónica distribuida las personas se encuentran en distintos lugares, pero están trabajando o interactuando al mismo tiempo. Esto podría ser una llamada por teléfono o una conferencia telefónica, algún tipo de Chat o una vídeo conferencia.
- Cuando los participantes que están realizando el proceso de colaboración están en diferentes lugares y cada uno trabaja en los tiempos que más le acomode, entonces decimos que la colaboración se denomina asíncrona distribuida. Usualmente en esta área tienen lugar los sistemas que apoyan la producción de un material final con la preparación de material individual, los sistemas de correos electrónicos y workflow (automatización de los procesos que se usan diariamente en una empresa).

24.2.1 Características

Las herramientas colaborativas en general comparten una serie de características comunes, pero un sistema Groupware debe tener en cuenta al menos cuatro aspectos fundamentales para el soporte eficiente de un proceso colaborativo:

- Percepción o conciencia de grupo
- Comunicación
- Coordinación
- Memoria de grupo

El concepto de percepción en sistemas colaborativos se puede ver como el contexto personal de trabajo basado en el entendimiento de las actividades de los demás miembros del grupo. La ausencia de percepción deja a los participantes en un estado similar al bloqueo de sus sentidos, imposibilitando su interacción con los demás. La manipulación de artefactos en un sistema colaborativo, especialmente en sistemas síncronos de tiempo real, debe proporcionar información acerca de las manipulaciones realizadas por el resto de participantes en esos artefactos. Esa información se conoce como “feedback” o retroalimentación.

También es necesario proporcionar diferentes mecanismos de comunicación (síncronos y asíncronos), que permitan crear las condiciones adecuadas para que se den los procesos de intercambio de información.

Por otro lado, se debe garantizar el acceso a los artefactos generados, su creación y mantenimiento de forma cooperativa, previniendo y evitando fallos de coordinación que lleven a situaciones como duplicación

de la información o varios participantes intentando utilizar concurrentemente un recurso compartido.

24.2.1 Groupware

El Groupware es un tipo de software colaborativo que ayuda a grupos de trabajo a realizar sus actividades a través de una red.

Las características más importantes de los groupware son:

- Proveer de un ambiente de colaboración, en el que realmente se perciba que el trabajo en grupo se lleva a cabo.
- Mantener la información en un solo sitio común para todos los miembros.
- Interactuar con otros usuarios, de forma escrita, voz o vídeo.

Los groupware se pueden clasificar en base a tiempo y espacio. En base al tiempo se clasifican en sincrónicos y asincrónicos; y en base al espacio, pueden estar en el mismo lugar o en forma distribuida. Las aplicaciones típicas de los groupware sincrónicos (los cuales soportan aplicaciones en tiempo real) son: pizarrones compartidos, teleconferencia, chat y sistemas de toma de decisiones.

Algunos ejemplos de aplicaciones típicas de los groupware asincrónicos son: e-mail, newsgroups, calendarios y sistemas de escritura colaborativos. Los groupware se están volviendo más populares dentro de las empresas, ya que resulta más barato instalar una Intranet y comprar o implementar un sistema de colaboración a estar transportando personal de un lugar a otro. Además si se necesita tomar una decisión urgente y las

personas se encuentran en diferentes partes del mundo, para cuando se reúnan la decisión posiblemente ya no funcione, o peor aun que la empresa quiebre; con los Groupware esto no pasaría, ya que se pueden tomar decisiones sin importar la distancia entre cada miembro del equipo.

24.2.2 Workflows

Los Workflows son sistemas que ayudan a administrar y automatizar procesos de negocios. Un workflow puede ser descrito como el flujo y control en un proceso de negocio. Entre los ejemplos de proceso de negocios tenemos: procesamiento de órdenes, informes de gastos, procedimientos de producción, etc. Cabe mencionar que los workflows son solo un camino para la información, para reducir tiempo, dinero y esfuerzo en la ejecución de un proceso de negocio. Las funciones más comunes que proporcionan los workflows son:

- Asignación de tareas al personal.
- Aviso al personal de tareas pendientes.
- Permitir la colaboración en las tareas comunes.
- Optimización de recursos humanos y técnicos, alineándolos a la estrategia de la empresa.

24.3 CORREO ELECTRÓNICO

El correo electrónico, o email, está catalogado como un servicio de red, que proporciona a los usuarios la capacidad para enviar y recibir

mensajes y archivos de forma rápida y eficiente a través de dispositivos digitales. El sistema trata de representar una analogía con el correo postal habitual, presentándose como una alternativa para el envío de mensajes de texto o cualquier tipo de fichero en formato digital. Dado que su coste operacional es bajo y su eficiencia es elevada, el correo electrónico está actualmente desplazando al correo postal original.

El origen del correo electrónico es anterior incluso a la red Internet. Los primeros pasos para la creación del sistema de correo electrónico se dieron en el MIT entorno a 1961, cuando se desarrolló un sistema que permitía a varios usuarios, desde terminales remotos, ingresar en un mainframe en el cual podían almacenar una copia de sus archivos en el disco. Éste fue uno de los pasos iniciales en la implementación de mecanismos para la compartición de información. En 1965 comenzó a utilizarse un sistema basado en el almacenamiento de mensajes compartidos entre los usuarios de una supercomputadora dando lugar al primer sistema de email utilizado. Posteriormente, en 1971, se incorporó al sistema de mensajería el uso de la arroba (@) como elemento para dividir el nombre de los usuarios de la máquina en la que se encontraban alojados.

24.3.1 Elementos del servicio de correo electrónico

Técnicamente hablando, el correo electrónico es un servicio proporcionado en internet, soportado por el protocolo SMTP (Simple Mail Transfer Protocol) y el protocolo POP (Post Office Protocol). Como en todo servicio, la arquitectura del sistema consta de una parte cliente, habitualmente utilizada por los usuarios para enviar y recibir correos, y una parte servidora, que proporciona los mecanismos adecuados para el almacenamiento y transferencia de los correos entre los diferentes clientes.

Los protocolos definen los esquemas de comunicación entre los clientes y los servidores para que los mensajes se transmitan de un sitio a otro. El protocolo SMTP es el protocolo encargado del envío de los mensajes, mientras que el protocolo POP es el encargado de la recepción de los mensajes.

El **cliente de correo electrónico**, también llamado **Mail User Agent (MUA)** es un programa que básicamente permite gestionar los mensajes recibidos así como recibir correos nuevos. Habitualmente se hace referencia a cliente de correo electrónico, se hace referencia a aplicaciones stand-alone que proporcionan un amplio abanico de funcionalidades para la gestión de nuestro correo. Sin embargo, actualmente la mayoría de los proveedores de servicio de correo permiten el acceso a través de los navegadores web, proporcionando interfaces web a modo de cliente para la consulta y gestión de nuestro correo electrónico. Existe una gran diferencia respecto del funcionamiento de ambas opciones; cuando se utiliza un cliente de correo electrónico, todos los mensajes disponibles se descargan en el ordenador en el que se esté ejecutando ese cliente de correo electrónico. Sin embargo, cuando se accede a la cuenta de correo a través de las interfaces web, los mensajes siguen almacenados en el servidor, siendo accesibles a través del cliente web, desde cualquier ordenador que disponga de una conexión a Internet.

Algunos ejemplos de clientes de correo electrónico stand-alone son:

- **Microsoft Outlook:** Cliente privativo de la compañía Microsoft. Es el cliente de correo estándar de Microsoft, incluido en el paquete Microsoft Office.
- **Mozilla Thunderbird:** Alternativa de software libre de Outlook, desarrollado por Mozilla.

Algunos ejemplos de proveedores de servicio de correo web son gmail, hotmail o yahoo!.

En cuanto al **servidor de correo electrónico** consiste en un conjunto de aplicaciones informáticas ubicadas en un equipo servidor, ya sea en red local o en Internet, cuya tarea consiste en realizar una serie de procesos que tienen la finalidad de transportar información entre los distintos usuarios del servicio. El servidor de correo electrónico es el encargado de gestionar a todos los usuarios registrados en el sistema con sus correspondientes identificaciones (direcciones de correo electrónico) que servirán para poder interactuar entre sí mediante el envío de correos.

El **servidor de correo electrónico**, dispone de una pieza software denominada Agente de Transferencia de Correo (MTA) o Agente de Transporte de Mensajes, cuyo objetivo consiste en transmitir los datos de una máquina a otra. En concreto, se centra en la parte de transferencia de datos entre distintos servidores, ejerciendo diferentes roles como servidor de otros servidores de correo, cliente de otros servidores de correo y como intermediario entre el cliente de correo que emite el mensaje y otro servidor de correo externo.

Actualmente, a excepción de las grandes corporaciones que disponen de su propia infraestructura TIC, la mayoría de los usuarios hacen uso de servidores de correo electrónico que pertenecen a alguna entidad proveedora de dicho servicio. Existen diferentes empresas y entidades que ofrecen servicios de correo electrónico, tanto de forma gratuita como de pago. Los servicios de correo gratuito son los más conocidos por los usuarios, y entre ellos podemos destacar los servicios de gmail, hotmail o yahoo!. Las entidades registradoras de dominio son las que habitualmente ofrecen servicios de correo electrónico asociados a la cuenta de dominio contratada. En cuanto a las soluciones software para la implantación de un servidor de correo electrónico, pueden destacarse Microsoft Exchange Server para plataformas Windows o Sendmail, Qmail, Zimbra y Postfix para Unix/GNULinux.

24.3.2 Dirección de correo electrónico

La dirección de correo electrónico es una secuencia de palabras que tienen por objeto identificar a un determinado usuario de un servicio de correo de forma inequívoca. Esta dirección de correo representa el identificador mediante el cuál el usuario puede enviar y recibir correos.

La sintaxis de una dirección de correo es la siguiente:

- **Nombre de usuario:** Es conjunto de palabras escogidas por el usuario que habitualmente suele coincidir con el nombre o algún identificativo de la persona o usuario que utilizará la cuenta de correo. Puede contener letras, números y algunos signos.
- **@:** es el signo o símbolo encargado de separar dos partes importantes de la dirección de correo, concretamente el nombre de usuario y el dominio.
- **Nombre de dominio:** El nombre de dominio en internet es una identificación asociada a un dispositivo o grupo de dispositivos. Habitualmente se corresponde con el nombre del proveedor del servicio de correo.

24.3.3 Proceso de envío de mensajes

Se detalla a continuación el proceso de envío y recepción de correos electrónicos y los elementos y protocolos que intervienen entre un ordenador A y un ordenador B.

El ordenador con el cliente A redacta un correo electrónico para el cliente B y lo envía. Al realizar la operación de envío, el cliente de correo en A contacta con el Servidor de correo A a través del protocolo SMTP, le transfiere el correo y le da la orden de enviarlo. Al recibir la petición, el servidor de correo A verifica que el correo pertenece a otro dominio. Para resolver la dirección a la cuál tiene que enviar el correo, realiza una consulta a un servidor de DNS para averiguar quién es el encargado de gestionar el dominio asociado al cliente B. Una vez obtenida la respuesta, y resuelto el servidor de correo B, el servidor de correo A se comunica con él a través del protocolo SMTP, enviándole el correo emitido desde el cliente A, y quedando este correo almacenado en el servidor B. Posteriormente, cuando el cliente B decida consultar el correo, accederá mediante el protocolo POP al servidor de correo B y se descargará los mensajes almacenados en dicho servidor que tengan por destinatario al usuario de Cliente B.

24.4 LISTAS DE DISTRIBUCIÓN

Las listas de distribución, o listas de correo electrónico son agrupaciones de usuarios de correo electrónico. Mediante un software apropiado se pueden configurar listados de direcciones de email para el envío masivo de información a múltiples usuarios a la misma vez. Cada lista de distribución de correo electrónico está a su vez referenciada por una dirección email. A grandes rasgos, cada vez que un usuario autorizado emite un email con la dirección de la lista de distribución como destinatario, en realidad la lista reenviará el email a todos los usuarios adscritos a esa lista.

Las listas de correo electrónico son una de las herramientas cada vez más utilizadas en las organizaciones para mantener a los usuarios informados con noticias e información de interés. De forma habitual, es necesario que los propios usuarios se registren en esas listas de las cuáles están interesados en recibir noticias o información.

Las listas de correo electrónico están gestionadas por el propio servidor de correo, o por software adicional específico para su gestión. Para el alta, baja o modificación de los datos de los usuarios, es habitual que los servidores de listas de correo electrónico pongan a disposición de los usuarios una o varias direcciones de correo a las cuáles enviar comandos. Además algunos servidores de listas de correo permiten diferentes modos de subscripción:

- Modo individual: el usuario de la lista recibe todos los mensajes que formen parte de la misma. De la misma forma, si el usuario dispone de los privilegios necesarios, puede enviar correos a la lista de distribución.
- Modo no correo: el usuario no recibe los mensajes que se envían a la lista pero puede enviar correos a la lista. Habitualmente esta opción permite la consulta de los correos a través de interfaz web.
- Modo resumen diario: también llamado modo digest, consiste en que el usuario solamente recibe un correo diario que incluye todos los mensajes enviados a la lista de correo.

Tipos de listas de correo electrónico:

- Boletín electrónico: se utiliza como medio unidireccional para la transmisión de información debido a que sólo pueden enviar mensajes a la lista determinadas personas encargadas de la publicación y gestión de dicho boletín.
- Lista de debate: En este tipo de lista, cualquier suscriptor puede enviar correos a la lista de distribución, y el resto de usuarios pueden contestarlos de la misma manera. De esta forma se pueden generar debates e intercambios de información. Las cadenas de correos van generando hilos que pueden ser contestados por cualquiera de los usuarios de la lista.

Existen en internet diferentes servicios que permiten la creación de listas de correo electrónico de forma gratuita, como por ejemplo Google Groups, Yahoo! o eListas.

A nivel de implementación, existen diferentes productos basados en software libre para la configuración y gestión del servicio de listas de correo, como por ejemplo phpList, Sympa, Mailman y Gmane.

24.5 GRUPOS DE NOTICIAS DE RED

Los grupos de noticias son un servicio proporcionado en Internet al cuál los usuarios pueden suscribirse para participar de forma similar a las listas de correo. En esencia, los grupos de noticias serían similares a un tablón electrónico de noticias categorizadas jerárquicamente por temáticas. El contenido dentro del servicio de noticias se organiza como un gran número de grupos, en los que se agrupan los diferentes temas. El nombre de cada uno de los grupos de noticias disponibles en la red consta de un

conjunto de identificadores separados por puntos, habitualmente relacionados con el dominio de la entidad que gestiona el servidor de noticias, o bien siguiendo un estándar definido para las principales redes de grupos de noticias. Esto permite al usuario suscribirse a un grupo o grupos determinados que resulten de su interés y recibir todos los mensajes que el resto de usuarios envían a ese grupo.

Este funcionamiento se asemeja bastante al de una lista correo, de hecho comparten un objetivo intrínseco que consiste en la generación de espacios de debate y foros de discusión sobre algún tema concreto. La diferencia es que con las listas de correo se reciben directamente los mensajes en el cliente de correo, mientras que con las news o grupos de noticias, se necesita conectarse a un servidor de noticias y extraer los grupos en los que el usuario esté interesado.

Una vez que el usuario se registra en un grupo o grupos determinados, puede agregar mensajes al sistema. Puede también publicar noticias que contesten o repliquen otras noticias previas, formando hilos de debate. Para la gestión de las noticias se necesita software específico para este servicio. Actualmente la mayoría de los clientes de correo web vienen preparados para desempeñar esta función. Las funcionalidades básicas que deben proporcionar son las de permitir seleccionar los grupos de interés para el usuario, lectura de noticias publicadas por otros y envío de noticias al servidor.

Dada la cantidad de mensajes que se generan a diario en los grupos de noticias, es habitual que los servidores de noticias públicos dispongan de mecanismo para evitar la saturación de sus sistemas de almacenamiento. Una de ellas consiste en estipular un tiempo de vida determinado para las noticias que se van almacenando en el sistema. Al cabo de ese periodo de vida, el contenido es eliminado.

Los grupos de noticias se clasifican jerárquicamente en función de sus temáticas, proporcionando una ayuda importante a la hora de localizar los temas de interés.

24.6 FOROS DE DISCUSIÓN

Los foros son aplicaciones web dinámicas que permiten a los usuarios el intercambio de opiniones. Se presentan como herramientas de comunicación e intercambio de conocimiento. Están íntimamente ligados con los sistemas de gestión de contenidos, dado que comparten muchas de las características de éstos últimos.

Habitualmente los foros disponen de sistemas integrados de gestión de usuarios y una parte privada que permite configurar la herramienta pasando por la configuración de la apariencia hasta la distribución interna de foros y subforos de discusión.

En la actualidad se considera a los foros como los descendientes modernos de los grupos de noticias. Mientras que para los grupos de noticias era necesaria la suscripción a un determinado grupo, y acceder a los mensajes a través de un cliente asociado específico (habitualmente los gestores o clientes de correo lo permiten), para interactuar con el foro, únicamente es necesario un navegador web. En función de la configuración particular de cada foro, podría ser necesario que los usuarios se registren para poder participar.

La dinámica de uso del foro por parte de los usuarios es controlada habitualmente por coordinador o moderador. En este sentido, existe en los foros una estricta política de roles y permisos, que permite controlar a nivel de usuario las actividades vinculadas con cada rol. Éste tipo de gestión de usuarios es común para la gran mayoría de aplicaciones web que existen

actualmente en las que el objetivo principal es la participación de los usuarios.

Están considerados como complementos de sitios web, fundamentalmente basados en gestores de contenidos, ampliando las funcionalidades de dichos sitios mediante la introducción de herramientas que permitan a los usuarios discutir o compartir información relevante acerca de la temática del sitio. Esto ha provocado el creciente desarrollo, dentro de la comunidad de software libre, de una gran cantidad de soluciones para la puesta en producción de foros de forma muy sencilla, bien sea instalando aplicaciones predefinidas y desarrolladas en una gran variedad de lenguajes orientados al web, o bien en forma de módulos y complementos que pueden ser integrados en la mayoría de los principales gestores de contenido que existen en el mercado.

Existe una gran variedad de soportes disponibles para la implementación de foros. Habitualmente los paquetes desarrollados preparados para la instalación están desarrollados en lenguajes orientados a desarrollo web como PHP, ASP, Perl, o Java. La arquitectura de este tipo de aplicaciones es similar a la de los sistemas de gestión de contenidos, disponiendo de una base de datos que asegura la persistencia del contenido publicado en el foro, así como el registro de las configuraciones y los usuarios autorizados en el sistema.

Cada tipo de foro es diferente, en lo que se refiere a las capacidades o funcionalidades que puede ofrecer. Los más simples se limitan únicamente a la organización y publicación de mensajes en forma de hilos, sobre los que los usuarios pueden ir aportando nuevas anotaciones. Los más recientes incluyen avanzados sistemas de administración de contenido y traen soporte integrado para la inclusión de contenido multimedia.

Los ejemplos más habituales de sistemas de foros que se pueden encontrar en un alto porcentaje de sitios en web son: phpBB, vBulletin, MyBB, SMF, YaBB, o JavaBB. Como se comentó anteriormente, muchos

sistemas de gestión de contenidos integran sus propios módulos con funcionalidad de foro, como es el caso de WordPress, Drupal o Joomla!.

24.7 CHAT

El término chat es un anglicismo que hace referencia al charla o cibercharla. Se utiliza para designar las comunicaciones escritas realizadas en tiempo real a través de Internet entre dos o más personas. Puede realizarse a través de canales públicos, o mediante canales privados, dependiendo del medio y protocolos que se utilicen. Éste tipo de características determinan las diferentes tipologías de chat:

- **Webchat:** Es un tipo de chat en el que los mensajes se transmiten a través de WWW. Es un tipo de chat de fácil acceso, dado que las interfaces están implementadas como aplicaciones web, accesibles desde cualquier navegador. Resulta sencillo de utilizar dado que existen una gran cantidad de componentes visuales que ayudan a personalizar rápidamente los estilos de escritura y visualización en este tipo de aplicaciones de acceso a los webchats, lo que lo hace resultar atractivo para usuarios noveles. Sin embargo el uso de los webchat está decayendo dado que las tareas de actualización del contenido de la página que carga el webchat, así como la inestabilidad de algunos navegadores hace que mantener las conversaciones en tiempo real sea difícil en algunas ocasiones.

- **IRC (Internet Relay Chat):** Representa la forma más conocida y antigua de chat que existe. IRC es un protocolo de comunicación en tiempo real basado en texto que permite comunicación entre usuarios sin necesidad de acuerdo previo de establecer la comunicación, es decir, que dos usuarios que se encuentren en un canal pueden comunicarse entre sí sin necesidad de haber establecido una comunicación previa. El IRC presenta un modelo cliente-servidor donde las aplicaciones cliente de los usuarios, que habitualmente son aplicaciones stand-alone, se configuran y conectan contra un determinado servidor de IRC, permitiendo establecer comunicación con el resto de personas que se encuentran conectadas a dicho servidor, bien mediante chat privado, o a través de canales de libre acceso. En este modelo de chat, existen agentes moderadores que intervienen en la administración y control de todo lo que sucede en cada servidor de IRC. El cliente más habitual de este tipo de redes es el *mIRC*.
- **Mensajería instantánea:** Puede considerarse otra modalidad de chat. En esencia es similar al IRC, dado que la arquitectura de este tipo de sistemas que proporcionan mensajería instantánea se basa en un modelo cliente-servidor en el cuál aplicaciones stand-alone se conectan contra el servidor y permiten enviar y recibir mensajes de otros usuarios conectados al servidor. Sin embargo la gran diferencia radica en que en los sistemas de mensajería instantánea, para que dos usuarios se comuniquen, deberá de existir un contacto previo mediante el cuál ambos usuarios accedan a establecer la comunicación. La mayoría de estos sistemas cuentan con su propia red que únicamente es accesible mediante el cliente propio de esa

red, desarrollado por una entidad o compañía concreta. En ese sentido, se presenta como un modelo de comunicación limitado y controlado que se está comenzando a adoptar en algunas empresas y corporaciones para establecer un mecanismo de intercambio de información de forma económica, controlada y fiable. Algunos sistemas de mensajería instantánea más comunes son el MSN Messenger, Yahoo Messenger o ICQ.

24.8 SISTEMAS DE VIDEOCONFERENCIA

Los sistemas de videoconferencia tienen como principal característica el permitir comunicación simultánea y bidireccional de señales de audio y vídeo, lo que proporciona capacidad para mantener reuniones con personas situadas en lugares alejados.

Éste tipo de sistemas habitualmente integran capacidades que abarcan parte de los sistemas vistos con anterioridad ya que integran la capacidad de establecer comunicación escrita (chat) y gestión de mensajería instantánea. Además pueden incluir capacidad para la transmisión de ficheros y edición en herramientas colaborativas.

La base tecnológica de los sistemas de videoconferencia es la compresión digital de los flujos de audio y vídeo en tiempo real.

En cuanto a la categorización de los sistemas de videoconferencia, podemos clasificarlos fundamentalmente en dos grandes grupos:

- **Sistemas de videoconferencia dedicados** : Disponen de los componentes hardware necesarios para realizar una videoconferencia en remoto. Son sistemas de alta calidad, especiales para las circunstancias en

las que se demanda una alta fiabilidad y calidad de los datos transmitidos. Por lo general, éste tipo de dispositivos constan de una cámara de vídeo de alta calidad y una consola. Dentro de este tipo de sistemas podemos distinguir varios tipos de dispositivos hardware en función del objetivo del sistema:

- o Grupos grandes: son dispositivos grandes , no portátiles, más costosos utilizados para grandes salas y auditorios. Requieren de instalación y mantenimiento adecuados.
- o Grupos reducidos: no son portátiles, son más pequeños y menos costosos, utilizados para salas de reuniones pequeñas. Requieren de instalación.
- o videoconferencia individual: Se trata de dispositivos portátiles, destinados a usuarios individuales, tienen cámaras fijas, micrófonos y altavoces integrados en la consola.
 - **Sistemas de videoconferencia de escritorio:** Los sistemas de escritorio, o sistemas de usuario, se basan en la combinación de parte software y hardware. En cuanto a parte software, se trata de algún cliente de mensajería con capacidad para realizar videoconferencia mediante la transmisión de una cámara web y un micrófono conectado al ordenador. En cuanto a los dispositivos hardware, simplemente serían necesarios una cámara web y un micrófono. En la actualidad, prácticamente la gran mayoría de los sistemas de mensajería instantánea soportan videoconferencia. Es el caso por ejemplo de los clientes de MSN Messenger o Skype.

24.9 BIBLIOGRAFÍA

- Jerri L. SEO: Optimización de Posicionamiento en Buscadores. Ledford Anaya Multimedia
- V. Canseco G. Gerónimo. Breve introducción a los sistemas colaborativos: Groupware& workflow. 1998.
- Ortega M. Velázquez Iturbide J.A. Paredes M., Fernández I. Escritura colaborativa y pdas: una propuesta de aprendizaje basada en resolución de problemas. 2003.
- Network Working Group. «[RFC 5321 - Simple Mail Transfer Protocol](#)»
- Mark Harrison (July 1995). *The USENET Handbook (Nutshell Handbook)*. O'Reilly. [ISBN 1-56592-101-1](#).
- Kate Gregory, Jim Mann, Tim Parker, and Noel Estabrook (June 1995). *Using Usenet Newsgroups*. Que. [ISBN 0-7897-0134-0](#).
- Bryan Pfaffenberger ([1994-12-31](#)). *The USENET Book: Finding, Using, and Surviving Newsgroups on the Internet*. Addison Wesley. [ISBN 0-201-40978-X](#).
- Kate Gregory, Jim Mann, Tim Parker, and Noel Estabrook (June 1995). *Using Usenet Newsgroups*. Que. [ISBN 0-7897-0134-0](#).
- Mark Harrison (July 1995). *The USENET Handbook (Nutshell Handbook)*. O'Reilly
- Videoconferencing and Videotelephony. Richard Schphorst. Editorial Artech House. Norwood, 1996.

Autor: Francisco Javier Rodríguez Martínez

Subdirector de Sistemas Escola Superior Enxeñaría Informática Ourense
Colegiado del CPEIG

**25. WEB 2.0. WIKIS. BLOGS.
COMUNIDADES VIRTUALES.
REDES SOCIALES.
SINDICACIÓN DE CONTENIDOS.
PODCAST. MODELOS DE TV EN
INTERNET. SUITES DE
OFIMÁTICA EN WEB.
ALMACENAMIENTO EN WEB.
ESCRITORIOS VIRTUALES.
MASHUPS. WIDGETS. MUNDOS
VIRTUALES. P2P. WEB
SEMÁNTICA.**

Tema 25.- Web 2.0. Wikis. Blogs. Comunidades virtuales. Redes sociales. Sindicación de contenidos. Podcast. Modelos de TV en internet. Suites de ofimática en web. Almacenamiento en web. Escritorios virtuales. Mashups. Widgets. Mundos virtuales. P2P. Web semántica.

ÍNDICE

25.1 Web 2.0.....	3
25.2 Wikis.....	6
25.3 Blogs.....	9
25.4 Comunidades Virtuales.....	10
25.5 Redes Sociales.....	12
25.6 Sindicación de contenidos.....	13
25.6.1 Fuente Web.....	14
25.6.2 Agregador de noticias.....	14
25.6.3 Formato RSS.....	15
25.6.4 Estándar Atom.....	15
25.7 Podcast.....	16
25.7.1 Podcasting Vs. Streaming.....	17
25.8 Modelos de TV en Internet.....	18
25.8.1 Características de la televisión IP.....	19
25.9 Suites Ofimáticas en Web.....	20
25.9.1 Feng Office.....	21
25.9.2 Google Docs.....	21
25.9.3 Office Web Apps.....	22
25.10 Almacenamiento en web.....	23
25.10.1 Dropbox.....	23
25.10.1.1 Funcionalidades de Dropbox.....	23
25.11 Escritorios Virtuales.....	24
25.11.1 eyeOS.....	24
25.12 Mashups.....	25
25.13 Mundos Virtuales.....	26
25.13.1 Second Life.....	27
25.14 P2P.....	28

25.14.1 Características.....	28
25.14.2 Tipos de redes P2P.....	29
25.14.2.1 Redes P2P centralizadas.....	29
25.14.2.2 Redes P2P híbridas, semicentralizadas o mixtas.....	29
25.14.2.3 Redes P2P puras o totalmente descentralizadas.....	30
25.15 Web semántica.....	30
25.15.1 Definición de web semántica.....	31
25.15.2 RDF, SPARQL y OWL.....	31
25.16 Bibliografía.....	32

25.1 WEB 2.0

El concepto de web 2.0 nace para describir aquellas aplicaciones web que se centran en el usuario, en contraposición a la web tradicional (o 1.0) que simplemente actúa como una mera presentadora de datos. La web 2.0 fomenta la interacción con el usuario, la interoperabilidad, y busca compartir información y la colaboración. Este concepto se ha desarrollado principalmente mediante servicios web, redes sociales, wikis, blogs y sistemas de almacenamiento de vídeos, entre otros.

Se puede entender a la web 2.0 como la evolución de una serie de aplicaciones tradicionales en otras enfocadas al usuario, no tanto desde un punto de vista tecnológico, sino de concepto e intención. Así, a través del concepto 2.0, ciertas aplicaciones irán abandonando el escritorio e irán migrando a la web, siempre basándose en la colaboración con el usuario y la interactividad. Para permitir el uso del software online y otras aplicaciones multimedia, la extensión de la banda ancha ha sido un factor fundamental.

La web 2.0 es una actitud de compartir información, colaboración, interacción, cambio continuo y la creación de una plataforma global.

La web 2.0 es una reinterpretación de la web, que describe los pasos para llegar a un modelo de comunicación colectiva más participativa e innovadora.

Uno de los principales cambios se producen en la gestión de los datos. En la web 1.0, es la empresa la que gestiona la información, a través de una red de expertos, o algún tipo de procesamiento artificial. Por su parte, la

web 2.0 es un concepto colaborativo en el que se espera que los datos sean obtenidos por medio de los usuarios.

En 2004, O'Reilly Media realiza una conferencia sobre web 2.0, donde se comienza a sentar las bases de este concepto. Desde el primer momento se deja claro que no se trata de un cambio tecnológico en la web, sino un cambio en la forma en la que desarrolladores y usuarios utilizan la web. Sin embargo, Tim Berners-Lee, el creador de la World Wide Web, ha calificado el término 2.0 como “palabrería”, ya que, según él mismo, la web ya contenía esos valores desde un principio.

Con anterioridad al concepto 2.0, la mayoría de aplicaciones web eran portales estáticos, programados en lenguaje HTML (Hyper Text Markup Language), con una periodicidad de actualización baja, y con escasa interacción con el usuario, que simplemente “consumía” contenido. Una primera aproximación al concepto 2.0 fueron las aplicaciones webs dinámicas, en las que las páginas son servidas al usuario dinámicamente a partir de contenido obtenido de una base de datos.

Algunos expertos en la web 2.0 mantienen que la web debe enfocarse a la interacción y a las redes sociales, de modo que la web sea un punto de encuentro, y dependa del usuario.

Dale Dougherty, de O'Reilly Media, usa por primera vez el término “web 2.0” junto con Craig Cline, de MediaLive, para ilustrar la idea de que la web se estaba refundando. Una de las principales críticas del concepto 2.0 es que no existe una definición formal. Dougherty argumentó su punto de vista con ejemplos de aplicaciones web 1.0 y 2.0. Así, lo que DoubleClick era en la web 1.0, lo es Adsense en la 2.0. Y lo que era Ofoto en la web 1.0, lo es Flickr en la 2.0. Otros ejemplos son Google (que mide el impacto de los sitios web mediante el número de enlaces a páginas web, y no tanto por

clicks absolutos) o la Wikipedia (un proyecto colaborativo a partir de una gran cantidad de pequeños usuarios, en lugar de un reducido equipo de expertos).

De este modo, en octubre de 2004 se realiza la primera conferencia sobre web 2.0, con Dougherty, Cline y John Battelle. Un año después se realiza una segunda conferencia, donde se une Tim O'Reilly para resumir los principales rasgos de la web 2.0. Entre ellos, encontramos la innovación, el diseño para múltiples plataformas, y la importancia de la participación del usuario. En la web 2.0, la aplicación está orientada por el usuario, que es el que alimenta y modifica una base de conocimiento de la aplicación, a partir de un diseño interactivo y en red (tal y como definió Xavier Ribes en 2007).

Algunas de las características que definen la web 2.0 son:

- Permite el uso de aplicaciones online, sustituyendo potencialmente a las aplicaciones de escritorio, y desde un punto de vista multiplataforma. Las aplicaciones ejecutadas en web son independientes del navegador y del sistema operativo desde el que se ejecutan, lo que facilita el desarrollo.
- Permite la transferencia de información y contenidos entre aplicaciones web.
- Permite una experiencia de usuario simple, con una curva de aprendizaje rápida.
- Permite añadir nuevas funcionalidades de una manera simple e intuitiva.
- Permite gradualmente la virtualización de las estructuras sociales en el mundo online.
- Hace que el papel del usuario gane importancia, llevándolo hasta el rol de co-desarrollador, y fomentando un desarrollo colectivo. Se

puede decir que un elevado número de usuarios pueden sustituir en algunos casos a un reducido grupo de expertos.

- Fomenta la interoperabilidad de las aplicaciones web, la incrustación de código externo y el uso de API's incluso por usuarios no expertos. En este punto es destacable la contribución de la tecnología RSS (Real Simple Syndication) que separa totalmente contenido y presentación de los datos. RSS permite conocer las actualizaciones de un portal web sin necesidad de visitarlo, y además hace posible crear sistemas de agrupación de información alimentado por distintas fuentes (los llamados agregadores, como Google Reader). RSS se basa en XML, que ha sido otro actor importante en la transmisión de información para la web 2.0.
- Fomenta la participación para la mejora continua de la aplicación.

25.2 WIKIS

Un wiki (del hawaiano “wiki wiki” = rápido) es un tipo de aplicación web que permite la edición de sus contenidos de forma concurrente, voluntaria y colaborativa por parte de usuarios, autenticados o no, a través de un navegador web, y con el objeto de acumular conocimiento de manera conjunta a modo de repositorio centralizado. Los wikis se basan en el esfuerzo democrático y compartido sobre una base de igualdad y facilidad: todo el mundo debe poder aportar nuevo contenido.

Cada página de contenido del wiki se corresponde con un nombre unívoco y simple que facilita su comprensibilidad, así como su enlazamiento desde otras páginas de wiki y portales externos. Además, existe un lenguaje wiki que facilita la edición y creación de jerarquías, categorías, tesauros y

taxonomías por medio de enlaces internos. Esto crea una estructura descentralizada que hace que la navegación por los wikis sea no lineal, ya que cada página contiene numerosos enlaces a otras páginas.

El origen de los wikis proviene de Ward Cunningham, quien desarrolló un servidor wiki como repositorio de patrones de diseño en Portland (Portland Pattern Repository) en 1995 (llamado WikiWikiWeb), y definió al wiki como 'la base de datos online más simple que podría funcionar'. Posteriormente, en 2001, Jimbo Wales y Larry Sanger usan un wiki como germen de su proyecto de enciclopedia Wikipedia, una enciclopedia libre y en red. Comienzan utilizando el software UseMod, aunque finalmente desarrollan un software propio, denominado Media Wiki, que se ha convertido en un estándar para otros wikis. Ha sido precisamente la Wikipedia, y otras enciclopedias colectivas, las que han colaborado en el auge de los wikis.

Cada artículo se co-escribe con el resto de la comunidad. Dentro de la colaboración múltiple, el wiki posibilita un historial de actualizaciones que actúa a modo de control de versiones temporal y por usuario. Al trabajar como un repositorio, los wikis permiten volver a versiones anteriores con facilidad. Normalmente no existe una supervisión, y la edición se basa en la negociación entre usuarios, pero la tendencia actual es que exista un reducido grupo de usuarios con un rol especial que revisa los contenidos y hace posible mantener la calidad en los contenidos y evitar incoherencias y sabotajes. En otros casos se requiere autenticación solamente para mantener el historial de cambios y firmar los contenidos.

Hoy en día, la versión inglesa de Wikipedia es el wiki más grande que existe. El resto de versiones en otros idiomas, y otras aplicaciones wiki más específicas, cuentan con menor número de usuarios debido a que sus comunidades son menos numerosas.

Lo que diferencia a un wiki de otras aplicaciones web de gestión de

contenidos es su rapidez para crear y modificar páginas, así como la simplicidad y legibilidad de su interfaz. Esto ha fomentado el alto número de participantes en los proyectos wiki, destacablemente mayor que en otros proyectos colaborativos web. Si bien el usuario posee un alto grado de libertad para editar contenidos, existen plantillas para que las páginas wiki guarden coherencia entre si, lo que hace aumentar la calidad del repositorio. Estas estructuras predefinidas facilitan que la edición de contenidos sea lo más simple posible. Además, los wikis tienen normalmente un diseño sencillo que no suele modificarse.

Los wikis tienen un componente de altruismo más notable que otras aplicaciones web. Si bien es colaborativo, y el usuario fomenta la pertenencia a una comunidad con intereses comunes, lo importante de la colaboración es el bien común, y no tanto el que un usuario destaque más o menos por sus contribuciones, ya que la autoría de los contenidos rara vez es exclusiva. No solo eso, los contenidos están en continua edición, de manera indefinida, lo que obliga a la reflexión y aun continua revisión de las ideas.

Es destacable la gran relación entre los wikis y el mundo educativo. Los wikis han cambiado radicalmente el modelo de consulta de conocimientos, pasando de las mastodónticas enciclopedias estáticas a los proyectos colaborativos actuales basados en wikis donde el usuario juega un papel fundamental.

Los software más utilizados para el desarrollo de wikis son: MediaWiki, TikiWiki o CitiWiki (en PHP), y JSPWiki o XWiki (en Java), entre otros. La aplicación solamente define la presentación básica de los datos (estilos, entorno...), pero la edición de los datos corre por parte de los usuarios.

25.3 BLOGS

Un blog (o weblog) es un sitio web de actualización frecuente que recopila artículos, presentando primero el más reciente, y que permite la interacción con los lectores por medio de comentarios sobre los artículos. El blog es cronológico (permite mantener una línea de tiempo de publicación), es colaborativo (pueden publicar varios autores), y es interactivo (los lectores pueden publicar sus comentarios, de modo que el autor pueda contestarles para conformar un diálogo). El administrador del blog puede tomar distintas opciones de diseño, como no permitir comentarios, y administrar los artículos (borrarlos o reordenarlos).

La temática del blog es variada, siendo su motivación primigenia el actuar a modo de diario personal o bitácora. Desde entonces, los hay corporativos, periodísticos, educativos, etc. El blog que se dedica esencialmente a la publicación de fotografías se denomina fotolog o fotoblog (y videoblog en el caso de vídeos). Una práctica habitual es proporcionar un gran número de enlaces que amplíen la información para cada entrada. En ocasiones las entradas permiten que se les haga *trackback* (un enlace inverso) para conocer quién ha enlazado la entrada desde otro sitio web.

Las entradas del blog suelen agruparse en categorías, y es frecuente la práctica de indicar palabras clave o etiquetas para facilitar la búsqueda por contenido. Los blogs también proporcionan archivos e índices mensuales y anuales que permiten una navegación ordenada por fecha. Así mismo, es habitual que las entradas proporcionen facilidades para ser compartidas en otros blogs, o por correo electrónico, así como por sindicación de contenidos, mediante el uso de tecnología RSS o Atom.

Gran parte del auge de los blogs se ha debido a su facilidad de mantenimiento y a las numerosas alternativas gratuitas disponibles. No son necesarios grandes conocimientos técnicos para administrar un blog, y ni

siquiera para crearlo, lo que los ha acercado al gran público. Además, como cualquier otro sitio web, un blog puede tener publicidad y generar ingresos.

Existen principalmente dos tipos de soluciones blog: las que proporcionan una solución completa de software y alojamiento web gratuito (como Blogger o LiveJournal), y las que simplemente proporcionan software que precisa ser instalado en un sitio web (como WordPress). Este último es un tipo específico de gestor de contenido (CMS).

25.4 COMUNIDADES VIRTUALES

Una comunidad virtual es aquella cuyos vínculos, interacciones y relaciones no tienen lugar en un espacio físico, sino en un espacio virtual como Internet.

Las comunidades virtuales surgen con Internet y obtienen su modelo de las comunidades no informáticas, existentes desde mucho antes. La primera comunidad virtual data de los años 70, aunque su mayor desarrollo se produce en los 90, volviéndose, en este momento, accesibles al público en general, gracias al nacimiento de la World Wide Web (WWW) y la expansión de herramientas como los chats, correo electrónico o mensajería instantánea. Hasta este momento, las comunidades se hallaban restringidas al ámbito científico y a expertos en informática.

Los usuarios sin acceso a Internet, implementaron y popularizaron el uso del Sistema de Tablón de Anuncios (BBS o Bulletin Board System), que se trataba de un sistema que funcionaba mediante un acceso mediante módem telefónica a una central (el BBS), el cual podía basarse en una o varias líneas de teléfono. En los BBS se podían mantener conversaciones,

intercambiar archivos, publicar comentarios, etc. En esta época las comunidades eran independientes, lo más habitual era que los usuarios particulares empleasen sus propios equipos domésticos para proporcionar servicio con hasta un único modem de entrada.

Actualmente, las comunidades virtuales han evolucionado, convirtiéndose en una herramienta muy útil desde el punto de vista empresarial. Esto se debe a la mejora que ofrecen a las organizaciones en su dinámica de trabajo interno, en las relaciones con los clientes o en el incremento de la eficiencia de sus procedimientos.

Desde el punto de vista social, las comunidades virtuales permiten a los usuarios relacionarse con los demás, adquiriendo así un carácter socializador.

Se estima que en el año 2000 más de 40 millones de personas participaban en comunidades virtuales, las cuales podemos caracterizar de la siguiente forma:

- Asociación virtual de personas
- Existe un propósito determinado que es la razón de ser de la comunidad virtual
- Existe un gran deseo de interacción entre los usuarios para satisfacer unas necesidades o desempeñar unos roles concretos
- Existen sistemas que evalúan y miden las interacciones y favorecen la cohesión entre los miembros

El principal inconveniente al que se enfrenta el desarrollo de las comunidades virtuales es la problemática de la organización interna de las mismas, que suele ser muy difícil de establecer y gestionar. En muchos casos, es demasiado costoso crear la estructura de la comunidad con lo que se puede llegar a perder el verdadero propósito de la creación del mismo.

Una comunidad virtual queda definida desde 3 puntos de vista:

- Comunidad virtual como lugar: emplazamiento donde los individuos pueden mantener relaciones económicas o sociales.
- Comunidad virtual como símbolo: los miembros de una comunidad desarrollan un sentimiento de pertenencia a una estructura mayor.
- Comunidad virtual como virtual: a pesar de las similitudes entre las comunidades físicas y las virtuales, una comunidad virtual se desarrolla principalmente en un entorno virtual que no puede ser asimilable con una localización física.

25.5 REDES SOCIALES

El concepto de red social, está estrechamente ligado con el de comunidad virtual, entendiéndose una comunidad virtual como un caso más específico de red social.

Una red social es una estructura de nodos donde distintos actores, que pueden ser individuos u organizaciones, están conectados mediante un serie de relaciones basadas en propiedades comunes. Una red social se asienta sobre cierto tipo de relaciones, económicas, laborales, familiares, políticos, deportivos, etc.

Una red social es distribuida cuando su emplazamiento no está limitado a un sitio en concreto sino que se distribuye a nivel geográfico. En el caso de una red social, es lógico pensar que no todos los actores participantes en dicha red se encuentren localizados en un único espacio.

Una red social se apoya en el uso de alguna tecnología de comunicación

que permite a los distintos usuarios interactuar entre si. En este caso, lo más habitual es emplear Internet como tecnología subyacente, sin embargo, también existen redes sociales basadas en tecnologías móviles e incluso en tecnologías no digitales como el teléfono, el fax o el correo postal.

Actualmente las redes sociales se orientan alrededor de un sitio web que ofrece a los usuarios una serie de servicios, como son chat, mensajería instantánea, carga de imágenes, vídeos, grupos de debate, etc. Uno de los servicios que tienen una mayor importancia son los del “software social”, que abarca todas aquellas aplicaciones que simulan procesos sociales del mundo real. El ejemplo más habitual es la simulación del efecto “amigo de un amigo”, en este caso la aplicación localiza a los amigos de nuestros amigos para poder así facilitar el contacto con nuevos usuarios.

Dentro de las redes sociales más empleadas hoy en día, podemos nombrar a Facebook, Youtube, Twitter, Myspace, Orkut, Hi5 etc.

25.6 SINDICACIÓN DE CONTENIDOS

Antes de definir qué es la sindicación de contenidos, es necesario aclarar que si bien la expresión correcta es “redifusión web”, el término “sindicación web” está muy expandido en su uso, especialmente en lo que se refiere a contenidos web, aunque esta redifusión puede llevarse mediante cualquier medio de comunicación.

La sindicación de contenidos (sindicación web o redifusión web) consiste en el reenvío o redistribución de contenidos desde un sitio web de origen, hasta otro sitio web receptor, el cual a su vez se puede ver como un emisor

de los contenidos, puesto que estos dejan de estar limitados a los usuarios del sitio web inicial. Esta redifusión de contenidos se hace habitualmente mediante una licencia o contrato entre los sitios web de origen y destino.

Los contenidos que se redistribuyen suelen codificarse en XML, aunque esto no es obligatorio y puede emplearse cualquier otro formato soportado por http.

Existen dos familias más destacadas en cuanto a formatos de redifusión web, que son RSS y Atom. De hecho, actualmente el término RSS (Really Simple Syndication) se ha empezado a usar indistintamente para referirse a cualquiera de los 2 formatos de fuentes web, el propio RSS o Atom.

Para poder leer una fuente web es necesario realizar una suscripción mediante un agregador, el cual muestra los nuevos contenidos que hayan sido publicados por el proveedor de la fuente web suscrita.

25.6.1 Fuente Web

Un canal web o fuente web (Web feed) es un medio de redistribución de contenidos web, que se emplea para suministrar información a los suscriptores de manera actualizada. Los cuales, deben contar con un programa “agregador” para acceder a todas las fuentes a las que están suscritos desde un mismo lugar.

Como ya comentamos anteriormente, los dos principales formatos de fuente web son RSS y Atom., ambos escritos en XML.

25.6.2 Agregador de noticias

Un lector RSS o agregador de noticias (eventualmente sólo agregador) es una aplicación que permite establecer una suscripción a fuentes de noticias

en formatos Atom, RSS y otros derivados de XML/RDF. La función del agregador consiste en reunir todas las noticias y contenidos publicados en los sitios con redifusión escogidos y mostrarlas de manera unificada al usuario. De tal forma que el usuario pueda saber qué webs han incorporado o modificado contenidos desde la última lectura, y en cada caso, cual es el contenido de las mismas.

Los lectores RSS se han vuelto más populares con la implantación de XML y la web semántica, y hoy en día existe un gran número de blogs y sitios web que ofrecen sus actualizaciones, las cuales son administradas y agregadas en un solo lugar, gracias a herramientas como las de Google Reader, Netvibes, etc.

25.6.3 *Formato RSS*

RSS es un formato XML para syndicar contenidos web que se emplea para difundir información a los usuarios suscritos a una fuente de contenido. Este formato se caracteriza por permitir la distribución de contenidos sin necesidad de emplear un navegador, ya que se utiliza un agregador de contenidos RSS, aun así, es posible emplear el navegador para ver los contenidos RSS.

De hecho, las últimas versiones de los navegadores permiten visualizar los RSS sin necesidad de un agregador.

Este formato, se desarrollo específicamente para aquellos sitios que se actualizan de forma habitual y mediante al cual se puede compartir la información y ser empleada en otros sitios web.

25.6.4 *Estándar Atom*

Atom hace referencia a 2 estándares relacionados entre si:

- Protocolo de Publicación Atom (AtomPub o APP): protocolo basado en

http para crear o actualizar recursos en web.

- Formato de Redifusión Atom: fichero en formato XML usado para redifusión web.

Para crear un contenido, que pueda ser tratado con agregador o por otro sitio web que redifunde los contenidos de la fuente, el propietario del sitio web puede emplear un software específico como un sistema de gestión de contenidos, el cual publica una fuente web de artículos recientes en un formato estándar y legible por los ordenadores.

El formato Atom fue desarrollado como una alternativa a RSS. Atom surge por la incompatibilidad existente entre algunas versiones del protocolo RSS. El formato de redifusión Atom se publicó como un “estándar propuesto” de la IETF con RFC 4287, mientras que el protocolo de comunicación se publicó como RFC 5023.

25.7 **PODCAST**

Podcasting consiste en distribuir archivos multimedia, generalmente audio o vídeo, mediante un sistema de redifusión que permita a los usuarios establecer suscripciones, los cuales emplean un programa de descarga para poder visualizar el contenido en el momento que se desee. También existe la posibilidad de descargar los contenidos sin una suscripción previa. El podcasting es un tipo de sindicación donde los archivos que se redistribuyen son de contenido multimedia.

Al principio el podcasting se refería exclusivamente a las retransmisiones archivos de audio, aunque más tarde se ha extendido el concepto para hacer referencia tanto a audio como a vídeo de manera indistinta.

El contenido de los podcasts es muy diverso, sobre tecnología, política, noticias, contenidos educativos, etc. En función del productor del podcast su complejidad, número de participantes y estructura varían significativamente. Algunos se asemejan a programas de radio, con varios participantes y diversas opiniones, y otros se parecen más a comunicados o monólogos de una sola persona, cuya duración generalmente es más corta.

Los podcasts suelen ser accesibles desde el sitio web en que han sido colocados. Existen blogs que permiten realizar podcasting mediante el uso de plug-ins gratuitos. Además estos archivos también se pueden descargar.

25.7.1 *Podcasting Vs. Streaming*

Antes de la aparición del podcasting, la forma habitual de transmitir contenidos multimedia era el streaming o webcasting. Mediante este sistema, proveedores de contenidos como cadenas de televisión o radios empleaban el streaming para emitir desde un servidor central.

Podcasting y streaming presentan ciertas diferencias, las más destacadas:

- Con streaming no se produce la descarga del fichero sino que este se reproduce en modo flujo mientras se está descargando. Cuando termina la reproducción, el fichero no se almacena en el equipo receptor. Esto presenta la ventaja del ahorro de espacio de almacenamiento, sin embargo, siempre que se quiera ver u oír nuevamente el archivo volverá a ser descargado y no puede ser reproducido si no existe una conexión a Internet.
- Con streaming, es necesario acceder al sitio Web donde está el canal

deseado e indicar que la reproducción del contenido debe iniciarse mediante algún tipo de enlace, botón, etc. Sin embargo, con podcasting, cuando el contenido está disponible, este se descarga de manera automática y puede ser escuchado en cualquier momento.

- El streaming presenta más problemas de compatibilidad entre los distintos sistemas empleados que el podcasting.
- El streaming es más sensible a problemas de conexión a Internet o de sobrecarga del servidor ya que la descarga se produce mientras se está reproduciendo el archivo.

25.8 MODELOS DE TV EN INTERNET

La televisión IP (IPTV) supone una nueva forma de comunicación audiovisual que consiste en la retransmisión de material audiovisual por Internet. Para la retransmisión de estos contenidos e emplea el protocolo TCP/IP, además este tipo de televisión se caracteriza por tener programación para todos tipos de usuarios y contenidos específicos que pueden ser seleccionados en la televisión por los propios usuarios.

Este modelo de televisión supone un avance al modelo de televisión habitual y es considerado como uno de los avances más interesantes y prometedores que la tecnología IP ha favorecido.

Mediante la red IP la programación de los diversos canales de televisión llega a todos los televidentes, este proceso se realiza mediante las funciones siguientes:

1. Las señales de video originales se digitalizan y convierten en paquetes de datos IP.
2. Este contenido, convertido a IP, se almacena para su redistribución, así como para su disponibilidad futura.
3. Estas tramas de paquetes se transportan a través de una red IP.
4. Las señales son recibidas en un equipo residencial cuya función es volver a convertir los paquetes IP en señales de televisión estándar.

Debido a la gran robustez de los equipos de redes con los que se cuenta actualmente, el servicio de la televisión IP puede ofrecerse con una alta calidad, funcionalidad y un buen nivel de servicio.

25.8.1 *Características de la televisión IP*

- Soporte para definición estándar y alta definición (HDTV)
- Nivel de interactividad completo. El equipo receptor al ser un dispositivo IP, mantiene una conectividad bidireccional, lo que permite al usuario servicios como:
 - o Video conferencia
 - o Acceso a cuentas bancarias
 - o Compra online de los productos que se estén publicitando en el momento
 - o Navegación por internet a través del dispositivo de TV
- Posibilidad de visualizar desde el principio programas ya iniciados, e incluso programas transmitidos con anterioridad.
- Reproducción a cámara lenta, posibilidad de pausar y retroceder la reproducción, en una retransmisión en vivo.
- Servicio de videgrabadora virtual, que permite grabar directamente o de forma programada cualquier programa.
- Servicio de vídeo bajo demanda, se puede seleccionar el programa

que se desea visualizar y su reproducción se inicia inmediatamente.

- Guías de programación interactivas, con filtros por diversos factores como horario, tipo de programa, contenido, etc.

Con todo esto, el paradigma de televisión tradicional cambia radicalmente ante el desarrollo de la televisión IP, por ejemplo, el sistema de publicidad que se emplea en la televisión IP es distinto al que se presenta en la televisión tradicional, donde se producen unos cortes de la programación habitual, de duración variable, donde se incorporan las cuñas informativas; sin embargo, en la televisión IP la publicidad aparece simultáneamente y de forma continuada a los contenidos que estemos visualizando.

Este modelo de televisión ha sido muy impulsado por las nuevas tecnologías de internet, pero su expansión será aun mayor, por el creciente desarrollo de dichas tecnologías y por los requisitos que exige esta televisión, que se limitan a una conexión a Internet, actualmente muy extendida. Además, este modelo de televisión, permite visualizar el contenido que el usuario desea, en el momento y formato elegido.

25.9 SUITES OFIMÁTICAS EN WEB

Un suite ofimática es un conjunto de herramientas que se utilizan habitualmente en entornos de oficina para el trabajo con documentos de cualquier tipo. Normalmente se incluyen en estos paquetes un editor de textos, un gestor de hojas de cálculo, un gestor de bases de datos, un programa de creación de diapositivas de presentación etc. Tradicionalmente todas las suites ofimáticas eran herramientas de escritorio. Actualmente existen distintas versiones de suites ofimáticas pero en web, a las cuales se accede mediante el uso de un navegador.

25.9.1 *Feng Office*

Feng Office es una aplicación libre de tipo Web Office, antes conocida como OpenGoo. Se trata de un sistema completo que proporciona funcionalidades para crear, publicar, colaborar y compartir documentos.

Feng Office permite crear y trabajar entre otros, sobre:

- *Documentos*: permite alojar documentos de todo tipo y editar directamente algunos de ellos.
- *Listas de tareas*: permite la creación de listas de tareas asignadas a distintos usuarios, con opciones de notificación, categorización, etc
- *Correo electrónico*: permite centralizar la gestión de las distintas cuentas de correo.
- *Calendario*: permite establecer reuniones y una gestión de las actividades diarias.
- *Agenda*: permite realizar una gestión de contactos.

Esta aplicación puede funcionar bajo un modelo SaaS (Software as a Service), donde los servidores del proveedor a través de un navegador, nos permiten trabajar con la aplicación, pero también es posible realizar una instalación de la aplicación en un servidor propio, en este caso los requisitos de este sistema pasan por un servidor web Apache, PHP y MySQL como base de datos.

25.9.2 *Google Docs*

Google Docs & Spreadsheets, es un programa web gratuito que permite crear y trabajar sobre unos documentos de manera individual o en grupo.

Google Docs se compone de:

- Procesador de textos
- Hojas de cálculo
- Programa de presentación sencillo
- Editor de formularios

Entre las ventajas de Google Docs, se encuentra el hecho de que puede ser usado tanto online como offline. En esta modalidad offline, los cambios que se introduzcan en los documentos serán actualizados de forma automática en cuanto la conexión con internet se restablezca.

Además recientemente se ha incorporado compatibilidad entre Google Docs y los dispositivos móviles, de tal forma que se pueda no solo acceder a los documentos sino también editarlos.

25.9.3 *Office Web Apps*

Office Web Apps es la solución de Microsoft para las suites ofimática en la web. Se trata de una versión gratuita basada en el conjunto de aplicaciones de Microsoft Office.

Office Web Apps, se compone de :

- Word Web App
- Excel Web App
- PowerPoint Web App
- OneNote Web App

Estas aplicaciones permite acceder a los documentos a través del navegador, así como compartir archivos y trabajar sobre ellos de forma colaborativa.

25.10 ALMACENAMIENTO EN WEB

Un servicio de almacenamiento de archivos online (servicio de alojamiento de archivos o centro de medios online) es un servicio de alojamiento online cuyo propósito es facilitar el almacenamiento de contenido estático, como archivos, documentos, etc. Por norma general este tipo de servicios provee de accesos a través de diversas interfaces, web, ftp, etc.

25.10.1 Dropbox

Dropbox es un servicio de alojamiento de archivos en la nube, que permite almacenar y sincronizar archivos entre distintos ordenadores e incluso con distintos usuarios. Como característica principal cabe destacar que se trata de un sistema multiplataforma y que presenta versiones tanto gratuitas como de pago.

El funcionamiento es muy sencillo, cada ordenador cliente instala un software que permite a los usuarios desplazar cualquier contenido a una carpeta designada, la cual se integra en el sistema de archivos del sistema que se trate. Una vez se sitúa un archivo en esa carpeta, o se modifica, éste es sincronizado en la nube y con todos los demás ordenadores donde esté instalado el cliente Dropbox de ese usuario. El acceso a los archivos de la carpeta de Dropbox también puede realizarse a través de la Web e incluso ser compartido por varios usuarios. Aunque Dropbox funciona como un servicio de almacenamiento, su propósito se centra más en la sincronización y compartición de archivos.

25.10.1.1 Funcionalidades de Dropbox

- Historial de revisiones: los archivos borrados de la carpeta Dropbox pueden ser recuperados desde la web o desde cualquiera de los ordenadores sincronizados.
- Historial del documento: se puede acceder al historial de un documento, de tal forma que se puede trabajar sobre el mismo, sin que esto afecte a las versiones preexistentes.
- Optimización de la conexión: al modificar un archivo en una carpeta Dropbox, el sistema sólo cargará las partes del documento que han sido modificadas cuando se produzca la sincronización.

25.11 *ESCRITORIOS VIRTUALES*

Un escritorio virtual consiste en un servicio de virtualización aplicado sobre un escritorio tradicional. En este caso el escritorio del usuario se ejecuta en un servidor, donde las órdenes de dicho usuario se transmiten online al servidor, el cual envía de vuelta los resultados de dichas acciones.

La virtualización de escritorio es relativamente reciente y describe la separación del entorno que percibe el usuario, que engloba sus datos y programas, de la máquina física en la que éstos se almacenan y ejecutan. En este caso, el usuario puede tener un sistema completo y emplear adicionalmente el escritorio virtual para cierto tipo de tareas, o incluso, el usuario puede contar con un sistema sencillo tipo terminal, donde toda las tareas del usuario se realizan directamente contra el servidor.

25.11.1 *eyeOS*

eyeOS es un sistema libre y multiplataforma que se basa en el estilo que tienen los escritorios en los sistemas operativos tradicionales, e incluye la

estructura de un sistema operativo así como ciertas aplicaciones ofimáticas como procesador de textos, calendario, navegador, gestor de archivos, etc.

Este sistema se diferencia de otros, en que no necesita de ningún software adicional para poder usarlo, puesto que todo el acceso se realiza mediante un navegador web. Recientemente, el sistema ha sido adaptado para poder utilizarse en dispositivos móviles.

25.12 MASHUPS

Un mashup es una aplicación o página web que usa y combina funcionalidades y datos de una o más fuentes para crear nuevos servicios. Implica una integración rápida y sencilla, generalmente con APIs abiertos y fuentes de datos, para producir resultados enriquecidos. Se toman una serie de datos existentes y se transforman en otros con un valor añadido que son más útiles tanto a nivel personal como profesional. Como principales características de los mashup se puede destacar la visualización, la combinación y la agregación.

Los mashup se componen de 3 partes:

- Proveedor de contenidos o fuente de datos. Los datos están accesibles a través de un API y mediante distintos protocolos como RSS.
- Sitio mashup: aplicación web que ofrece un servicio a partir de distintas informaciones que no son suyas.
- Navegador web: es la interfaz con la que el usuario interactúa con el mashup.

Un error muy frecuente es confundir los contenidos embebidos con los que

existen en un mashup. Un sitio que permite embeber por ejemplo un video o un archivo de sonido, no es un mashup, ya que no ha existido ningún tipo de procesamiento en estos datos que permita incrementar el valor que estos tienen para el usuario.

Existen distintos tipos de mashups:

- *De consumidores:* es el más conocido. Se integran datos de diversas fuentes y se accede a través de una interfaz sencilla. Ejemplo: Google Maps.
- *De datos:* se mezclan datos de tipo similar de distintas fuentes. Ejemplo: combinación de múltiples feeds RSS en uno solo.
- *Empresariales:* integra datos de fuentes tanto externas como internas. Ejemplo: incorporar mayor información a un informe estratégico mediante datos existentes en algún registro oficial.
- *De negocio:* es una combinación de los 3 anteriores.

25.13 MUNDOS VIRTUALES

Los mundos virtuales podemos verlos como un tipo de comunidad virtual, que simula un mundo artificial, el cual puede estar inspirado o no en la realidad. En este mundo virtual los distintos usuarios mediante sus avatares (personajes o representantes del usuario en el mundo virtual, caracterizados como gráficos en 2D o 3D) pueden interactuar entre sí y con otros objetos presentes en el mundo virtual. Para poder definirlo como un mundo virtual, es necesario que dicho mundo tenga una línea temporal activo, persistente y disponible las 24 horas. La interacción que se establece entre los usuarios de un mundo virtual es habitualmente en tiempo real.

Aunque actualmente la mayoría de los mundos virtuales tiene un propósito recreativo, existen muchos mundos con propósito y formas diferentes.

- *Entretenimiento (Social):*
 - o MMORPG (massively multiplayer online role-playing games): Videojuego de rol multijugador masivo en línea.
 - o MMOFPS (massively multiplayer first-person shooter)
 - o Metaverso: muy similar a MMORPG; consiste en entornos 3D completamente inmersivos.
 - o MMORLG (massively multiplayer online real-live games)
 - o Juegos sociales: su principal intención es facilitar la interacción entre personajes que generalmente ya se conocen.
- *Educativo:*
 - o MMOLE (massively multilearner online learning environments)
- *Profesional (Simuladores):*
 - o Simuladores de vuelo
 - o Reproducción de entornos especialmente costosos o difíciles de simular

25.13.1 Second Life

Second Life (SL) es un metaverso accesible de forma gratuita en Internet, cuyos usuarios suelen emplear unos programas llamados viewers para acceder al sistema, en el cual los usuarios interactúan a través de avatares. Los usuarios de SL pueden explorar el mundo, interactuar con otros usuarios, relacionarse, participar en actividades, comerciar, etc. Para poder acceder a SL es necesario crear una cuenta, lo cual da acceso directo a un avatar 3D personalizable.

25.14 P2P

Una red P2P (Peer-to-peer, red de pares o red punto a punto) es una red de ordenadores en la que todos o algunos de los aspectos funcionan sin que existan clientes ni servidores fijos, sino una serie de nodos que actúan como iguales entre sí, donde cada uno de ellos es a la vez cliente y servidor.

Este tipo de redes permite el intercambio directo de información entre los ordenadores que están conectados. Habitualmente para compartir ficheros de cualquier tipo, aunque también se emplea para telefonía VoIP.

25.14.1 Características

A continuación se detallan algunas características de las redes P2P:

- *Anonimato*: es importante que el autor de un contenido, su lector, editor y el servidor que lo almacena sean anónimos
- *Descentralización*: por definición los nodos P2P son iguales y la red descentralizada. Ningún nodo es imprescindible para el funcionamiento de la red.
- *Robustez*: al tratarse de redes distribuidas, la robustez también se ve incrementada ya que en caso de producirse un fallo, al existir una réplica de los datos en múltiples destinos, la información deseada siempre se puede encontrar, al no depender de un servidor central.
- *Seguridad*: consiste en identificar y evitar nodos maliciosos, así como el contenido potencialmente peligroso, etc. Los mecanismos de seguridad más destacados en este caso son: cajas de arena, reputación, comunicaciones seguras, comentarios sobre los ficheros, cifrado multiclave, etc.
- *Escalabilidad*: cuanto mayor número de nodos estén conectados a

una red P2P mejor será el funcionamiento. Cuando se incorporan nuevos nodos, con sus recursos, los recursos totales del sistema aumentan.

25.14.2 Tipos de redes P2P

25.14.2.1 Redes P2P centralizadas

Este tipo de red se caracteriza por:

- Arquitectura monolítica donde todas las transacciones se hacen a través de un único servidor, el cual almacena y distribuye los nodos donde se almacenan los contenidos.
- Todas las peticiones dependen de la existencia del servidor.
- Administración dinámica.
- Privacidad de los usuarios limitada.
- Falta de escalabilidad.

25.14.2.2 Redes P2P híbridas, semicentralizadas o mixtas

Este tipo de redes se caracteriza por:

- Existe un servidor que atiende peticiones pero no almacena información.
- El servidor administra los recursos, enrutamientos y comunicación entre nodos.
- Los nodos son los encargados de almacenar la información.
- El servidor central reconoce la información que desea compartir cada nodo.
- Puede existir más de un servidor que gestione los recursos

compartidos.

- Los nodos pueden seguir en contacto directo entre ellos en caso de que el servidor o servidores caigan.

25.14.2.3 Redes P2P puras o totalmente descentralizadas

Este tipo de redes se caracteriza por:

- Son las más comunes y versátiles puesto que no necesitan de ningún tipo de gestión central.
- Se reduce la necesidad de usar un servidor central.
- Cada nodo es a la vez cliente y servidor.
- Las conexiones se establecen entre usuarios, con la ayuda de un tercer nodo que permite enlazar dicha conexión.
- No existe un enrutador central.

25.15 WEB SEMÁNTICA

La web ha influido mucho en el modo de comunicación de los últimos tiempos y si bien tiene multitud de ventajas, como el acceso a millones de recursos independientemente de nuestra localización, también existen dificultades como son la sobrecarga de información y la heterogeneidad de las fuentes de información, lo que nos lleva a un problema de interoperabilidad.

Con la Web semántica estos problemas se solucionan, permitiendo que los usuarios deleguen ciertas tareas en el software. Gracias a la incorporación de mayor “semántica” a la web, el software es capaz de procesar el contenido, combinarlo, realizar deducciones, etc.

25.15.1 Definición de web semántica

La web semántica (semantic web) se basa en la idea de incorporar metadatos ontológicos y semánticos a la web. Esta información adicional, describe el significado, contenido y relación entre los datos. Además debe ser proporcionada de manera formal para que pueda ser evaluada automáticamente por equipos de procesamiento. Al enriquecer la web con más significado, se pueden obtener soluciones a problemas comunes en la búsqueda de información.

La Web se basa fundamentalmente en documentos HTML, lo cual no es demasiado versátil a la hora de categorizar los elementos que configuran el texto. La función de la web semántica es resolver estas deficiencias de tal forma que se puedan describir los contenidos de una web, mediante tecnologías como RDF, OWL, además de XML. Este tipo de tecnologías aporta descripciones explícitas de los distintos recursos incorporando una serie de etiquetas interpretables por los gestores de contenidos, de tal forma que sea posible la interpretación de los documentos, tratamiento de su información, etc.

25.15.2 RDF, SPARQL y OWL

La Web semántica, para realizar una adecuada definición de los datos, emplea fundamentalmente RDF, SPARQL y OWL.

- *RDF*: proporciona información sobre los recursos de la web, de forma simple y descriptiva.
- *SPARQL*: es el lenguaje de consulta de RDF. Permite realizar búsquedas sobre los recursos de la web semántica.
- *OWL*: es un mecanismo que permite desarrollar vocabularios

específicos que se puedan asignar a los recursos. Proporciona un lenguaje para definir ontologías que se pueden usar a través de distintos sistemas.

Las ontologías se encargan de definir los conceptos empleados para describir y representar un área de conocimiento, incluyen las definiciones de conceptos básicos y la relación entre los mismos.

25.16 BIBLIOGRAFÍA

<http://www.wikipedia.es>

<http://www.maestrosdelweb.com>

<http://www.wikispaces.com>

<http://www.w3c.com>

Autor: Francisco Javier Rodríguez Martínez
Subdirector de Sistemas Escola Superior Enxeñaría Informática Ourense
Colegiado del CPEIG

26. SISTEMAS DE INFORMACIÓN GEOGRÁFICA. ARQUITECTURA DE LOS SISTEMAS DE INFORMACIÓN.

Tema 26: Sistemas de Información Geográfica

ÍNDICE

26.1 Introducción.....	2
26.2 Conceptos básicos.....	6
26.2.1 <i>Georreferenciación.....</i>	6
26.2.1.1 <i>Georreferenciación directa.....</i>	6
26.2.1.2 <i>Georreferenciación indirecta o discreta.....</i>	7
26.2.2 <i>Modelo de Datos.....</i>	8
26.2.2.1 <i>Modelo Ráster.....</i>	9
26.2.2.2 <i>Modelo Vectorial.....</i>	13
26.3 Arquitectura de un SIG.....	17
26.3.1 <i>Clasificación de los SIG.....</i>	20
26.4 Áreas de Aplicación.....	22
26.4.1 <i>Demografía.....</i>	22
26.4.2 <i>Gestión y Planificación Urbana.....</i>	22
26.4.3 <i>Gestión de Instalaciones.....</i>	23
26.4.4 <i>Aplicaciones de gestión e inventario de recursos.....</i>	23
26.4.5 <i>Gestión Catastral.....</i>	24
26.5 Proveedores y Usuarios de Información Espacial.....	24
26.6 Infraestructuras de Datos Espaciales.....	26
26.6.1 <i>Principios de los IDE.....</i>	26
26.6.2 <i>Componentes de los IDE.....</i>	27
26.6.2.1 <i>Datos.....</i>	27
26.6.2.1.1 <i>Datos de referencia.....</i>	27
26.6.2.1.2 <i>Datos temáticos.....</i>	28
26.6.2.2 <i>Metadatos.....</i>	29
26.6.2.3 <i>Servicios.....</i>	30
26.7 Bibliografía.....	33

26.1 INTRODUCCIÓN

Como información espacial (geográfica, georreferenciada o geodatos) nos referimos a todo tipo de información relativa a sucesos o elementos para la cual se incluye una referencia a su localización, la cual está situada sobre o en las inmediaciones de la superficie de la Tierra. La forma de referenciar la posición de estos elementos o estos sucesos puede realizarse de distintas formas, mediante una simple dirección postal, con coordenadas geográficas (longitud y latitud) o con coordenadas cartesianas en algún sistema de referencia cartográfico.

La mayor parte de la información en formato electrónico almacenada actualmente en sistemas de todo tipo, es información espacial o que podría serlo. El porque de este auge de la información espacial la encontramos en una serie de características que justifican el interés de asociar a una información la referencia de su localización.

Por una parte tenemos la cualidad de la información espacial para su representación en forma gráfica y simbólica mediante mapas. Los mapas son un sistema de comunicación que ha sido utilizado desde las primeras civilizaciones y con el que está familiarizado prácticamente todo el mundo. Además los mapas han tenido gran importancia a lo largo de la historia militar, económica y política de las naciones, por lo que han sido considerados siempre como un recurso clave a cuyo desarrollo se han dedicado importantes esfuerzos.

Por otra parte, la capacidad que posee la información espacial para integrar conjuntos de información que de otra forma serían inconexos, mediante la aplicación de las relaciones espaciales de coincidencia, proximidad o adyacencia inherentes a dicha localización espacial. Esta característica es probablemente la que mayor potencial otorga a la información espacial, constituyendo la base del análisis espacial.

La primera manifestación de los sistemas de información geográfica los podemos encontrar, como se comentaba anteriormente, en los mapas, sin embargo, ya en épocas más recientes, las aportaciones de las tecnologías de la información en el ámbito de la cartografía han sido muy importantes. Se pueden destacar aquellos avances destinados a la mejora de los procesos de producción cartográfica, las orientadas a la explotación y análisis de la información cartográfica.

En lo tocante a la producción cartográfica, actualmente se cuenta con técnicas muy depuradas para la producción de mapas en todas sus fases, desde la captura de datos (fotogrametría aérea, imágenes de satélite, teledetección, telemetría láser, GPS, etc), hasta los diferentes procesos que componen la fase de elaboración de la cartografía. Estas técnicas han permitido no sólo notables mejoras en la calidad, diversidad y flexibilidad de los productos cartográficos, sino que ha hecho posible, disponer de información cartográfica muy actualizada

En lo tocante al análisis de la información geográfica es necesario destacar en primer lugar las importantes limitaciones prácticas que presentan los mapas tradicionales para su utilización en análisis mediante técnicas manuales. La superación de estas limitaciones es ha sido la motivación inicial para el desarrollo de los Sistemas de Información Geográfica, SIG (o GIS de acuerdo con la terminología anglosajona), que se ha convertido en la otra gran rama de aportaciones de las tecnologías de la información en el ámbito de la cartografía.

El desarrollo de los primeros GIS datan de finales de los años 60 y supuso un gran cambio en la utilización de la información espacial que se hacia hasta ese momento. De hecho las técnicas y metodologías de análisis espacial de la información, que hasta el momento habían sido poco examinadas por la excesiva complejidad asociada a los tratamientos manuales, se vieron paulatinamente mejoradas y en muchos casos empezó

a ser posible su utilización con el procesamiento automatizado de la información espacial en formato digital.

Un Sistema de Información Geográfica está orientado a la captura, manipulación, recuperación, análisis, representación, etc, de información georreferenciada, aquella en la que la posición espacial ocupada por los objetos del mundo real que se modelizan forma parte inherente a dicha información.

Los SIG gozan de gran aceptación desde sus primeras implantaciones lo cual se debe en gran medida a su capacidad para construir modelos orientados a la resolución de problemas cuyo universo de discurso se caracteriza por tener un componente espacial.

Estas primeras realizaciones fueron impulsadas principalmente por organizaciones con responsabilidades en la gestión de recursos con implantación territorial como son ordenación del territorio, recursos naturales, censo, defensa, etc.

Desde estas primeras implantaciones, en los años 60, hasta la década de los 80, el desarrollo de los SIG se produjo de una forma relativamente lenta debido sobretodo a la capacidad y coste de la tecnología digital disponibles en aquel momento. Desde la segunda mitad de los 80 se produce un gran auge, tanto en diversificación de las áreas de aplicación de esta tecnología como en la oferta de productos comerciales, lo que ha otorgado gran popularidad y difusión a los SIG en todo tipo de organizaciones.

Actualmente la evolución se caracteriza por una serie de factores que impiden una plena estabilidad del sector:

- Evolución de las tecnologías en las que se apoyan los SIG, como son, gestores de bases de datos, procesamiento paralelo, visualización, etc.

- Alto grado de relación entre los SIG e Internet , que está en permanente evolución.
- La tecnología disponible se orienta a implementaciones que no aprovechan el potencial de la misma.
- Restricciones institucionales que todavía impiden el acceso y utilización de la información cartográfica de que se dispone a todos los niveles.

26.2 CONCEPTOS BÁSICOS

26.2.1 Georreferenciación

La georreferenciación es el proceso por el cual se identifica una determinada posición en la superficie terrestre o sus inmediaciones. Se dice que una información es o está georreferenciada cuando mediante algún procedimiento se ha asociado a dicha información la posición del elemento o suceso al que se refiere la misma.

La posición es lo que distingue a la información espacial de cualquier otro tipo de información, por lo cual es de gran importancia el método utilizado para especificar dicha posición, sobretudo cuando deben combinarse informaciones espaciales de diferentes procedencias que pueden haber utilizado procedimientos de georeferenciación distintos.

Existen dos técnicas para asociar la posición a una información: *la georreferenciación directa y la indirecta (o discreta)*.

26.2.1.1 Georreferenciación directa

La georreferenciación directa se basa en la utilización de coordenadas para definir posiciones. El sistema de coordenadas geográfico es el más sencillo a nivel conceptual, según el cual, para definir la posición de un punto se utilizan la longitud y latitud del mismo. Este es un procedimiento muy sencillo que se complica notablemente cuando lo que queremos localizar es una distancia o una superficie y no un punto, puesto que entran en juego procedimientos de trigonometría esférica. Por ello, es muy habitual la utilización de sistemas de coordenadas cartesianas definidos para un determinado sistema de proyección.

Entre los sistemas de proyección válidos para todo el globo terráqueo, también denominados globales, el más utilizado es el correspondiente a la proyección *Universal Transversal Mercator (UTM)*.

Este sistema de proyección es el que emplean la mayoría de organismos cartográficos, tanto nacionales como internacionales, además, casi todos los receptores GPS proporcionan coordenadas UTM. Los principales problemas de este sistema de proyección radican en el trabajo con datos de diferentes husos o en el empleo de latitudes muy altas.

A la península Ibérica le corresponden los husos UTM 29, 30 y 31 (a las Islas Canarias les corresponde el huso 28).

La georreferenciación directa es de tipo continuo, es decir, se puede situar una posición con la precisión que sea necesaria. Por contraposición a la georreferenciación discreta que sólo permite referenciar un número finito de posiciones en el espacio.

26.2.1.2 Georreferenciación indirecta o discreta

La georreferenciación indirecta o discreta consiste en el uso de nombres, topónimos, etc. para indicar la posición de un lugar e incluso si este descriptor no existe, se emplean construcciones léxicas de aproximación partiendo de un lugar si referenciado, como pueden ser, “al lado del colegio”, “ más allá del banco”, “cerca del teatro”, etc. En muchos casos las coordenadas de estos lugares de referencia sí son conocidos y contamos con mecanismos lo suficientemente accesibles para obtener la posición deseada.

La referencia de este tipo más empleada es la dirección postal, asociada a multitud de registros de información a pesar de sus limitaciones de localización y que es de gran utilidad en aplicaciones donde por ejemplo la escala que se necesita no es muy detallada

26.2.2 *Modelo de Datos*

El modelo de datos es el mecanismo por el cual se realiza la representación de los objetos del mundo real en el sistema de información.

Los modelos de datos utilizados han variado poco desde los inicios de los SIG, siendo, el modelo de datos ráster y el modelo de datos vectorial, los más utilizados.

- Modelo de datos Ráster: se parte de una concepción de la realidad, o parte de la misma, y se representa como algo continuo, por lo que dicha realidad tiene asociada una distribución de los valores que toma en cada posición (o en un conjunto discreto de posiciones seleccionadas).
- Modelo de datos Vectorial: la abstracción del mundo real conduce a la distinción de una serie de objetos diferenciables, relevantes para el problema en cuestión, que son los representados en el sistema.

Independientemente del modelo empleado, su desarrollo debe llevarnos, tras sucesivas abstracciones en las fases de diseño lógico y físico, a conseguir la representación de los elementos de información que se emplean en un SIG:

- Georreferencias: información posicional.
- Información relativa a las características de los objetos modelizados: información temática.

- Información sobre las relaciones espaciales existentes entre los objetos: información topológica.
- Información sobre las relaciones de tiempo: información temporal. Este tipo de información es muy importante en cierto tipo de problemas, si bien generalmente se trata como un atributo adicional.

El tipo de modelo de datos que se seleccione condicionará todas las operaciones que puedan ser realizadas con el mismo. Si bien existen muchos sistemas comerciales que permiten la combinación de ambos, lo cual puede ser conveniente en el tratamiento de determinado tipo de problemas.

26.2.2.1 Modelo Ráster

El modelo de datos Ráster tiene su origen en las técnicas de captura de datos temáticos y geográficos a partir de imágenes satelitales y de fotografía aérea (técnicas de teledetección). Estas técnicas comparten muchos puntos con las tecnologías de tratamiento de imágenes.

La región a modelar se considera dividida siguiendo una matriz o malla rectangular de celdas (píxeles) de generalmente cuadradas y de igual tamaño¹. A cada una de estas celdas se le asigna el valor de la propiedad o atributo que se va a representar, el cual se determina en base a una convención preestablecida, por ejemplo, el valor que toma el atributo en el centro de la celda, en uno de los vértices o el valor medio en la celda, etc. Este valor podría ser, el nivel de gris en una escala de 256 valores, la

1

El tamaño de la celda se denomina resolución.

temperatura media de un cierto lugar, las precipitaciones en una región, etc.

Un conjunto de datos de tipo ráster de gran utilidad e importancia es el modelo digital de características relevantes para su resolución. En la práctica, es corriente manejar hasta varias decenas, o incluso cientos de capas. Por ejemplo, para representar los niveles de rojo, verde y azul de una imagen RGB sería necesario utilizar 3 capas, una para cada color, en cada píxel de la imagen.

De acuerdo con esto, los objetos reales a representar son los segmentos del terreno correspondientes a las celdas, o más concretamente, el valor del atributo que se está representando en dicho segmento del terreno. Hoy en día es habitual obtener imágenes de grandes extensiones de terreno con resoluciones de 50x50cm o incluso inferiores.

En el modelo de datos ráster no existe una representación explícita de entidades físicas del mundo real, no se representan explícitamente los edificios, ni los ríos, por ejemplo. Es por esto, que este modelo no es útil para la representación de información topológica, es decir, del tipo “un elemento es contiguo a” o “un elemento está sobre” otro. Este modelo tampoco guarda explícitamente la posición de las celdas, ya que, si se conoce la orientación de la malla de celdas respecto a una referencia, la secuencia de barrido (filas y columnas) y las coordenadas geográficas de una de ellas, puede obtenerse la georreferencia de cualquier celda.

Las técnicas de organización y compresión que se emplean para el almacenamiento interno de la información que se asocia a cada capa son muy relevantes y buscan un equilibrio entre el volumen de información y la eficiencia del acceso a la misma. Existen muchas técnicas, la más elemental de todas ellas, consiste en recorrer la imagen siguiendo la

secuencia de barrido y almacenar los valores de los atributos en sucesivas celdas. El problema de esta técnica radica en su ineficiencia.

Para solucionarlo, se suelen emplear técnicas de compactación de datos, como son, Run Length Encoding (RLE) en la cual, se almacenan pares (L,V), donde L es el número de celdas contiguas en que repite el valor V del atributo.

Otras técnicas más complejas se basan en estructuras de datos orientadas a la indexación espacial y a la compresión de datos, denominadas quadrees. En estas técnicas, se realiza de manera recursiva una división de la información inicial en cuadrantes cada vez menores a los que se aplican procedimientos de compresión.

Una técnica de compresión cada vez más utilizada es la basada en wavelets, que aunque implica una cierta pérdida de información, la suple al conseguir unos niveles de compresión muy elevados.

En un SIG tipo ráster, las funcionalidades de tratamiento de información más habituales son las que se mencionan en las categorías siguientes:

- *Operaciones locales en una capa:*
 - o Recodificación de capas: asignar nuevos códigos para un atributo a partir de los ya existentes.
 - o Filtrado(resaltado o suavización): se obtiene una nueva capa a partir de otra dando a cada celda un valor que se obtiene de los valores de las celdas vecinas.
 - o Determinación de pendientes y rumbos de máxima pendiente: a partir de un modelo digital del terreno (MDT), se representa

el atributo de elevación (cota) de los puntos situados en una matriz regular de tamaño preestablecido.

- *Operaciones de presentación:*
 - o Generación de leyendas.
 - o Determinación de isolíneas (curvas de nivel).
 - o Determinación de perspectivas con drapping: representación de la capa correspondiente a un atributo concreto sobre una vista tridimensional obtenida partiendo de un MDT.
- *Operaciones de mantenimiento de datos:*
 - o Intercambio de datos con otros sistemas.
 - o Intercambio de datos con otros formatos.
 - o Remuestrear: cambiar el tamaño y orientación de las celdas para hacerlas compatibles con los datos de entrada o para cambiar de escala.
 - o Vectorización: conversión de la información ráster a vectorial.

La estructura de datos que se obtiene tras la realización de las operaciones es la capa, que representa la variación espacial de un único atributo como la sucesión de valores tomados por dicho atributo en las sucesivas celdas. Por lo tanto, para un problema será preciso representar tantas capas como atributos sean de elevaciones.

- *Operaciones con varias capas:*

- o Superposición (overlay): se obtienen nuevas capas a partir de dos o más capas existentes mediante operaciones booleanas o aritméticas con las mismas.
 - o Cálculo de pasillos: determinar zonas que distan de una determinada característica menos de un valor dado.
 - o Determinar cuencas visuales: zonas vistas desde uno o varios puntos dados.
- *Agrupación de celdas:*
 - o Determinar zonas de celdas contiguas con el mismo valor de atributo.
 - o Cálculo de áreas, formas, distancias, perímetros, etc.

26.2.2.2 Modelo Vectorial

En el modelo vectorial, se utilizan tres principios geométricos para representar las entidades geográficas. Estas bases geométricas son:

- El punto es la entidad básica de representación de entidades con posición, pero se acepta que carece de dimensión.
- El arco representa las entidades unidimensionales y se define mediante vértices o nodos.
- El polígono se utiliza para las entidades bidimensionales y se define mediante los arcos que lo delimitan.

Cada entidad geográfica que se representa mediante el modelo vectorial tiene asignado un identificador único en el sistema. Dicho identificador

permite referenciar las entidades en cualquier momento y vincularlas con sus atributos alfanuméricos(información temática).

Para especificar la definición geométrica se emplean las coordenados de los puntos y vértices a partir de los que se definen las distintas entidades. Podemos hablar por tanto de una georreferenciación continua, sin que la resolución suponga un impedimento como pasaba en el modelo de datos ráster.

Al contrario de lo que sucede en el modelo ráster, en el que se representan todas las posiciones del espacio que se estudia, en el modelo de datos vectorial sólo se almacena la información de las entidades territoriales relevantes, lo que supone un acercamiento al modelo de razonamiento espacial que se emplea habitualmente.

A pesar de esto, la diferencia más relevante entre este modelo y el ráster, es la capacidad que tiene para expresar las relaciones espaciales que existen entre las entidades (información topológica), que son las que otorgan al modelo la capacidad semántica precisa para representar el conocimiento territorial. Sin embargo, esta ventaja en la representación espacial también implica un aumento en la complejidad de este modelo en comparación con el modelo de datos ráster.

Los primeros SIG basados en el modelo vectorial almacenaban de forma separada la información geométrica y topológica de la información correspondiente a los atributos. Para la información asociada a los atributos se empleaban SGBD relacionales convencionales y para la información geométrica y topológica se empleaban estructuras de datos y ficheros de tipo propietario, diseñados para optimizar el rendimiento de las operaciones a realizar, recayendo en el sistema GIS el peso del mantenimiento de las relaciones entre todos ellos. Este tipo de arquitectura se denomina modelo georrelacional.

Dada la mejora en el rendimiento de los SGBDR ya no existe motivo para mantener esta separación, por lo que actualmente se tiende a que todos los datos con los que trabaja un GIS se almacenen en BD relacionales convencionales, o quizá ampliados mediante extensiones geográficas. Las bases de datos que se emplean son normalmente de propósito general y externas al propio SIG, dando lugar a las llamadas bases de datos geoespaciales (Geodatabases).

Este nuevo enfoque en el almacenamiento de los datos espaciales ha resultado un pilar fundamental en la evolución de los SIG en las organizaciones, ya que se ha cubierto el espacio existente entre los sistemas orientados a proyecto o departamentales y los sistemas de información espacial de alcance corporativo.

Las principales funcionalidades de los modelos de datos vectoriales son:

- Conversión entre diferentes formatos.
- Análisis espacial: estudios basados en los operadores espaciales habituales como son, adyacencia, superposición, proximidad, etc. Los operadores se emplean (booleanos o aritméticos) sobre los atributos de las entidades de las capas iniciales.
- Acceso a la base de datos y recuperación de la información de las entidades que satisfacen una serie de cláusulas, que pueden plantearse tanto en términos tanto espaciales como de sus atributos temáticos.
- Medida de áreas, perímetros y distancias.
- Análisis estadísticos: correlaciones espaciales, análisis de patrones, etc.
- Presentación de resultados.

Si bien, tanto el modelo vectorial como el ráster, tienen sus ventajas y sus inconvenientes y se admite de forma global que cada modelo se adecúa más a un tipo distinto de problemas, también existen soluciones híbridas que permiten la combinación de ambos modelos.

- Los modelos ráster son más adecuados para problemas que admiten algún tipo de formulación analítica.
- Los modelos vectoriales son más adecuados se adecuan mejor a problemas de gestión que admiten una formulación mediante polígonos, redes, etc.

Como evolución del modelo de datos vectorial, tenemos el modelo de datos orientado a objetos en el que el elemento central es el conjunto de elementos geográficos y las relaciones entre los mismos. Cada objeto geográfico es un paquete que integra geometría, métodos y propiedades. Los objetos geográficos del mismo tipo se agrupan en clases, donde cada uno de estos objetos sería una instancia de la clase. La definición de la clase incluye también las relaciones topológicas y geográficas o espaciales.

26.3 ARQUITECTURA DE UN SIG

En los primeros desarrollos de los SIG encontramos principalmente sistemas software cerrados de gran tamaño y complejidad (SIG monolítico), que eran utilizados principalmente por grupos de usuarios reducidos con un nivel de especialización bastante elevados, además, se orientaban a tareas muy concretas y generalmente presentaban poca o ninguna integración con otros sistemas. Actualmente los sistemas se diferencian mucho de estos iniciales, son cada vez más habituales y sencillos, no requieren de usuarios expertos para su manejo y permiten la integración de la información con otros sistemas.

En un sistema SIG podemos hablar de arquitecturas de 3 capas, así tenemos:

- **Capa de Presentación:** incorpora todas las funcionalidades que permiten la interacción entre el usuario y el sistema, para acceso al acceso a la información y presentación de resultados. Habitualmente esto se traduce en una GUI que facilita el acceso a las herramientas de la siguiente capa o también en una aplicación externa que pueda acceder a determinadas funciones de geoproceto.
- **Capa de Proceso:** abarca una serie de herramientas diferentes que integran el núcleo del SIG.
- **Capa de Gestión de Datos:** centraliza el acceso a los datos, que pueden localizarse en distintos almacenes. Además, integra también muchas de las funciones que se encargan de proporcionar transparencia sobre los detalles de los datos: sistemas de proyección, formatos, transformación de coordenadas, etc.

Para implementar estas capas funcionales podemos tener los mismos o diferentes sistemas físicos, teniendo una gran cantidad de posibilidades. Si se hace una desagregación completa, cada una de estas capas residirá en uno o más servidores diferentes, adaptado a las necesidades específicas del entorno de implantación del SIG.

En el mercado de los SIG comerciales, se están asumiendo cada vez mas una serie de estándares de facto que han ido surgiendo en los últimos años debido a las tecnologías de componentes (Java Beans, .NET, ...) y de plataformas interoperables de objetos distribuidos (SOAP, CORBA). Estas tecnologías, permiten construir nuevos SIG de forma extensible e integrando funcionalidades proporcionadas por diversos proveedores.

Desde la perspectiva de los almacenes de datos, se tiende cada vez mas al uso de los sistemas post relacionales, que permiten integrar en sistemas relacionales tradicionales algunas características de las BDOO e incluso incluyen extensiones espaciales del modelo multimedia del estándar SQL3.

Por otro lado, el avance en el campo de las telecomunicaciones y más en concreto, de Internet, con un gran potencial tanto para la transmisión de grandes cantidades de información y acceso a datos, ha favorecido la expansión de las arquitecturas de geoprocso basadas en servicios web.

Los servicios web permiten concebir y desarrollar sistemas que integran, con un mínimo nivel de acoplamiento, información y servicios de geoprocso interoperables de múltiples fuentes y en distintos formatos, a los que se accede en un entorno de red distribuido.

Estas nuevas arquitecturas pretenden satisfacer el deseo de la comunidad SIG de disponer de un acceso ilimitado y en cualquier momento a información actualizada e interoperable. La disponibilidad de este tipo de

servicios está facilitando una expansión del intercambio y de la difusión electrónica de la información espacial.

Por otra parte, este crecimiento en la implantación de productos y servicios de información cartográfica en la red, establece los principios para el asentamiento real de un entorno en el que sea posible el intercambio de información geográfica y servicios de geoproceso. Cabe destacar también la acción tan importante que en esta línea está desarrollando el consorcio OpenGIS, en el que se aglutinan los principales entes involucrados en el sector de la información espacial y todos los sistemas y tecnologías que la soportan (usuarios, universidades, administraciones, industrias software, ...). El propósito de estos colectivos es elaborar de forma consensuada, especificaciones de interfaces interoperables en el campo de las tecnologías de la información espacial.

Desde la creación de OpenGIS, a mediados de los años 90, han sido ya muchas las realizaciones prácticas en las que ha tomado parte y siendo, sus especificaciones estándares de facto en el área de las tecnologías de la información espacial. Además, en muchos casos estos estándares son la base para la formulación de estándares internacionales.

Por ejemplo, los dos siguientes, son servicios web que ya han sido enteramente especificados:

- Servicio de Entidades Vectoriales: facilita información relativa a la entidad o entidades que se encuentran almacenadas en una capa vectorial y que reúnen las características especificadas durante la consulta.
- Servicio de Mapas en la Web: genera mapas en el formato deseado para ser visualizados en un navegador u otro tipo de cliente sencillo. Estos mapas serán la respuesta a alguna consulta con ciertos parámetros realizada previamente.

Podemos concluir que las arquitecturas de los SIG tienden a ser distribuidas, interoperables y en red, apoyadas sobre estándares abiertos de Internet.

26.3.1 *Clasificación de los SIG*

De acuerdo con la funcionalidad que integran y el tipo de problema que pretenden resolver, podemos distinguir los siguientes grupos de sistemas de información geográfica.

1. *SIG Profesional*: se enfocan hacia usuarios con un alto nivel de especialización y formación en este campo. Integra todas las funciones que se pueden necesitar en un SIG a nivel de recopilación y edición de datos, administración de BD, análisis y geoproceto avanzado y todas las herramientas específicas que puedan ser necesaria para mantenimiento de la información.
2. *SIG de Sobremesa*: se enfocan hacia la explotación y utilización de la información. Incorpora herramientas de análisis de la información, además de mecanismos avanzados para la presentación de resultados como son, informes, gráficos, mapas, etc. Presentan una gran facilidad de manejo, con lo cual los usuarios no necesitan ser expertos en el ámbito, además las herramientas que integran son potentes y facilitan el acceso avanzado a la información.

3. *Visualizadores SIG*: se trata de herramientas sencillas que se centran exclusivamente en la visualización de la información, de distintos tipos y formatos..
4. *WebGIS*: se trata de proporcionar el acceso a datos cartográficos y a las funcionalidades (servicios) de los SIG a través de la red. Cada vez más se tiende hacia la estandarización de este tipo de servicios liderado por OpenGIS.
5. *SIG de Componentes*: con la expansión en el campo de la ingeniería de software de los desarrollos basados en componentes, se ha alcanzado la posibilidad de incorporar funcionalidades espaciales en todo tipo de aplicaciones (captación espacial de aplicaciones), lo que supone un nuevo impulso para la generalización del uso de la información espacial a nuevos campos, en los que se pueden realizar interesantes sinergias.
6. *SIG de Dispositivos Móviles*: se apoya en el uso de PDAs y Smartphones. Estos dispositivos tienen capacidad suficiente como para soportar casi todas las funciones de un sistema tradicional.

26.4 ÁREAS DE APLICACIÓN

Los productos SIG comerciales son cada vez más comunes y populares, por lo que recoger todas las áreas posibles de aplicación es una ardua tarea. Sin embargo, en el siguiente listado se presentan las más destacadas o donde el número de desarrollos es mayor.

26.4.1 Demografía

En esta categoría se recogen todas las aplicaciones, que si bien pueden ser de naturaleza muy diversa, comparte el hecho de que utilizan características demográficas y socioeconómicas, y la distribución espacial de las mismas para la toma de decisiones.

Los datos en los que se apoyan este tipo de sistemas suelen proceder de registros estadísticos confeccionados por algún organismo (oficial o no).

Las aplicaciones dentro de esta categoría se suelen centrar en el marketing evaluación del impacto de un servicio, selección de lugares para el establecimiento de negocios o servicios, etc.

26.4.2 Gestión y Planificación Urbana

Esta categoría se orienta a actividades propias de gestión municipal como son, la gestión de servicios de infraestructura (alumbrado, alcantarillado, mobiliario urbano, etc.), la gestión del tráfico, la gestión de tasas y licencia, el emplazamiento para instalaciones y servicios comunitarios, etc.

Este tipo de sistemas suele manejar escalas grandes y se usa como base el callejero del municipio en cuestión. Además este tipo de aplicaciones suele emplear un modelo de datos de tipo vectorial.

26.4.3 *Gestión de Instalaciones*

En esta categoría se agrupan los desarrollos orientados a compañías de suministros y servicios, como son electricidad, agua, ferrocarril, etc. Las aplicaciones tipo de este grupo pasan por la gestión del mantenimiento, la relación con el cliente (notificaciones de cortes de suministro), diseño de instalaciones, etc.

Estos sistemas se caracterizan por:

- La precisión necesaria suele ser elevada.
- Existe una fuerte estructura en red, necesaria para la realización de análisis.
- Se establecen conexiones con bases de datos externas.
- Existe una jerarquía de componentes de la red.

26.4.4 *Aplicaciones de gestión e inventario de recursos*

En esta categoría se incluyen campos como la gestión forestal, la planificación agraria, la evaluación del impacto ambiental, la gestión del territorio, la del patrimonio natural y la del medio ambiente.

Normalmente manejan escalas pequeñas con diversas calidades en los datos e incluso sin contrastar. Estas aplicaciones usan modelos de datos tanto vectoriales como ráster.

26.4.5 *Gestión Catastral*

Esta categoría se orienta a la gestión de la propiedad inmobiliaria y por su importancia ha adquirido un término específico, Sistemas de Información Territorial (SIT).

En nuestro país contamos con el Sistema de Información Catastral, que cuenta con datos y descripciones de las propiedades tanto a nivel urbano, como a nivel rústico.

26.5 PROVEEDORES Y USUARIOS DE INFORMACIÓN ESPACIAL

De manera tradicional ha sido el sector público el encargado de la construcción de la infraestructura cartográfica de un país, además de las muchas consideraciones que justifican este hecho, hay que tener en cuenta también que son las propias administraciones públicas las principales consumidoras de esta información espacial.

Por ejemplo, algunas de las actividades para las que las administraciones hacen uso de información espacial son:

- Protección civil
- Registro catastral
- Censos estadísticos y electorales

- Gestión de recursos naturales
- Protección del medioambiente
- Inventario del patrimonio
- Gestión de los dominios públicos
- Planificación de infraestructuras
- Organización territorial

Además de estas, existen muchos otros servicios públicos con una clara implicación territorial, como son, los servicios sociales y asistenciales, servicios educativos y de salud pública, etc.

26.6 INFRAESTRUCTURAS DE DATOS ESPACIALES

Una IDE (Infraestructura de Datos Espaciales) es un sistema informático integrado por un conjunto de recursos (catálogos, servidores, programas, datos, aplicaciones, páginas Web,...) dedicados a gestionar Información Geográfica (mapas, ortofotos, imágenes de satélite, topónimos,...), disponibles en Internet, que cumplen una serie de condiciones de interoperabilidad (normas, especificaciones, protocolos, interfaces,...) que permiten que un usuario, utilizando un simple navegador, pueda utilizarlos y combinarlos según sus necesidades.

El establecimiento de una IDE, a nivel local, regional, estatal o global, requiere del acuerdo de los productores, integradores y usuarios de datos espaciales del ámbito territorial en el que se establece. Este acuerdo debe considerar también las IDE definidas, o en definición, en otros ámbitos territoriales superiores, hacia las cuales deberá converger.

La justificación del establecimiento de una IDE, esta ligada a dos ideas fundamentales:

- La necesidad de manera fácil, cómoda y eficaz de los datos geográficos existentes. La Información Geográfica ha sido hasta ahora un recurso de costosa producción y difícil acceso por varios motivos: formatos, modelos, políticas de distribución, falta de información,...
- La oportunidad de reutilizar la Información Geográfica generada en un proyecto para otras finalidades diferentes, dado el alto coste de su producción.

26.6.1 Principios de los IDE

Todas las iniciativas para el establecimiento de una IDE incluyen unos principios comunes:

- Marco Institucional: el establecimiento de acuerdos entre los productores de información geográfica, especialmente entre los productores oficiales, para generar y mantener los datos espaciales fundamentales («Framework data») para la mayoría de las aplicaciones basadas en sistemas de información geográfica.
- Estándares: el establecimiento de normas a las que deberá ajustarse la información geográfica, los intercambios de esta y la interoperación de los sistemas que la manejan.
- Tecnología: el establecimiento de la red y mecanismos informáticos que permitan: buscar, consultar, encontrar, acceder, suministrar y usar los datos espaciales o geográficos. Como por ejemplo permitir incorporar los metadatos organizados en catálogos y ofrecerlos en la red a través de servidores.
- Política de datos: El establecimiento de las políticas, alianzas y acuerdos de colaboración necesarios para aumentar la disponibilidad de datos espaciales y compartir los desarrollos tecnológicos.

26.6.2 Componentes de los IDE

26.6.2.1 Datos

En la actualidad existe un consenso internacional que clasifica los datos espaciales que pueden manejar las IDEs en:

26.6.2.1.1 Datos de referencia

Son aquellos datos georreferenciados fundamentales que sirven de esqueleto para construir o referenciar cualquier otro dato fundamental o temático. Constituyen el marco de referencia que proporciona el contexto geográfico a cualquier aplicación.

Cumplen la función de ser la Información Geográfica de referencia utilizada como base común que permite mezclar e integrar datos de aplicaciones de todo tipo al ser el vínculo o nexo de unión.

La iniciativa europea INSPIRE ha definido los temas que deben ser considerados como Datos de Referencia, en los Anexos I y II en la Propuesta de Directiva por la que se establece una Infraestructura de Información Espacial de la Comunidad (INSPIRE):

- Sistema de Coordenadas.
- Cuadrículas Geográficas.
- Nombres geográficos.
- Unidades Administrativas.
- Redes de Transporte.
- Hidrografía.
- Lugares Protegidos.
- Elevación.
- Identificadores de Propiedad.
- Parcelas Catastrales.
- Cubierta Terrestre.
- Ortoimágenes.

26.6.2.1.2 Datos temáticos

Son los datos propios de aplicaciones específicas que explotan la Información Geográfica con una finalidad concreta. Incluyen valores cualitativos y cuantitativos que se corresponden con atributos asociados a los datos de referencia como por ejemplo: vegetación, geología, clima, tráfico, contaminación, etc.

26.6.2.2 Metadatos

La estructura y el contenido de los metadatos deben estar basados en una norma aceptada y ampliamente utilizada. Uno de los beneficios de las normas es que son fruto de la experiencia y del consenso, ya que han sido desarrolladas y revisadas por un grupo internacional de expertos que han aportado una considerable diversidad cultural y social. En particular, las normas ISO19100 relativas a Información Geográfica proporcionan una base desde la que pueden desarrollarse perfiles, o particularizaciones de la norma, nacionales y sectoriales.

En la actualidad existen diferentes normas y perfiles dentro del campo de los metadatos que es interesante mencionar:

- ISO 19115 “Geographic information – Metadata”

Norma Internacional de metadatos perteneciente a la familia ISO 19100 desarrollada por el Comité Técnico 211, perteneciente a la Organización de Estandarización Internacional (ISO) que proporciona un modelo de metadatos y establece un conjunto común de terminología, definiciones y procedimientos de ampliación para metadatos. Ha sido adoptada como Norma Europea por el CEN/TC287 y como Una Norma Española por AEN/CTN148 “Información Geográfica”, por lo que está disponible en español.

- [Núcleo Español de Metadatos “NEM”](#)

Recomendación definida por el Grupo de Trabajo de la IDEE, establecida en forma de perfil de ISO19115. Es un conjunto mínimo de elementos de metadatos recomendados en España para su utilización a la hora de describir recursos relacionados con la información geográfica. Está formado por la ampliación del Núcleo (Core) de la Norma ISO 19115 de Metadatos, con los ítems de ISO19115 necesarios para incluir los elementos del Dublín Core Metadata, la descripción de la Calidad y los elementos requeridos por la Directiva Marco del Agua.

- Dublín Core Metadata Iniciativa

La iniciativa Dublín Core Metadata es un foro abierto dedicado al desarrollo de estándares en la línea de los metadatos. Tiene como actividades principales: la formación de grupos de trabajo, conferencias globales y talleres y desarrollo de prácticas en el campo de los metadatos. Esta iniciativa definió 15 elementos básicos y esenciales para describir un recurso cualquiera (fichero, mapa, libro,...) y en la actualidad es la iniciativa de metadatos más utilizada. Para más información consultar la página Web: <http://dublincore.org/>

26.6.2.3 Servicios

Mucho más adecuado que concebir una IDE como algo basado en los datos geográficos disponibles, es pensar que una IDE es en realidad un conjunto de servicios, que ofrecen una serie de funcionalidades que resultan útiles e interesantes a una comunidad de usuarios. De forma que el énfasis se pone en los servicios, en la utilidad. Se establece un juego nuevo con reglas nuevas; desde el punto de vista de las IDEs, al usuario no le interesa ya tanto descargarse los datos en su sistema, sino obtener directamente las respuestas que necesita y que un servicio le ofrece.

Los servicios IDE ofrecen funcionalidades accesibles vía Internet con un simple navegador o browser, sin necesidad de disponer de otro software específico para ello.

- Servicio de Mapas en Web (WMS)

Su objetivo es poder visualizar Información Geográfica. Proporciona una representación, una imagen del mundo real para un área requerida. Esta representación puede provenir de un fichero de datos de un SIG, un mapa digital, una ortofoto, una imagen de satélite,... Está organizada en una o más capas, que pueden visualizarse u ocultarse una a una. Se puede consultar cierta información disponible y las características de la imagen del mapa. Una especificación del Open Geospatial Consortium

(OGC) establece cómo debe ser un WMS estándar e interoperable, que permita superponer visualmente datos vectoriales, ráster, en diferente formato, con distinto Sistema de Referencia y Coordenadas y en distintos servidores.

- Servicio de Fenómenos en Web (WFS)

Ofrece el poder acceder y consultar todos los atributos de un fenómeno (feature) geográfico como un río, una ciudad o un lago, representado en modo vectorial, con una geometría descrita por un conjunto de coordenadas. Habitualmente los datos proporcionados están en formato GML, pero cualquier otro formato vectorial puede ser válido. Un WFS permite no solo visualizar la información tal y como permite un WMS, sino también consultarla libremente. Una especificación Open Geospatial Consortium establece cómo debe ser un WFS estándar e interoperable.

- Servicio de Coberturas en Web (WCS)

Es el servicio análogo a un WFS para datos ráster. Permite no solo visualizar información ráster, como ofrece un WMS, sino además consultar el valor del atributos o atributos almacenados en cada píxel. Una especificación Open Geospatial Consortium establece cómo debe ser un WCS estándar e interoperable.

- Servicio de Nomenclátor (Gazetteer)

Ofrece la posibilidad de localizar un fenómeno geográfico de un determinado nombre. Se define como un servicio que admite como entrada el nombre de un fenómeno, con las posibilidades habituales de nombre exacto, comenzando por, nombre incluido,...y devuelve la localización, mediante unas coordenadas, del fenómeno en cuestión. Adicionalmente, la consulta por nombre permite fijar otros criterios como la extensión espacial en que se desea buscar o el tipo de

fenómeno dentro de una lista disponible (río, montaña, población,...). Si hay varios que cumplen la condición de búsqueda, el servicio presenta una lista de los nombres encontrados con algún atributo adicional para que el usuario pueda elegir el que desea. Evidentemente este servicio necesita disponer de un conjunto de nombres con coordenadas. Una especificación Open Geospatial Consortium establece cómo debe ser un Servicio de Nomenclátor estándar e interoperable.

- Servicio de Geoparser

Un Servicio de Geoparser analiza palabra por palabra un texto digital dado, efectúa comparaciones con un conjunto de nombres geográficos dado y crea los vínculos o enlaces necesarios para que exista una referencia permanente en el texto original a los fenómenos geográficos aludidos. Transforma el texto original en un hipertexto con vínculos geográficos. Este servicio se basa y utiliza un Servicio de Nomenclátor.

- Servicio de Catálogo (CSW)

Un Servicio de Catálogo permite la publicación y búsqueda de información (metadatos) que describe datos, servicios, aplicaciones y en general todo tipo de recursos. Los servicios de catálogo son necesarios para proporcionar capacidades de búsqueda e invocación sobre los recursos registrados dentro de una IDEs. Una especificación Open Geospatial Consortium establece cómo debe ser un Servicio de Catálogo estándar e interoperable.

- Descriptor de Estilo de Capas (SLD)

Esta especificación de la OGC describe un conjunto de reglas de codificación que permite al usuario definir estilos de simbolización de las entidades personalizados. Es recomendable leer esta recomendación junto con la última versión de la especificación WMS.

Los servicios OGC pueden ser encadenados y combinados en un Geoportal, ofreciendo por ejemplo la posibilidad de: buscar un fenómeno por nombre (Nomenclátor) y visualizar el resultado sobre unos datos de referencia (WMS); localizar un producto seleccionando algunas características (Catálogo) y visualizarlo en pantalla (WMS o WCS). También es posible basarse en un servicio OGC para implementar servicios que ofrezcan funcionalidad adicional, por ejemplo desarrollar un servicio de camino mínimo por carretera basado en un WFS que acceda a todos los atributos de un conjunto de datos de poblaciones y carreteras.

26.7 BIBLIOGRAFÍA

- <http://www.idee.es/>
- <http://www.ucgis.org/>
- <http://www.arcgis.com/home/>
- <http://gos2.geodata.gov/wps/portal/gos>
- <http://www.opengeospatial.org/>
- Información geográfica y sistemas de información geográfica. Juan A. Cebrián de Miguel
- Sistemas de información geográfica. [Joaquín Bosque Sendrá](#)
- Sistemas de Información Geográfica Aplicados a la Gestión del Territorio. Juan Peña Llopis

Autor: Francisco Javier Rodríguez Martínez

Subdirector de Sistemas Escola Superior Enxeñaría Informática Ourense

Colegiado del CPEIG

27. ARQUITECTURA DE LAS REDES INTRANET E INTERNET: CONCEPTO, ESTRUCTURA Y CARACTERÍSTICAS. SU IMPLANTACIÓN EN LAS ORGANIZACIONES.

TEMA 27. ARQUITECTURA DE LAS REDES INTRANET E INTERNET: CONCEPTO, ESTRUCTURA Y CARACTERÍSTICAS. SU IMPLANTACIÓN EN LAS ORGANIZACIONES.

27.1. INTRODUCCIÓN Y CONCEPTOS

27.2. INTERNET

27.3. INTRANET/EXTRANET

27.4. IMPLANTACIÓN DE REDES EN ORGANIZACIONES

27.5. ESQUEMA

27.6. REFERENCIAS

27.1. INTRODUCCIÓN Y CONCEPTOS

Una red son dos o más nodos comunicados entre sí. A partir de ahí, la red puede aumentarse en cualquier número de nodos y conectarse a otras redes. **Internet** es una red de alcance mundial que conecta las diferentes redes físicas de una manera descentralizada, como una red lógica única.

En el mundo de la informática un nodo puede ser cualquier componente de una red, desde dispositivos de interconexión a equipos o estaciones de trabajo a cualquier otro tipo de cliente, como equipos portátiles y dispositivos móviles.

Por debajo de estas redes, además, tendremos diferentes tipos de redes físicas que tomarán diferentes medios y tecnologías. Internet proporcionará un mecanismo de comunicación común basado en la familia de protocolos TCP/IP, de manera que cualquiera de estas redes que implante o acepte esta familia de protocolos podrá comunicarse con las demás.

De entre todos los servicios que proporcionar Internet, el buque insignia es el World Wide Web (WWW, o *la Web*) el conjunto de protocolos que permite la consulta de archivos de hipertexto o páginas web emplazados en

diferentes sitios de alojamiento o sitios web.

Una **Intranet** es una red interna a una organización o institución, que tiene por objeto proporcionar un conjunto de servicios accesibles exclusivamente desde la red local o desde un conjunto de redes aisladas del exterior a través de Internet.

La idea principal de una Intranet es que sus servicios sean solo accesibles por parte de los usuarios de la organización o institución de una forma personal. Estos servicios pueden incluir servidores web, servidores de correo electrónico, sistemas de gestión de archivos, contenidos y utilidades de comunicación o mensajería.

Extendiendo este concepto a Internet, cuando los servicios están disponibles hacia fuera, pero solo para los usuarios de la organización o institución, se estará hablando de una **Extranet**. En el caso de la Extranet se establece un mecanismo de seguridad o autenticación de los usuarios para garantizar que pertenecen a la organización o institución. En consecuencia una Extranet no será ni una Intranet ni un sitio de Internet, sino la publicación de los servicios de una Intranet a través de Internet mediante un sistema de autenticación de los usuarios de la organización o institución.

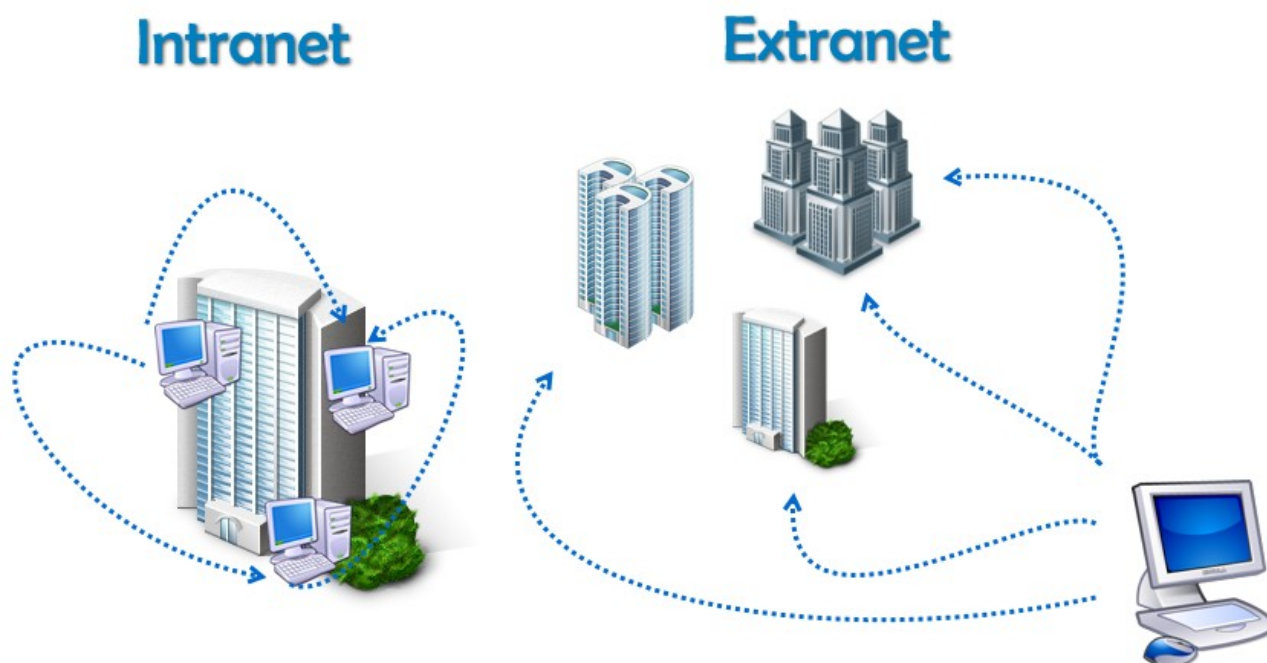


Figura 1: Intranet y Extranet

27.2. INTERNET

27.2.1. CARACTERÍSTICAS BÁSICAS

Internet tiene sus orígenes a finales de la década de los 60 y fue una evolución de la red experimental ARPANET (Red de la Agencia de proyectos de investigación avanzada), desarrollada por el departamento de Defensa de los EE.UU.

La idea original era disponer de una red en la que, en caso de que se

produjesen daños o la desaparición de algún nodo o punto de la misma, la red permaneciese activa entre los nodos o elementos restantes, garantizando así la supervivencia de la información y el funcionamiento del medio de comunicación. A partir de este concepto puede entenderse el funcionamiento distribuido y completamente descentralizado que posee el sistema actualmente, de suerte que cada nodo individual tiene la misma importancia y peso en el conjunto a la hora de dar servicio o comunicarse con los demás.

Posteriormente se desarrolló sobre la red un software básico de control de la transmisión de información que terminaría por dar lugar a la **familia de protocolos TCP/IP**. Esta familia de protocolos representa un conjunto de normas y estándares que definen el mecanismo de comunicación entre los diferentes nodos de la red. Cualquier red física que implante o dé soporte a este conjunto de protocolos podrá comunicarse con otras redes que también lo hagan. A partir de uno de estos protocolos podemos especificar otro de los factores fundamentales que explican el funcionamiento de esta red o concepto de Dirección **IP** (Protocolo de Internet). Esta dirección representa la dirección o nombre de cada nodo de la red, siendo un identificador único para cada uno de ellos. Las direcciones IP se componen de cuatro cifras numéricas separadas por puntos que toman valores entre 0 y 255. Como por ejemplo: 192.168.1.1. Con el fin de aumentar el rango de direcciones se diseñó el **IPv6** que pasa a valores de 128 bits, con ocho grupos de cuatro dígitos hexadecimales, como por ejemplo: FEDC:BA98:7654:3210:FEDC:BA98:7654:3210.

Enderezo IP	Significado
::	Ausencia de dirección
0:0:0:0:0:0:0:0	Ausencia de dirección
0	
::1	Loopback

::1.2.3.4	Compatible con IPv4
::ffff:0:0	Dirección Ipv4 mapeada
Ff00::	Multicast
FF01:0:0:0:0:0: :0:101	Multicast

Tabla 1: Ejemplos de direcciones Ipv6.

Como este tipo de identificación puede resultar difícil de recordar, se emplea en conjunción el Sistema de Nombres de Dominio (**DNS**). En este sistema diferentes nodos de la red hacen las funciones de traductores entre direcciones IP y nombres de Dominio, siendo éstos varias palabras separadas por puntos, como por ejemplo www.xunta.es. Esto indica, en última instancia, la zona o tipo de organización a la que pertenece el sitio, en este caso España, con el acrónimo “es”, a continuación la organización, institución o mnemotécnico, en este caso “xunta”, y por último el usuario o protocolo, en este caso “www”.

Por último otro concepto fundamental es lo de **clientes y servidores**. El objetivo de la red será doble comunicar y dar servicios. En este caso podemos distinguir tres tipos de nodos:

1. **Servidores**. Proveen de servicios a la red, tales como contenidos web, correo electrónico, vídeo, gestión de las comunicaciones, seguridad, etc...
2. **Clientes**. Nodos que representan el equipo de trabajo de un usuario final, el cual hace uso de uno de los servicios de la red que le proporciona un servidor.
3. **Elementos de interconexión**. Son nodos específicos de comunicación. Se encargan de gestionar las comunicaciones, retransmitir y dirigir los mensajes.

El modelo de Internet puede aplicarse sobre redes más pequeñas, de

menos equipos y una extensión menor. La idea de Internet es una red global, con servicios y comunicación a escala mundial. Abstrayendo funcionamiento y protocolos, pueden hacerse redes más pequeñas con un servicio reducido a su ámbito. A partir de ahí tenemos la clasificación habitual de las redes, que incluye:

1. **Redes de área local.** (En inglés *Local Area Network* o LAN). Interconexión de varios ordenadores y elementos de interconexión limitada físicamente a un edificio o entorno de alrededor de 200 metros – 1 Kilómetro. Ejemplos de estas redes serían las redes corporativas o institucionales dentro de un mismo edificio, como puede ser la red interna de una Consellería y, por norma general, incluyen además servicios de Intranet.
2. **Redes de área metropolitana.** (En inglés *Metropolitan Area Network* o MAN). Interconexión de varios ordenadores y elementos de interconexión en un área extensa, como puede ser una ciudad, provincia o comunidad autónoma. Ejemplo de este tipo de redes sería la red corporativa de la Xunta de Galicia. Por norma general este tipo de redes incorporan servicios de Intranet/Extranet.
3. **Redes de área amplia.** (En inglés *Wide Area Network* o WAN). Interconexión de varios ordenadores y elementos de interconexión en distancias de 100-1000 Kilómetros. Ejemplo de este tipo de redes sería la propia red Internet.

En la siguiente figura, podemos ver un ejemplo de red de área local, con algunos elementos básicos. Diferentes equipos de trabajo, conectados por nodos de interconexión y con algún servicio como el proporcionado por el servidor web. Esta pequeña red puede encontrarse integrada en una red de mayor alcance, con servicios de Intranet y como medio de comunicación con el resto del mundo a través de Internet.

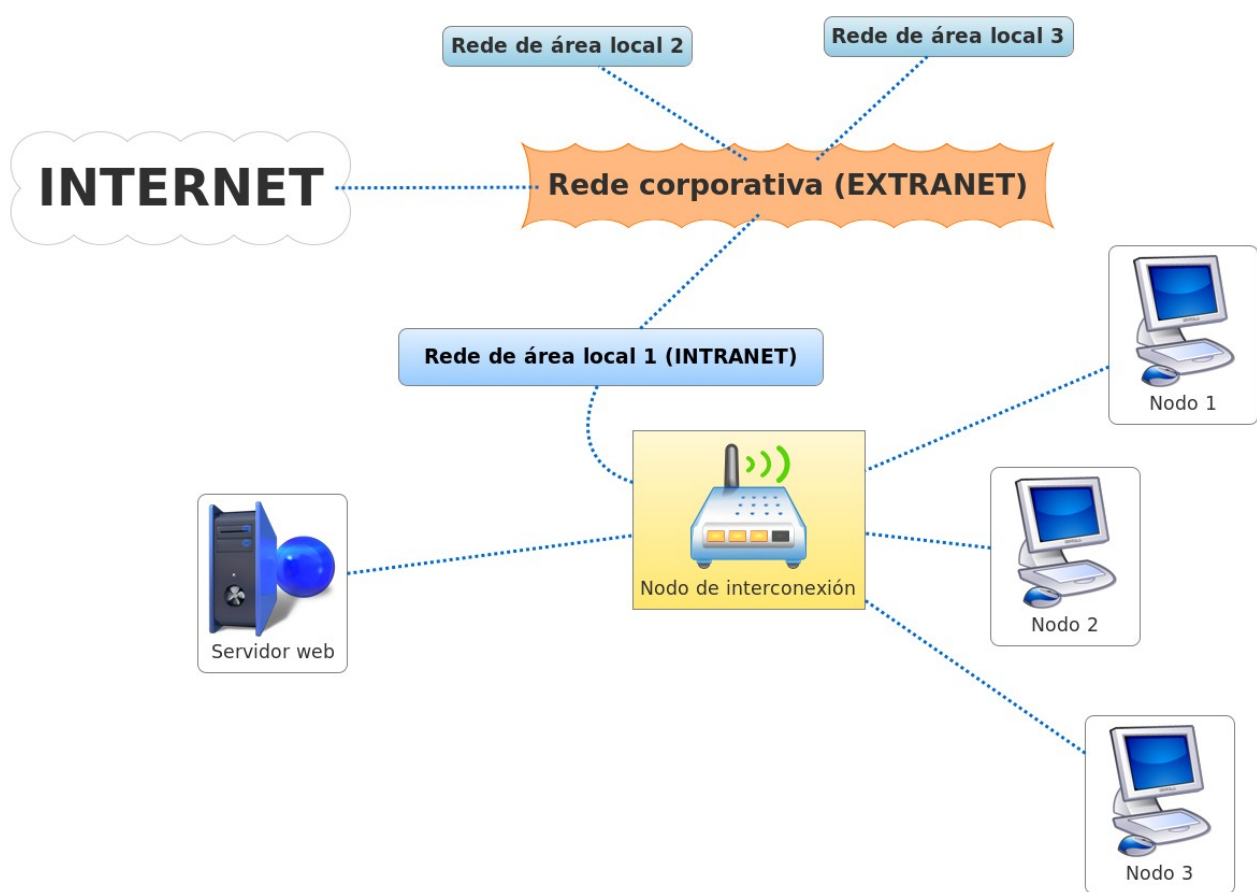


Figura 2: Ejemplo de red de área local conectada a una red corporativa y a Internet.

LEYENDA: Red Corporativa (EXTRANET), Red de área local 1, Red de área local 2, Red de área local 3, etc..

27.2.2. TIPOS DE CONEXIÓN A INTERNET

Para conectar otra red o equipo cliente, ya sea un ordenador de sobremesa, portátil, teléfono móvil, PDA, etc..., a la red Internet el primer paso será disponer de un **proveedor de acceso, o ISP** (en inglés *Internet Service Provider*, proveedor de servicios de Internet). Se trata de empresas que proporcionan y gestionan la conexión a la red de sus clientes, empleando diferentes tecnologías. Por norma general, los ISP proporcionan un hardware de conexión a la red específico y, quizás un software para gestionarlo.

Entre las tecnologías de conexión más empleadas hoy en día disponemos de:

1. **RTC.** La red telefónica conmutada, que emplea la misma red que los teléfonos fijos en Galicia. En este caso se trata de un soporte

analógico, por lo que para enviar datos digitales habrá que convertirlos empleando un dispositivo denominado **Módem** (modulador – demodulador), o variantes más avanzadas con mayores características como la enrutación, al estilo de los **Módem-Routers**. De este modo, un usuario que quiera acceder a Internet precisará disponer de una línea telefónica y un Módem o Módem-Router. Estos dispositivos pueden ser internos, como sucede normalmente en los dispositivos portátiles o externos. En este último caso, la conexión con el equipo de trabajo se realizará conectando el dispositivo por un cable/puerto (Por ej. USB) o con conectividad sin hilos. Actualmente esta tecnología se encuentra en un estado prácticamente obsoleto, debido a que no puede transmitir datos y voz a la vez, y a que su velocidad máxima es muy baja (alrededor de 56 Kbps).

2. **ADSL**. La línea de abonado digital asimétrica convierte la línea telefónica en una línea de alta velocidad, debido a que aprovecha toda la potencia de los hilos, estableciendo tres canales independientes:

- a) Canal de alta velocidad para transmitir datos.
- b) Canal de alta velocidad para recibir datos.
- c) Canal de alta velocidad para voz.

De este modo se permite que a través de la misma línea se envíen datos y voz a la vez. El concepto “asimétrica” viene dado porque las velocidades de subida y bajada de datos son diferentes, siendo más altas las velocidades de bajada, al interpretar que las necesidades de los usuarios van en este sentido. Los elementos de hardware empleados en este caso serán Módem-Routers proporcionados por un ISP. Las velocidades de descarga conseguidas son muy superiores al RTC, yendo de 512 Kbps a un máximo teórico para VSL (una evolución de la ADSL de muy alta tasa de transferencia) de 55 Mbps, si bien los proveedores en Galicia proporcionan bastante menos.

3. **Sin hilos.** Aunque en origen las redes sin hilos fueron diseñadas para redes de área local, actualmente también se emplean para posibilitar accesos a Internet. Basados en el conjunto de estándares Wi-Fi (en inglés *Wireless Fidelity*) llegan a conseguir velocidades de alrededor de 54 Mbps, alcanzando un máximo teórico de 600Mbps. El hardware necesario en este caso será un Router Wi-Fi sin hilos que haga las funciones de punto de acceso (en inglés *hotspot*) y en el equipo de trabajo una antena receptora integrada en una tarjeta de red (interna o externa).
4. **Cable.** Redes basadas en tecnologías de fibra óptica. lo que implica que necesita una línea de transmisión de esta tecnología. El hardware empleado es similar al de la ADSL, pero en este caso será un Cable-Módem el encargado de gestionar la comunicación, aunque el término Cable-Router sería más idóneo en este caso, pues la gestión es más avanzada que en el caso del Módem. Las velocidades son muy elevadas, esta tecnología también resulta muy cara en contrapartida, llegando a 10 Gbps de máximo teórico con 1 Gbps habituales. De cara al usuario y en Galicia, el ancho de banda es mucho menor, los proveedores más habituales suelen proporcionar velocidades similares a las de la ADSL.
5. **Satélite.** La conexión vía satélite se emplea en ubicaciones con poca infraestructura donde no es posible aplicar las tecnologías anteriores, como ADSL o Cable. En Galicia se recurre a este tipo de tecnologías en zonas del entorno rural o zonas de alta montaña. Esta tecnología tiene un coste muy alto, pero presenta una amplia cobertura. El hardware necesario requiere la instalación de una antena parabólica y en la oferta habitual de los ISP proporcionan 2 Mbps de subida y bajada.

6. **Módem Móvil.** Las últimas tecnologías desarrolladas para teléfonos móviles como GSM, GPRS o UTMS/3G permiten que los operadores ofrezcan a los usuarios servicios de Internet, bien directamente desde **el dispositivo móvil** o bien conectando otro equipo de trabajo a la red a través del mismo. Emplean un protocolo específico denominado WAP (en inglés *Wireless Application Protocol*) y las velocidades de conexión varían, dependiendo de la tecnología, desde 56 Kbps hasta 2 Mbps con las tecnologías de última generación. El hardware básico es un teléfono móvil que soporte estas tecnologías, pudiendo precisar algún elemento de conexión extra para conectarlo con otros equipos de trabajo.
7. **PLC.** (Del inglés *Power Line Communication*) Esta tecnología ofrece conexión a Internet a través de la red eléctrica. Como la ADSL, esta tecnología aprovecha una infraestructura de cableado ya existente para ampliar los canales, empleando medias y altas frecuencias. Requiere hardware específico: los denominados **Módem PLC**. Consigue velocidades de hasta 134 Mbps, y a pesar de que el ancho de banda es incluso superior al de la ADSL y la infraestructura de cableado eléctrico puede ser incluso superior que el telefónico, en Galicia el uso de esta tecnología está muy poco extendido.

27.2.3. SERVICIOS DE INTERNET

El fin último de acceder a Internet o a otra red es hacer uso de los **servicios** que se encuentran en ella, y que veremos a continuación:

1. WWW

En el caso de Internet, el servicio más empleado es la Red global mundial o

WWW (siglas en inglés de *World Wide Web*), se trata de un sistema de publicación e intercambio de información distribuido que relaciona unos contenidos con otros a través de enlaces. Este sistema se extendió rápidamente gracias a su facilidad de uso.

En este contexto surge el **Hipervínculo**, que viene siendo un texto u otro objeto que contiene un enlace; picando el mismo se accede a otra información situada en otra zona del documento o en otro documento distinto. Esta funcionalidad permite relacionar unos documentos con otros o, lo que es lo mismo, unos nodos con otros formando una red denominada “tela de araña” (en inglés *web*), de ahí que cada documento pasase a denominarse “página web”. Cuando se trata de texto, los enlaces suelen aparecer resaltados en color azul y subrayados, e incluso puede cambiar el estilo del puntero del ratón para que no pasen desapercibidos.

Los documentos denominados páginas web, son documentos en lenguajes estándar como HTML o XML que pueden incluir diferentes tipos de información: texto, hipervínculos, gráficos y otros elementos multimedia. Estas páginas web se alojan en servidores web distribuidos por todo el mundo, en lo que se conoce como “**sitios web**”. Cuando el servidor se encuentra conectado a la red, la conjunción de direcciones IP y nombres de dominio permitirá acceder a los documentos del sitio y visualizarlos mediante unos programas denominados **navegadores** de Internet. Este tipo de programas implantan el protocolo http, que funciona sobre la familia de protocolos TCP/IP, encargándose de gestionar la comunicación entre el cliente y el servidor web. Para acceder a la dirección de una página web podemos hacerlo tanto mediante enlaces como directamente desde la barra de direcciones del navegador sin más que insertar directamente en ella el nombre o dirección web del sitio.

Las direcciones web sirven para identificar los recursos de la red y se

denominan **URL** (en inglés *Uniform Resource Locator*) o localizador uniforme de recurso. Las URL pueden ser de la forma: <https://www.xunta.es:80/ruta/index.htm>, teniendo los siguientes componentes:

- a) El protocolo de la red que se emplea para recuperar la información del recurso especificado, en este caso “https”, siendo uno de los más habituales junto a “http”, “ftp”, “mailto”, “file”, o “ldap”. Normalmente el protocolo HTTP es opcional en la mayoría de los navegadores ya que se trata del protocolo más utilizado.
- b) El nombre de dominio, o servidor con el que se comunica, en este caso “www.xunta.es”.
- c) El puerto de comunicación que emplea ese protocolo en el servidor, en este caso “:80”, siendo este opcional pues los protocolos suelen llevar un puerto asociado por defecto.
- d) La ruta del recurso en el servidor, (en inglés *path*), en este caso “/ruta”.
- e) El nombre del archivo alojado en esa ruta o directorio, en este caso “*index.htm*”.
- f) Otros campos como parámetros o propiedad propias de determinados protocolos.

2. Correo electrónico

El servicio de correo **electrónico** (e-Correo) proporciona los mecanismos para facilitar el envío y recepción de mensajes que pueden incluir texto y otras aportaciones a modo de archivos multimedia. En este servicio se identifica cada usuario con una cuenta que llevará su nombre de usuario para el dominio de ese servidor de correo seguido del símbolo “@” (arroba) y el nombre de dominio (DNS) de ese servidor. Como por ejemplo: usuario@xunta.es. El acceso al correo electrónico puede hacerse con dos sistemas diferentes, o bien accediendo con un correo web o bien con un

cliente de correo electrónico. En el **correo web** (en inglés *webmail*) se accede desde un navegador a una página de administración del correo, que requiere la autenticación del usuario y permite hacer las operaciones como en cualquier otro sitio web. En este caso es idéntico a cualquier otro servicio www, es decir emplea los protocolos HTTP o HTTPS según el nivel de seguridad del servidor. No requiere software adicional y cualquier equipo que haya instalado un navegador permitirá acceder a un servidor de correo remoto.

La alternativa es emplear software a modo de clientes de correo electrónico específicos que permiten conectar un software de gestión de correo con el servidor a través de los protocolos de correo **POP3** o **IMAP**. Estos dos protocolos permiten obtener y enviar mensajes de correo desde y hacia un servidor remoto. La diferencia entre ambos protocolos es que POP3 se encuentra más orientado hacia la recepción de correo que para el envío, con lo cual, al conectarse descarga todos los mensajes al equipo cliente y los elimina del servidor, mientras que el protocolo IMAP los mantiene. En líneas generales, IMAP proporciona más funcionalidades que POP3, siendo un poco más complejo, por lo que no se encuentra instalado en todos los servidores de correo. Para especificar cómo deben encaminarse los correos, se emplean los **Registros MX** (en inglés *Mail Exchange Record*), recursos DNS que indican los servidores de correo por prioridad. El MTA (en inglés *Mail Transfer Agent*) solicita el Registro MX ante una petición DNS encaminando posteriormente el envío. Existen muchos riesgos de seguridad asociados a los correos, además de la posibilidad de envío de virus, Hoax o troyanos, algunos servidores permiten el envío abierto u Open Relay.

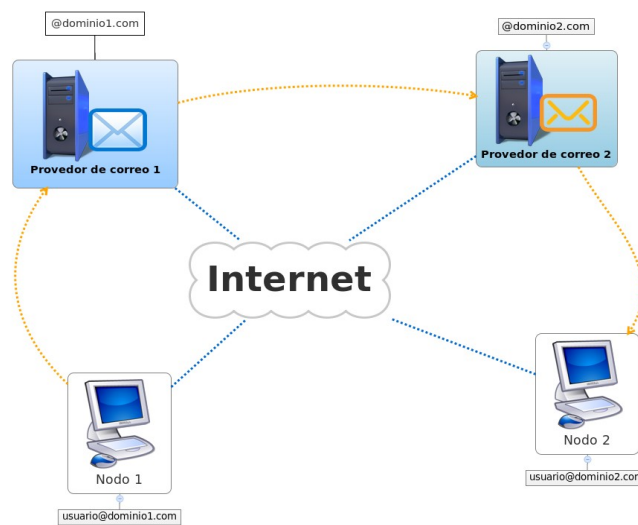


Figura 3: Funcionamiento del correo electrónico.

LEYENDA: Proveedor de correo 1, Proveedor de correo 2...

3. Transferencia de archivos (FTP)

El servicio de transferencia de archivos o FTP (en inglés *File Transfer Protocol*) es un protocolo que define los estándares para el servicio de transferencia de archivos a través de Internet. Se trata de un sistema cliente-servidor al estilo de los anteriormente comentados, donde un equipo cliente se puede conectar con un servidor de archivos remoto para descargar o enviar uno o más ficheros, independientemente del sistema

operativo del equipo cliente. Como sucedía con el correo electrónico, puede gestionarse desde un navegador empleando el servicio *www*, o bien con un cliente FTP que haga transparentes y usables las diferentes funcionalidades del servicio. Una cuenta de usuario especial es la que tiene como usuario y contraseña “anonymous”, que se emplea para acceder a servidores FTP anónimos o públicos, se trata de un estándar de facto para permitir acceder a cualquier persona a los contenidos de un directorio público de un servidor FTP. Ampliaciones de este protocolo en el campo de la seguridad dan lugar a la evolución a SCP (en inglés *Secure Copy*) y SFTP (en inglés *SSH File Transfer Protocol*) ambos añaden la seguridad **SSH** (en inglés *Secure Shell*), en el primero limitado a transferencia de archivos y en el segundo con más opciones.

4. Conexión o acceso remoto (Telnet)

Este servicio permite el acceso remoto a otro equipo a través de la red y trabajar con ella desde nuestro equipo a través de una consola como si estuviésemos conectados directamente la ella, como un usuario de esa máquina. **Telnet** es el protocolo de red que permite realizar este tipo de comunicaciones, que precisan que en el servidor remoto esté activado el servicio de Telnet para aceptar las comunicaciones. Necesita una cuenta de usuario y contraseña para el servidor de Telnet, que en muchos casos puede coincidir con un usuario del equipo remoto. Los problemas de seguridad de las versiones iniciales del Telnet se arreglaron con su evolución a SSH, una nueva versión del sistema con técnicas de cifrado y con nuevas funcionalidades. Como ocurría con el Telnet, SSH es tanto el nombre del protocolo como lo del programa que el implanta, y como sucedía con el FTP y con el correo electrónico existe software de gestión que facilita al usuario a conexión vía Telnet o SSH. La posibilidad de estar en un ordenador mientras se trabaja en otro resulta muy útil para tareas

administrativas, sobre todo para los administradores de red o para situaciones de teletrabajo.

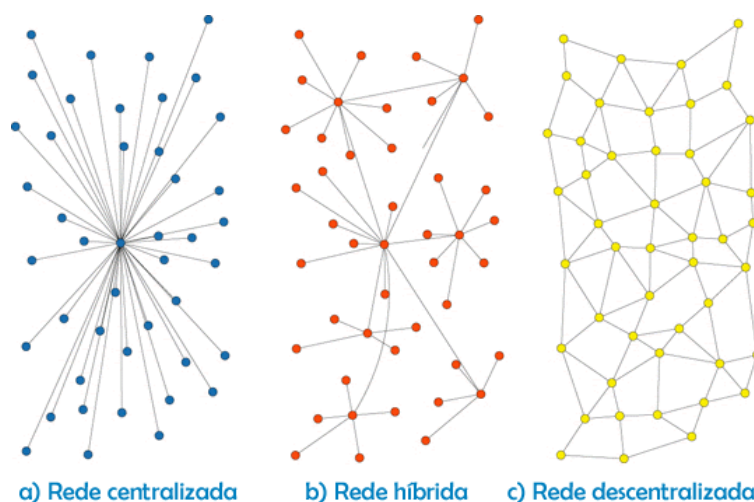
Un paso más allá, los **terminales en modo gráfico** permiten, además de texto, mostrar imágenes, con lo cual accederíamos desde nuestro equipo a un escritorio idéntico a cómo lo veríamos si nos encontrásemos físicamente en el equipo remoto. Los clientes de este servicio emplean los protocolos RDP o X11, dependiendo del sistema operativo, para sistemas Windows y Unix/Linux respectivamente.

5. P2P

Los servicios P2P tienen su origen en el concepto de las “redes entre iguales” (en inglés *peer-to-peer*). La característica principal de este tipo de redes es que todos los nodos que participan en la red tienen el mismo peso en la misma, todos actúan como clientes y como servidores. Se trata de subredes dentro de Internet establecidas a partir de un determinado software de gestión para P2P. En un principio estas redes podían tener nodos centrales para gestionar las comunicaciones, si bien la base del intercambio de archivos seguía siendo distribuida. Cada nodo, equivalente a un usuario conectado a la red P2P, comparte sus recursos con todos los demás nodos, si bien la manera más habitual es compartir archivos que en ocasiones permiten realizar cálculos de coste elevado o procesamiento de datos masivos con orientación científica. Según dispongan de nodos centrales podemos hablar de los siguientes tipos de redes:

- a) Redes P2P centralizadas, en forma de estrella, con un servidor central que monopoliza la gestión y administración de la red.
- b) Redes P2P híbridas, donde además del nodo central existen nodos de segundo nivel que centralizan la gestión de subredes.

- c) Redes P2P descentralizadas, donde todos los nodos son clientes y servidores con el mismo peso.



Leyenda: a) Red centralizada b) Red Híbrida c) Red descentralizada

Figura 4: Topologías habituales de las redes P2P.

6. Conversación (Chat)

Este servicio permite que dos o más usuarios conectados simultáneamente a Internet mantengan conversaciones interactivas en tiempo real. El IRC (en inglés *Internet Relay Chat*) es el protocolo de comunicación basado en texto que sustenta el servicio. Las conversaciones tienen lugar en los denominados canales de IRC, de manera que cada canal puede sostener una conversación paralela entre dos o más nodos cualesquiera de la red. Existen múltiples clientes que, como ocurría con los servicios anteriores, facilitan el uso del servicio a los usuarios. En sus orígenes permitía solo el envío de mensajes de texto, pero han evolucionado hasta permitir el envío de archivos, transmisión de voz y vídeo, e incluso conexión de escritorio remota.

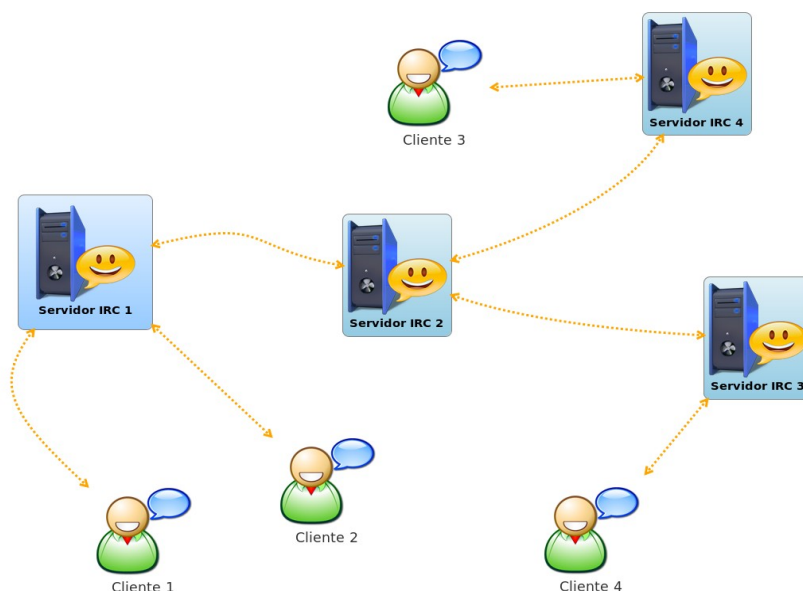


Figura 5: Ejemplo de una red IRC.

27.2.4. MOTORES DE BÚSQUEDA

Otra característica de Internet, fruto de la gran cantidad de información que almacena, sería la existencia de unas herramientas denominadas **Motores de búsqueda** (en inglés *browsers*). Estas herramientas buscan los archivos almacenados en los servidores web y los indexan para poder proporcionar resultados de búsquedas de palabras clave en los mismos en un tiempo óptimo. Los motores de búsqueda emplean un **robot** (o simplemente *bot*) que hace las funciones de rastreador de la web. Periódicamente este robot recoge información sobre los sitios y páginas web, que recorre desde un punto de partida hasta los enlaces de cada

documento que recorre. De este modo puede descubrir nuevos documentos en un sitio, siempre y cuando estén vinculados desde otros documentos ya encontrados del sitio. En determinadas ocasiones podemos no desear que el documento sea incorporado a los buscadores, por lo que pondremos antes el código HTML, para indicarle al robot que se salte ese documento. La información que recoge un robot incluye el texto y parte del código de la página web, no pudiendo interpretar imágenes, animaciones o vídeos n, si no es a través de su descripción. Para que un sitio web pase a existir hace falta darlo de alta en, al menos, uno de los buscadores; basta con incluir la página principal del sitio, siempre y cuando el resto de páginas estén ligadas desde ella.

A partir de la información recogida por el robot se elabora un **índice** o catálogo de documentos orientado a facilitar la búsqueda de información. Con cada nueva búsqueda, la información de rastreo deberá actualizarse y, por consiguiente, también el índice o catálogo, incorporando las nuevas páginas descubiertas, eliminando las que fueron borradas, así como los cambios de cada documento.

De cara al usuario, el motor de búsqueda proporcionará una **interface de búsqueda** vía web o cliente software, donde a partir de un término insertado le dará cómo resultado los enlaces encontrados que mejor se correspondan por orden de importancia. Los factores llave del resultado de un buscador serán, por tanto, el tiempo de respuesta, optimizado gracias al índice, y la importancia o adaptación de los resultados a los términos empleados en la búsqueda.

Por norma general, los buscadores implantan sus propios algoritmos de importancia o posicionamiento, que establecen un peso para cada página en función del número de visitas, número de páginas que la enlazan, aspectos comerciales, valoración de los usuarios y un largo etcétera. En el

resultado de una búsqueda aparecerán primero las páginas que tengan un mayor posicionamiento o importancia.

27.3. INTRANET/EXTRANET

En líneas generales, una Intranet se comporta igual que Internet, siendo una Internet limitada al ámbito de la organización para la que da servicio, es decir una Internet personal. Una Intranet sería una Internet que restringe el acceso a los sistemas de información. A efectos de alcance y servicios, podremos disponer de las mismas posibilidades en cada tipo de red. En lo que concierne a su funcionamiento, también es idéntica al de Internet: cada equipo o nodo también dispondrá de una dirección IP, pero en este caso no se corresponderá con las direcciones IP de Internet sino que será una dirección IP personal, para uso interno. Si parte de los equipos se encuentran abiertos a Internet pasaremos a hablar de Extranet, pudiendo convivir ambas en la misma organización.

En otra variante, una Extranet puede comunicar dos Intranets con distinta localización geográfica, estableciendo, por ejemplo, una Red personal virtual o VPN (en inglés *Virtual Private Network*) que define una red personal lógica sobre una red pública. Existen varias arquitecturas de VPN:

- 1) **VPN de acceso remoto.** Conecta directamente los usuarios a red a través de Internet, teniendo en cuenta solo que el usuario se autentica de manera correcta.
- 2) **VPN punto a punto (Tunneling).** Requiere un servidor VPN que responde a las conexiones a través de Internet y crea un túnel VPN, que consiste en enmascarar un protocolo de red sobre otro. De este modo se pueden transmitir los paquetes con protocolos cifrados como SSH.

- 3) **VPN LAN.** En esta solución no se emplea Internet para el acceso remoto, sino que se hace sobre la propia red de la organización. En redes sin hilos, permite establecer un nivel de seguridad añadido donde, además de los protocolos de seguridad de la Wi-Fi, se incluyen las credenciales de seguridad del túnel VPN.

Particularizando y concretando los servicios que ofrece Internet, podemos definir una serie de servicios básicos que puede proporcionar una Intranet/Extranet:

a) Acceso a sistemas de información

- ✓ Acceso a documentación: manuales, publicaciones, guías y formularios internos.
- ✓ Acceso a sistemas de información y bases de datos corporativas.
- ✓ Consulta y edición de informes, formularios y listas.
- ✓ Agenda, calendarios y planificaciones de trabajo en grupo.
- ✓ Acceso a información de contacto de la organización.
- ✓ Páginas de noticias y enlaces de interés.

b) Recursos compartidos

- ✓ Acceso a recursos compartidos: conexión a Internet, impresoras, escáneres, etc...
- ✓ Acceso a sistemas de intercambio de archivos.
- ✓ Buscadores de recursos e información.

c) Flujos de trabajo

- ✓ Gestión de usuarios y perfiles.
- ✓ Acceso a aplicaciones/equipos remotos.
- ✓ Acceso a repositorios de versiones.
- ✓ Acceso a aplicaciones de gestión y control de incidencias.



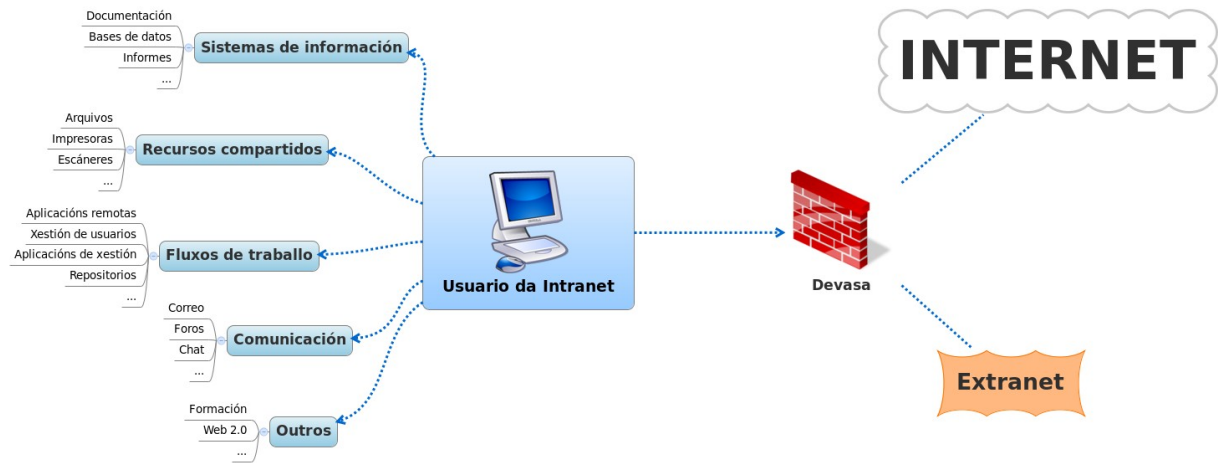
- ✓ Soporte a trabajadores móviles o tele-trabajadores.

d) Comunicación

- ✓ Servicios de mensajería interna, correo electrónico, foros y videoconferencia.

e) Otros

- ✓ Realización de actividades de formación.
- ✓ Acceso a herramientas de la Web 2.0: portales, blogs, wikis, redes sociales, etc...



LEYENDA: Archivos / Aplicaciones remotas, Gestión de usuarios, aplicaciones de gestión – FLUJOS DE TRABAJO / OTROS

USUARIO DE LA INTRANET

CORTAFUEGOS

Figura 6 : Servicios básicos de una Intranet/Extranet.

Para poder soportar esta larga lista de servicios, una Intranet debería estar dotada de los siguientes **componentes** básicos:

1. Soporte e infraestructura de red.

El modelo más sencillo de Intranet sería dos equipos de una organización conectados en red. A partir de ahí, la red puede crecer tanto como requiera la organización, pudiendo incluir cualquier número de redes, subredes, equipos y elementos de interconexión. La implantación de esto equivaldría

a la de una red LAN, siendo preciso definir una topología, un conjunto de tecnologías (Ethernet, Fibra óptica, Wi-Fi, etc...), dispositivos de interconexión y de seguridad y una política de asignación de direcciones IP y nombres de dominio DNS. En un paso más allá, habría que extender la red hacia el exterior en caso de que se quiera definir parte de la misma como Extranet, teniendo en cuenta también este conjunto de características. A este respecto hay que tener en consideración el Plan de Direccionamiento e Interconexión de Redes de Área Local en la Administración (2010), el cual establece los rangos de asignación de direcciones IP. Para la Xunta de Galicia establece el siguiente **rango**:

10.179.0.0 - 10.180.0.0	<i>Xunta de Galicia</i>
------------------------------------	-------------------------

Así como otras **recomendaciones**, tales como:

- ✓ Cada entidad u organismo puede gestionar independientemente sus planes de numeración IP pero siguiendo el plan para evitar direcciones duplicadas con los otros organismos.
- ✓ Emplear máscaras de red de 24 bits, para tener redes de 254 nodos por segmento, con lo cual tendríamos la máscara 255.255.255.0 independientemente de la situación física del nodo.
- ✓ La asignación del grupo de bits para *el Host* se realizará de manera ascendente para permitir subredes en las zonas aun no asignadas.
- ✓ Emplear valores de direcciones IP bajos para servidores y equipos de comunicaciones.
- ✓ Valores tirando por lo alto de los anteriores para equipos de usuarios, ordenadores personales y estaciones de trabajo.
- ✓ Seguir el plan de numeración en cada subred.
- ✓ Mantener al día a documentación de los cambios que se producen en el mismo.

2. Servidores.

Los servidores serán los proveedores de servicios en la Intranet/Extranet encontrándonos diferentes requisitos hardware y software según la función que van a desempeñar. Según su perfil dentro de la red encontramos dos tipos:

- a) **Servidores dedicados.** Invierten toda su potencia a dar servicio a la red, dedicando todos sus recursos a tal función.
- b) **Servidores no dedicados.** Funcionan tanto como servidor como estación de trabajo, repartiendo sus recursos en las dos funciones.

Por otra parte, atendiendo al tipo de servicio que proporcionan, podrían clasificarse de la siguiente manera:

- 1) **Servidores de archivos.** Almacenan archivos y directorios y gestionan el acceso a los mismos por parte de los usuarios de la Intranet. En sistemas avanzados proporcionan información de versiones, permisos y servicios de transferencia, sincronización, replicación y soporte de protocolos SMB/NetBIOS, CIFS, NFS y FTP así como funcionalidades de integración del estilo de Samba.
- 2) **Servidores de impresión.** Controlan las impresoras, fax o escáneres en red, realizando tareas de gestión de colas, asignación de prioridades y detección de errores, con soporte para protocolos IPX/SPX, LDP, IIP, CUPS o vía Socket.
- 3) **Servidores de comunicaciones.** Realizan la gestión de las comunicaciones de telefonía, voz sobre IP (VoIP) o videoconferencia. Sistemas avanzados que incluyen contestadores automáticos y sistemas de respuesta robótica paralela automática. Deben soportar diferentes protocolos como TCP/IP, IPX, PPP, SLIP/CSLIP, SNMP, LAT o NetBEUI.



- 4) **Servidores de correo.** Almacenamiento y gestión de mensajes exclusivo para usuarios de la Intranet/Extranet, con soporte para SMTP, IMAP, POP3 y seguridad SSL/TLS.
- 5) **Servidores de mensajería instantánea.** Gestionan las comunicaciones de Chat o conversación instantánea entre los usuarios de la Intranet/Extranet con soporte IRC, MUC, SIMPLE, MNP o XMPP.
- 6) **Servidores de red.** Realizan funciones de interconexión de las redes y subredes que forman la Intranet/Extranet. Gestiones de cachés (en inglés *proxy*), enrutado, servicios de cortafuego (en inglés *firewall*), NAT, DHCP, etc...
- 7) **Servidores de acceso remoto.** Gestionan la conexión remota de equipos desde otras localizaciones con protocolos XDMCP, NX, RFB o RDP. Optimizan la elevada carga del uso de aplicaciones y escritorios de manera remota e incorporan mecanismos de autenticación avanzados.
- 8) **Servidores de aplicaciones.** Permite que los clientes trabajen con aplicaciones de coste de implantación/configuración elevado o con una alta demanda de recursos de manera remota. Las soluciones más habituales se basan en las plataformas JEE, .NET, PHP y Coldfusion.
- 9) **Servidores de copias de seguridad.** Permiten mantener un sistema de control de almacenamiento de copias de seguridad de datos o servidores en discos duros redundantes o cintas, en ocasiones en otras localizaciones pero dedicados o SAN. El objetivo de estos sistemas es restaurar el sistema a un estado funcional y seguro después de un error, caída o desastre que provoque la pérdida de la funcionalidad de la red, convirtiendo las redes locales en NAS. Actualmente, con el avance de las conexiones van ganando fuerza los *backups* en la nube.
- 10) **Servidores de Bases de datos.** Proveen los servicios de acceso a las Bases de datos así como la gestión de las mismas desde



ordenadores con más recursos que las estaciones de trabajo. Resulta habitual su comunicación con otros servidores para proporcionar servicios conjuntos. Algunos de los ejemplos más representativos son Oracle, DB2, SQL Server, MySQL y PostgreSQL.

- 11) **Servidores web.** Soportan el servicio de contenidos web a escala interna, controlando el acceso a las páginas y documentos HTML y XML. Los dos ejemplos más representativos son Apache e IIS.
- 12) **Otros.** Cualquier otro servicio de importancia para la Intranet/Extranet debería tener un servidor dedicado especializado que destinase todos sus recursos a la gestión y soporte de ese servicio. Algunos de estos servicios podrían ser el control y gestión de usuarios (Servidores LDAP), servidores de informes, control de versiones, etc...

3. Control de Seguridad

En todas las redes y sistemas de comunicación es importante dedicar recursos al control de la seguridad, principalmente en las partes visibles desde fuera, es decir las partes de la Extranet, pero tampoco hay que olvidar las partes propias de la Intranet. La mayor parte de la seguridad recae sobre los **cortafuegos**, que filtran las comunicaciones con el exterior, restringen aplicaciones y controlan las direcciones IP y físicas de las máquinas según una serie de reglas y filtros de control. Asimismo disponen de herramientas de monitorización y registro que permiten hacer seguimientos y auditorías de la red.

Por otra parte, se puede restringir la comunicación con el exterior empleando equipos de interconexión puente que den servicio al resto de la red. Estos dispositivos de **gestión de caché**, hacen la función de repetidores en la red, pero aíslan a los equipos internos y permiten

centralizar y reforzar la seguridad y el control en este equipo, en lugar de en toda la red. Los equipos pasarela deberían incluir todos los servicios básicos como Web, FTP o mensajería instantánea.

La seguridad debe contemplarse también en los **clientes**, aunque una correcta gestión en los servidores protege por extensión a los equipos de trabajo. Hace falta prestar especial atención al control de los usuarios de cada equipo, controlar accesos físicos, gestión de contraseñas, y dotarlos de un software antivirus idóneo. En ocasiones puede ser necesario controlar el acceso de los usuarios al mismo equipo, distinguiendo en diferentes perfiles usuario/administrador o más según las necesidades de la organización.

4. Administración de la red.

El papel de administrador de la red resulta fundamental para asegurar el correcto funcionamiento y seguridad del sistema, además de para dar soporte y participar de la resolución de incidencias.

Mención especial merece el control de las comunicaciones que se realizan entre los usuarios, teniendo especial cuidado con temas como correos masivos o SPAM, o envío masivo o no autorizado fuera de la organización. Entre las labores o funciones del administrador o administradores encontraríamos:

- ✓ Establecimiento y mantenimiento de políticas de gestión de usuarios y roles, permisos y accesos.
- ✓ Mantenimiento y soporte físico del hardware de la red.
- ✓ Configuración y mantenimiento de cortafuegos, antivirus y cachés, así como cualquier otro equipamiento o software de conexión de la red.
- ✓ Evaluación de la calidad del servicio.

- ✓ Realización de auditorías periódicas de control y evaluación de la seguridad y rendimiento.
- ✓ Atención a los usuarios, soporte y resolución de incidencias.
- ✓ Documentación del diseño y descripción de la red, configuraciones de servidores y protocolos de restauración/recuperación de la red en caso de error o desastre.

27.4. IMPLANTACIÓN DE REDES EN ORGANIZACIONES

Cuando las organizaciones conectan su red y servicios con Internet tienen varias alternativas:

1) Integrar por completo la red corporativa en Internet. De este modo cada equipo de la organización pasa a ser un nodo de Internet, con direcciones IP de Internet. Desde cualquiera localización se podrá tener acceso a los servicios y equipos de la red directamente, sin limitaciones. Esta solución presenta riesgos de seguridad, ya que el conjunto de la red queda expuesto a ataques desde el exterior, y cada nodo se convierte en un potencial punto débil.

2) Integrar parcialmente la red y equipos. En este tipo de soluciones a mayoría de la red aparece oculta al exterior, fuera de Internet, para evitar los riesgos de seguridad. Desde el exterior se pueden ver algunos servidores de la organización y del mismo modo desde la red se puede acceder a servidores externos, pero restringido los servicios y comunicaciones. Cuando la integración es parcial se puede hablar de redes de los tipos Intranet y Extranet. Partiendo de surgen otras muchas cuestiones, número de usuarios, distribuciones físicas que abarcará la red, servicios que se implantarán, y un largo etcétera. Resulta obvio que el primer paso de la implantación de una Intranet/Extranet será la planificación. En la planificación se abordarán los siguientes puntos:

1. Planteamiento de objetivos.

Los **objetivos** de la red quedará definidos por el su alcance. Habría que realizar tareas tales como:

- ✓ Estimación del número de usuarios y su posible evolución.
- ✓ Determinar la ubicación de la red y posibles subredes, situación de posibles redes externas y las necesidades de comunicación con las mismas.
- ✓ Considerar los sistemas de información y necesidades de acceso a los mismos, teniendo en cuenta también los flujos y procesos internos.
- ✓ Definir los servicios que se proporcionarán en la Intranet/Extranet al por menor, con estimaciones de carga predicciones de su evolución futura, etc...

A partir de los objetivos puede irse elaborando la lista de requisitos de la Intranet/Extranet, como paso previo al diseño de la red. La documentación en ambos puntos debería ser lo más completa posible.

2. Selección de tecnologías

En un segundo paso, tomando los objetivos y requisitos, habría que seleccionar las tecnologías más acomodadas tanto a nivel de hardware, físico, como de software. A escala física suele optarse por redes Ethernet, pero pueden precisarse redes sin hilos. Asimismo, cada red precisaría diferentes elementos de interconexión dependiendo de la tecnología, y lo mismo para clientes y servidores. Desde sistemas operativos a software de gestión y control de cada servicio, gestores de contenidos y otros propósitos, debería seleccionarse atendiendo a las necesidades especificadas por los objetivos y requisitos, sin olvidar otros aspectos como costes, la existencia y disponibilidad de soporte para cada tecnología y complejidad de instalación, configuración y mantenimiento.

3. Definición de los recursos necesarios.

Una vez seleccionadas las tecnologías que estarán presentes en el diseño de la selección habría que definir el número de recursos necesarios para la implantación. Esto incluye número, tipo y software de los equipos clientes, y lo mismo para los equipos de interconexión de la red y servidores. Este paso sería el **diseño** de la red en sí, desde el cableado a la lista completa de software necesario. Según las particularidades de la Intranet/Extranet podría ser preciso el desarrollo de software a medida, lo cual habría que incluir también en esta fase del diseño.

4. Definición de políticas de seguridad.

Paralelamente habrá que establecer y documentar los protocolos y políticas de seguridad como:

- ✓ La asignación de cuentas de usuario y contraseñas y usuarios de los equipos y servidores, así como caducidad y revisión del cambio de contraseñas en las mismas.
- ✓ Equipos que comunican con el exterior y que precisan más seguridad y equipos que pertenecerán a la DMZ (zona desmilitarizada).
- ✓ Filtros de aplicaciones, de direcciones IP y direcciones físicas.

A continuación vendría la implantación en sí, siendo el recomendable establecer un período de prueba y realimentación previo para ofrecer un producto de mayor calidad.

1. Período de prueba.

Durante este período se realizarán pruebas completas del funcionamiento de la Intranet/Extranet. Deberían incluirse casos de prueba para los diferentes servicios y las comunicaciones entre las diferentes subredes y

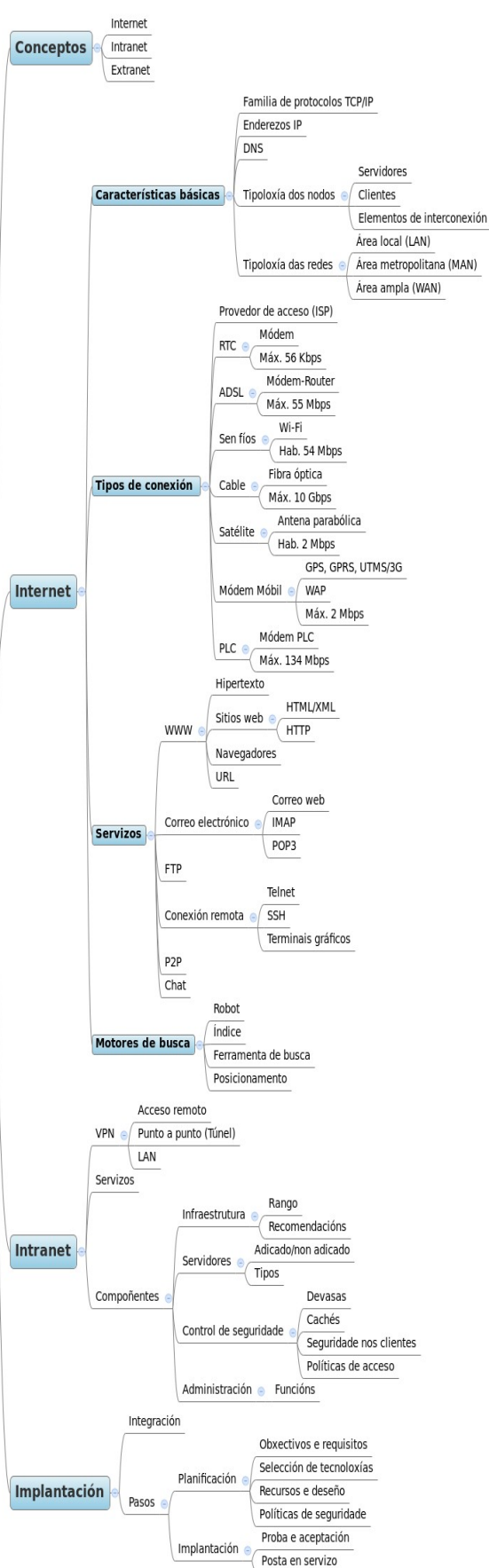
redes externas. Con la calidad como objetivo, habría que realizar pruebas más complejas cómo las de carga, buscando los picos de demanda de recursos, y casos de ataques de seguridad controlados. Todo ello mientras se realiza la monitorización y posteriores pruebas de auditoría del sistema permiten elaborar un informe completo de los límites y deficiencias de la red, útil para detectar puntos débiles que arreglar antes de la puesta en servicio.

2. Puesta en servicio.

Luego de las sucesivas pruebas y una vez obtenidos resultados de aceptación puede llevarse a cabo a puesta en servicio definitiva de la Intranet/Extranet, abriéndola a todos los usuarios. En los primeros momentos de la puesta en servicio hace falta realizar la monitorización y auditoría de los sistemas al igual que se hizo durante el período de prueba, pues en este primer momento podrán detectarse problemas y debilidades reales que pudieron pasar desapercibidas durante las pruebas controladas realizadas anteriormente.

27.5. ESQUEMA

Internet e Intranet



LEYENDA: Direcciones IP /Tipología de los nodos - Tipología de las redes / Área amplia / Proveedor de acceso / Inalámbrico / Servicios /Terminales gráficos / Componentes / Motores de

búsqueda / Infraestructura / Posicionamiento / Módem móvil / Recomendaciones / Dedicado - No dedicado / Control de seguridad / Cortafuegos / Seguridad en los clientes / Funciones / Objetivos y requisitos / Selección de tecnologías / Recursos y diseño / Políticas de seguridad / Prueba y aceptación / Puesta en servicio.

27.6. REFERENCIAS

Abel Rodríguez Ávila.

Iniciación a la red Internet. Concepto, funcionamiento, servicios y aplicaciones de Internet. (2007).

Irene Rodil e Camino Pardo.

Operaciones auxiliares con tecnologías de la información y la comunicación. (2010).

Ministerio de la Presidencia

Plan de direccionamiento e interconexión de redes en la Administración. (2010).

Ralph Stair e George Reynolds.

Principios de Sistemas de información. Enfoque administrativo. (1999).

Autor: Juan Marcos Filgueira Gomis

Asesor Técnico Consellería de Educación y O.U.

Colegiado del CPEIG

28. MODELO DE CAPAS: SERVIDORES DE APLICACIONES, SERVIDORES DE DATOS, GRANJAS DE SERVIDORES. INTEGRACIÓN DE CONTENIDO, SONIDO, IMAGEN Y ANIMACIÓN. SCRIPTS DEL CLIENTE.

TEMA 28. MODELO DE CAPAS: SERVIDORES DE APLICACIONES, SERVIDORES DE DATOS, GRANJAS DE SERVIDORES. INTEGRACIÓN DE CONTENIDO, SONIDO, IMAGEN Y ANIMACIÓN. SCRIPTS DEL CLIENTE.

28.1. INTRODUCCIÓN Y CONCEPTOS

28.2 MODELO DE CAPAS: SERVIDORES DE APLICACIONES, SERVIDORES DE DATOS, GRANJAS DE SERVIDORES.

28.3 INTEGRACIÓN DE CONTENIDO, SONIDO, IMAGEN Y ANIMACIÓN.

28.4 SCRIPTS DEL CLIENTE.

28.5. ESQUEMA

28.6. REFERENCIAS

28.1. INTRODUCCIÓN Y CONCEPTOS

En una red formada por equipos informáticos los **nodos** suelen realizar tres **funciones** diferenciadas:

1. Facilitar la comunicación e interconexión de los nodos de la red.
2. Proporcionar servicios o información a otros nodos.
3. Realizar funciones de equipo de trabajo, haciendo uso de las comunicaciones, servicios e información disponible.

En este contexto los nodos o equipos que realizan las funciones de proporcionar servicio o información al resto se denominan **Servidores** y los que hacen uso de los servicios **Clientes**, formando en su conjunto lo que se da en denominar **Arquitectura Cliente-Servidor**. Se trata de una de las arquitecturas más extendidas en los entornos distribuidos, permitiendo la heterogeneidad en los clientes y un acceso transparente a la información. Los servidores permanecen a la escucha de la red en todo momento para

atender a las solicitudes o demandas de los clientes.

El esquema de funcionamiento **básico** seguiría el siguiente modelo:

1. El cliente solicita un servicio al servidor a través de la red.
2. El servidor a la escucha recibe la petición del servicio y la pone en la cola de demanda.
3. El servidor obtiene el resultado de la petición.
4. El servidor envía la respuesta de la petición al cliente a través de la red.
5. El cliente obtiene el resultado y lo procesa.

A partir de estos conceptos básicos podemos extraer las **características básicas** de la arquitectura Cliente-Servidor:

- a) **Servicios.** Son la base de las peticiones entre los clientes y los servidores, se trata de cualquier entidad susceptible de ser demandada por uno o más clientes.
- b) **Recursos compartidos.** Elementos y servicios de la red, tanto lógicos (software, datos e información), como físicos (hardware, impresoras, unidades en red, etc.).
- c) **Comunicación asíncrona basada en el envío de mensajes.** Este tipo de arquitecturas emplean protocolos de comunicación asimétricos donde los clientes inician conversaciones y los servidores esperan que se establezca la comunicación escuchando la red. Toda la comunicación se realiza mediante el envío de mensajes y respuestas.
- d) **Transparencia.** La localización, la organización lógica y física, así como la implementación de los servicios resulta transparente a los clientes. El uso de los mismos se limita a hacer una petición a la red y obtener la respuesta.
- e) **Escalabilidad.** Horizontal en los clientes a la hora de permitir añadir

nuevos nodos sin más que añadirlos a la red y vertical en los servidores, de modo que administrando un único punto puede mejorarse la potencia, el rendimiento, el mantenimiento y la recuperación de errores.

Fruto de la escalabilidad de esta arquitectura surgen las **granjas de servidores**, consistentes en emplear varios servidores a la vez suministrando el mismo servicio y repartiéndose las peticiones o carga del sistema. La gestión de una granja de servidores será compleja debido a la necesidad de balancear la carga para obtener el mayor rendimiento posible.

Uno de los servicios más extendidos actualmente es el web o WWW, (siglas en inglés de *World Wide Web*), se trata de un sistema de publicación e intercambio de información distribuido que relaciona unos contenidos con otros a través de enlaces. En este servicio los clientes solicitan información a modo de páginas web, tratándose de documentos en lenguajes estándar como HTML o XML que incluyen diferentes tipos de información: texto, hiperenlaces, y elementos multimedia. Entre estos elementos multimedia encontramos:

- a) **Texto.** Distinguiendo entre sin formato, con formato o enriquecido (tipo de letra, tamaño, color, color de fondo, etc.) e hipertexto texto con un vínculo o enlace a otro texto o documento.
- b) **Sonido.** Digitalización del habla, la música u otros sonidos.
- c) **Gráficos.** Representan esquemas, planos, dibujos vectoriales, etc. son documentos que se construyen a partir de una serie de primitivas: puntos, segmentos, elipses, etc. aplicándoles a continuación todo tipo de transformaciones o funciones: giro, cambio de atributos, escalado, efectos, etc.
- d) **Imágenes.** Representaciones fieles de la realidad, como fotografías.

Son documentos formados exclusivamente por píxeles, punto a punto y por tanto no se estructuran o dividen en primitivas.

- e) **Animación.** Representación de una secuencia de gráficos por unidad de tiempo, para ofrecer la sensación de movimiento. Asimismo ofrece posibilidades de interacción ante eventos.
- f) **Vídeo.** Representación de una secuencia de imágenes por unidad de tiempo, para ofrecer la sensación de movimiento.

Documentos complejos agrupan diversos componentes multimedia en una misma página o documento. Los sistemas de publicación actuales permiten que la **multimedia digital on line** pueda transmitirse **en flujo** (en inglés *streaming*), que se encuentra disponible tanto on line en tiempo real como bajo demanda. En este modelo no es necesario descargar o acceder a la totalidad del documento para acceder a los contenidos sino que se proporciona acceso directo a cualquier parte del flujo y reproducción desde ese punto.

Otra característica de las páginas web o documentos HTML/XML es que pueden incluir **código de script para los clientes**. Este código representa un guión o secuencia de instrucciones a manera de un programa sencillo. Este programa puede ser interpretado por el navegador del equipo cliente con unos permisos limitados en el equipo y focalizados principalmente en la página o documento web en el que se encuentran incrustados o desde el que son llamados. Existen diferentes tecnologías para estos lenguajes de script siendo las más conocidas: Javascript, Visual Basic Script, Flash, y la evolución de Javascript: AJAX, aceptados con mayor o menor fortuna por los navegadores actuales, muchas de ellas denominadas tecnologías RIA en un acercamiento de las aplicaciones web a las aplicaciones de escritorio.

28.2 MODELO DE CAPAS: SERVIDORES DE APLICACIONES, SERVIDORES DE DATOS, GRANJAS DE SERVIDORES

La distribución de los sistemas de información fue evolucionando a lo largo del tiempo en función de las demandas y crecimiento de las redes y el aumento de la complejidad de las arquitecturas de red.

28.2.1. Arquitectura en una capa: Superordenador central.

La arquitectura más simple estaría formada por **un superordenador central** (en inglés *mainframe*) que centraliza toda la capacidad de procesamiento y almacenamiento de la red, también denominada monolítica. En este modelo el acceso a la información se hace directamente a través de la computadora principal o bien a través de clientes ligeros que se limitan a hacer las funciones de terminales. En esta arquitectura centraliza todo el coste de administración y mantenimiento se dedica al servidor central. Los terminales carecen de programas propios, y tienen recursos de memoria o disco mínimos, pudiendo incluso carecer de disco. Cualquier instalación o avance en el servidor repercute al momento en la red de modo que cualquier programa instalado estará disponible para todos los clientes. Por el contrario, si tenemos en cuenta la sostenibilidad del sistema en caso de caída o errores en el servidor central toda la red se ve afectada, al igual que si un cliente sobrecarga el sistema todos los demás se verán afectados en cuanto a rendimiento. A su vez los mainframes se organizan según arquitecturas paralelas tipo **SNA** (en inglés *Systems Network Architecture*) con un diseño de red con comunicación P2P a través de APPN (en inglés *Advanced Peer-to-Peer Networking*).

28.2.2. Arquitectura en dos capas: Modelo Cliente-Servidor.

En este modelo el sistema se estructura en dos capas, una capa a nivel de usuario que almacena y procesa parte de la información y otra capa remota a nivel de servicios que almacena y da funcionalidad a la totalidad de clientes de la red. De este modo se consigue descargar de parte de la carga de la red a los servidores centrales y mantiene la capa de servicios transparente a los usuarios con la posibilidad de escalar el sistema mejorando o aumentando el número de servidores sin que estos lleguen a notar el cambio en algo más que el rendimiento. Sin embargo, un modelo más distribuido en lo relativo a los clientes obliga a un mayor mantenimiento de los mismos por parte de los administradores. Otro de los puntos a tener en cuenta es la consistencia de los datos entre cliente y servidor, de manera que hace falta coordinar cada servicio por separado. En esta línea el uso de protocolos de comunicación soporta el uso efectivo por parte de los clientes de los servicios de la red permitiendo la heterogeneidad de los clientes siempre y cuando los implementen.

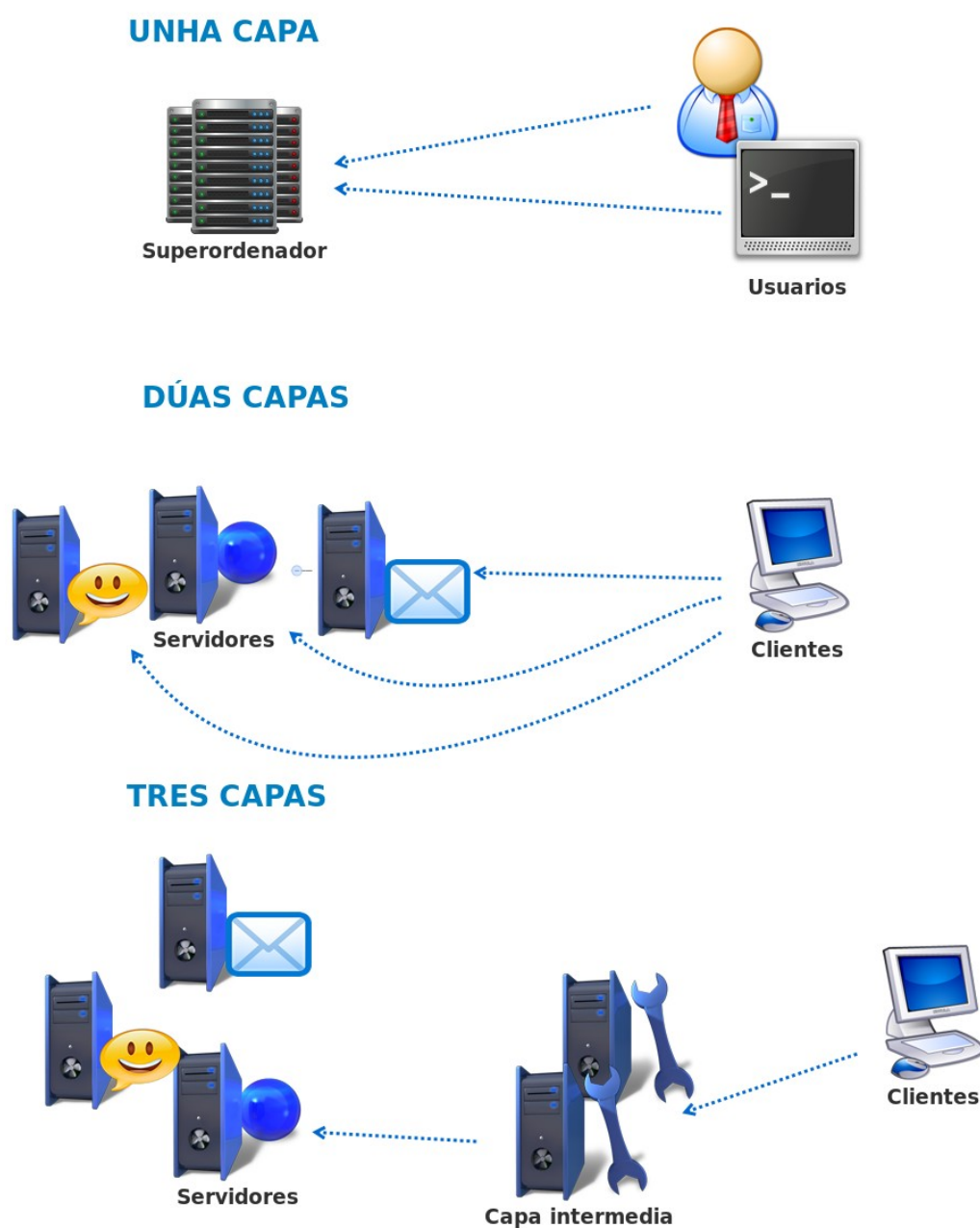


Figura 1: Arquitecturas en capas

28.2.3. Arquitectura en tres capas: Granjas de servidores.

Debido a los inconvenientes de los sistemas de una única capa, que obligan a mantener un servidor central de tamaño demasiado grande para un mantenimiento y rendimiento eficientes, y de dos capas, que obligan a

mantener cada servidor independiente del resto para un único servicio, se optó por el establecimiento de una capa más entre las de cliente y servidor. En esta capa se agrupan varios servidores en una DMZ soportando el mismo servicio dando lugar a una redundancia que tiene como ventajas una mayor tolerancia a fallos y un avance de rendimiento. A efectos de la red las granjas de servidores proporcionan un único servicio lógico o virtual integrado por cualquier número de servidores físicos. Cada servidor de la granja debe ser una réplica exacta del servidor lógico en cuanto a datos y software instalado. Para escalar el sistema se añade a la granja un nuevo servidor réplica del virtual y aumenta la disponibilidad de recursos. El ejemplo más habitual de granja de servidores es un servicio web, donde, si por ejemplo un servidor atiende a mil usuarios y tenemos previstos picos de diez mil usuarios simultáneos, pondremos una granja de diez servidores para atender el servicio y otros dos más en previsión de caída de alguno o picos puntuales todavía más altos. La escalabilidad de las granjas en función de los servicios ofertados define tipologías básicas como *Datacenters*, servidores de aplicaciones, de importación, de *front-end* existiendo elementos específicos para control de carga, Teredo o de dominio, entre otros.

28.2.3.1 Componentes intermedios: *Middleware*

Para dar el efecto de transparencia a los clientes, ese sistema requiere de una serie de componentes intermedios, es decir que se encuentran “por el medio” (en inglés *middleware*) de las capas principales. Estos componentes se encargan de recibir y repartir las peticiones de los clientes entre los servidores de la granja, cuidar el balanceo de carga, el mantenimiento de la sesión, etc. El ***middleware*** se describe como un conductor o intermediario entre sistemas, dirigiendo las peticiones de datos y servicios a otros nodos de la red. Entre sus principales características destacarían:

- a) Simplificar el desarrollo de aplicaciones al capsular comunicaciones

entre sistemas.

- b) Facilitar la interconexión de los sistemas de información con independencia de la red física.
- c) Mejorar la escalabilidad del sistema, aumentando la capacidad sin pérdida de funcionalidad.
- d) Mejorar la tolerancia a fallos del sistema, fiabilidad.
- e) Aumentar la complejidad de administración y soporte.

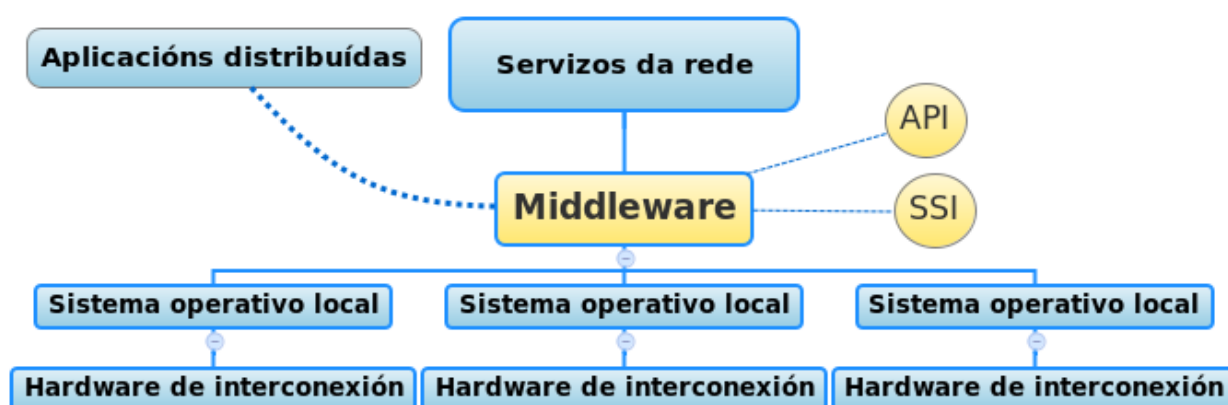


Figura 2: El middleware en un sistema distribuido.

En un sistema distribuido el *middleware* es el software de conectividad que permite disponer de un conjunto de servicios sobre plataformas distribuidas heterogéneas. Actúa como una capa de abstracción de las funciones del sistema distribuido haciendo transparente en la red los sistemas operativos y el hardware de interconexión de las redes de comunicaciones. Proporciona una Interfaz de Programación de Aplicación (**API**) para la comunicación y acceso a aplicaciones y servicios distribuidos. Por otra parte proporciona una interfaz única de acceso al sistema denominada **SSI** (del inglés *Single System Image*), la cual da al cliente la sensación de acceder a un único servidor, el virtual.

Para garantizar la heterogeneidad en la comunicación de los sistemas el *middleware* se estructura en tres **capas o niveles de comunicación** separados:

- 1) **Protocolo de transporte.** Protocolos de comunicaciones comunes a la capa de transporte de la red, como TCP o UDP. Establecen niveles de seguridad, control de sesiones, etc.
- 2) **Sistema Operativo en Red o NOS** (en inglés *Network Operating System*). Extensión del sistema operativo de los clientes que captura las peticiones y las dirige hacia el servidor acomodado para devolver a continuación la respuesta del mismo al cliente.
- 3) **Protocolo de servicio.** Protocolo específico del servicio o aplicación en el sistema Cliente-Servidor.

Los middleware acostumbran a clasificarse según el tipo de comunicación que realizan en el Sistema Operativo en Red y a los parámetros que comunican (infraestructura, acceso a datos, aplicaciones, etc.), los **tipos de middleware** más habituales serían:

1. **Llamadas a procedimientos remotos** (en inglés *Remote Procedure Call* o RPC). Los Clientes invocan directamente procedimientos o funciones de procesos que se ejecutan en servidores remotos, permitiendo distribuir la lógica de la aplicación remota a través de la red. Las llamadas pueden realizarse de manera asíncrona o síncrona. Mantiene al mínimo la información de la sesión y en caso de ruptura de la misma el cliente reinicia la comunicación de cero.
2. **Publicación/suscripción.** Este middleware realiza una monitorización del sistema detectando los servicios y procesos activos. Los componentes registran su interés en determinados eventos, cuando estos eventos son detectados por el monitor envía esa información a los suscriptores. La interacción es asíncrona recayendo por completo en el servicio de notificación/monitorización.
3. **Middleware orientado a mensajes** (en inglés *Message Oriented*

Middleware o MOM). La comunicación se basa en el envío de mensajes asíncronos por parte de los nodos (cliente, servidor, servicio o aplicación). Los mensajes se recogen en colas priorizadas en el nodo destino y se almacenan hasta que pueden responderse. El funcionamiento del sistema es análogo a cómo funciona un servicio de correo electrónico.

4. **Middleware basado en objetos** (en inglés *Object Request Broker* u ORB). Incorpora a RPC los paradigmas de orientación a objetos. Define una arquitectura cliente servidor donde los servicios devuelven objetos, siendo estos la unidad de comunicación. Los nodos piden los objetos por el nombre siendo estos entregados por un servicio de resolución de nombres. Ejemplos de implementaciones de este *middleware* serían: CORBA, RMI, COM, .NET Remoting, etc.
5. **Middleware de acceso a datos** (en inglés *Oriented Data Access Middleware*). Proporcionan la API transparente de acceso a datos agrupando las operaciones de manejo de la conexión con las bases de datos. Ejemplos de este tipo de API serían JDBC y ODBC. Por norma general realizan conexiones síncronas y operaciones transaccionales.
6. **Arquitecturas orientadas a servicios** (en inglés *Service Oriented Architecture* o SOA). Las funcionalidades o procedimientos se publican desde cualquier servidor a modo de servicios. Los servidores publican el servicio y permanecen a la escucha hasta que llega una petición, la procesan y devuelven una respuesta al cliente del servicio. Ejemplos de este *middleware* son los Servicios Web y los Servicios CORBA.

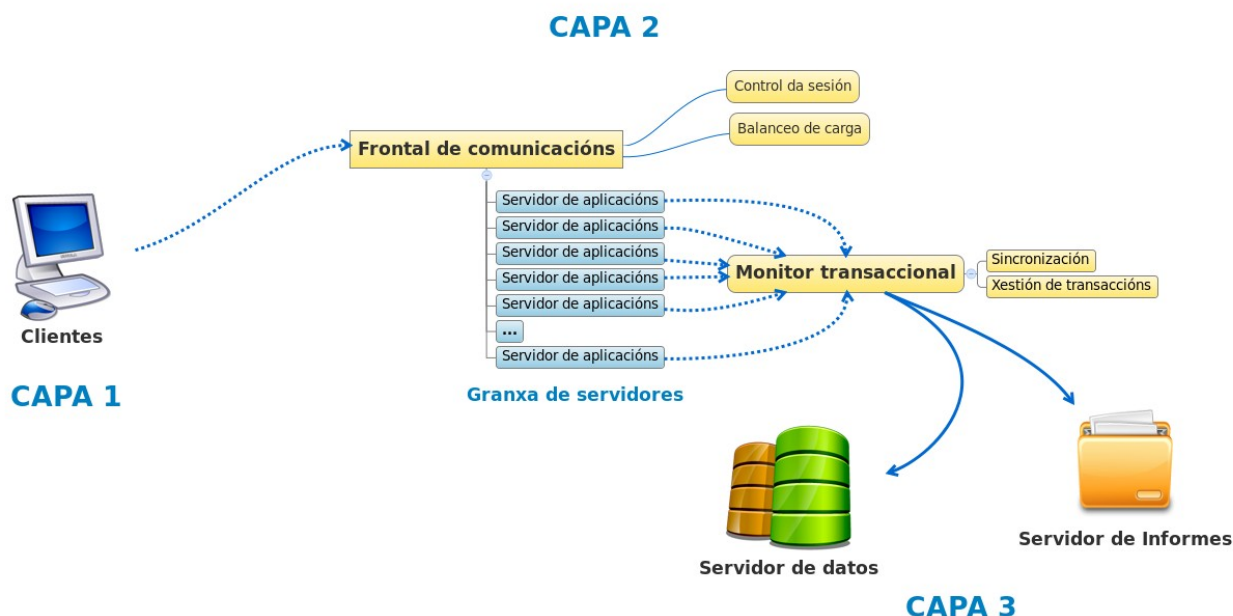


Figura 3: Granja de servidores.

Las granjas de servidores se completan con dos componentes fundamentales, funciones que de manera general realiza el *middleware*:

1. **El frontal de comunicaciones.** El frontal de comunicaciones (en inglés *front-end*) es el punto de acceso único a la granja de servidores, simulando un único servidor lógico. Aunque cada servidor de la granja pueda tener su propia dirección IP lo normal es que el frontal tenga uno propio y sea esta la forma de que los clientes accedan a él, o bien directamente o bien a través de un nombre de dominio (DNS).
- ✓ **Balanceo de carga.** Consiste en dividir la carga de trabajo de los clientes entre los servidores de la granja. Puede implementarse vía hardware, software o una combinación de ambas. Para hacerlo vía hardware el frontal de comunicaciones debe disponer de un equipo específico, aunque hay enrutadores que permiten esta funcionalidad.

- ✓ **Control de la sesión.** Si a causa del balanceo de la carga diferentes peticiones de un mismo cliente van hacia servidores diferentes, hace falta coordinar a los servidores en el seguimiento de una sesión o que puedan compartirla.
 - ✓ **Priorización.** En caso de tener peticiones simultáneas el frontal debe ser capaz de atender primero a los clientes críticos o de mayor prioridad, así como de asignar el procesamiento de sus tareas a aquellos servidores dotados de más recursos.
2. **Los monitores transaccionales.** Los monitores transaccionales son los encargados de mantener las redes de consistencia de los datos y los procesos que se realizan simultáneamente en los servidores de la granja. Tiene que garantizar que una modificación de datos fruto de una petición se realiza como una transacción, es decir, o se realiza completamente o no se realiza en absoluto. Cada transacción tiene que tener lugar independientemente de que tenga lugar otra simultánea, deben procesarse de manera aislada. Las principales funciones serán:
- ✓ **La gestión de las transacciones.** Se encarga de controlar la atomicidad y secuencialidad de las transacciones, para garantizar la consistencia de datos y operaciones. La gestión de transacciones debe garantizar el correcto funcionamiento del sistema cuando la carga de trabajo o el número de usuarios son muy elevados. Debe contemplar la posibilidad de errores en las aplicaciones y caídas de elementos del sistema durante las transacciones, permitiendo operación de vuelta atrás. Vista en detalle la gestión de transacciones constará de:
 1. **Gestor de transacciones** (en inglés *Transaction Manager*). Controla el inicio de transacción, registra los recursos que precisa y gestiona las operaciones de confirmación de la

transacción (en inglés *commit*) y de vuelta atrás y recuperación del estado inicial de la transacción (en inglés *rollback*).

2. **Gestor de registro** (en inglés *Log Manager*). Guardar los estados de los recursos que están en uso por parte de las transacciones, elaborando un historial de versiones de los mismos. Esta información es compartida por los distintos gestores de transacciones siendo lo que permite garantizar la consistencia de los recursos empleados.
 3. **Gestor de bloqueos** (en inglés *Lock Manager*). Gestiona el acceso simultáneo por parte de varios procesos a los recursos, permitiendo bloquearlos para evitar que dos o más accesos a la vez den lugar a inconsistencias. Asimismo lleva a cabo la detección de cuando se libera un recurso y envía una notificación al gestor de transacciones.
- ✓ **Sincronización.** La sincronización de las comunicaciones resulta compleja en este modelo, ya que un cliente puede acceder a un servicio empleando diferentes servidores de la capa intermedia, incluso simultáneamente. Según el comportamiento del servicio podemos encontrar soluciones síncronas, donde se espera siempre a la respuesta del servidor, simple pero con riesgo de bloqueo. Frente a las asíncronas donde se envía la petición y ya llegará la respuesta, con lo cual no hay bloqueos, pero la respuesta podría no llegar nunca sin más opción que detectarlo a través de tiempos de espera agotados.

28.2.6. Arquitecturas en n-Capas.

Las arquitecturas en tres capas pueden extenderse a n-capas cuando en la capa intermedia se incorporan otros elementos de interconexión como distribuidores o sistemas de cortafuego. También puede dividirse la capa de

servidores por servicios o diferentes capas de acceso a datos o presentación de información. La separación en capas es una organización lógica del sistema con la cual puede establecerse cualquier número de capas según las necesidades del mismo. Cualquier especialización de servidores que se quiera hacer en la red y provoque un nuevo agrupamiento podemos identificarla con una nueva capa.

28.2.7. Arquitecturas para Red entre iguales (P2P).

En los modelos distribuidos de igual a igual o P2P (en inglés *Peer-to-Peer*), todos los equipos (excepto los elementos de interconexión) tienen el mismo papel doble de cliente/servidor en la red. Hacen uso de servicios y los proporcionan. En esta arquitectura, por tanto, no se pueden agrupar los nodos y pierde sentido hablar de capas. Estas redes no resultan excelentes para todo tipo de servicios, en muchos casos, por ejemplo a la hora de funcionar como servidor web, requerirían un coste muy alto para el control de la consistencia del sitio web, mantenimiento y configuración del servidor, etc. Por el contrario, en situaciones donde los nodos caen a menudo, por ejemplo un servidor atacado continuamente, la redundancia de nodos garantiza que el sistema siga funcionando. Otros servicios como el intercambio de archivos, o el procesamiento compartido presentan más ventajas a la hora de emplear una arquitectura de este tipo como solución de implantación. Los modelos más habituales son centralizados, puros o descentralizados o híbridos, según el peso de cada nodo individual en la red o de la existencia de servidores con responsabilidad de control y gestión en el modelo. La adaptación de este modelo por parte de los ISP da lugar a P2P híbridas de servicio denominadas P4P (en inglés *Proactive network Provider Participation for P2P*). Otros modelos similares serían los P2M, que actúan en arquitecturas híbridas empleando el correo electrónico como soporte del envío de datos.

La gestión de este tipo de redes se realiza fundamentalmente vía software. En este caso el software deberá realizar las mismas funciones ya vistas para la arquitectura de tres o más capas: frontal de comunicaciones y gestión de transacciones. Por debajo acostumbran implementar servidores propios como Kademia, eDonkey, Gnutella, FastTrack, BitTorrent u OpenNap entre otros.

28.2.8. SERVIDORES.

28.2.8.1. Servidor web.

Se trata de servidores que proporcionan el servicio WWW a través del protocolo HTTP. En esencia se trata de una aplicación ejecutándose en un servidor a la espera de peticiones HTTP por parte de un cliente respondiendo con los documentos solicitados generalmente páginas web y los objetos que enlazan: imágenes, archivos de script , animaciones, etc. En funciones más avanzadas estos servidores añaden seguridad a través de conexiones encriptadas con protocolos tipo HTTP Seguro o HTTPS. Por regla general, los servidores de aplicaciones se integran en arquitecturas de mínimo tres **capas**:

- 1) **Primera capa.** Capa de interacción con los usuarios, principalmente a través de navegadores web.
- 2) **Capa intermedia.** Capa de los servidores web, que pueden estar distribuidos en un modelo de granja de servidores. Cada servidor incorporaría los módulos necesarios para seguridad, lenguajes de servidor interpretados, correo, mensajería, acceso a datos y otras funcionalidades.
- 3) **Tercera capa.** Capa de servidores de acceso a datos, como servidores de archivos, base de datos o informes.

Entre los **servidores web de uso más extendido** actualmente se encontrarían:

- ✓ **Apache.** Uno de los más utilizados, por ser un servidor libre que ofrece prestaciones a nivel de otras soluciones propietarias además de una gran facilidad de uso y configuración.
- ✓ **Internet Information Server (IIS).** Servidor propietario con soporte para aplicaciones .NET o ASP entre otras.
- ✓ **Otros:** Java Web Server, AOLServer, Cherokee, Tomcat, lightHttpd, etc.

Los servidores web pueden disponer de módulos para la ejecución de programas de servidor interpretados, como son los de las tecnologías Python, PHP, ASP, JSP, Tcl,...

28.2.8.2. Servidor de aplicaciones.

Los servidores de aplicaciones son servidores web con capacidad de procesamiento ampliada, pudiendo ejecutar aplicaciones y componentes de lógica de negocio y recursos relacionados como el acceso a datos. Debido a esto permiten realizar el procesamiento de aplicaciones de cliente en el propio servidor. Proporcionan soporte como middleware o software de conectividad y para diferentes tecnologías de servidor. Por regla general, los servidores de aplicaciones se integran en arquitecturas de mínimo tres **capas**:

- 1) **Primera capa.** Capa de interacción con los usuarios, principalmente a través de navegadores web.
- 2) **Capa intermedia.** Capa de los servidores de aplicaciones, que pueden estar distribuidos en un modelo de granja de servidores. Un subconjunto de los servidores de aplicaciones darán servicio a los usuarios/clientes mientras otro grupo se encargará de soportar la operativa común del dominio, como librerías o aplicaciones y

servicios web de los que hagan uso las aplicaciones para usuarios/clientes.

- 3) **Tercera capa.** Capa de servidores de acceso a datos, como servidores de archivos, base de datos o informes.

El servidor de aplicaciones suele tener integrado un servidor web, para gestionar de manera independiente el servicio WWW a través del protocolo HTTP.

Además de este servicio presenta un amplio conjunto de herramientas:

- ✓ Servidor web integrado.
- ✓ Contenedor de programas de servidor (en inglés *servlets*).
- ✓ Contenedores de objetos de lógica de negocio (como por ejemplo EJBs).
- ✓ Sistemas de mensajería.
- ✓ Software de conectividad con bases de datos.
- ✓ Balanceo de carga.
- ✓ Gestión de límites y colas de conexiones (en inglés *Pool*) para bases de datos y objetos.
- ✓ Etc.

En esencia, un servidor de aplicaciones realiza las mismas funciones que un servidor web, pero cuando la demanda de uso es grande y estamos ante un sistema complejo la solución pasa por emplear un servidor de aplicaciones que ofrezca las siguientes **ventajas**:

- ✓ **Centralización.** Centraliza en los servidores la administración y configuración de la lógica de negocio de las aplicaciones, de manera que aspectos como el mantenimiento de los accesos a base de datos pueden realizarse de manera centralizada. Asimismo cambios derivados de actualizaciones, migraciones o recuperaciones ante errores tienen lugar desde uno único punto.

- ✓ **Seguridad.** Al existir un único punto de acceso a datos puede reforzarse la defensa y los sistemas de control de errores en ese punto, mejorando su gestión y protección.
- ✓ **Rendimiento.** Como punto intermedio permite gestionar las peticiones de los clientes a la Base de datos.
- ✓ **Escalabilidad.** Un mismo servidor de aplicaciones puede dar servicio a varios clientes, y por tanto aumentando el número de servidores se mejora el rendimiento del sistema.

Entre los **servidores de uso más extendido** actualmente se encontrarían:

- ✓ **Jboss, Glassfish.** Servidores de aplicaciones libres bajo licencia GPL.
- ✓ **BEA Weblogic, IBM Websphere, Oracle Application Server.** Alternativas propietarias integradas en paquetes de aplicaciones con funcionalidades de gestión y monitorización extendidas.
- ✓ **Tomcat, Internet Information Server (IIS), Jetty.** Proporcionan funciones parciales de servidores de aplicaciones, con lo cual en ocasiones se definen más bien como contenedores de programas de servidor.

28.2.8.3. Servidor de acceso a datos.

Los servidores de acceso a datos ocuparían la última capa de los sistemas de información encargándose del acceso directo a los datos, existiendo diferentes tipos según el sistema de información empleado para su almacenamiento o publicación:

- ✓ **Servidores de archivos.** En este tipo de servidores la información se almacena directamente en archivos, por tanto la función de estos equipos será la de permitir el acceso remoto a los mismos desde los clientes u otros servidores. Los protocolos más habituales ofrecen servicio solo desde redes locales pero en sistemas avanzados pueden

proporcionar servicios como FTP o WebDAV para conexión remota a través de Internet. Actualmente el término empleado para referirse a estos servidores es NAS (en inglés *Network-Attached Storage*), pero ésta tan sólo sería la tecnología más habitual frente a otras como DAS (en inglés *Direct Attached Storage*), basada en SCSI o SAN (en inglés *Storage Area Network*) basada en fibra óptica. No requieren un software muy específico como otros tipos de servidores sino más bien soporte para diferentes protocolos y tecnologías. Por norma general acostumbran a estar dispuestos en RAID (en inglés *Redundant Arrays of Independent Disks*), equipos de almacenamiento redundante.

- ✓ **Servidores de bases de datos.** Albergan uno o más sistemas de gestión de bases de datos (en inglés *database management system*, o DBMS), software de gestión que se encarga de la comunicación entre las aplicaciones y las bases de datos. Permiten realizar operaciones de definición, manipulación y seguridad de los datos a través de una API de comunicación con las aplicaciones y un lenguaje estructurado de consulta como el SQL. Admiten accesos simultáneos a los datos, seguridad y gestión de transacciones.

Estos sistemas suelen presentar además programas o consolas de administración avanzadas para realizar las tareas generales de gestión de la base de datos.

- ✓ **Servidores de informes.** Pueden considerarse una capa intermedia entre los servidores de datos y los de aplicación, donde se establecen servidores o granjas de servidores que sirven los datos en documentos predefinidos multiformato: hojas de cálculo, PDF, XML, HTML, etc. El software de este tipo de servidores suele incorporar software de gestión para el servidor, y software de auto-edición de informes, para definir modelo de informes compuestos de cabeceras, imágenes, fórmulas, subinformes, etc. que generarán dinámicamente los informes a partir de consultas sobre los datos.

CAPA DE USUARIO

CAPA DE SERVIDOR DE APLICACIONES



CAPA DE ACCESO A DATOS

Figura 4: Arquitectura en 3 capas con servidor web, de aplicaciones y base de datos.

Entre los **servidores de uso más extendido** actualmente se encontrarían:

- ✓ **Servidores de archivos.** No requieren gestores especializados pero sí soporte software a los protocolos: CIFS, NFS, SMB, FTP, WebDAV, etc. Así como utilidades tipo Samba o FreeNAS.
- ✓ **Servidores de bases de datos.**
 - ✓ De licencia libre: PostgreSQL, MariaDB, Firebird, SQLite, Apache derby,...
 - ✓ Dual, dependiendo de su uso: MySQL.
 - ✓ Software propietario: SQLServer, Oracle, Access, Paradox, Informix, DBase, etc.
- ✓ **Servidores de informes.** Jasper Reports, Jreports, Crystal Reports, Oracle Reports etc.

28.3 INTEGRACIÓN DE CONTENIDO, SONIDO, IMAGEN Y ANIMACIÓN.

El modelo más habitual de integración de elementos multimedia a través de Internet es a través del servicio WWW, empleando la web. En este servicio los clientes solicitan información a modo de páginas web, tratándose de documentos en lenguajes estándar como HTML o XML, basados en etiquetas que se encargan de estructurar y referenciar los contenidos del documento. De este modo pueden incluirse diferentes tipos de información: texto, hiperenlaces, y elementos multimedia: sonido, imágenes, gráficos, vídeo y animaciones, además de otros formatos o tecnologías que a su vez integran estos elementos.

Para reproducir la mayoría de los formatos básicos de imagen, sonido y vídeo los navegadores suelen disponer de componentes idóneos mientras que para los formatos y tecnologías específicos acostumbran a precisar de *Plug-Ins* o complementos externos que precisan instalación y actualización independiente del navegador. Según esto se distinguirá por tanto dos formas de integración multimedia:

- a) **Nativa.** En este caso el elemento multimedia se almacena en un archivo externo de un formato propio del tipo de elemento, si por ejemplo se trata de una imagen en GIF o JPG, y desde el documento HTML o XML se hace referencia al archivo a través del sistema de etiquetado. Casi todos los navegadores actuales, a excepción de los que son en modo texto, reconocen estos formatos básicos con lo cual serán capaces a partir del archivo de reproducir el contenido y transmitirlo de manera correcta al usuario.
- b) **Dependiente.** En este otro caso los elementos multimedia emplean tecnologías externas que requieren complementos o *Plug-Ins* externos al navegador que deben instalarse aparte para poder representar la información correctamente. Estas tecnologías hacen las funciones de conector y especificado su contenido a través del etiquetado HTML o XML son capaces de aparecer como un elemento multimedia básico. Dentro de estos conectores destacarían los

vídeos y animaciones Flash y Silverlight, programas de cliente como los controles Active X y los applets de Java, y documentos en formatos enriquecidos como el PDF.

Los sistemas de publicación actuales permiten que la **multimedia digital on line** pueda transmitirse **en flujo** (en inglés *streaming*), tanto de sonido (en inglés *Podcast*) como de vídeo y videoconferencia. El mundo del vídeo on line es dentro de la multimedia uno de los que presenta mayores problemas a la hora de trabajar en entorno web, pues precisa más recursos de almacenamiento, ancho de banda para reproducción, problemas de conversión y mantenimiento de formatos de codificación (en inglés *codecs*).

Un último aspecto problemático es la sincronización de todos estos puntos en un proceso automático en un servidor, lo que da lugar a soluciones complejas y de poca sostenibilidad. Las principales tecnologías que dan soporte a este tipo de arquitecturas multimedia son: Windows Media, ASF (en inglés *Advanced Streaming Format*), Quicktime, Real Media, VideoLAN y Flash Video.

Elemento multimedia	Formatos de archivo	Observaciones
Sonido	AAC, MP3, RealAudio, WMA, OGG, MIDI, WAV, AIFF, etc.	<i>Los cuatro primeros producen pérdida de información en la conversión.</i>
Imagen	JPEG, GIF, BMP, TIFF, PNG, JPG, TGA, etc.	<i>El JPEG produce pérdida de información en la conversión.</i>
Vídeo	AVI, MPG, QuickTime (MOV y QT), WMV, Ogg, RMVB, DIVX, Matroska, etc.	<i>Tan sólo algunas tecnologías son adecuadas para flujos de vídeo on line.</i>
Gráficos	PNG, PSD, CDR, XCF, SVG, EPS, etc.	<i>Muchos pertenecen exclusivamente al programa de edición que los genera, excepto SVG y PNG.</i>

Animaciones	Flash (SWF), Silverlight (XAML), Javascript (JS), etc.	<i>Excepto Flash que comprime en un único archivo los demás emplean otras tecnologías de definición abiertas.</i>
Documentos enriquecidos	RTF, PDF, PostScript, etc.	<i>Llevar incrustados otros elementos multimedia.</i>

Tabla 1: Formatos de archivo multimedia.

El servidor de *streaming* permite que se pueda ver parte del video sin descargarlo por completo gracias al uso de un *buffer* que carga parte del archivo previamente. Los formatos de vídeo empleados deben permitir, por lo tanto, estas reproducciones parciales. El flujo busca conseguir lo máximo que permita el ancho de banda y protocolos del sistema, parando la reproducción y esperando a que continúe la carga si la información disponible no es suficiente.

La existencia de un servidor de flujo de vídeo o *streaming*, posibilita los siguientes **servicios**:

- ✓ **Vídeo bajo demanda** o VoD (en inglés *Video on Demand Media Streaming*). En este modelo el vídeo, incluyendo el sonido correspondiente y otros archivos complementarios como subtítulos o textos alternativos para tecnologías asistivas, se encuentra alojado en un servidor específico y los usuarios solicitan el envío de información según lo precisen, en cualquier punto del mismo, con lo que se produce una respuesta personalizada con un flujo parcial a partir de la posición solicitada. Los usuarios pueden realizar diferentes interacciones (simultáneas), yendo adelante, atrás o situarse en cualquier punto del vídeo. Con este sistema siempre se

envía la información almacenada y se hace una precarga de todo el vídeo a partir de la posición solicitada, no siendo necesario disponer del archivo o archivos completos para su visualización.

- ✓ **Vídeo en tiempo real.** (En inglés *Live Media Streaming*). El contenido se crea en el mismo momento de la difusión a modo de las videoconferencias. Se trata de un modelo orientado a la multidifusión de la información, produciéndose un envío del flujo de vídeo a los usuarios una vez que el archivo o parte del mismo pasa a estar creado en el servidor. No tiene porque ser el mismo flujo para todos los clientes, sino que permite flujos paralelos, con la posibilidad de pausas o retrocesos, pero no avances.

En una **arquitectura de streaming**, deberían considerarse cuando menos los siguientes elementos:

- ✓ **Sistemas de edición de vídeo.** Módulos de producción, compresión y conversión de vídeo en formatos aptos para *streaming*.
- ✓ **Sistemas de almacenamiento** que permita alta capacidad de entrega, elevado espacio, tolerancia a errores y sistemas de copias de seguridad. En sistemas con mucha demanda pueden requerir técnicas de tipo:
 - **Diseminación de archivos.** Emplea varios discos diseminando la información para permitir que el servidor acceda a ellos en paralelo.
 - **Almacenamiento terciario jerárquico.** Emplea diferentes soportes almacenando los archivos más demandados en los soportes de mayor rendimiento como discos, y los menos demandados en soportes como cintas, lo cual permite reducir costes.
 - **Técnicas en espejo.** Replica toda la información en diferentes discos separados en espejo, con lo cual se aumenta también la tolerancia a errores.

- ✓ **Servidor de streaming.** Disponiendo de líneas de alto ancho de banda, con soporte de **Calidad de servicio** o QoS (en inglés *Quality of Service*).
- ✓ **Clientes.** Con extensiones o complementos que soporten los formatos de la arquitectura. El complemento hará una función doble, gestionar la precarga del vídeo y permitir su reproducción parcial según la información disponible.

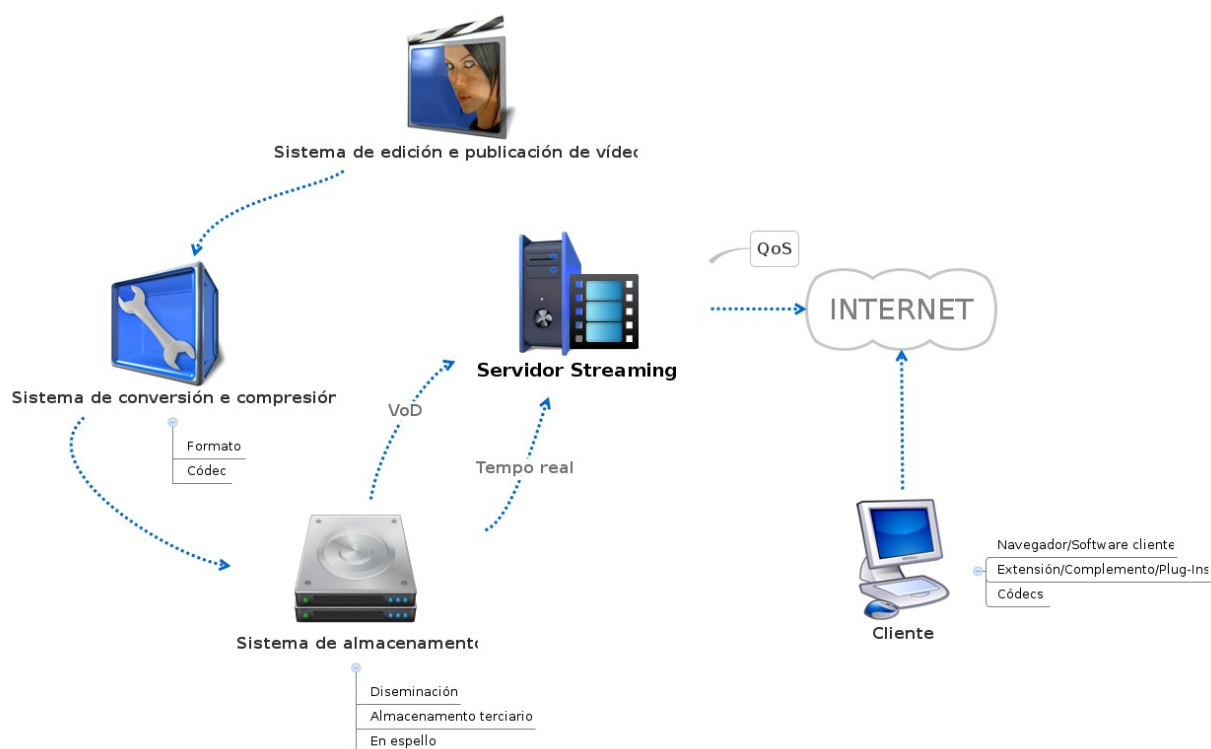


Figura 5: Arquitectura de un servidor Streaming.

Mención especial requieren, respecto del almacenamiento, las **bases de datos multimedia**, son sistemas gestores de bases de datos con orientación a objetos, identificando cada tipo de elemento multimedia con un objeto de la base de datos. Existen varios tipos principales:

- 1) **Bases de datos referenciales.** Hacen referencia detallada a objetos multimedia, incorporando información descriptiva tanto sobre

el elemento (título, autor, sinopsis, ...) como información técnica (formato, duración, códec, ...)

- 2) **Bases de datos descriptivas.** Incorporan información descriptiva o semántica del contenido del elemento, como puede ser la descripción de un vídeo paso a paso, o el texto alternativo de una imagen. El objetivo de estas soluciones es dar cabida a las búsquedas semánticas y soporte de accesibilidad para tecnologías asistivas.
- 3) **Elementos multimedia integrados.** Los objetos multimedia se almacenan como campos dentro de la base de datos y no como ficheros externos, por norma general el tamaño de los campos de las bases de datos relacionales se encuentra limitado en comparación con las necesidades de los elementos multimedia, pero el avance de rendimiento y eficacia del sistema pueden hacer necesarias este tipo de soluciones. El ejemplo más habitual serían los bancos de imágenes y algunos tipos de gestores documentales.

Además de la Web **en otros servicios** se puede realizar **integración multimedia** como son los de mensajería instantánea y el correo electrónico. Para el caso del correo, el protocolo **MIME** (en inglés *Multipurpose Internet Mail Exchange*) se desarrolló para permitir la integración de elementos multimedia en los mensajes de correo, con el objetivo de realizar una aproximación al HTML. El funcionamiento básico es asociar cada tipo de elemento multimedia a un tipo MIME (texto, imagen, documento HTML) esta información permite a los navegadores y clientes de correo electrónico determinar con qué tipo de contenido se está trabajando para representarlo correctamente con su complemento o *Plug-In* correspondiente.

28.4 SCRIPTS DEL CLIENTE.

Los *scripts* del cliente son programas interpretados diseñados para ejecutarse en los navegadores con el objetivo de dotar a las páginas de mayor interactividad con el usuario y dinamismo en una aproximación a las aplicaciones de escritorio. El **funcionamiento básico** de un *script* consiste en interpretar una serie de comandos a través de los cuales puede modificar y manipular objetos y reaccionar ante eventos de la interfaz cómo respuestas a periféricos (ratón, teclado, etc.), o cambios en los elementos del documento (botones, elementos de formularios, etc.). Sus usos básicos son validaciones, manipulación de formularios, procesamiento de funciones y carga asíncrona de datos.

Los *scripts* de cliente proporcionan las siguientes **ventajas**:

- ✓ Modificar el contenido de la página sin recargarla del servidor en función de las interacciones con el usuario.
- ✓ Modificar parámetros de configuración del navegador y otros elementos de la página web.
- ✓ Mejorar la interacción entre el usuario y el documento, en general la usabilidad.

Por el contrario, presentan una serie de inconvenientes o desventajas:

- ✓ Problemas de accesibilidad, pues se complica la posibilidad de presentar alternativas a usuarios que no soporten la tecnología de *script*.
- ✓ Problemas de seguridad, pues toda la lógica de interacción aparece sin protección descargada en el equipo del usuario, con lo cual disponen del código fuente del programa de *script*.

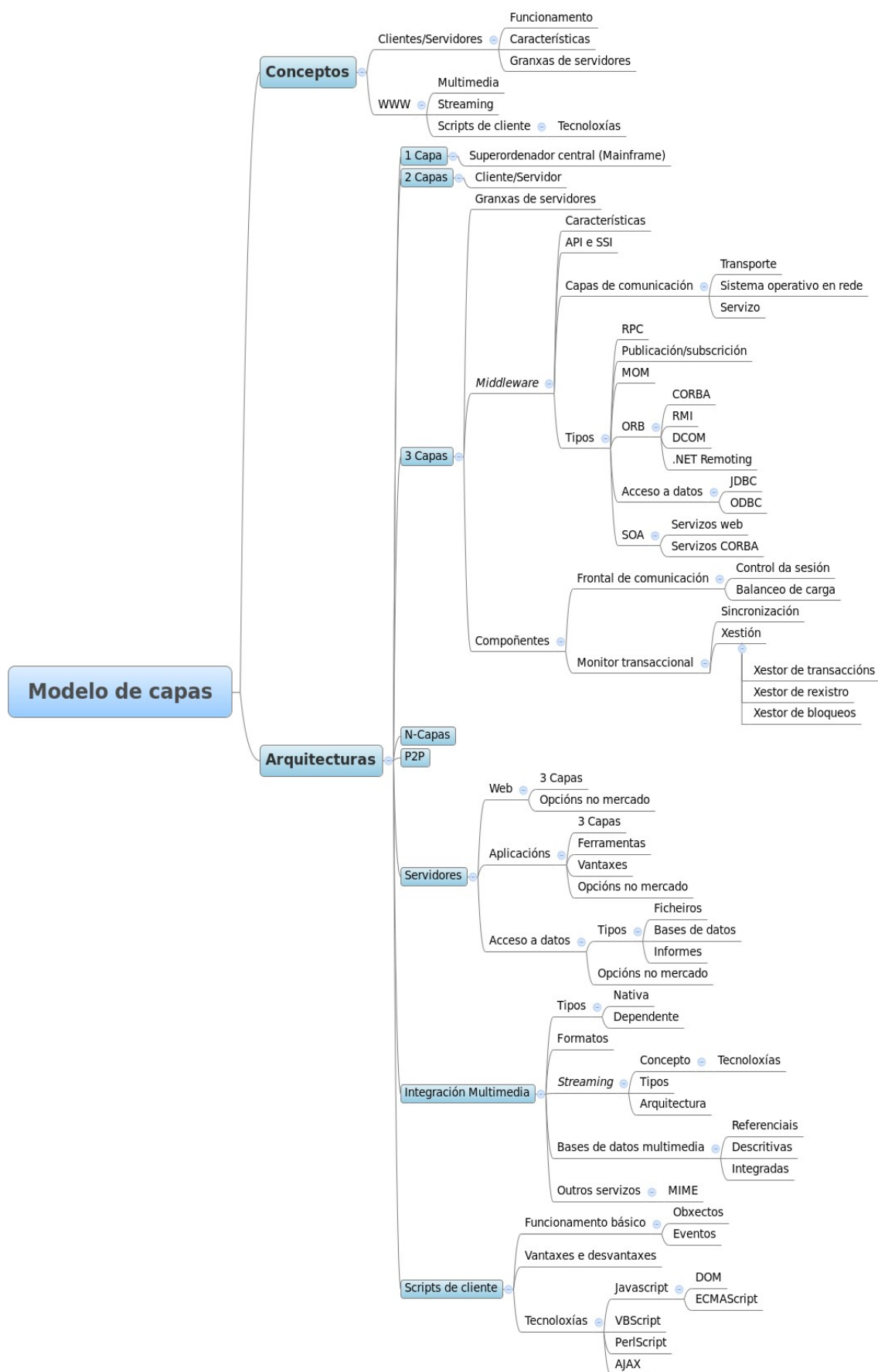
Las **tecnologías de *script*** más empleadas son Visual Basic Script, Javascript, con su evolución AJAX y PerlScript. El principal problema a la hora de seleccionar una tecnología cuando se diseña una página web es el

soporte que recibirá por parte de los navegadores, pues hay que recordar que los lenguajes de *script* serán en última instancia interpretados en el navegador.

- a) **Javascript.** Basado en el lenguaje Java, es una de los lenguajes de script de uso más extendido. Hay que señalar, que tiene aplicación con otras tecnologías además de la web como en documentos PDF o aplicaciones de escritorio. Para permitir la interacción con los elementos de un documento web este lenguaje dispone de una API que implementa el DOM (en inglés *Document Object Model*) o Modelo de Objetos para la Representación del Documento, estandarizado por el W3C (en inglés *World Wide Web Consortium*). En un intento por estandarizar este lenguaje surge el ECMAScript una especificación del lenguaje aceptado como estándar ESO,
- b) **Visual Basic Script.** Similar al Javascript en lo relativo a funcionamiento y estructura pero basado en Visual Basic. Tiene menor soporte dentro de los diferentes navegadores, excepto en el Internet Explorer.
- c) **PerlScript.** Basado en lenguaje C su uso no está tan extendido como las tecnologías anteriores aunque tiene menos limitaciones. Debido a esto fue derivando hacia lenguaje de servidor.
- d) **AJAX.** Acrónimo de Javascript Asíncrono y XML (en inglés *Asynchronous Javascript And XML*). Esta es una tecnología de *script* de cliente asíncrona, de suerte que puede realizar cargas de datos sin que afecten a la recarga de la página. AJAX es un conjunto de tecnologías que hace uso de:
 - 1) XHTML y hojas de estilo en cascada (CSS) para la estructura y diseño de los contenidos.
 - 2) El lenguaje Javascript como lenguaje de programación para funciones y definición del programa cliente.

- 3) El objeto *XMLHttpRequest* para intercambio de información asíncrona con el servidor. Por tanto, hace falta que el navegador soporte este objeto, siendo empleado en ocasiones el objeto *Iframe*.
- 4) XML y DOM como estándares asociados para intercambio de datos y manipulación del documento.

28.5. ESQUEMA



28.6. REFERENCIAS

José Antonio Destrezas.

Mundo IP. Introducción a los secretos de Internet y las redes de datos.
(2004).

Andrew S. Tanenbaum.

Redes de computadoras. (2003).

Sergio Luján Mora.

Programación de aplicaciones web: historia, principios básicos y clientes web. (2003).

TRADUCCIÓN DE FIGURAS:

Figura 1.- Arquitectura en capas

- Una capa
- Dos capas

Figura 2.- El Middleware en un sistema distribuido

- Aplicaciones distribuidas
- Servicios de la red

Figura 3.- Granja de Servidores

- Frontal de Comunicaciones
 1. Servidor de aplicaciones
 2. Gestión de transacciones
- Granja de Servidores

Figura 4.- Arquitectura en 3 capas con servidores web, de aplicaciones y base de datos

- Capa de servidor de aplicaciones

1. Granja de servidores
 2. Contenedor de programas de servidor
 3. Contenedor de objetos
 4. Sistema de mensajería
 5. Pool de conexiones
- Servidor Web
 1. Granja de servidores
 2. Lenguajes interpretados
 3. Seguridad

Figura 5.- Arquitectura de un servidor streaming

- Tiempo real
- Sistema de almacenamiento terciario
 1. Almacenamiento terciario
 2. En espejo

Autor: Juan Marcos Filgueira Gomis

**Asesor Técnico Consellería de Educación e O. U.
Colegiado del CPEIG**



29. ARQUITECTURA WEB EN .NET. ARQUITECTURA WEB EN J2EE.

TEMA 29. ARQUITECTURA WEB EN .NET. ARQUITECTURA WEB EN J2EE.

29.1. INTRODUCCIÓN Y CONCEPTOS

29.2 ARQUITECTURA WEB EN .NET

29.3 ARQUITECTURA WEB EN J2EE

29.4. ESQUEMA

29.5. REFERENCIAS

29.1. INTRODUCCIÓN Y CONCEPTOS

El desarrollo de aplicaciones, servicios web y otros componentes software tiene hoy en día dos vertientes principales, la plataforma .NET y la plataforma J2EE, o JEE nombre con el que es conocida actualmente al cambiar de versión. La competencia entre estas dos tecnologías es muy fuerte, pues proporcionan soluciones similares fuertemente soportadas por las compañías de uno y del otro bando.

.NET es la plataforma de desarrollo propuesta por la empresa Microsoft para el mundo de los servidores de aplicaciones que funciona como herramienta de diseño y programación, además proporciona un amplio conjunto de utilidades extendidas de apoyo al desarrollo en este tipo de entornos. Por su parte **JEE**, (en inglés *Java Platform, Enterprise Edition*) o Java EE, es una evolución de la plataforma Java para desarrollar y soportar componentes software según un conjunto de especificaciones de modo que puedan operar en un servidor de aplicaciones, incluyendo también herramientas de diseño y programación.

A pesar de que ambas plataformas persiguen el mismo objetivo, tienen una serie de particularidades o diferencias que se ven acentuadas por las guerras comerciales entre las empresas que las soportan. Mientras JEE

tiene soporte multiplataforma, .NET funciona sólo bajo la familia de Sistemas Operativos Windows. Mientras JEE se basa exclusivamente en el lenguaje Java, en .NET se permiten muchos lenguajes de alto nivel, aunque en la práctica los principales sean C# y VB .NET. JEE lleva más años de experiencia en el mercado, mientras que .NET es más reciente. Asimismo JEE presenta mayor soporte en cuanto a soluciones y posibilidades de software libre, que son muy escasas y de poca calidad en .NET. Con JEE se puede instalar una infraestructura de alto rendimiento de manera completamente gratuita.

29.2 ARQUITECTURA WEB EN .NET

.NET es, según la empresa Microsoft, una plataforma para el desarrollo de servidores, clientes y servicios. Representa un conjunto de tecnologías que tienen como núcleo principal el .NET Framework, un marco de desarrollo y componente software que puede instalarse en Sistemas Operativos de la familia Windows (Windows 2003, Vista, Windows 7, ...). Existe una versión adaptada para móviles disponible en Windows Mobile. La norma ESO/IEC 23271 recoge un conjunto funcional mínimo que deben cumplir los productos software desarrollados para que puedan funcionar dentro del marco de trabajo. Esta y más normas se recogen en los estándares:

- a) **Estándar ECMA-334.** Especificación del lenguaje C#. (2006).
- b) **Estándar ECMA-335.** Especificación del lenguaje de infraestructura común (CLI). (2010).

Por el contrario, otros componentes como ASP .NET, *Windows Forms* o ADO .NET no se encuentran estandarizados. Paralelamente, una vez publicados los documentos de especificación de la arquitectura .NET apareció el **Proyecto Mono** con el objetivo de implementar el marco de trabajo .NET Framework empleando código abierto, para a partir de ahí desarrollar aplicaciones para sistemas UNIX/Linux.

29.2.1 .NET Framework

Marco de trabajo que proporciona el conjunto de herramientas y servicios para el desarrollo de componentes software, aplicaciones, servidores y servicios web. Puede dividirse en tres bloques principales:

- 1) El **Entorno de Ejecución Común** (en inglés *Common Language Runtime* o CLR). Se encarga de la gestión de código en ejecución, control de memoria, seguridad y lo otras funciones relacionadas con el Sistemas Operativo.
- 2) La **Biblioteca de Clases Base** (en inglés *.NET Framework Base Classes*). Realizan la función de API de servicios a disposición de los desarrolladores para tareas como gestión de ficheros, mensajería, procesos en varios hilos, acceso a datos, encriptación, etc.
- 3) **Control de acceso a datos**, que permite realizar las operaciones de acceso a datos a través de clases y objetos del *framework* incluidos en el componente ADO.NET.
- 4) El **Motor de Generación de la Interfaz de Usuario**, que permite crear interfaces para aplicaciones de escritorio o web empleando componentes específicos como ASP.NET para web, *Web forms* para aplicaciones de escritorio o *Web services* para servicios web.

29.2.2 Entorno de Ejecución Común (CLR)

El Entorno de ejecución común o CLR es el encargado de gestionar el código en tiempo de ejecución. De manera análoga a la Máquina virtual de Java este entorno permite ejecutar aplicaciones y servicios web o de escritorio en cualquier cliente o servidor que disponga de este software. A diferencia de la Máquina virtual de Java el soporte de .NET es multilenguaje permitiendo C++, C#, ASP .NET, Visual Basic, Delphi, y muchos otros. Además permite integrar y heredar componentes entre diferentes lenguajes, con mayor o menor fortuna a la hora de sacar beneficio de lenguajes antiguos.

El entorno de desarrollo compila el código fuente en cualquiera de los lenguajes soportados a un código intermedio denominado **CIL** (en inglés *Common Intermediate Language*) de manera análoga al BYTECODE de Java. A este lenguaje intermedio se llega empleando la especificación CLS (en inglés *Common Language Specification*) donde se especifican unas reglas necesarias para crear el código intermedio CIL compatible con el CLR. Asimismo, el CLR dispone de compiladores como JIT (en inglés *Just In Time*) o AOT (en inglés *Ahead of Time*) adaptados a cada lenguaje.

JIT genera el código máquina real en cada máquina a partir de ese código intermedio consiguiendo independencia del hardware. Esta compilación se hace en tiempo de ejecución a medida que la aplicación o servicio invoca métodos o funciones. Para agilizar el procesamiento este código máquina obtenido en tiempo de ejecución se guarda en la memoria caché actualizándose tan sólo cuando se produce algún cambio en el código fuente, momento en el que se repite el proceso. Por el contrario, **AOT** compila el código antes de ejecutarse con lo cual logra un mayor rendimiento en ejecución pero menos independencia de la plataforma. En lo relativo a JIT suele distinguirse entre:

- 1) **Jitter estándar.** Compila el código CIL a nativo bajo demanda.
- 2) **Jitter económico.** No optimiza, traduce cada instrucción, así precisa menos tiempo y memoria de compilación.
- 3) **Prejitter.** Realiza una compilación estática de un componente software completo.

Las principales **ventajas** de este modelo de compilación son:

- ✓ La reutilización de componentes escritos en diferentes lenguajes en una misma aplicación o servicio web.

- ✓ **Modularidad** gracias a la implementación del patrón Interfaz para

cada componente o librería ya que será accesible desde cualquier lenguaje a través de su API (ASP, C#, Java, Phyton, etc.)

- ✓ **Integración multilenguaje**, ya que cada lenguaje con un compilador a CIL puede integrarse en la plataforma con lo cual cada componente en ese lenguaje puede integrarse una aplicación o servicio web .NET.
- ✓ **Seguridad**. Por el aislamiento del código de usuario respecto de los accesos a datos y otras partes críticas del Sistema Operativo.



Figura 1: Estructura multilenguaje del CLR

El CLR cumple además la función de proporcionar una amplia gama de servicios a las aplicaciones. A través de la API de cada servicio los componentes web pueden tener acceso a funcionalidades comunes, como:

- a) **Seguridad acceso al código o CAS** (en inglés *Code Access Security*). Controla qué tipo de operaciones puede realizar un código según se identifique en la firma del ensamblado o en el origen del código. Asimismo reconoce directivas de administración del sistema para componentes o a nivel de *host*. Cuando un componente trate de acceder a recursos protegidos del sistema se lanzará el CAS para comprobar los permisos, pero a este nivel no se pueden establecer comprobaciones dinámicas, como por ejemplo contra Bases de datos.
- b) **Atributos de protección del host o HPA** (en inglés *Host Protection*

Attributes). Mantiene una lista de atributos protegidos, denegando el acceso o modificación de los mismos. Algunos de estos atributos serían *SharedState*, para estados compartidos, *Synchronization*, para permitir la capacidad de sincronizar procesos en el *host* o *ExternalProcessmgmt* que indica si los procesos en el *host* se pueden controlar externamente a través de la API.

- c) **Dominios de aplicación.** Definen dominios aislados de código para restringir el acceso de los componentes software, creando una zona reservada para un subproceso. Por norma general el CLR crea para cada aplicación un dominio en tiempo de ejecución pero puede precisar dominios específicos para componentes DLL o externos.
- d) **Comprobación de la seguridad de tipos.** Reserva espacios de memoria para cada objeto según lo especificado para su tipo. Cuando el espacio es aleatorio o queda algún hueco fuera del espacio del objeto, quiere decir que ese objeto no tiene seguridad de tipos. Con la compilación JIT se realiza una comprobación en tiempo de ejecución para verificar si cada objeto tiene seguridad de tipos. Del mismo modo impide variables sin valores iniciales o *cast* no seguros.
- e) **Cargador de clases.** Permite cargar en memoria clases y tipos de datos a partir de la interpretación de los metadatos. Existe además la posibilidad de crear cargadores personalizados, aunque sólo para Java, ya que por motivos de rendimiento resulta más adecuado emplear un ensamblado con otros lenguajes. En la compilación el cargador realiza la función de evitar código innecesario a través de funciones *stubs* que sustituye con el código correcto bajo demanda.
- f) **Recolección de basura** (en inglés *Garbage Collector*). Este servicio se ejecuta de manera continua para buscar y eliminar de memoria los objetos que no sean referenciados o terminen el tiempo de espera de utilización.

- g) **Motor de interacción COM.** Realiza funciones de conversión de datos y mensajes o *marshaling* desde y hacia objetos COM, lo que permite la integración con aplicación *Legacy*.
- h) **Motor de depuración.** Permite realizar un seguimiento de la ejecución del código aunque mezcle diferentes lenguajes.
- i) **API multihilo** (en inglés *multithread*). Proporciona una API y las clases necesarias para gestionar la ejecución de hilos paralelos.
- j) **Gestor de excepciones.** Realiza la gestión estructurada e integración con *Windows Structured Exception Handling* de excepciones aunque el error provenga de diferentes lenguajes en un mismo componente e incluso en el código aún no ejecutado. Este código puede incluir excepciones SHE del tipo C++ o resultados HRESULTS típicos de COM.
- k) **API de la Biblioteca de Clases Base (BCB).** Interfaz con la BCB del marco de trabajo que realiza la integración del código con el motor de ejecución.

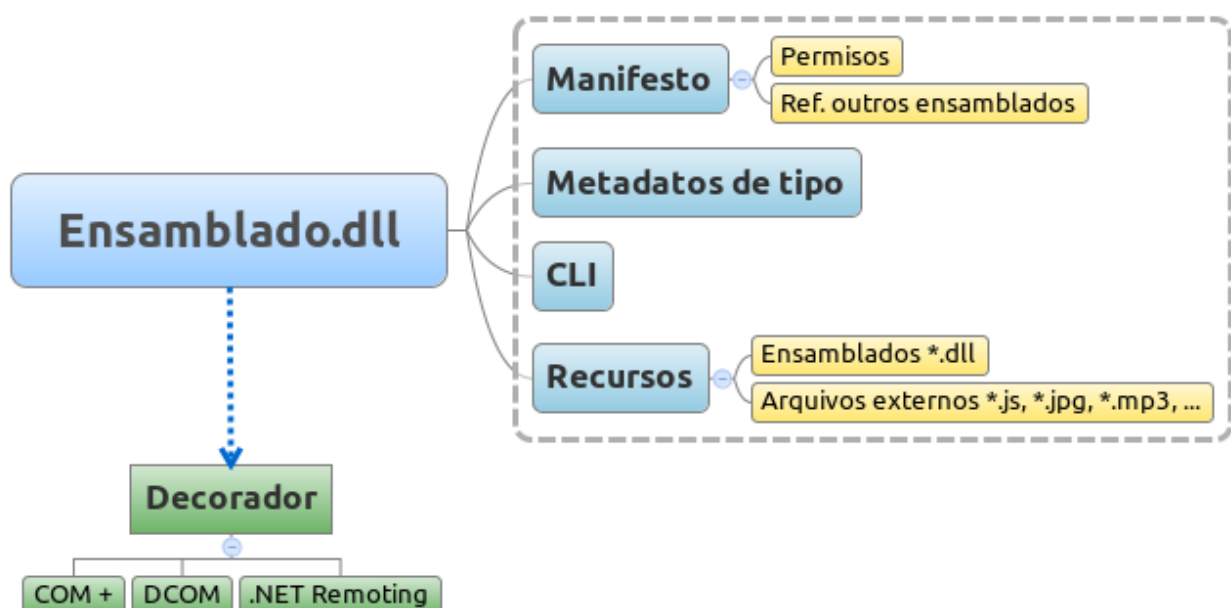


Figura 2: Ensamblados.

En el .NET Framework cuando se compila un programa o aplicación web se genera un archivo denominado **ensamblado** que contiene el código compilado al lenguaje intermedia CLI y un manifiesto con permisos y referencias a otros ensamblados, componentes software o servicios web. Son paquetes o librerías EXE o DLL destinadas al control de versiones, seguridad y comprobaciones de implementación al por menor. Los ensamblados llevan una indicación que define el entorno de ejecución en el que se debe lanzar: COM+, DCOM, .NET Remoting,...

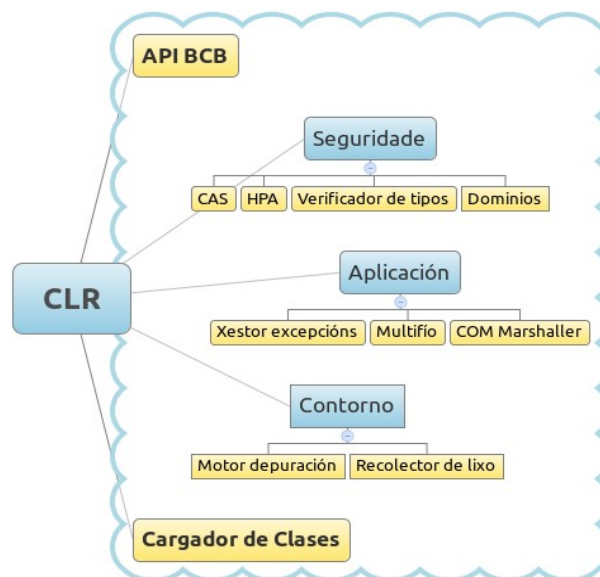


Figura 3: Servicios del CLR

29.2.3 Biblioteca de Clases Base (BCB)

La Biblioteca de Clases Base es una API de alto nivel para permitir acceder a los servicios que ofrece el CLR a través de objetos en una jerarquía denominada **espacio de nombres**. Agrupa las funcionalidades de uso frecuente permitiendo su redefinición. Se encuentra implementada en CIL por lo que puede integrarse en cualquier otro lenguaje. Es un conjunto de clases, interfaces y tipos valor que son la base sobre la que se crearán las aplicaciones, componentes y controles del .NET Framework. Permite

realizar operaciones como: soporte para diferentes idiomas, generación de números aleatorios, manipulación de gráficos e imágenes, operaciones sobre fechas y otros tipos de datos, integración con APIs antiguas, operaciones de compilación de código adaptada a los diferentes lenguajes de .NET, elementos para interfaces de usuario, tratamiento de excepciones, acceso a datos, encriptación, administración de memoria, control de procesos, etc.

Espacio de nombres	Utilidad y objetos
System	Tipos básicos, tablas, excepciones, fechas, colector de basura, etc.
System.Collections	Manipulación de colecciones como pilas, colas, <i>hash</i> , etc.
System.Fecha	Arquitectura ADO.NET (Objetos <i>DataSet</i> , <i>DataTable</i> , <i>DataRow</i> , <i>DataRowView</i> , ...)
System.IO	Manipulación de E/S archivos y otros orígenes de datos
System.Net	Gestión de comunicaciones de red (TCP/IP, <i>Sockets</i> , ...)
System.Security	Gestión de las políticas de seguridad del CLR
System.XML	Acceso y manipulación de datos en documentos XML con compatibilidad con el W3C (Transformaciones en <i>System.Xml.Xls</i> y serialización para servicios web en <i>System.Xml.Serialization</i>)
System.Web	Servicios para gestión de caché, seguridad y configuración para Servicios Web, estado de las sesiones e interfaces de usuario
System.Web.Services	Gestión de los requerimientos de Servicios Web
System.Web.UI	Controles para interfaces de usuario <i>HTMLControl</i> para mapeo de etiquetas HTML y <i>WebControl</i> para estructurar controles de usuario avanzados como <i>DataGrids</i>
System.Windows.Forms	Creación de la IU del cliente
System.Drawing	Acceso a funcionalidades gráficas básicas de la GDI+ (Funcionalidades avanzadas en <i>System.Drawing.Imaging</i> , <i>System.Drawing.Text</i> y <i>System.Drawing.Drawing2D</i>)

System.Reflection	Acceso a metadatos sobre los ensamblados, módulos, miembros, parámetros y otras entidades del código administrado
System.JSON	Proporciona compatibilidad basada en estándares JSON, notación de objetos JavaScript (en inglés <i>JavaScript Object Notation</i>)
System.Threading	Manipulación de procesos e hilos de ejecución
System.Text	Proporciona clases para manipular la codificación de caracteres UNICODE y UTF-8 conversión de bloques de caracteres en bloques de bytes y viceversa
System.Transactions	Contiene clases que permiten crear y administrar transacciones, admitiendo participantes distribuidos, notificaciones de fase e inscripciones duraderas
System.Resources	Proporciona clases e interfaces que permiten crear, almacenar y administrar recursos de localización
System.Runtime.Remoting	Proporciona la interfaz para acceso remoto y marco para la implantación de sistemas de componentes distribuidos
Microsoft.CSharp	Clases para realizar la compilación y ejecución de código en C# (Lo mismo para otros lenguajes)

Tabla 1: Principales espacios de nombres.

29.2.4 Control de acceso a datos.

El control de acceso a datos, documentos XML y servicios de datos en el marco .NET Framework se recoge en la arquitectura ADO .NET, como evolución del *ActiveX Data Objects*. Su orientación principal es el acceso a datos del gestor de base de datos relacional *SQL Server*, orígenes XML y orígenes de datos vía objetos OLE DB y ODBC. Las **conexiones** se realizan identificando los proveedores de datos a través de los objetos (Connection, Command, DataReader y DataAdapter). Una vez establecida la conexión entra en escena el principal elemento del marco, el *Dataset* que recoge los **resultados** cargados a partir de un origen. A su vez puede particularizarse con otros elementos de la base de datos con objetos como: *DataTable*,

DataRow, DataRow, DataColumn o *Constraint*. Los **objetivos** de diseño principales de este marco son:

- ✓ Soporte a la tecnología ADO previa.
- ✓ Integración con tecnologías basadas en XML.
- ✓ Soporte a modelo de arquitectura multicapa.

En las últimas versiones se incorpora el **Marco de Entidades** (en inglés *Entity Framework*) que permite realizar Consultas Integradas en los Lenguajes (en inglés *Language Integrated Query*) o **LINQ**.

Este marco permitirá emplear LINQ sobre muchos componentes de acceso a datos nuevos: *LINQ to SQL*, *LINQ to DataSet* y *LINQ to Entities*. Asocia una llave lógica a las entidades, dotando al modelo relacional o conceptual de orientación a objetos. Utilidades del marco de trabajo como **SQLMetal** permiten la generación automática de clases a partir de la base de datos o documentos XML.

29.2.5 Motor de Generación de Interfaces de Usuario

Aparte del marco de trabajo encargado de la generación de interfaces de usuario y servicios web sería la arquitectura ASP .NET. El conjunto de clases correspondientes se agrupan en los espacios de nombres: System.Web, System.Web.Services, System.Web.UI. Las páginas web desarrolladas con ASP .NET tienen la extensión **ASPX** y son conocidas con **Formularios Web** (en inglés *Web Forms*). Paralelamente a esta tecnología de presentación encontraríamos **Formularios Windows** (en inglés *Windows Forms*) para aplicaciones de escritorio y tecnologías para Móviles, siendo la primera la más empleada para aplicaciones de servidor. En el espacio System.Web.UI se recogen las dos clases principales de controles, los HTML para acceso directo a las etiquetas estáticas de estos lenguajes y los controles web que incorporan código de servidor dinámico. La arquitectura recomendada

emplea el modelo **Code-Behind** en el que se crea un archivo separado con el código de servidor, a diferencia de la arquitectura DNA para ASP anterior. Los **Controles de usuario** (en inglés *User Controls*) siguen la misma estructura que los Formularios Web, pero derivan del espacio `System.Web.UI.UserControl`, y se guardan en archivos **ASCX**, que deberían seguir también el modelo Code-Behind. El marco incorpora también elementos para control del estado y la sesión así como otros para seguridad, autenticación de usuarios, uso de papeles, uso del servicio Indigo o **WCF** (en inglés *Windows Communication Foundation*). Asimismo, permite la integración con AJAX, a través de la incorporación de un **Toolkit** en la aplicación, o **WPF** (en inglés *Windows Presentation Foundation*) basado en XALM y marco para Silverlight.

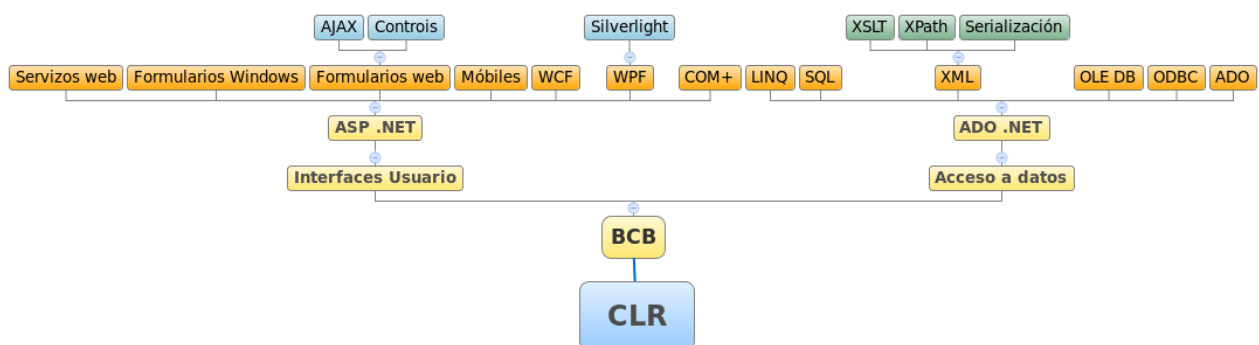


Figura 4: Arquitectura general

29.2.6 Niveles lógicos.

En los modelos y soluciones que propone esta estructura se establecen una serie de servicios genéricos presentes en la mayoría de las aplicaciones corporativas actuales. Esta división permite definir un diseño y una arquitectura específicos para cada nivel, facilitando el desarrollo y soporte de la aplicación.

1. **Servicios de usuarios.** Se encuentran en la primera línea de interacción con los usuarios y proporcionan la interfaz de acceso al

sistema que deriva en llamadas a los componentes del nivel de Servicios corporativos. En ocasiones se consideran dentro de este nivel procesos fuera de las interfaces de usuario, como procedimientos de control o automatizados que no requieren la presencia de un usuario.

2. **Servicios corporativos.** Encapsulan la lógica corporativa proporcionando una API de las funcionalidades básicas del sistema. Esto permite abstraer los servicios de usuario de la lógica corporativa y mantener diferentes servicios de usuario a partir de las mismas funcionalidades. Cada funcionalidad puede necesitar disponer de varios servicios corporativos.
3. **Servicios de datos.** Sería la parte más aislada del usuario, proporcionando el acceso a datos y a otros sistemas o servidores. Establecen diferentes API genéricas de las que pueden hacer uso los Servicios corporativos. Contienen una amplia gama de orígenes de datos y sistemas de servidor, encapsulando reglas de acceso y formatos de datos.

29.2.6 Soluciones de integración.

Con la tecnología .NET existen tres principales planteamientos de soluciones arquitectónicas:

- 1) **SOA** (en inglés *Service Oriented Architecture*). Entiende la comunicación entre aplicaciones y componentes como servicios, no necesariamente servicios web, demandados por clientes o subscriptores y proporcionados y publicados por proveedores.
- 2) **MOA** (en inglés *Message Oriented Architecture*). La comunicación se realiza por paso de mensajes forzando un modelo SOA distribuido.
- 3) **EAI** (en inglés *Enterprise Integration Application*). Especifica una serie de requerimientos de integración y comunicación en sistemas

regulados por los patrones de integración Mediación y Federación, donde un sistema EAI hace funciones de *Hub* o *bus* de comunicaciones.

29.3 ARQUITECTURA WEB EN J2EE

JEE representa un conjunto de especificaciones para plataformas de desarrollo basadas en lenguaje Java para servidores de aplicaciones en arquitecturas de múltiples capas. El **JCP** (en inglés *Java Community Process*) es el organismo encargado de validar los requisitos de conformidad para cada plataforma y aceptarla. Las plataformas JEE constan de los siguientes componentes:

- 1) Un conjunto de especificaciones.
- 2) Un test de compatibilidad o CTS (en inglés *Compatibility Test Suite*)
- 3) Una implementación de referencia para cada especificación.
- 4) Un conjunto de guías de desarrollo y buenas prácticas denominadas JEE Blueprints.

Las principales **especificaciones** que incluye JEE dan soporte a Servicios web, RPC basado en XML, Mensajería XML, despliegues, servicios de autorización, conexión remota RMI, JSP, JSF, JSTL, Servlets, Portlets, Applets, JavaBeans, esquemas XML, acceso a datos JDBC, documentación Javadoc, transformaciones XSL, etc...

El soporte multiplataforma del Java tiene su base en la **Máquina Virtual** (VM/JVM o KVM/CVM para móviles), una plataforma lógica capaz de instalarse en equipos con diferente hardware y Sistema operativo e interpretar y ejecutar instrucciones de código **Java bytecode**. La especificación de la VM también se recoge como especificación por la JCP y del mismo modo están disponibles test de compatibilidad. La forma más habitual para la VM es mediante un compilador JIT pero también permite interpretación. Del mismo modo se permite ejecución segura mediante el

modelo de las Java Applets. Programas de cliente que se ejecutan en una VM dentro del navegador después de descargar vía HTTP código del servidor, que se ejecuta en una *Sandbox* muy restringida.

Los componentes software web y de negocio dentro de esta tecnología se despliegan a través de **Contenedores** (en inglés *containers*). Los contenedores son implementaciones de arquitecturas JEE que proporcionan los servicios del servidor de aplicaciones a los componentes, incluyendo seguridad, acceso a datos, manejo de transacciones, acceso a recursos, control de estados, gestión del ciclo de vida y comunicaciones, entre otros. Antes de ejecutarse un componente software debe configurarse como un servicio JEE y desplegarse dentro de un contenedor. Los principales serían los contenedores web para Servlets y JSP, los contenedores EJB para componentes de la lógica de negocio, contenedores de aplicaciones cliente y contenedores de Applets para los programas de cliente y código de cliente para el navegador respectivamente.

Los principales **servicios** que proporciona JEE junto con sus respectivas API serían:

- 1) **HTTP y HTTPS.** Para control de las comunicaciones web y SSL a través de estos protocolos. Las API de servidor vienen dadas por los paquetes de clases Servlets y JSP y la de clientes en el paquete Java.Net.
- 2) **JDBC** (en inglés *Java Data Base Connection*). API de acceso a datos en sistemas gestores de bases de datos relacionales vía SQL. Por un lado aporta la interfaz para ser empleada por los componentes software y por otra la interfaz para que los proveedores puedan desarrollar los controladores específicos. Las versiones más recientes son las JDBC 3.0 y 4.0, que incluyen los paquetes *java.sql* y *javax.sql*.
- 3) **JSTL** (en inglés *Java Server Pages Standard Tag Library*). Proporciona las funcionalidades de para etiquetas en las páginas JSP.

- 4) **RMI-IIOP** (en inglés *Remote Method Invocation-Internet Inter-ORB Protocol*). Proporciona la API para permitir comunicaciones en aplicación distribuidas a través de JAVA RMI, como por ejemplo para acceder a componentes EJB. Los protocolos más habituales son JRMP, de RMI e IIOP, de CORBA.
- 5) **IDL** (en inglés *Java Interface Definition Language*). Permite la comunicación de clientes con servicios CORBA a través del protocolo IIOP, servicios SOAP o RPC.
- 6) **JNDI** (en inglés *Java Naming and Directory Interface*). Proporciona el servicio de nombres y directorios, indicando el contexto de cada objeto y las relaciones entre ellos. Se divide en dos interfaces, la API de programación y una SPI que permite conectar con proveedores de servicios de nombres y directorios siendo los principales LDAP, CORBA y RMI.
- 7) **JAXP** (en inglés *Java API for XML Processing*). Soporta el procesamiento de documentos XML que cumpla con los esquemas del W3C a través de DOM, SAX y XSLT.
- 8) **JMS** (en inglés *Java Message Service*). Proporciona la API de envío de mensajes para comunicarse con un MOM (en inglés *Message-Oriented Middleware*), una abstracción independiente del proveedor para comunicaciones entre sistemas.
- 9) **JavaMail**. Proporciona la interfaz para controlar el envío y recepción de correos electrónicos. Puede soportar el formato MIME gracias a su integración con marco de trabajo JAF.
- 10) **JAF** (en inglés *Java Beans Activation Framework*). API que proporciona el marco de trabajo para activación que soporta las peticiones de otros paquetes.
- 11) **JTA** (en inglés *Java Transaction API*). Orientada hacia el manejo de transacciones y a permitir la comunicación entre contenedor y

componentes del servidor de aplicaciones como los monitores transaccionales y los administradores de recursos.

- 12) **JAX-RPC** (en inglés *Java API fuere XML-based RPC*). Proporciona soporte para comunicaciones remotas de tipo RPC entre clientes y servicios web con los estándares HTTP y SOAP. Soporta otros estándares como WSDL, así como SSL y TTL para autenticación. El SAAJ (en inglés *SOAP with attachments API for Java*) añade la posibilidad de archivos o notas adjuntados con los mensajes.

Cada componente se denomina **Módulo** JEE de modo que una aplicación estará formada por un conjunto de módulos siendo cada uno un componente para un contenedor. Existen tres tipos de módulos:

- 1) **Archivos JAR** (en inglés *Java Archive*). Agrupación de archivos Java y recursos según el formato ZIP. Empaquetan componentes EJB según la estructura de directorios del código, añadiendo una carpeta especial, META-INF, con metadatos.
- 2) **Archivos WAR** (en inglés *Web Application Archive*). Agrupan en un único archivo una aplicación web, incluyendo Servlets, archivos JSP, contenido estático y otros recursos web.
- 3) **Archivos EAR** (en inglés *Enterprise Application Archive*). Agrupa en un único archivo varios módulos de una aplicación como archivos WAR o componentes EJB y otras librerías en archivos JAR empaquetados con sus respectivos recursos. Asimismo se incluye el descriptor de despliegue de la aplicación en la carpeta META-INF.
- 4) **Archivos RAR** (en inglés *Resource Adapter Archive*). Contiene un adaptador de recursos de manera análoga a un controlador JDBC y similar a los EAR, pudiendo ir contenido en un archivo de este tipo. El formato viene definido en la especificación JCA (en inglés *Java EE Connector Architecture*).

De manera general conviene considerar a la plataforma como JEE, si bien,

existen diferentes **ediciones**, siendo las principales:

- 1) **J2ME**. (en inglés *Java 2 Platform Micro Edition*). Para desarrollo de aplicaciones para dispositivos móviles, electrodomésticos y equipos PDA. Se desarrolló mediante el JPC bajo la especificación JSR 68.
- 2) **J2SE**. (en inglés *Java 2 Platform Standard Edition*). Para desarrollo de aplicaciones de uso general en estaciones de trabajo. Se desarrolló mediante el JPC bajo diferentes especificaciones según las versiones existentes: 1.4, 5.0 y 6.
- 3) **J2EE**. (en inglés *Java 2 Platform Enterprise Edition*). Para desarrollo de aplicaciones destinadas a servidores de aplicaciones para dar soporte a sistemas distribuidos en N capas. Estandarizada por el JPC a partir de la versión 1.4 acostumbra a denominarse JEE.

Para cada edición puede distinguirse entre la SDK (en inglés *Software Development Kit*), con el software y recursos destinados al desarrollo de aplicaciones y el JRE (en inglés *Java Runtime Environment*) con el entorno y librerías principales para permitir la ejecución de las aplicaciones.

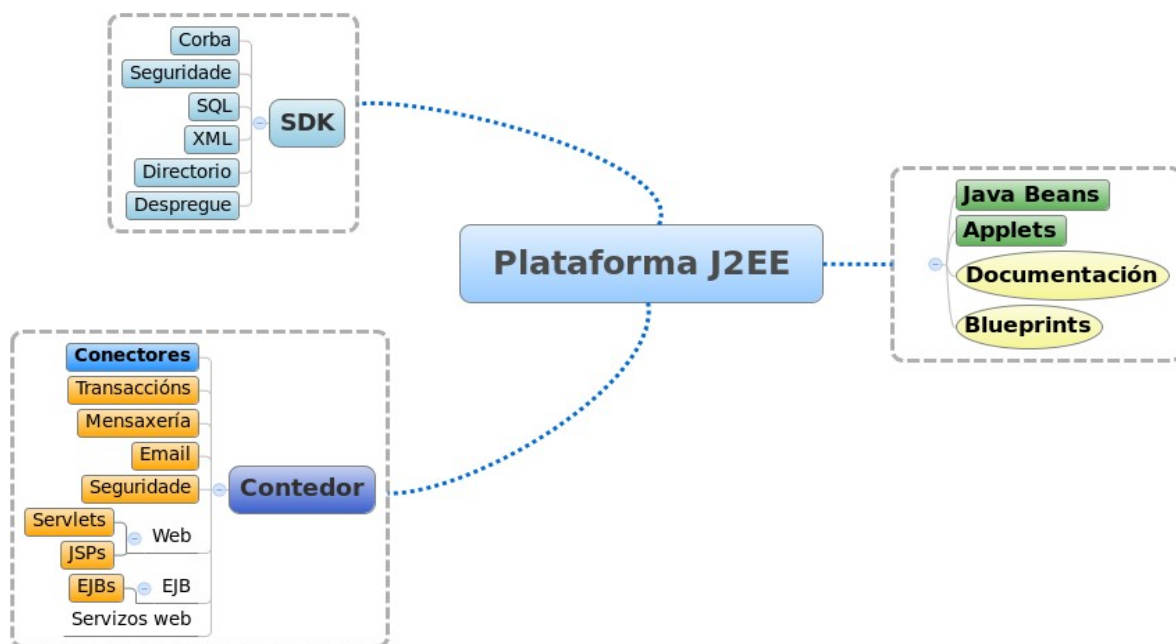


Figura 5: Plataforma J2EE.

29.3.1 Modelo de desarrollo

El modelo de desarrollo más habitual en la arquitectura JEE es un modelo separado en múltiples capas siendo el habitual un mínimo de tres, pero pudiendo llegar a 5 ó 7 según la complejidad del sistema. El objetivo es minimizar el solapamiento entre ellas para que los cambios y modificaciones se limiten al mínimo necesario con el ideal de que se pueda cambiar una de las múltiples capas sin tener que modificar el resto. Se mejora la sostenibilidad, crecimiento del sistema y la reutilización de componentes en el mismo y entre sistemas. Asimismo se permite una mayor heterogeneidad de clientes o elementos de cliente y presentación al modificar sólo la capa más próxima al usuario. El diseño del modelo es análogo a soluciones en .NET pero la implantación diferente. Las 5 capas más habituales se describirán a continuación.

29.3.1.1 Capa de cliente.

Agrupar los elementos de la interfaz de usuario más próximos al cliente. Ejemplos de estos elementos serían el código (X)HTML/XML y Javascript, los Applets, archivos de recursos y tecnologías RIA. Los tipos de aplicaciones cliente más habituales serían los navegadores web, las aplicaciones de escritorio y actualmente cobran fuerza las aplicaciones para dispositivos móviles. Un aspecto importante en este modelo es garantizar que los EJB de la lógica de negocio sean accesibles tan sólo desde interfaces remotas a través del patrón *SessionFacade*. La variedad de interfaces actual hace que aparezcan *frameworks* de generación dinámica de los mismos basados en el lenguaje **XUL** (en inglés *XML User-Interface Language*), basada en XML. Permite incrustar XHTML y otros lenguajes como MathML o SVG además de CSS. Existen varias alternativas de librerías XUL como Luxor, XWT, Thinlets o SwingML.

29.3.1.2 Capa de presentación.

Contiene toda la lógica de interacción directa entre el usuario y la aplicación. Se encarga de generar las vistas más acomodadas para mostrar la información a través de formatos y estilos adecuados. Se componen de una serie de Servlets y páginas JSP que se encargan de devolver el código que irá a la capa de cliente después de comunicarse con la capa de lógica de negocio para obtener los resultados. Puede localizarse en una aplicación de escritorio o en un contenedor web. Además de ensamblar las diferentes vistas, controla el flujo de navegación y hace funciones de autenticación, permisos de acceso y autorización de usuarios, etc... El patrón más habitual en esta capa será el MVC (en inglés *Model View Controller*). Entre las tendencias actuales se encuentran implementaciones de este modelo como Swing o JFace para aplicaciones de escritorio, mientras que dentro de los *frameworks* web se encontrarían Struts, JSF, Tapestry, Expresso y muchos otros. Siendo Struts una especie de estándar de hecho. Estos *frameworks* además incorporan otros servicios como etiquetas personalizadas JSTL para interfaces de usuario, manejo de XML, acceso a datos, modelos, filtros, etc.

29.3.1.3 Capa de lógica de negocio.

Contiene los componentes de negocio reutilizables EJB o POJO, que representan el conjunto de entidades, objetos, relaciones, reglas y algoritmos del dominio o negocio en el que opere el sistema. En esta capa la solución POJO es una opción sencilla que puede mezclar elementos de las capas de integración y datos, mientras que los EJB distinguen los objetos de sesión y las entidades, recomendado en los Blueprints de Sun, emplazando cada uno en su correspondiente capa. El patrón básico en esta capa será el *SessionFacade* donde un único Bean de sesión se encarga de recibir las llamadas de cliente-presentación y dirigir las dentro del contenedor de EJB aislando esta capa.

De manera análoga se establece el modelo de los Bean de mensajería, que realizan comunicación asíncrona mediante JMS en un servidor MOM (en inglés *Messaging Oriented Middleware*), que puede ser un servidor externo

al servidor de aplicaciones. También funciona con un patrón Fachada centralizando las llamadas remotas.

29.3.1.4 Capa de Integración.

Agrupar los componentes encargados del acceso a datos, sistemas *legacy*, motores de reglas de *workflow*, acceso a LDAP, etc... Pueden realizar cambios de formato en la información, pero transformaciones más complejas deberían realizarse en la capa de lógica de negocio, restringida ésta a la lógica de acceso a datos o DAO (en inglés *Data Access Objects*) y los encapsuladores de datos y entidades VO (en inglés *Value Object*). Los VO pueden implementarse como POJO o EJB de entidad. Como ocurría anteriormente en el caso de los POJO se gana en facilidad pero se pierden servicios y funcionalidades como los de persistencia. Los EJB suman complejidad, pero mejoran el rendimiento en memoria. En lo tocante al acceso a datos aparecen las siguientes alternativas:

- 1) **JDBC.** Para POJO o Beans de entidad con control de persistencia. Es una solución sencilla, con pocas funcionalidades pero que hace uso de una API de uso extendido.
- 2) **DAO.** Va un paso más allá que el JDBC incorporando interfaces para abstraer el acceso a datos y hacerlo independiente del lenguaje del gestor. Cada interfaz tendrá una implementación diferente para cada gestor de bases de datos.
- 3) **Frameworks de persistencia.** Hacen las funciones de motores de correspondencia de objetos a bases de datos relacionales definiendo entidades y relaciones vía XML. Realizan gran parte de las funciones de acceso a datos automáticamente. Las soluciones de uso más extendido son los *frameworks* Hibernate, iBatis, TopLink, JPA o a través de EJB.
- 4) **JDO** (en inglés *Java Data Objects*). Sistema de persistencia estándar a partir de una especificación JEE, añadiendo además de la correspondencia entre el modelo relacional y los objetos la

posibilidad de permitir definir los objetos sobre la base de datos. Las implementaciones de uso más extendido son OJB, XORM, Kodo JDO o LiDO.

29.3.1.5 Capa de sistemas de información.

Se encuentra integrada por los sistemas de bases de datos, ficheros, sistemas 4GL, ERP, Data Warehouse, Servicios web y cualquier otro sistema de información de la organización. En esta capa irían los conectores para diferentes sistemas de información heterogéneos y los propios recursos que integran los sistemas de información. Las soluciones más habituales se enumeran a continuación.

- 1) **JCA** (en inglés *J2EE Connector Architecture*). Define una interfaz de acceso común independiente del sistema, con la misma API para todos. Se basa en el concepto de adaptador de recursos, siendo cada adaptador un controlador específico para un sistema de información. Las operaciones básicas que define la especificación son: gestión de las conexiones de acceso a JCA, seguridad, transacciones, multiproceso, paso de mensajes y portabilidad dentro de los servidores de aplicaciones.
- 2) **JMS** (en inglés *Java Message Service*). El servicio de mensajes Java emplea colas de mensajes para el traspaso de información entre componentes software estableciendo una infraestructura MOM con dos modelos de API, Punto a punto, entre dos únicos clientes o Publicador/subscriptor donde varios clientes según su papel envían o leen mensajes.
- 3) **Servicios web**. Permiten la comunicación entre sistemas heterogéneos a través del acceso a la URL de aplicaciones empleando protocolos basados en XML como SOAP o SAAJ. Los clientes acceden al servicio a partir de su interfaz definida ante WSDL (en inglés *Web Service Definition Language*) o insertada en alguno

registro de servicios web.



Figura 6: Modelo de desarrollo en capas.

29.3.2 Servidores de aplicaciones.

El servidor de aplicaciones será el encargado de soportar la mayoría de las funcionalidades y servicios de la tecnología JEE, siendo el núcleo de esta arquitectura. Cuando un servidor de aplicación implementa la tecnología JEE tiene que proporcionar todos los componentes definidos en la especificación y por tanto cualquier aplicación JEE podrá desplegarse y ejecutarse en el mencionado servidor.

El servidor de aplicaciones dispondrá de diferentes contenedores para Applets y aplicaciones clientes, web y EJB, siendo estos últimos los que se encargarán de operar con la lógica del dominio, gestión de transacciones, persistencia, control del flujo, etc.

- Tomcat.** Sin presentar todas las funcionalidades de un servidor de aplicaciones, este servidor libre de Apache incorpora el servidor web Apache y soporte para JSP y Servlets con el contenedor Catalina.

Presenta diferentes módulos de soporte de aplicación como seguridad SSL, SSO, JMX, AJP, JSF, conector Coyote para peticiones HTTP, soporte para Comet, Colector de basura reducida así como herramientas web para despliegue y administración.

- b) **JBoss**. Uno de los servidores de aplicaciones libres de uso más extendido compuesto por un Contenedor de Servlets para JSP y Servlets y un Contenedor de Beans. A diferencia de Tomcat implementa todo el conjunto de servicios especificados por JEE. Como contenedor de Servlets emplea una adaptación de Tomcat o el contenedor Jetty. Entre los módulos y funcionalidades que soporta destaca que permite la creación de cluster, soporte EJB, JMX, Hibernate, JBoss AOP para dotar a clases Java de persistencia y funcionalidad transaccional, sistema caché, JSF, Portlets, JMS, Servidor de correo, gestión de contenidos foros y portales, entre otras muchas.
- c) **Geronimo**. Otro producto libre de Apache, compatible con JEE que incluye JDBC, RMI, JM, Servicios web, EJB, JSP, Servlets y otras tecnologías. La principal característica de este servidor es que integra un gran número de otras soluciones ya existentes: Tomcat y Embarcadero como contenedores web, OpenEJB como contenedor de Servlets, OpenJPA, Apache Axis, Apache CXF y Scout Apache para servicios web, Derby para el acceso a datos, y WADI para establecer clusters y balanceo de carga, entre otros.
- d) **JonAS**. Otra alternativa libre a JBoss, aunque no soporta por completo JEE. Permite integración con Tomcat o Jetty como contenedores web y tiene contenedor de EJB. Entre módulos y servicios incorpora: Xplus, Hibernate, TopLink, OpenJPA, JORAM como implementación de JMS, varios protocolos RMI (IIOP, JRMP, IRMI), soporte LDAP, servicios web Axis y otros muchos.
- e) **Glassfish**. Alternativa libre de Sun, ahora Oracle, que tiene como base el *framework* para persistencia Toplink. Incorpora además

módulos para soporte EJB, JAX-RS, JSF, RMI, JMS, servicios web, en la línea de los anteriores, y novedades como Apache Félix, una implementación de OSGi (en inglés *Open Services Gateway*) y Grizzly que hace uso de la nueva API de Java de E/S (NIO) para mejorar la escalabilidad.

- f) **WebSphere.** Alternativa comercial de IBM con una versión de libre distribución. La versión libre, más ligera, se basa en el servidor Geronimo diferenciándose de este en que incluye soporte para DB2, Informix, soporte RAC de Oracle y otras bases de datos así como mejores librerías para XML. Otras tecnologías serían: los Servlets SIP (en inglés *Session Initiation Protocol*) que utilizan elementos multimedia en tiempo real, mensajería instantánea y juegos on line; el *framework* Spring; protocolos de seguridad Kerberos y SAML. La diferencia con otros servidores es que posee herramientas de administración más avanzadas, sobre todo para sistemas en cluster y soporte para *mainframes*.
- g) **Weblogic.** Alternativa comercial de Oracle basada en Glassfish, incorporando servicios del Weblogic server sobre la JVM JRockit. En concreto Weblogic Server proporciona los Servicios web Oracle WebLogic Server Services Web, la Application Grid como solución de *grid* de datos, soporte de conectividad con Tuxedo (WTC), soporte de RAC para Oracle, SAML, una API de integración con .NET a JMS.NET, Spring y el *framework* de diagnosis WLDF.
- h) **Coldfusion.** Alternativa comercial de Adobe de las más valoradas actualmente, diferenciándose por el soporte a tecnologías RIA principalmente Flash. Implementa parte de los servicios JEE pero puede integrarse con otros servidores de aplicaciones como WebSphere o Jboss, pudiendo desplegarse como aplicación Java. Además lleva incorporado el servidor de aplicaciones Adobe JRun. Destaca por el soporte en tecnologías AJAX, Flex, PDF, RSS, Flash

Remoting, integración .NET y herramientas de administración avanzadas.

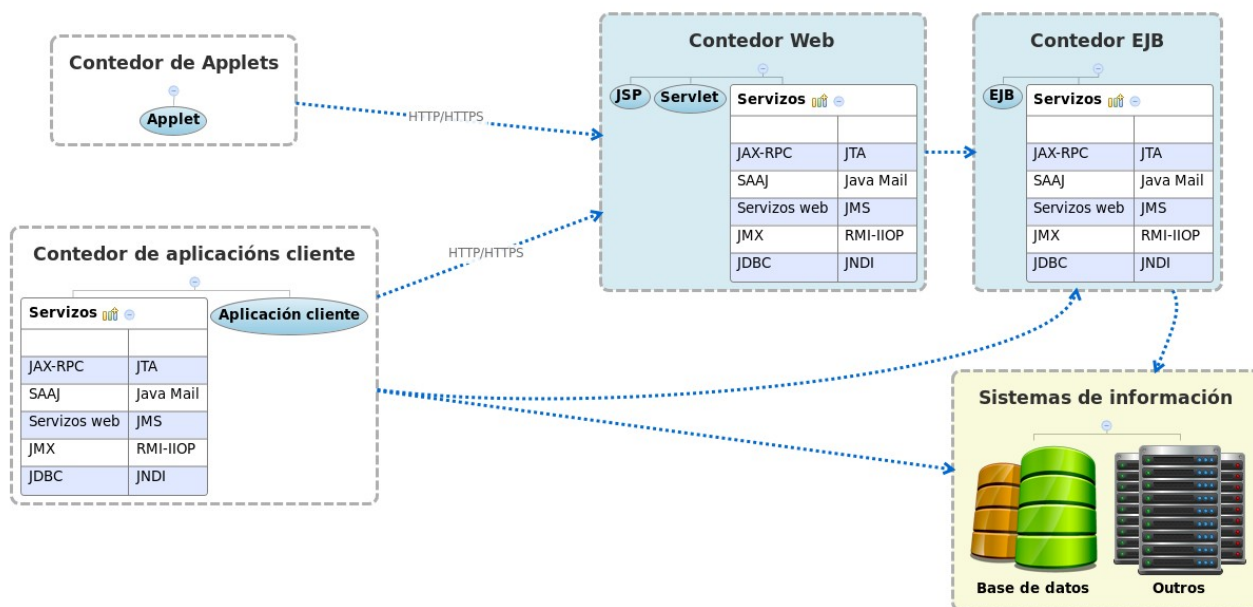
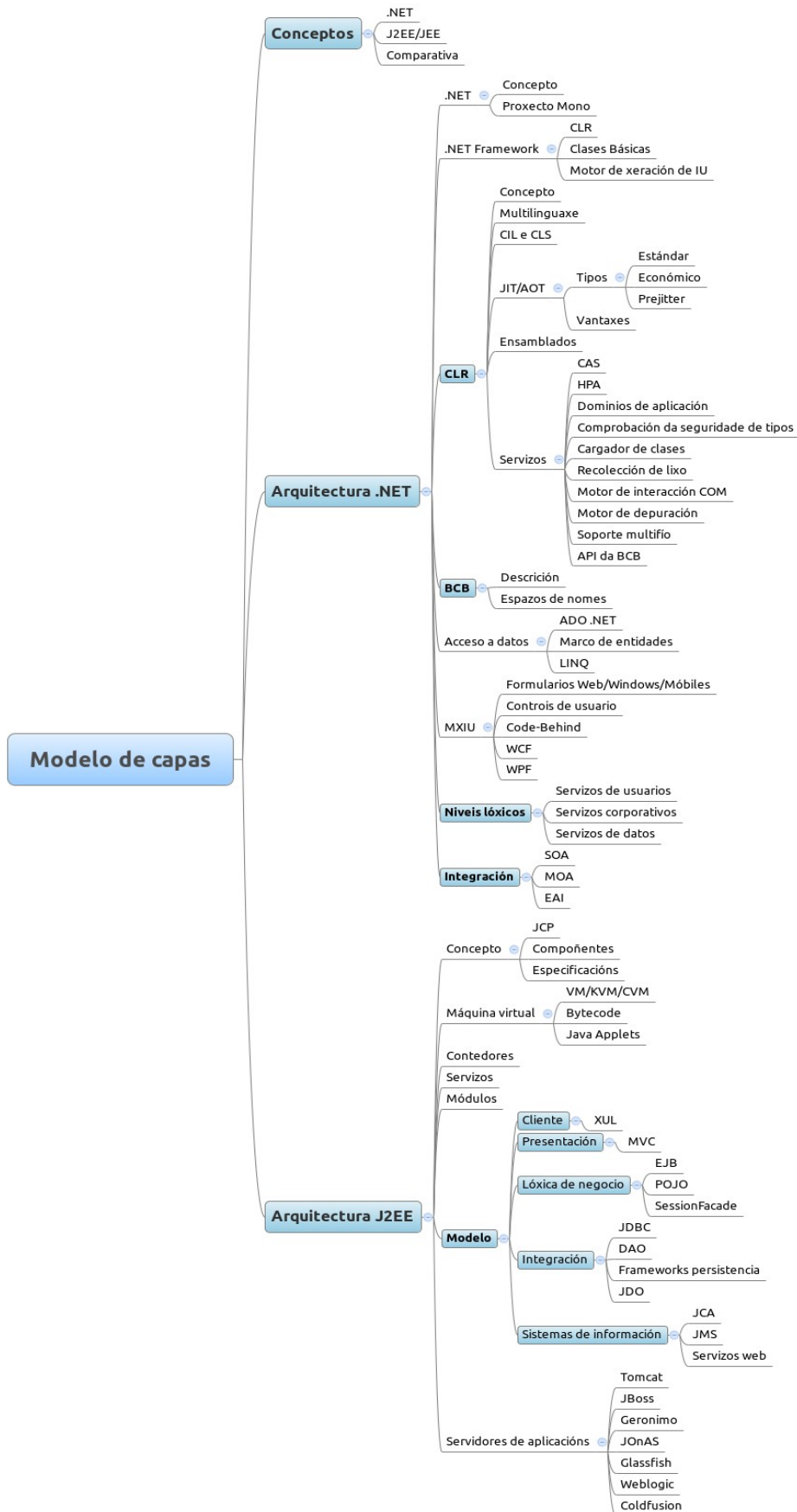


Figura7: Arquitectura J2EE

29.4. ESQUEMA



TRADUCCIÓN DE TEXTO DE FIGURAS:

FIGURA 1: ESTRUCTURA Multilenguaje de CLR

- Estación de trabajo

FIGURA 2: ENSAMBLADOS

- Manifiesto. Otros ensamblados
- Archivos externos

FIGURA 3: SERVICIOS DE CLR

- Seguridad
- Gestor de excepciones
- Multihilo
- Entorno
- Colector de basura

FIGURA 4: ARQUITECTURA GENERAL

- Controles
- Servicios web
- Móviles

FIGURA 5: PLATAFORMA J2EE

- Contenedores:
 1. Seguridad
 2. Despliegue
 3. Transacciones
 4. Servicio web

FIGURA 6: MODELO DE DESARROLLO EN CAPAS

- 3-Lógica de Negocio
- Servidor de aplicaciones
- Transacciones
- Ficheros
- Servicios web

FIGURA 7: ARQUITECTURA J2EE

- Contenedor
- Servicios
- Otros

29.4 ESQUEMA

- Proyecto Mono. Multilenguaje. Motor de generación de IU. Ventajas. Recolección de basura. Soporte Multihilo. Espacios de nombres. Controles de usuario. Servicios. Componentes. Especificaciones. Contenedores. Lógica de negocio. Servidores de aplicaciones

29.5. REFERENCIAS

Varios autores.

Biblioteca MSDN de Microsoft. (2003).

Jef Ferguson y otros.

La biblia de C#. (2003).

Benjamín Aumaille.

J2EE. Desarrollo de aplicaciones Web. (2002).

I. Singh, B. Stearns y otros.

Designing Enterprise Applications with the J2EE Platform. (2002).

Autor: Juan Marcos Filgueira Gomis

Asesor Técnico Consellería de Educación e O. U.

Colegiado del CPEIG

30. ARQUITECTURA SOA. SERVICIOS WEB. TECNOLOGÍAS XML.

TEMA 30. ARQUITECTURA SOA. SERVICIOS WEB. TECNOLOGÍAS XML.

30.1 INTRODUCCIÓN Y CONCEPTOS

30.2 ARQUITECTURA SOA

30.3 SERVICIOS WEB

30.4 TECNOLOGÍAS XML

30.5 ESQUEMA

30.6 REFERENCIAS

30.1. INTRODUCCIÓN Y CONCEPTOS

Los sistemas actuales tienen una gran complejidad debido a la integración de múltiples componentes heterogéneos. La comunicación y relación entre estos componentes es uno de los grandes problemas actuales siendo **SOA** (en inglés *Service Oriented Architecture*) uno de los actuales modelos de solución. Esta arquitectura entiende la comunicación entre aplicaciones y componentes como servicios, no necesariamente servicios web, demandados por clientes o subscritores y proporcionados y publicados por proveedores. Las arquitecturas para servidores de aplicaciones de uso más extendido como .NET y JEE acostumbran a definir una **capa de integración** que agrupa los componentes encargados del acceso a datos, sistemas *legacy*, motores de reglas de workflow, acceso a LDAP, etc. Para la comunicación de los componentes de esta capa existen varias soluciones como JCA, JMS y servicios web, está última una de las más aceptadas actualmente.

Los **Servicios web** permiten la comunicación entre sistemas heterogéneos a través del acceso a la URL de aplicaciones empleando protocolos basados en XML como SOAP o SAAJ. Los clientes acceden al servicio a partir de su interfaz definida en presencia de WSDL (en inglés *Web Service Definition*

Language) o insertada en algún registro de servicios web.

El uso de XML se convierte en un estándar de integración, siendo la base de las comunicaciones en esta capa, tanto para estructurar como para almacenar e intercambiar información, extendiendo su uso a otros ámbitos. Las **tecnologías XML** son un conjunto de módulos que ofrecen servicios como: XSL/XSLT para diseño de documentos, Xpath como lenguaje de rutas para acceso a documentos, el lenguaje de consulta XQL, y otros como XLink o XPointer.

30.2 ARQUITECTURA SOA

SOA define una arquitectura orientada a servicios que busca simplificar el modelo de integración de sistemas distribuidos heterogéneos. En esta arquitectura los componentes publican e invocan servicios en la red a través de mecanismos de comunicación como JCA, JMS, SOAP, RPC o Servicios web. Los servicios son funcionalidades de la lógica de negocio que pueden invocarse de manera remota para obtener un resultado. Se definen en presencia de una interfaz explícita, como por ejemplo a través de WSDL, independiente de su implementación empleando estándares de comunicación basados en XML. SOA define tres **bases** fundamentales:

- 1) **Orientación al intercambio de mensajes.** La base del sistema es la comunicación entre los nodos del sistema.
- 2) **Abstracción de componentes.** Cada sistema se reduce a su interfaz y el conjunto de servicios que define, con lo cual permite la integración entre cualquier tipo de sistema.
- 3) **Metadatos.** Descripciones e información asociada a servicios y mensajes, mejorando la capacidad semántica del sistema.

A nivel lógico los principales componentes en una arquitectura SOA son:

- a) **Servicios.** Entidades o funcionalidades lógicas definidos en interfaces públicas, que pueden o no requerir autenticación.

- b) **Proveedor de servicios.** Componente software que implementa un servicio y publica su interfaz.
- c) **Cliente de servicios.** Componente software que invoca un servicio de un proveedor.
- d) **Localizador de servicios.** Proveedor de servicios que registra las interfaces y permite a los clientes buscar en el registro y acceder a su localización.
- e) **Servicio de interconexión.** Proveedor que comunica solicitudes de servicio a otros proveedores.

El concepto de BPM o Gestión de procesos de negocio (en inglés *Business Process Management*), está muy relacionado con SOA. BPM es un modelo de gestión centrado en procesos de negocio y de cómo integrar sus funcionalidades en sistemas heterogéneos. A partir de la identificación y gestión de los procesos de la organización puede implantarse una solución BPM a través de una arquitectura SOA. Fruto de esta idea aparecen soluciones como:

- ✓ **BPMN.** Nota para el modelado de procesos de negocio.
- ✓ **BPEL.** Lenguaje de ejecución de procesos de negocio con servicios web para la orquestación de servicios. Generalmente se realiza una conversión de BPMN a BPEL.
- ✓ **BPEL4WS.** Lenguaje de definición y ejecución de procesos de negocios empleando servicios web (en inglés *Business Process Execution Language for Web Services*). BPEL4WS es resultado de la convergencia de WSFL (en inglés *Web Services Flow Language*) y XLANG, permitiendo componer Servicios web como servicios compuestos denominados Servicios de negocio.

Arquitectura SOA

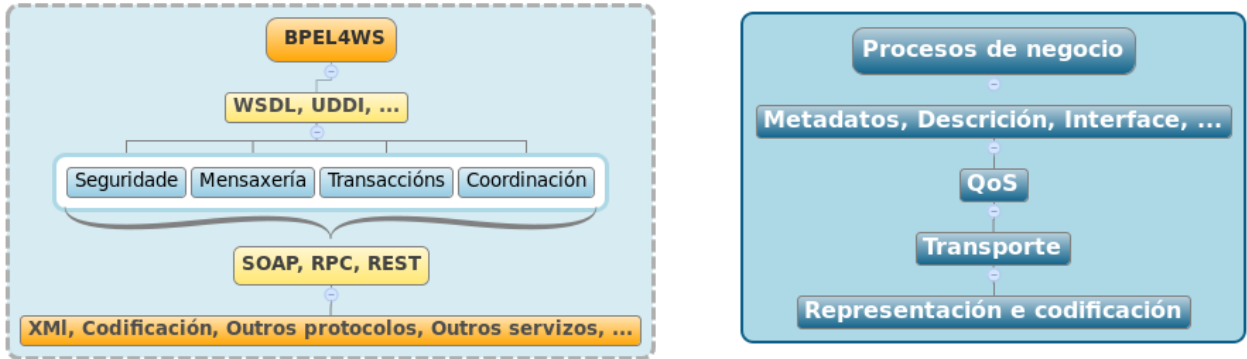
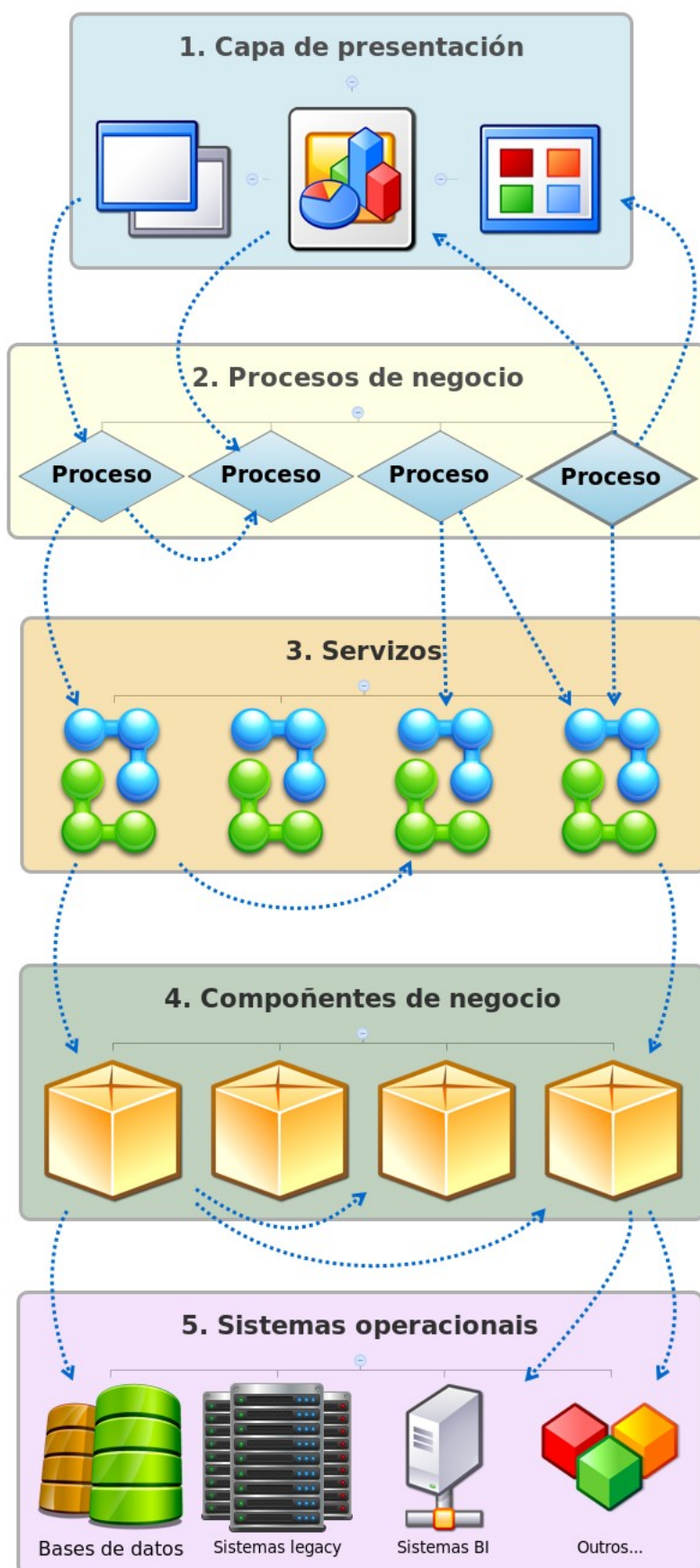


Figura 1: Arquitectura SOA.

La integración en la arquitectura SOA de los BPM permite establecer lo que se da en llamar **SOA Governance**, una estructura para la toma de decisiones y establecimiento de responsabilidades en la organización a través de la implantación de políticas, monitorización de servicios, incorporación de buenas prácticas, principios arquitectónicos, avance continuo de los procesos de negocio, etc. en definitiva análisis y diseño de soluciones que permitan cumplir con éxito la implantación de SOA en una organización.

En el aspecto **conceptual SOA** describe una serie de guías o patrones para servicios alineados con un modelo de negocio. Un modelo conceptual de SOA permite definir un diseño en múltiples capas donde los servicios se relacionan con procesos de negocio y sistemas de información. La división más habitual considera 7 capas diferenciadas, que se pueden ver gráficamente en la Figura 2:

- 1) **Capa de Presentación.** Interfaces de usuario en sitios web, aplicaciones y portales que invocan funcionalidades de los procesos de negocio.



6 Capa de Integración (ESB)

7 Capa de SOA Governance

- 2) **Capa de Procesos de negocio.** Representa los procesos y flujos operativos o workflows que invocan los clientes desde la capa de presentación u orquestación de servicios. Los procesos por norma general se representarán con BPEL y se implementarán con alguna herramienta de transformación.
- 3) **Capa de Servicios.** Funcionalidades de los componentes de la lógica de negocio que se publican para uso de los clientes. Se referencian a partir de la interfaz siendo transparentes a su implementación.
- 4) **Capa de Componentes de negocio.** Son los encargados de proporcionar las funcionalidades que se publicarán en los servicios así como cualquier otra intermedia o común al sistema. A este nivel irían los servidores de aplicaciones, otros servicios web, aplicaciones, paquetes y librerías.
- 5) **Capa de Sistemas operacionales.** En este nivel irían los sistemas de información de la organización, sistemas *legacy*, sistemas CRM o ERP, aplicaciones de BI, etc...
- 6) **Capa de Integración.** Agiliza la integración de servicios a través de sistemas tipo Buses de Servicios Empresariales o ESB, que realizan funciones de enrutamiento, monitorización y administración, transformaciones de los mensajes, etc... dentro del área de comunicaciones.
- 7) **Capa de SOA Governance.** Realiza funciones de administración, monitorización y control de la calidad del servicio en áreas como seguridad, disponibilidad y otros factores generales no recogidos en la capa de integración.

Existen **patrones de diseño** tomando como punto de partida esta arquitectura, se trata de patrones para Servicios web y patrones **POSA** (en inglés *Service-Oriented Architecture Patterns*). Algunos de los principales son:

- **Service Oriented Architecture.** Patrón que define la arquitectura SOA estableciendo reglas, relaciones y dependencias entre los componentes del sistema. Permite buscar servicios dinámicamente con independencia de la plataforma y sin requerir implementación, con transparencia. Este patrón es una variante ampliada del **Broker Pattern** de POSA. En este patrón un Servicio o nodo intermedio ayuda a localizar el servicio y puede obligar a realizar todas las comunicaciones a través de él o bien una vez establecida dejar que esta sea directa entre el cliente y el servicio.
- **Architecture Adapter.** Patrón genérico que facilita la comunicación entre diferentes arquitecturas gracias a la independencia de usar XML/SOAP y la generación de clases proxy. Este patrón es implementado por *frameworks* para Servicios web como Apache Axis (Java).
- **Service Directory.** Facilita la localización de Servicios web a partir de una especificación fuerte de las interfaces a través del catálogo UDDI de interfaces WSDL.
- **Service Factory.** Permite la selección de servicios del proveedor aislando el código de comunicación UDDI. Del mismo modo el patrón de extendido Service Factory Cache hace funciones de caché en el servicio. Simplifica en parte a API del patrón Service Directory.
- **Service Facade.** Proporciona un servicio web controlador que actúe como punto de entrada de la lógica de negocio u objeto de fachada. Puede emplear simultáneamente otros mecanismos de comunicación como CORBA.
- **Event Monitor.** Se emplea para notificar que un Servicio web de larga duración invocado remotamente completa la solicitud. Cuando el Servicio no dispone de mecanismos de notificación hace falta establecer un intermediario.
- **Business Object.** Un BO engloba un concepto del dominio, equiparable a un VO para entornos distribuidos.

- **Business Process.** Un BP engloba un proceso de la lógica de negocio, representando la jerarquía formada por las diferentes implementaciones de sus funcionalidades y la interfaz del servicio.
- **Asynchronous Business Process.** Este patrón se encarga de gestionar la llamada y notificación de respuesta al cliente cuando estas pueden ser de larga duración.
- **Business Object Collection.** Agrupa diferentes procesos de negocio en un mismo BOC.
- **Observer Services.** Se basa en un registro de servicios donde el observador notifica al cliente sobre eventos que derivados de los servicios en los que esta registrado.
- **Publish/Suscribir Services.** Evolución del patrón Observer Services incorporando un sistema de notificaciones para sustituir al registro. Se emplea cuando los servicios web no incorporan un sistema de notificación y precisan un intermediario.
- **Data Transfer Object.** Permite enviar múltiples objetos en una misma llamada reduciendo el número de conexiones.
- **Partial Population.** Permite que los clientes seleccionen parte de la información del mensaje de respuesta a la solicitud de servicio buscando un mejor aprovechamiento del ancho de banda.
- **Microkernel.** Separa un núcleo de funcionalidad mínimo de partes especificadas por el cliente.
- **Web Service Interface.** Proporciona una interfaz que puede emplearse desde los clientes para invocar los métodos de un proxy de Servicio web genérico en lugar de depender de la clase proxy generada a partir de la WDSL.

REST (en inglés *Representation State Transfer*) representa un modelo de comunicación donde cada petición HTTP contiene la información necesaria para responder a la petición sin tener que almacenar el estado de la sesión. En REST todos los servicios son recursos, identificados por URIs y se

diseñan sus representaciones mediante XML, JSON o microformatos. REST representa una arquitectura SOA que no hace uso de Servicios web, SOAP ni RPC.

Actualmente dentro del marco de la Web 2.0 surge una nueva variante en las arquitecturas SOA, el concepto de **Mashup**, un sitio o aplicación web que hace uso de contenido de otras aplicaciones o servicios vía HTTP. Este contenido es recuperado en un modelo de Servicios web a través de su API pública evitando caer en el Web Scraping. Para emplear los Mashups como XML se emplean lenguajes específicos como EMMML (en inglés *Enterprise Mashups Markup Language*). Las arquitecturas Mashup constan de tres componentes:

- ✓ **Los proveedores de servicios.** Orígenes de datos que publican a través de una interfaz los métodos de acceso a los mismos y permiten su consulta vía Atom, RSS, REST, JSON, Bases de datos o interfaces WSDL de Servicios web.
- ✓ **Aplicación o Servicio web Mashup.** Proporciona un nuevo servicio a partir de la información obtenida de los proveedores.
- ✓ **Clientes.** Usuarios finales, u otras aplicaciones o servicios que hacen peticiones al Mashup. En los clientes acostumbran a emplearse tecnologías RIA del tipo de AJAX o Comet.

Otro concepto que se puede relacionar con SOA es el de la **Nube** (en inglés *Cloud Computing*). La nube se fundamenta en emplear la red Internet para publicar servicios, que pueden o no requerir identificación. En la nube todo son servicios, aplicaciones, bases de datos, redes, y se gestionan y se acceden como tal. La arquitectura de la nube se estructura habitualmente en tres capas:

- 1) **Software como servicio** o SaaS (en inglés *Software as a Service*). Sería el nivel más alto, orientado a los usuarios y clientes finales. Se incluirían las aplicaciones propias y aplicaciones de terceros del estilo

de Google Aps. La misma infraestructura del proveedor sirve a múltiples organizaciones finales.

- 2) **Plataforma como servicio** o PaaS (en inglés *Platform as a Service*). Serían la capa intermedia encargada de encapsular sistemas o *middleware* permitiendo correr aplicaciones sobre ellas. Ejemplos de este servicio serían Google App Engine o Windows Azure. De este modo una organización externa proporciona un servicio de infraestructura y soporte para otras organizaciones.
- 3) **Infraestructura como servicio** o IaaS (en inglés *Infrastructure as a Service*). En este caso se ofrecen servidores para computación, red, almacenamiento o bases de datos a través de diferentes técnicas como por ejemplo a través de máquinas virtuales.

El **Bus de Servicios Empresariales** o ESB (en inglés *Enterprise Service Bus*) representa otras de las características de SOA, aunque no es imprescindible en una arquitectura de este tipo. Se trata de un componente que hace abstracción del sistema de mensajes de la organización a través de un sistema único para todos los elementos de un sistema SOA. El ESB proporciona funciones de transformación, adaptación, conexión y enrutamiento que pueden ser implementadas en SOA. En una arquitectura SOA con un ESB todas las aplicaciones y servicios se conectan a un punto único y central que administra las comunicaciones, realizando funciones de *middleware*. El ESB se construye sobre tecnologías XML, XSLT, XPath, JMS o propias de Servicios web. Hace uso de elementos denominados Contenedores de Servicios o Brokers que hacen la función de servidores de comunicaciones. Entre los servicios que proporciona se encuentran:

- ✓ Funcionalidades de enrutamiento, fraccionamiento y combinación de mensajes bajo la base de los patrones EIP (en inglés *Enterprise Integration Pattern*).
- ✓ Funciones de supervisión y control de la calidad del servicio a través de Acuerdo de Nivel de Servicios o SLA de los servicios.

- ✓ Funciones de monitorización, seguridad y mediación de protocolos.

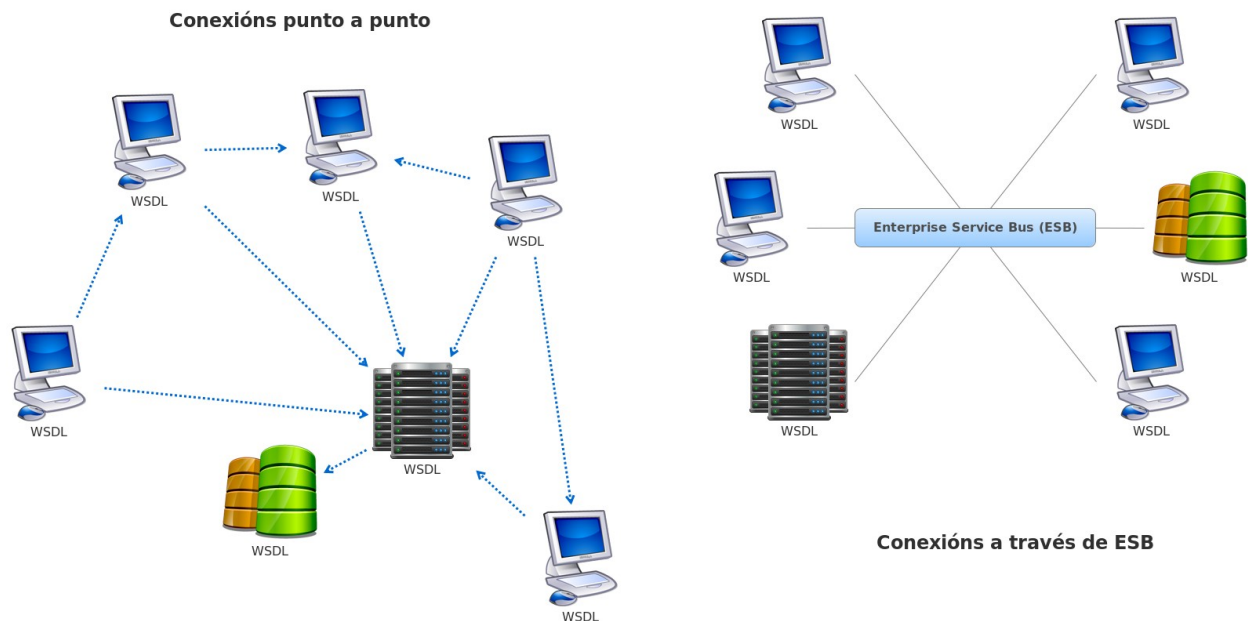


Figura 3: Bus de Servicios Empresariales (ESB).

El Bus sustituye la comunicación directa entre dos aplicaciones o servicios, de modo que la comunicación se hace de manera transparente a través del ESB. Emplea un sistema de mensajería, como por ejemplo Tibco, soportando varios MEP o patrones de intercambio de mensajes, así como colas para reenviar las peticiones a los proveedores de servicios y las respuestas a las solicitudes a los clientes. Existen *frameworks* que recogen los componentes precisos para implantar un ESB como Mule ESB, este es un *framework* ligero destinado a mensajería y control de eventos. Permite integraciones con otros *frameworks* como Struts o Spring y soporta muchos componentes de servicio como JMS, SOAP, BPEL, JBI (en inglés Java Business Integration), y otros.

Por último señalar que las arquitecturas SOA pueden completarse con módulos específicos según las necesidades de la organización, como:

- ✓ **Seguridad.** Con la adopción de diferentes tecnologías, SSL, Kerberos, X.509, Firmas XML, Encriptación XML, XML Canonicalization, SAML (en inglés *Security Assertion Markup Language*) o XKMS (en inglés *XML Key Direction Specification*), que administra la llave pública o PKI de las infraestructuras.
- ✓ **Orquestación y coreografía de servicios.** En este modelo la interacción entre servicios no se produce directamente sino que se define una entidad que define la lógica de interacción, facilitando la colaboración que será un servicio de control primario. En BPEL el servicio primario será un proceso BPEL, pero también se puede definir con BPEL4WS, WSFL o XLANG. Mientras la orquestación precisa de un director de orquesta o servicio central, el modelo de coreografía establece interacciones punto a punto a partir de reglas de colaboración generales. Para la coreografía existen lenguajes específicos como WS-CDL (en inglés *Web Services Choreography Description Language*) que tienen definida la forma de representar las interacciones.
- ✓ **Gestión transaccional.** Existen varias tecnologías que coordinan las transacciones entre servicios autónomos. El BTP (en inglés *Business Transaction Protocol*) donde ninguno de los servicios gestiona una transacción, sino que esta se comunica a todos y deciden si se unen o no, con comunicaciones basadas en XML en un formato propio. Otros mecanismos como WS-Transaction y WS-Coordination se encargan de gestionar transacciones llevadas a cabo por varios servicios a la vez, con protocolos SOAP y WSDL. Por su parte JEE disponen de la especificación JAXTX para transacciones complejas con el objetivo de aislar estas de los contenedores.

30.3 SERVICIOS WEB

Los Servicios web son uno de los modelos de implementación de SOA. Un

Servicio web que proporciona un servicio vía web en una red a través de una interfaz que le permite recibir peticiones y transmitir respuestas. Para soportar este sistema se desarrollaron una gran variedad de protocolos y tecnologías. Los principales son el HTTP/HTTPS para peticiones y respuestas y el XML como formato de intercambio. Los principales **componentes** comunes a los servicios web serían:

- a) **SOAP** (en inglés *Simple Object Access Protocol*). El protocolo de comunicación, sobre la capa de transporte basado en XML, que sirve para invocar los servicios a través de un protocolo siendo los más habituales HTTP o SMTP, pero realmente es independiente y permite otros como POP3 o JMS. Permite tanto describir el contenido del mensaje y reglas de codificación de los tipos de datos, como aspectos de seguridad y transaccionalidad. Se encuentra estandarizado por el W3C, lo que garantiza la comunicación entre sistemas heterogéneos que lo implementen.
- b) **UDDI** (en inglés *Universal Description, Discovery and Integration*). Directorio donde se publican los servicios proporcionando la información necesaria para permitir su invocación. Presenta dos API que permiten a los servicios publicar sus funcionalidades y a los clientes enviar las peticiones y obtener los resultados. Cada servicio se publica en el UDDI proporcionando la URL de su WSDL y meta-información. De manera general se entiende que UDDI proporciona tres tipos de servicios: información general sobre los proveedores de los servicios (páginas blancas), categorías y clasificaciones de servicios (páginas amarillas) y las reglas de negocio o información técnica sobre los servicios (páginas verdes).
- c) **WSDL** (en inglés *Web Services Description Language*). Lenguaje basado en XML y XML Schema que permiten la descripción de la interfaz de los Servicios web y que está estandarizado por el W3C. En un documento WSDL se definen los tipos de datos, los mensajes, los

endpoints, los *bindings* y los servicios.

- d) **Serialización de datos.** Se emplean definiciones de XML Schema para especificar cómo codificar los datos en conjunción con las reglas de codificación de SOAP. Aunque el mecanismo más habitual sea el SOAP Document/Literal existen otros mecanismos como: RPC/Encoding, Document/Encoding o RPC/Literal.

Según lo visto anteriormente para las arquitecturas SOA en general, se pueden definir varios tipos de servicios según su complejidad, comenzando por los de nivel básico a los de niveles más complejos.

	Servicios de nivel básico	Servicios de alta complejidad
Función	Integración de la funcionalidad de una aplicación	Elemento llave de una arquitectura SOA
Protocolos y tecnologías	SOPA, UDDI, WSDL	ebXML, BPEL, BTP, RossetaNet, Apache Axis, ...
Tipo de contenido	Plano	MIME, PDF, ...
Comunicaciones	Punto a punto	Multiparty, ESB, ...
Mensajería	JMS, RPC, ...	Colaboración y <i>workflows</i>
Transaccionalidad	No transaccional	Transaccional
Seguridad	SSL, autenticación, ...	Firma digital, XML-encryption, Kerberos, ...

Tabla 1: Complejidad de los servicios web.

Según el tipo de comunicaciones las APIs más habituales son:

- a) **API de mensajería.** Clientes y servicios disponen de sistemas de mensajería que les permiten comunicarse en formato XML. Al estar

orientadas hacia los sistemas de mensajería presentan una alta QoS.

- b) **API de RPC.** La solución más habitual, que emplea un compilador intermedio de WSDL para generar el *stub* y el *skeleton* para cliente y servidor respectivamente, tal y como sucede con CORBA. Este sistema es lo que acostumbran a emplear los *frameworks* actuales como Apache Axis.
- c) **API para servidores de aplicaciones (JEE/.NET).** Estas API vienen disponibles en las bibliotecas de clases de cada arquitectura, como por ejemplo en JEE se dispone de: JAXM (en inglés *Java API for XML Messaging*) para intercambio de mensajes; JAX-RPC (en inglés *Java API for XML-based RPC*), que permite enviar peticiones remotas a terceros y recibir resultados; y JAXR (en inglés *Java API for XML Registries*), que proporciona acceso a registros de negocio y mecanismos para compartir información.

El **proceso de implementación de un servicio web** consiste en implementar las funcionalidades del servicio reutilizando las clases generadas a partir de un WSDL o de una API (JAX-RPC, Axis,...). Se pueden aprovechar las herramientas existentes en los ID, u otras más específicas con Ant o *WsdI2java*. Una vez implementadas las clases con la lógica del servicio se generan las clases en un war y se despliegan en un contenedor de Servlets o en un IIS. Sobre el modelo de programación se emplean diferentes variantes:

- a) **Estilo CORBA.** Se generan todas las clases al compilar empleando clases de las API (Axis, JAX-RPC, ...)
- b) **Dynamic Proxy.** La interfaz WSDL se crea al compilar, pero el proxy en el cliente sólo se compila en tiempo de ejecución.
- c) **Dynamic Invocation Interfaz.** Tanto WSDL como cliente se generan en tiempo de ejecución. El cliente busca e invoca el servicio vía

broker.

Otro de los factores a considerar es el tema de la **seguridad** en los Servicios web, que por la propia naturaleza de las arquitecturas SOA resulta un tema complejo. Los principales elementos de seguridad en lo que respecta la JEE, aunque muchas serían extensibles a .NET, serían:

- ✓ Para JAX-RPC a API **XWS-Security** que facilita la integración de aspectos de seguridad.
- ✓ El estándar **XML-DigitalSignature** para firma digital.
- ✓ El estándar **XML-Encrytion** para encriptación de mensajería.
- ✓ **Certificados X.509** para autenticación.
- ✓ Bases de datos de certificados basadas en **JKS** (en inglés *Java Key Store*).

Dentro de la arquitectura los diferentes mecanismos se integrarían nivel a nivel de la siguiente manera:

- 1) **Nivel de transporte.** Autenticación básica, autenticación por certificado vía SSL/TLS. Codificación de usuario/contraseña en los *stubs* y reglas de seguridad para *endpoints*.
- 2) **Nivel de mensaje.** Firma de contenidos con certificados XML-DigitalSignature, certificados X.509 y encriptación.

Entre las **posibilidades** existentes para implementar Servicios web se encuentran:

- ✓ APIs Java: JAX-RPC, JAXM, SAAJ (mensajes SOAP como objetos), JWSDL (Acceso a descripciones WSDL), JAXR (Acceso al UDDI), *framework* Apache Axis, ...
- ✓ .NET: ASP .NET, MS SOAP Toolkit,...
- ✓ Otras tecnologías: NuSOAP para PHP, Axis para C++,...

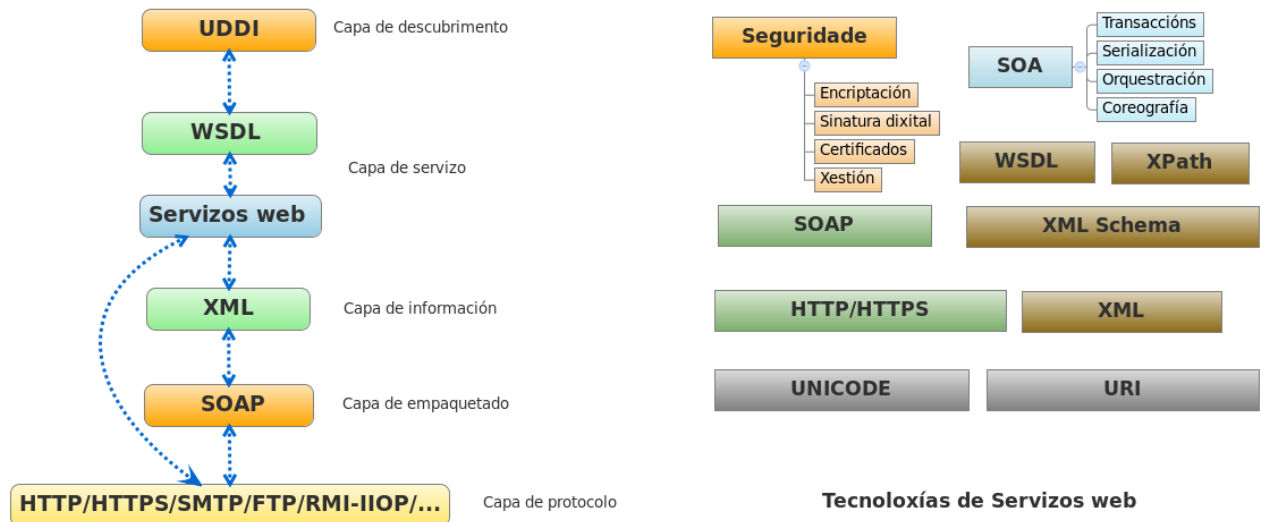


Figura 4: Tecnologías de Servicios web.

30.4 TECNOLOGÍAS XML

El lenguaje XML (en inglés *xtensible Markup Language*) es un metalenguaje para etiquetado desarrollado por el W3C. En SOA el XML representa el estándar para intercambio de información estructurada entre sistemas heterogéneos. En esencia, XML es un lenguaje de marcas que permite la creación de otros lenguajes de marcas, con diferentes usos en SOA, cada uno de estos lenguajes se denomina Aplicación XML y representa un modelo de datos de acuerdo a un esquema semántico.

El XML resulta más estricto que otros lenguajes como HTML, admitiendo varios mecanismos de validación o corrección:

- ✓ **Formación.** Un documento XML se denomina “bien formado” cuando sigue las reglas léxicas (tipo de caracteres, codificación,...) y sintácticas (anidación correcta, marcas de apertura y cierre de estructura,...) debidas.
- ✓ **Validación.** Un documento XML se considera “validado” cuando

cumple un conjunto de reglas y limitaciones denominadas en conjunto gramática o Esquemas XML (en inglés *XML Schema*). Existen varios formatos para gramáticas: los DTD heredados del SGML, los XML-Schema, que son recomendación del estándar por el W3C y otros más específicos como el XML Data.

Las **tecnologías principales más empleadas** del modelo XML en arquitecturas SOA vienen dadas por:

- ✓ **XML Schema.** Lenguaje de esquema para describir la estructura y reglas de validación de un documento XML. Se diferencia del DTD en que permite un gran número de tipos de datos. Los documentos de esquema son de extensión XSD (en inglés *XML Schema Definition*). La programación de esquemas se basa en los espacios de nombres y los elementos y atributos que contienen. Después de validar un documento contra un XSD se puede expresar su estructura y contenido en términos del modelo de datos del esquema. Esta funcionalidad se denomina PSVI (en inglés *Post Schema Validation Infoset*), y permite transformar el documento en una jerarquía orientada a objetos.
- ✓ **XSL.** XSL funciona como un lenguaje avanzado para crear hojas CSS transformando y realizando otras operaciones sobre documentos XML, dándoles formato. A su vez puede descomponerse en tres lenguajes o dialectos XML, todos consejos del W3C, que integran la familia XSL:
- ✓ **XSLT** (en inglés *Extensible Stylesheet Language Transformations*). Estándar para documentos XML que permiten transformar documentos XML en función de modelos de una sintaxis a otra permitiendo estructuras de programación, funcionando a modo de intérprete. Las reglas de los modelos se definen programáticamente y la principal capacidad de este lenguaje es que permite separar el contenido de la presentación, o diferentes

presentaciones en documentos XML lo que se adapta perfectamente a los modelos de separación en capas vistos.

- ✓ **XSL-FO** (en inglés *Extensible Stylesheet Language Formatting Objects*). Documentos XML que especifican formatos de datos u objetos para su presentación. La utilidad básica de estos documentos es la presentación, con lo cual se complementan con XSLT en la salida de datos de las aplicaciones. Permite la generación de documentos multiformato: XML, (X)HTML e incluso PDF. Existen procesadores específicos para este tipo de operaciones como Apache FOP.
- ✓ **XPath o XML Path Language**. Permite identificar partes de un documento XML, accediendo a sus atributos y elementos como si fuesen nodos, a través de la construcción de expresiones que recorren y procesan un documento XML. En XSL permite seleccionar y recorrer el documento XML de entrada de la transformación, pero por extensión tiene otros muchos usos actualmente, sirviendo de base para otros lenguajes XML.

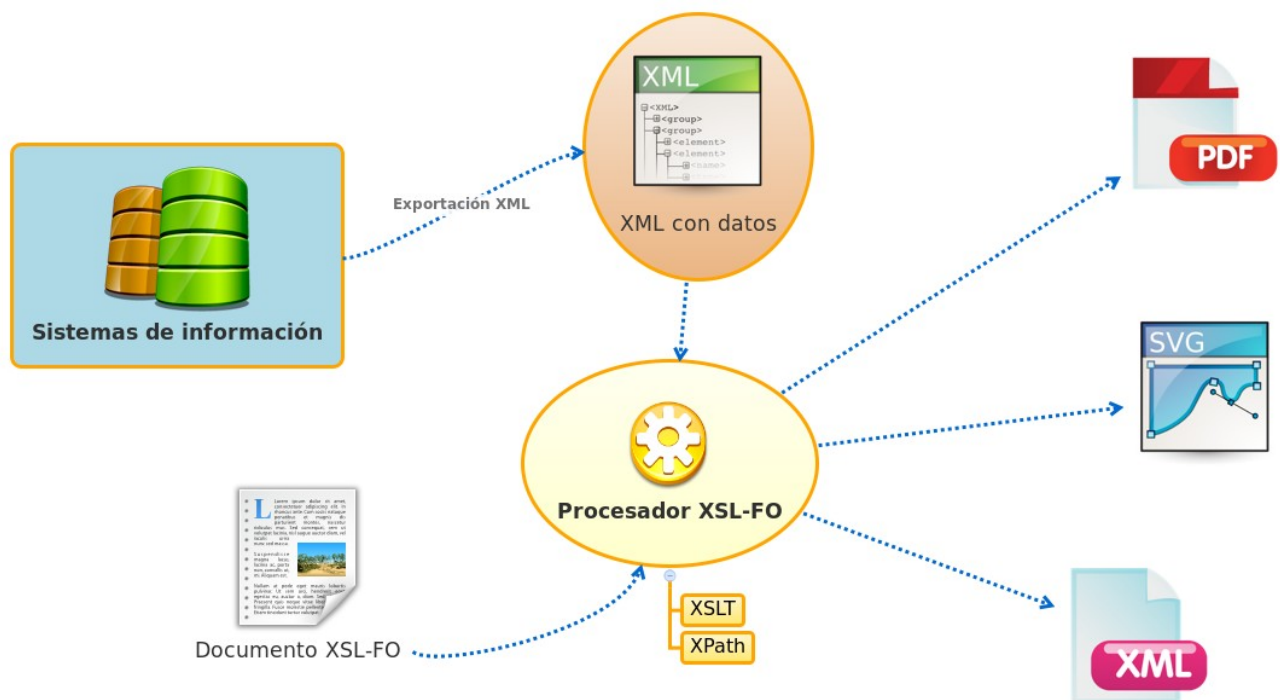


Figura 5: Familia XSL.

- ✓ **XPointer.** Recomendación del W3C que permite localizar puntos concretos o fragmentos en un documento que expande las funcionalidades de XPath a través de rangos.
- ✓ **XLink.** Recomendación del W3C que define un mecanismo para añadir hiperenlaces en archivos XML u otros recursos, con la opción de navegar en los dos sentidos, con enlaces bidireccionales o varios archivos enlazados, multienlaces. En XLink todo en la red es un recurso, y se puede enlazar desde un localizador, definiendo las relaciones entre recursos con arcos. Asimismo permite agregar a un vínculo información sobre si mismo como metadatos.
- ✓ **XQuery.** Lenguaje de consulta desarrollado por el W3C para recuperar colecciones de datos XML, con muchas similitudes con SQL. Permite extraer y manipular información de documentos XML o cualquier otro sistema de información que permita representación vía XML como Bases de datos o documentos ofimáticos. Emplea XPath

para acceder a los documentos añadiendo unas expresiones propias denominadas FLWOR. Asimismo realiza transformaciones de documentos XML y búsquedas de elementos textuales en la web o en recursos XML/(X)HTML. En las arquitecturas SOA resultan especialmente útiles para recuperar información de Bases de datos y presentarla a través de Servicios web.

- ✓ **XForms.** Lenguaje de definición de Interfaces de usuario desarrollada por el W3C, centrada especialmente en la parte de formularios web y su integración en documentos (X)HTML, ODF o SVG. Se aplica el paradigma de separar el contenido, propósito y estructura. En aplicación del MVC incorpora un modelo declarativo de compuesto de reglas y validación para datos y tipos de datos de los formularios, así como envío de parámetros; una capa de vista compuesta de los controles de la interfaz de usuario; un controlador para orquestar las manipulaciones de datos, interacciones entre el modelo y la vista y envíos de datos. Otras evoluciones de esta tecnología serían AJAXForms y XSLTForms, incorporando AJAX y XSLT a esta tecnología. Por otra parte, existen otros lenguajes relacionados con las interfaces de usuario que siguen dialectos de XML, muchas de ellas con capacidad para interactuar con XForms como: XAML, XUL, UIML, UsiXML, AUIML,...

El grupo de tecnologías anteriores podrían definirse como lenguajes XML de propósito general. En muchas ocasiones el XML se emplea de manera concreta para representación de datos complejos o con necesidades específicas para nuestro dominio. En la tabla 2 se recogen algunos ejemplos de lenguajes XML empleados para representación o adaptación de información a necesidades concretas, bien para entornos de trabajo como

XHTML y WML o bien en dominios específicos como aplicaciones de información geográfica o diseño gráfico.

	Función
XHTML	HTML con especificaciones más estrictas para presentar una mayor compatibilidad con la web semántica y los otros estándares XML
MathML	Expresar planteamientos matemáticos
SVG	Especificación para describir gráficos vectoriales y animaciones
SMIL	Permitir la integración multimedia en XHTML y SVG
WML	Adaptación del HTML para móviles y PDA
VoiceXML	Convertir habla en XML a partir de gramáticas de reconocimiento de voz
SSML	Para habla sintética
GML/KML	Para sistemas de modelado e información geográfica
X3D	Representación de gráficos en 3D
EBML	Para almacenar jerarquías de datos en formato binario de longitud variable

Tablas 2: Lenguajes XML complementarios.

El uso tan extendido del XML obliga a disponer de herramientas que permitan el tratamiento sencillo de los documentos, recorrer, manipular, procesar, etc... Muchas tecnologías disponen de *frameworks* específicos para **tratamiento de XML**:

- ✓ **DOM** (en inglés *Document Object Model*). Especificación del W3C de una API (org.w3c.dom) para manipular documentos XML/HTML, acceder a su contenido, estructura y estilos, a través de un analizador sintáctico. DOM genera un árbol jerárquico en memoria donde almacena todo el documento. A través de un procesador se permite acceder a cualquier nodo del árbol, o insertar/eliminar nuevos nodos.

El principal inconveniente de este modelo es que precisa gran cantidad de memoria por la necesidad de cargar todo el documento, pero tiene las ventajas de ser muy sencillo de implementar y de permitir la generación de XML. Se apoya en tecnologías XSLT y Xpath. Frameworks como Xerces se basan en DOM para tratamiento de XML así como otros basados en AJAX del tipo de JQuery, Prototype, Dojo, etc... Asimismo existen alternativas recientes similares a DOM, diseñadas explícitamente para JEE que resultan más fáciles de emplear, JDOM (org.jdom) y DOM4J (org.dom4j).

✓ **SAX** (en inglés *Simple API for XML*). API inicialmente para Java (org.xml.sax), pero que después evolucionó a otros lenguajes como C++, Perl, Python,..., que disponen de un analizador que genera eventos al conseguir puntos llave del documento analizado. Recorre el documento de manera secuencial a través de un administrador de eventos, el `DocumentHandler`, evento a evento, con lo cual no precisa cargar el documento en memoria pero no permite vuelta atrás sin ir de nuevo al inicio. Esto lo hace muy adecuado para documentos de gran tamaño. Otros *frameworks* más completos se basan a su vez en SAX, como: Xerces, Crimson, Piccolo u Oracle XML Parser.

✓ **StAX** (en inglés *Streaming API for XML*). Define un analizador sintáctico de flujo de datos integrado en JEE, con soporte para generación de XML. Se emplean dos estilos de análisis Cursor API e Iterador Event Iterator API, ambos basados en iteraciones para solventar las limitaciones de SAX y DOM. En este modelo el documento XML se transmite en un flujo de datos donde se va solicitando el siguiente evento (*Pull*) con el fin de optimizar recursos de memoria. Se distingue entre Streaming Pull Parsing donde el cliente sólo obtiene los datos solicitados previamente (SAX) y el Streaming Push cuando el analizador envía al cliente datos del XML al localizar un elemento.

✓ **JAXP** (en inglés *Java API for XML Processing*). API de Java (`javax.xml.parsers` y `javax.xml.transform`) que proporciona acceso a través de dos factorías abstractas para trabajar con instancias de analizadores DOM y SAX a través de diferentes implementaciones, así como soporte para StAX, espacios de nombres y XSLT (Xalan). También lleva incorporado el analizador Crimson. Suele integrarse en entornos con Servicios web para agrupar en un mismo *framework* todas las posibilidades de tratamiento de XML.

✓ **JAXB** (en inglés *Java Architecture for XML Binding*). API JEE (`javax.xml.bind`) que proporciona un conjunto de interfaces para analizar y generar XML de manera automática. A partir del modelo definido en XML realiza la generación de clases Java equivalentes. El esquema suele definirse vía DTD, a partir del cual un desarrollador puede construir un árbol de objetos Java que se corresponden con el XML. De este modo se evitan las limitaciones de memoria de DOM.

Paralelamente se dispondrá de componentes específicos para entornos basados en **Servicios web** como WSDL, los más habituales serían:

✓ **SAAJ**. API (`javax.xml.soap`) de SOAP y SOAP con aportaciones (en inglés *SOAP with Attachments*) que permite enviar documentos XML y aportaciones en formato MIME que pueden ser o no XML. Se acostumbra a emplear a bajo nivel por otras API para operaciones de mensajería.

✓ **JAX-RPC**. API de JEE para facilitar el desarrollo de componentes software que hagan uso de XML para comunicaciones a través de llamadas a procedimientos remotos (RPC), en la línea de IDL-CORBA y RMI. A diferencia de estas alternativas JAX-RPC emplea XML como soporte a Servicios web. Permite correspondencia entre objetos y

estructuras XML. En arquitecturas SOA el JAX-RPC sería la tecnología a través de la que el cliente envía la petición de servicio. Por debajo emplea SOAP, pero este nivel permanece transparente a la API. Sus funciones abarcan: Mensajería asíncrona, Enrutamiento de mensajes, Mensajería con entrega garantizada.

- ✓ **JAXR** (en inglés *Java API for XML Registries*). API de JEE para acceso a registros de servicios en estándares abiertos como ebXML o UDDI. Permite a los servicios la posibilidad de auto-registrarse. Asimismo soporta el uso de consultas SQL para la búsqueda de registro a través del objeto SQLQueryManager. Hace uso de JAXM para mensajería.
- ✓ **JAX-WS** (en inglés *Java API for XML Web Services*). Componente del servicio web base Metro, que sería evolución y ampliación de JAX-RPC y se encontraría integrado con JEE (javax.xml.ws). Hace uso de anotaciones Java para describir elementos de las clases, como metadatos y permiten automatización de tareas.

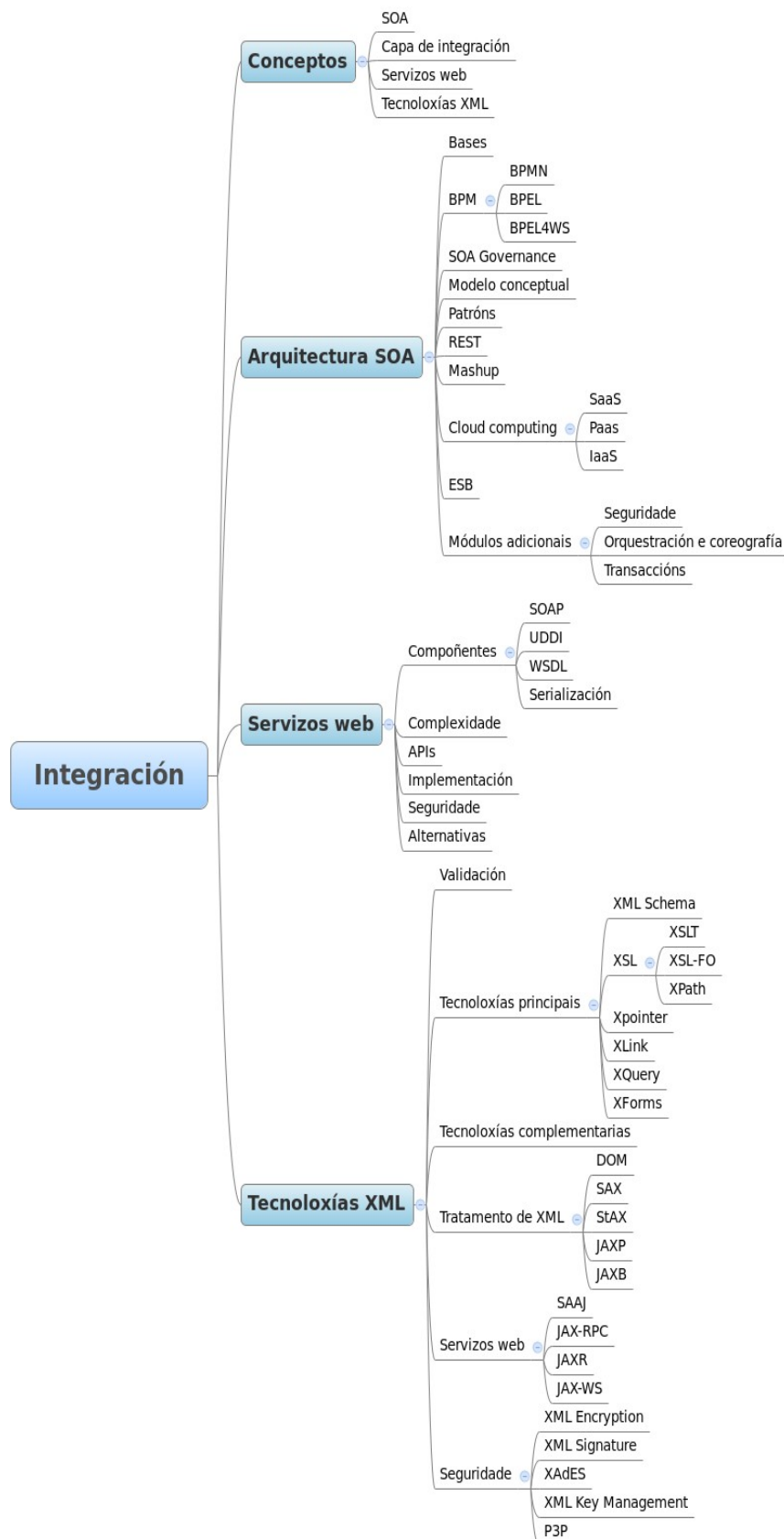
Por último dentro del ámbito de la **seguridad**, existen una serie de soluciones derivadas de la capacidad insuficiente ante arquitecturas SOA de TLS o SSL. Así hay que destacar las siguientes tecnologías:

- ✓ **XML Encryption.** La encriptación XML es un consejo del W3C que especifica el proceso para cifrar datos o documentos completos y representar esa información encriptada en un documento XML. Permite supercifrado y soporta los algoritmos TripleDES, AES y RSA.
- ✓ **XML Signature.** Firma digital que garantiza la integridad de las partes en una comunicación. Asimismo proporciona autenticación de mensajes, integridad de datos, soporte de transacciones sin repudio y firmas para cualquier contenido digital o XML. En el documento se añade un elemento Signature que encapsula el contenido de la firma

digital incluyendo una referencia al objeto firmado, la indicación del algoritmo de canonización, y el valor resultante de la firma.

- ✓ **XAdES** (en inglés *XML Advanced Electronic Signatures*). Firma digital avanzada XML, que añade un conjunto de extensiones a XML Signature, permitiendo por ejemplo que las firmas sean válidas durante largos períodos de tiempo
- ✓ **XML Key Management**. Protocolo para distribuir y registrar llaves públicas y certificados evitando la complejidad de PKI. Está compuesto de dos partes: X-KRSS o registro de llave pública, un conjunto de protocolos que soportan el registro de pares de llaves; y X-KISS información de llave pública, que define un conjunto de protocolos para procesamiento y envío de información asociada en identificada con XML Signature y cifrada con XML Encryption.
- ✓ **P3P** (en inglés *Platform for Privacy Preferences*). Especificación del W3C que define un estándar de gestión de datos y de privacidad, así como un formato XML para expresar políticas de privacidad, con el objetivo de permitir a los usuarios si y cómo quieren revelar información personal.

30.4. ESQUEMA



TRADUCCIÓN FIGURAS:

FIGURA 1: ARQUITECTURA SOA

- Seguridad
- Mensajería
- Otros protocolos
- Otros servicios
- Descripción, interfaz

FIGURA 2: MODELO CONCEPTUAL SOA

- Servicios
- Componentes de negocio
- Sistemas operacionales

FIGURA 3: BUS DE SERVICIOS EMPRESARIALES (ESB)

- Conexiones punto a punto
- Conexiones a través de ESB

FIGURA 4: TECNOLOGÍA DE SERVICIOS WEB

- Capa de descubrimiento
- Capa de servicio. Servicios web
- Seguridad
 1. firma digital
 2. gestión
- SOA
 1. transacciones
 2. orquestación
- Tecnologías de servicios web

30.4 ESQUEMA

- Servicios web. Tecnologías XML. Patrones. Módulos adicionales. Seguridad. Orquestación y coreografía. Transacciones.
- Servicios web
 1. Componentes

2. Complejidad
 3. Seguridad
- Tecnologías XML
 1. Tecnologías principales
 2. Tecnologías complementarias
 3. Servicios web
 4. Seguridad

30.5. REFERENCIAS

Varios autores.

Web Services Architecture. W3C Working Group. (2004).

César de la Torre y Roberto González.

Arquitectura SOA con tecnología Microsoft. Buenas prácticas y diseño de aplicaciones empresariales. (2008).

Joan Ribas Lequerica.

Web Services. (2003).

Patrick Cauldwell y otros.

Servicios Web XML. (2002).

Autor: Juan Marcos Filgueira Gomis

**Asesor Técnico Consellería de Educación e O. U.
Colegiado del CPEIG**



31. PATRONES DE DISEÑO Y FRAMEWORKS. MVC. JSF. ANTIPATRONES.

TEMA 31. PATRONES DE DISEÑO Y FRAMEWORKS. MVC. JSF. ANTIPATRONES.

31.1 INTRODUCCIÓN Y CONCEPTOS

31.2 PATRONES DE DISEÑO Y FRAMEWORKS

31.3 MVC

31.4 JSF

31.5 ANTIPATRONES

31.6 ESQUEMA

31.7 REFERENCIAS

30.1 INTRODUCCIÓN Y CONCEPTOS

Para muchos problemas de diseño que se repiten tanto en desarrollos software como en implantaciones hardware existen soluciones comunes de aplicación dentro del mismo contexto. Estas soluciones recurrentes se denominan **patrones de diseño** y se basan en el concepto de reutilización y aprovechamiento de soluciones ya existentes en problemas nuevos. Los patrones, según el autor, suelen dividirse en diferentes familias, siendo la clasificación más habitual en patrones de diseño, de arquitectura e interacción. A su vez, los patrones de diseño se clasifican como creacionales, estructurales y de comportamiento. Asimismo, se definen los patrones de programación como patrones específicos para lenguajes de programación o sistemas concretos. Cabe señalar que en una misma solución o diseño puede convivir cualquier número de patrones que sea necesario, ya que en muchos casos se trata de soluciones parciales a problemas concretos, no de soluciones generales. Frente al concepto de patrón surge el de antipatrón, que define errores de diseño comunes o problemas que se repiten a menudo para ayudar a identificarlos. Los patrones y antipatrones pueden definirse ante lenguajes de definición del

estilo del Lenguaje Unificado de Modelado o **UML** (en inglés *Unified Modeling Language*), que, soportado por el **OMG**, es uno de los más empleados actualmente.

En las aplicaciones JEE y .NET uno de los patrones de uso más extendido es el Modelo Vista Controlador o MVC (en inglés *Model View Controller*) que se basa en la separación de una aplicación en tres capas o componentes diferenciados, interfaz de usuario, lógica de negocio y sistemas de información.

Este patrón se integra en **frameworks**, o componentes software que implementan funcionalidades comunes a conjuntos de aplicaciones, y que pueden seguir los modelos de patrones de diseño. El patrón sería la solución de diseño abstracta y el *framework* una implantación concreta del mismo. Algunos *frameworks* como Struts representan el esqueleto de una aplicación, con implementación del patrón MVC entre otros, aportando así directamente todas las funcionalidades precisas para su funcionamiento interno. Si en una misma aplicación añadimos nuevos *frameworks* dispondremos de funcionalidades añadidas. De este modo, el *framework* **JSF** (en inglés *Java Server Faces*) proporciona, complementariamente a Struts herramientas que facilitan el desarrollo de interfaces de usuario.

31.2 PATRONES DE DISEÑO Y FRAMEWORKS

Las principales ventajas del empleo de patrones en soluciones software pasan por facilitar la comunicación interna entre componentes, ahorrar tiempo y otros recursos, mejorar la calidad de las operaciones de todo el ciclo de vida de desarrollo y facilitar el aprendizaje. A día de hoy es un hecho consumado que su aplicación correcta reporta un beneficio directo en cualquier desarrollo o implantación.

31.2.1 Clasificación general

Existen muchas clasificaciones de los patrones, según el autor(es), pero la más habitual hace referencia al ámbito de aplicación del patrón tomando cómo referencia la ingeniería del software:

- 1) **Patrones de diseño.** Proporcionan un esquema de aplicación en partes de un sistema software. Definen estructuras que resuelven un problema de diseño de utilidad en diferentes aplicaciones.
- 2) **Patrones de arquitectura.** Proporcionan un esquema u organización estructural para definir sistemas completos o subsistemas, incluidas responsabilidades y relaciones entre sistemas.
- 3) **Patrones de interacción.** Proporcionan un diseño de interfaz para aplicaciones o aplicaciones web.
- 4) **Patrones de programación** (en inglés *Idioms patterns*). Patrones a bajo nivel para lenguajes de programación o tecnologías específicas. Definen representaciones de implementaciones de componentes y relaciones, considerando funcionalidades propias de cada lenguaje.

31.2.2 Clasificación de patrones para tecnologías de servidores de aplicaciones

A mayores fueron surgiendo patrones para otros ámbitos de aplicación, como programación multihilo, flujos de trabajo para procesos de sistemas empresariales, arquitecturas SOA o integración de sistemas. En definitiva, puede concluirse que el concepto de patrón puede extenderse a cualquier problema que nos encontremos y el nivel de abstracción que precisemos en la solución. Existen diferentes catálogos de patrones, siendo los más conocidos:

- ✓ **GoF**, (en inglés *Gang of Four*) para problemas de diseño. (1995).
- ✓ **POSA**, (en inglés *Pattern Oriented Software Architecture*) para soluciones en arquitecturas SOA. (1996).

- ✓ **J2EE**, para soluciones específicas de esta tecnología. (2003).
- ✓ **PoEAA** (en inglés *Patterns of Enterprise Application Architecture*). Para sistemas complejos en arquitecturas empresariales distribuidas en capas. (2003).
- ✓ **GRASP** (en inglés *General Responsibility Assignment Software Patterns*). Patrones generales para asignación de responsabilidades y transiciones. (2005).

En concreto, para el ámbito de los servidores de aplicaciones como .NET y JEE en cuanto a arquitectura y análisis pueden destacarse los siguientes, atendiendo a su nivel de utilización:

- a) **Patrón de análisis Party (Grupo)**. Agrupa las responsabilidades similares de los tipos de colectivos de una organización en un supertipo. Se emplea para facilitar el modelado de estructuras en organización, siendo cada tipo una organización, empresa, rol o papel y almacenar los datos personales de cada miembro. Situaciones especiales obligan a adaptaciones de este patrón como ocurre en el Party Type Generalizations, que permite la generalización de tipos de grupo que heredan de un subtipo, como por ejemplo para una persona que tiene varios roles a la vez.
- b) **Patrón de análisis Accountability**. Establece una relación de responsabilidad entre dos partes o perfiles. Con los tipos Accountability y Accountability Type permite expresar la clase de relación entre ambos. puede hacer uso del patrón Party para obtener una mayor flexibilidad. Según sean las relaciones, puede dar lugar a patrones más complejos como Hierarchic Accountability o Jerarquía de responsabilidad que añade limitaciones a los elementos de responsabilidad; o que tiene aplicación a la hora de delegar tipos de responsabilidad a un subpatrón Party.
- c) **Patrón arquitectónico MVC** (en inglés *Model View Controller*).

Estructura un componente software en 3 capas, el modelo con la lógica de negocio, funcionalidades y sistemas de información, la vista con la interfaz de usuario y el Controlador que recibe los eventos de la entrada y coordina las actividades de la vista.

- d) **Patrón arquitectónico PAC** (en inglés *Presentation Abstraction Control*). Similar al MVC, este patrón define un sistema interactivo basado en una jerarquía de agentes cooperantes que realizan funcionalidades concretas. Se divide en tres capas: Presentación con interacción persona-máquina, Abstracción con la lógica y sistemas de información y el Control que centraliza las comunicaciones entre agentes, procesa eventos externos y actualiza el modelo. La principal diferencia con el MVC radica en que se pueden hacer diferentes agentes o subsistemas de aplicación, operando de forma independiente o jerarquizada.
- e) **Patrón arquitectónico Capas** (en inglés *Layers*). Representaría la abstracción genérica de los patrones anteriores a un sistema multicapa, orientado hacia distribución jerárquica de roles y responsabilidades. Permite aumentar o disminuir el nivel de abstracción, más o menos capas, aislando el mantenimiento y actualización de cada capa. Cada nivel o capa ofrece servicios a la capa superior y usa los de la inferior.
- f) **Patrón arquitectónico Pipes and Filters**. Orientado también a arquitecturas SOA, en este modelo cada componente posee un conjunto de entradas y salidas. Representa la lectura de flujos de datos, transformándolos en un flujo de salida sin tener que procesar toda la entrada, como ocurre en los modelos Streaming, y de ahí que se denominen Filtros a los componentes que reciben las entradas y tuberías o conductos a los que encaminan el flujo hacia la salida. Permite representar procesamientos en paralelo, así como ejecución concurrente.
- g) **Patrón arquitectónico Blackboard**. Proporciona un modelo de

soluciones aproximadas cuando no se puede aplicar una solución concreta. Permite reutilizar las fuentes de conocimiento y un mejor soporte de cambios y mantenimiento de la solución aproximada.

- h) **Patrón Microkernel.** Dentro de los patrones para sistemas adaptables, este modelo separa un kernel funcional mínimo del extendido para soportar sistemas software con requisitos que cambian a lo largo del tiempo. Ideado para sistemas operativos, cada uno de ellos sería una vista del Microkernel central, permitiendo que se pueda extender el sistema de manera fácil.
- i) **Patrón Reflection.** Otro patrón sistemas adaptables que modela un mecanismo para cambiar dinámicamente la estructura y comportamiento de un sistema. Establece dos niveles: Metadatos, para que el software lleve una descripción de sí mismo y Lógica de aplicación. Los cambios de comportamiento pueden reflejarse en los metadatos, pero esto puede pasar inadvertido.
- j) **Patrón arquitectónico Broker.** Orientado a arquitecturas SOA y sistemas distribuidos, donde varios clientes hacen peticiones a un servidor o servicio remoto. El agente Broker se encarga de coordinar la comunicación entre el cliente y el proveedor del servicio. Las principales ventajas de este patrón son permitir la transparencia de localización del servicio, permitir cambios y ampliación de nuevos componentes sin que el sistema se vea afectado, avance de la portabilidad e interoperabilidad con otros agentes Broker.
- k) **Patrón Publisher Subscriber.** Orientado a arquitecturas SOA y sistemas distribuidos, inserta una capa entre clientes y servidores que se encarga de llevar cuenta de la comunicación de manera transparente. Representa una arquitectura de mensajería sin acoplamiento.

En lo tocante al diseño, los principales patrones suelen agruparse en tres

grandes categorías: Patrones creacionales, estructurales y de comportamiento. Los **creacionales** incluirían:

- a) **Abstract Factory.** Aporta una interfaz que permite la creación de familias de objetos dependientes o relacionales sin tener que especificar las clases completas. Ejemplos de este patrón serían los Widgets y componentes de interfaces gráficas.
- b) **Builder.** Constructor virtual que separa la construcción de un objeto complejo de su representación, de tal manera que se obtienen diferentes representaciones en un mismo proceso.
- c) **Factory Method.** Patrón que define una interfaz para la creación de objetos, dejando que las subclases decidan qué clase instanciar, haciendo que el proceso de generación del subtipo sea transparente al usuario.
- d) **Prototype.** Permite la creación de nuevos objetos clonándolos de una instancia de un objeto ya existente.
- e) **Singleton.** Patrón de instancia única que asegura que de una clase solo existirá una única instancia, definiendo un punto de acceso común a la misma.
- f) **Object Pool.** Patrón para la obtención de objetos por clonación. Creará una instancia de un tipo de objeto de la clase a clonar. Está pensado para casos donde la creación tenga un coste muy alto y se permita la utilización de objetos genéricos del Pool.

Por otra parte, dentro de los **estructurales**:

- a) **Adapter.** Patrón que convierte la interfaz de una clase en otra interfaz adaptada a necesidades específicas como determinados clientes o interfaces requeridas por compatibilidad.
- b) **Bridge.** O patrón Handle/Body, separa una abstracción de su implementación, de modo que ambas puedan cambiar de forma de

manera independiente, sin que cambios en una afecten a la otra.

- c) **Composite**. Patrón que permite manipular objetos compuestos como si de uno simple se tratara. Hace uso de la composición recursiva y la estructura en forma de árbol para poder presentar una interfaz común.
- d) **Decorator**. Responde a la necesidad de añadir funcionalidades a objetos dinámicamente. Crea una jerarquía de clases donde las hijas heredan de las madres las funcionalidades e incorporan algunas propias.
- e) **Façade**. Proporciona una interfaz común de acceso a un conjunto de interfaces de un sistema. Facilita el empleo del sistema interno con otras interfaces de alto nivel. Los clientes solo pueden comunicarse a través de la interfaz única que hace de fachada.
- f) **Flyweight**. Permite eliminar la redundancia entre objetos que presentan la misma información. Factoriza los atributos comunes a estos objetos en una clase ligera.
- g) **Proxy**. Proporciona un punto de control de acceso o intermediario para el control de otro(s) objeto(s). Presenta diferentes niveles de aplicabilidad:
 - ✓ *Proxy remoto*. Representa a un objeto remoto de manera local, codificando la petición y argumentos antes de enviarla al objeto remoto.
 - ✓ *Proxy virtual*. Crea objetos de alto coste bajo demanda, con posibilidad de caché de la información de los mismos limitando los costes de acceso.
 - ✓ *Proxy de protección*. Controla el acceso a objetos remotos comprobando que los clientes disponen de los permisos necesarios.
 - ✓ *Proxy de referencia inteligente*. Análogo a un puntero con operaciones adicionales sobre un objeto para temas de concurrencia, acceso a memoria, etc...

El último bloque serían los patrones de comportamiento:

- a) **Chain of responsibility.** El patrón cadena de responsabilidad permite establecer la línea que deben llevar los mensajes, denominada cadena de objetos receptores, permitiendo que varios objetos puedan capturar un mensaje, como puede ser una excepción Java. Cualquiera de los receptores podría responder a la petición según el criterio establecido.
- b) **Comando u Orden.** Patrón que encapsula una operación en un objeto, de modo que se puedan hacer operaciones extendidas como almacenamiento y colas de peticiones y soporte de acciones de hacer y deshacer.
- c) **Intérprete.** Define una representación para la gramática de un lenguaje junto con su intérprete.
- d) **Iterator.** Patrón con el objetivo de permitir recorrer objetos compuestos, como pueden ser las colecciones, sin necesidad de contemplar aspectos de implementación o representación interna de los mismos. Define una interfaz donde se ofrecen diferentes métodos para recorrer el objeto complejo.
- e) **Mediador.** Define un objeto que facilita la interacción entre otros de distinto tipo, coordinando la comunicación entre ellos. El objetivo es encapsular la interacción de esos objetos para evitar el acoplamiento entre ellos.
- f) **Memento.** Representa el estado de un objeto o sistema complejo para permitir su almacenamiento y modificación, de modo que se pueda restaurar volviendo a estados anteriores en el tiempo.
- g) **Observador.** Permite definir una dependencia de uno a muchos, de modo que eventos o modificaciones de estado disparen la notificación de los cambios a todos los objetos o sistemas dependientes.

- h) **Estado.** Se emplea para permitir que un objeto cambie su comportamiento en el caso de modificarse su estado. De este modo, diferentes clases pueden representar a un mismo objeto a lo largo del tiempo.
- i) **Estrategia.** Permite definir una familia de algoritmos o métodos de resolución, permitiendo seleccionar dinámicamente cuáles aplicar y que de este modo sean intercambiables.
- j) **Template Method.** Define el esqueleto de un algoritmo para una operación, delegando partes del mismo a las clases concretas. De este modo las subclases pueden redefinir pasos concretos del método de resolución.
- k) **Visitor.** Representa un algoritmo u operación realizada sobre la estructura de un objeto, permitiendo la definición de nuevas operaciones sin alterar el tipo de los elementos sobre los que se realiza la operación.

En una última categoría podrían incluirse los patrones propios de lenguajes de programación o tecnologías concretas, siendo los **patrones JEE**, la mayoría Core J2EE Patterns, aquellos con un uso más extendido dentro del mundo de los servidores de aplicaciones y los servicios web:

- a) **Intercepting Filter.** Intercepta las peticiones de la capa de presentación antes o después de su procesamiento, permitiendo realizar operaciones sobre los datos como auditorías, comprobaciones de seguridad, conversiones o validaciones. Permiten conectarse en cascada y activar o desactivar sin que afecte al funcionamiento general de una aplicación. Permite diferentes estrategias como Custom Filter, Estándar, Base Filter y Template Filter.
- b) **Front Controller.** Centraliza el control de las peticiones de la capa de presentación, dirigiéndolas hacia el componente apropiado para

validación de parámetros, invocación de elementos de la lógica de negocio, etc... Un controlador se encarga de recoger las peticiones y factorizar el código repetitivo.

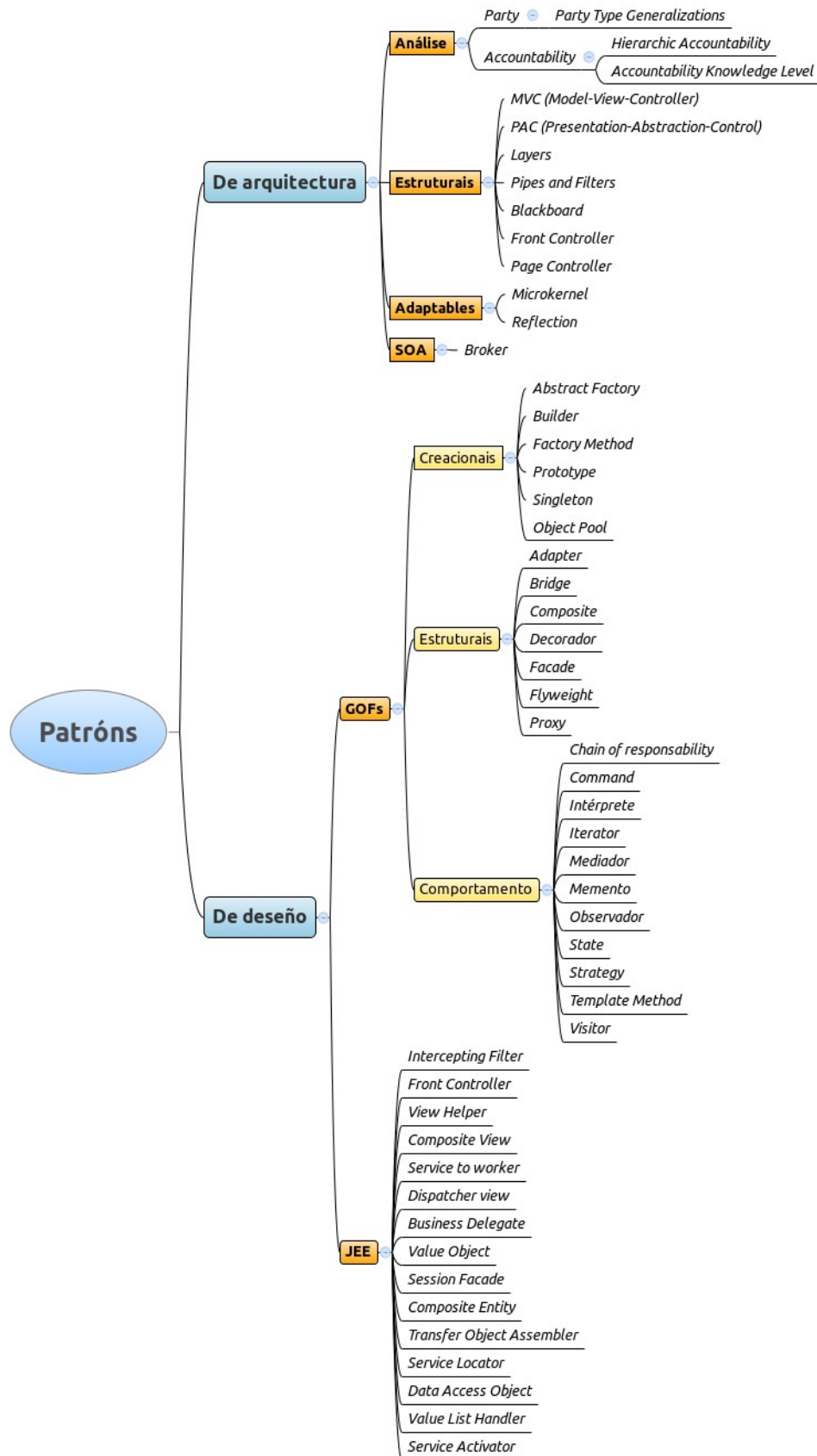
- c) **View Helper.** Aporta una clase que engloba código común, con aplicación tanto para la capa de negocio como para la de presentación. Cada vista contiene código para formato, delegando las responsabilidades de procesamiento en las clases de ayuda implementadas como Java Beans o Custom Tags. Asimismo, pueden almacenar modelos de datos intermedios haciendo adaptaciones previas del negocio, como conversiones o validaciones; lo lógico, por la separación en capas, es que estas operaciones no sean muy complejas.
- d) **Composite View.** Define una jerarquía de vistas compuestas de diferentes vistas particulares, permitiendo modificar las partes en tiempo de ejecución y a partir de modelos. De este modo se incluyen dinámicamente las vistas concretas en vistas compuestas de la aplicación a través de los mecanismos de que disponen a tal efecto JSP y Servlets.
- e) **Service to worker.** Agrupa varios patrones a modo de framework para permitir combinar un controlador (Front Controller), y un Dispatcher o controlador de vistas (View Helper), para manejar las peticiones de los clientes y generar la presentación dinámicamente como respuesta. Los controladores solicitan el contenido a los Helpers que llenan el modelo de negocio intermedio.
- f) **Dispatcher View.** Con una estructura similar a la del Service to worker, en este modelo tanto Controlador como Dispatcher tienen responsabilidades más limitadas, ya que lógica de procesamiento y control de la vista son básicas.
- g) **Business Delegate.** Permite la abstracción a implementación de componentes complejos como EJB o JMS de la capa de presentación. De este modo pueden crearse clases Proxy que almacenen y encolen

las peticiones pudiendo proporcionar control de prioridades, gestión de excepciones o caché. El patrón emplea un componente denominado Lookup Service, responsable de ocultar los detalles de implementación del código de búsqueda dentro de la lógica de negocio.

- h) **Value Object (VO).** Encapsula un conjunto de datos que representan un objeto o entidad del negocio. Cuando se solicita a un Bean un conjunto de información, éste puede crear el objeto Value Object y llenar sus atributos para devolverlo al cliente.
- i) **Session Façade.** Emplea un Bean de sesión como fachada para encapsular las interacciones de los componentes de negocio y ofrecer un servicio de acceso uniforme, a través de los interfaces requeridos solo a través de los casos de uso. Proporciona una abstracción de alto nivel implementada a modo de Bean.
- j) **Composite Entity.** Permite ampliar los Beans de entidad cuando estos son de pequeño tamaño; de este modo pueden aumentarse manteniendo la compatibilidad. El abuso de este patrón se considera un antipatrón, ya que puede dar lugar a estructuras muy complejas. Un Bean Composite Entity representa un grafo de objetos, y por tanto debe emplearse con cuidado.
- k) **Transfer Object Assembler.** Simplifica el acceso a los sistemas de información a través de un conector común. Cada objeto de negocio tendrá un Transfer Object (TO) con los detalles de acceso a datos (Beans, JDO, JDBC, ...) y un Bean de sesión funcionará como interfaz común.
- l) **Service Locator.** Se emplea para abstraer la utilización de JNDI a través de un objeto Service Locator y para ocultar las complejidades de la creación del contexto inicial, así como de la búsqueda e instanciación de EJBs a través de un punto de acceso común.
- m) **Data Access Object (DAO).** Se emplea un objeto como medio de acceso a sistemas de información, en especial Bases de datos.

Abstrae y encapsula las operaciones relacionadas con la tecnología de persistencia empleada (JDBC, JDO, LDAP, Beans, TopLink, Hibernate, iBATIS, etc...). Controla los parámetros de conexión, obtención de datos y almacenamiento, proporcionando una interfaz de acceso común.

- n) **Value List Handler.** Implementado como Beans de sesión, se encarga de manejar la ejecución de consultas SQL, cachearlas y procesar los resultados. Accede directamente a un DAO que se encarga, a su vez, de hacer la conexión con el sistema de información y recuperación de los datos. Una vez obtenidos los almacena como TO o VO, permitiéndole al cliente recorrerlos gracias a la implementación del patrón Iterator.
- o) **Service Activator.** Proporciona un modelo para mensajería asíncrona como JMS. El Service Activator recibe los mensajes y localiza y llama a los métodos de los componentes de negocio que se van a encargar de resolver la petición.



LEYENDA: Patrones, de diseño/ análisis, estructurales / / creacionales,
estructurales, comportamiento /

Figura 1: Resumen de los principales patrones en arquitecturas de servidores de aplicaciones.

La implementación de estos patrones no suele hacerse a medida, sino que se recurre a los **frameworks**. Muy relacionados entre sí, los *frameworks* representan una arquitectura de pequeño tamaño que proporciona una estructura genérica, integrando diferentes patrones de modo que puedan ser reutilizados o integrados de manera fácil en las aplicaciones. En un *framework* los patrones tienen una implementación concreta sobre la definición abstracta del patrón. En última instancia son un conjunto de clases e interfaces que cooperan para ofrecer un software reutilizable.

31.3 MVC

El patrón Modelo-Vista-Controlador es el más empleado para estructurar una aplicación, atendiendo a una correcta separación en capas: entrada, procesamiento y salida. Sus principales **ventajas** son una reducción del acoplamiento, facilidad de desarrollo, claridad en el diseño, avance en el mantenimiento, mayor escalabilidad, una mayor cohesión con cada capa fuertemente especializada, y una mayor flexibilidad y agilidad en las vistas, permitiendo su modificación dinámica, sincronización, anidamiento y la existencia de múltiples vistas.

Las **capas** del modelo se concretan en:

- 1) **Modelo** (en inglés *Model*). Encapsula tanto datos como las funcionalidades o casos de uso. Tiene que funcionar independientemente de cualquier representación que tomarán los datos en la salida y cualquier comportamiento que se especifique en

la entrada del sistema. A todos los efectos será una caja negra que recibe peticiones de devuelve resultados, encargándose de manejar los datos y controlar sus transformaciones. Normalmente implementa los patrones DAO, VO y Fachada.

- 2) **Vista** (en inglés *View*). Capa en la que se integran todos los componentes que afecten a la interfaz de usuario. Recibe las peticiones del usuario y las envía hacia el controlador, obteniendo de este las respuestas. Se permiten múltiples vistas del mismo modelo, pero toda la lógica de presentación debe ir en esta capa.
- 3) **Controlador** (en inglés *Controller*). Recibe peticiones de la vista, tales como eventos, refrescos, etc... que recoge con un gestor de eventos o Handler y son traducidos a solicitudes de servicios o casos de uso, enviando las peticiones al modelo. A menudo implementan patrones como Comando o Front-Controller para encapsular las acciones.

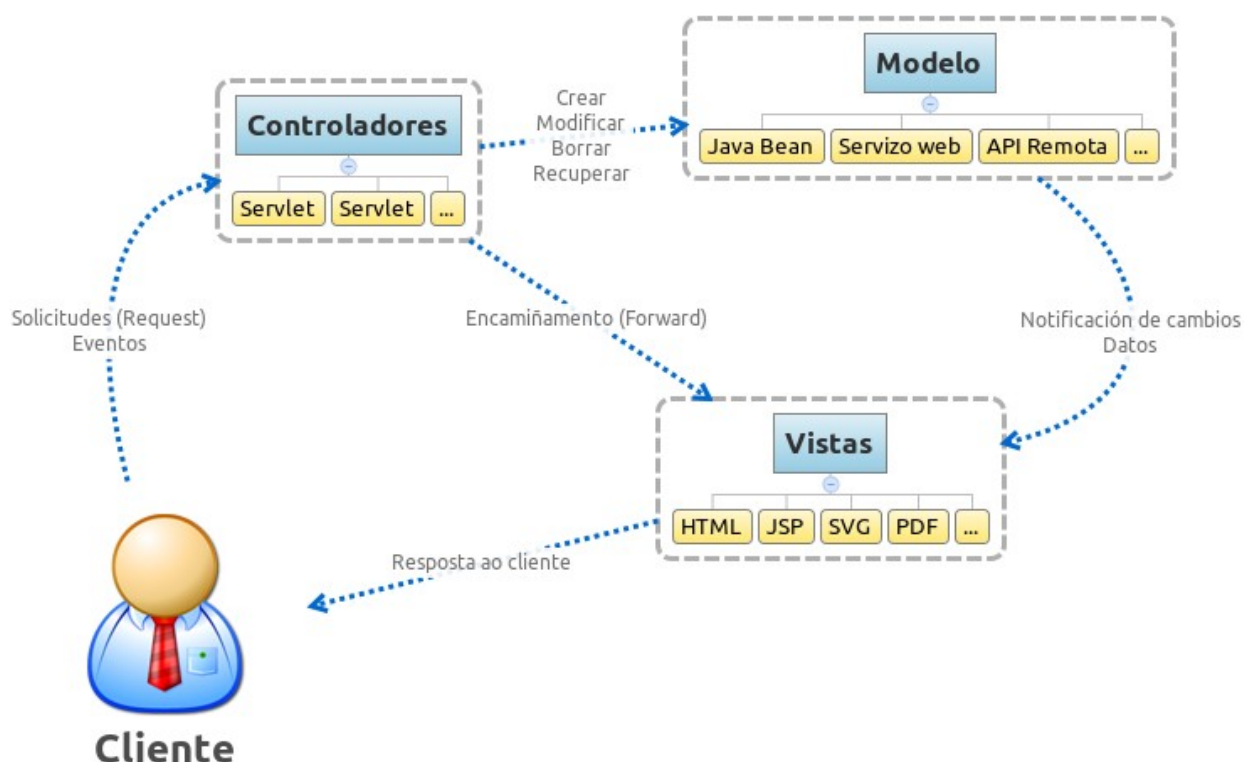


Figura 2: Modelo-Vista-Controlador con tecnologías JEE.

Leyenda: Encaminamiento / Respuesta al cliente

Como patrón de arquitectura, el MVC puede contener a su vez los siguientes **patrones** de diseño:

- ✓ **Observador.** Para proporcionar el mecanismo de publicación y suscripción que permita notificar cambios del modelo en las vistas.
- ✓ **Composite View.** Para permitir la creación de vistas compuestas en una jerarquía.
- ✓ **Estrategia.** Para llevar cuenta de la relación entre las vistas y los controladores, ya que permite modificar dinámicamente aspectos del control.
- ✓ **Factory Method.** Para especificar al controlador una vista como predeterminada.
- ✓ **Decorador.** Para añadir funcionalidades adicionales a las vistas.
- ✓ **Proxy.** Para distribuir la arquitectura en diferentes emplazamientos y mejorar características de rendimiento.

El modelo MVC se concreta tanto en *frameworks* .NET (Windows Forms, ASP .NET, Spring .NET, Maverick .NET, MonoRail, ...) como en JEE (Struts, Spring, Tapestry, Aurora, JSF, etc..). Asimismo, es un modelo que se encuentra extendido a muchas otras tecnologías como PHP, Ruby, Perl, Python, etc ...

Los *frameworks* que implementan el MVC suelen presentar una serie de **características generales**, comunes a todos ellos y que incluyen:

- ✓ Implementación de diferentes patrones de diseño orientados a la reutilización de diseño y código.
- ✓ Controles de validación de campos de formularios.
- ✓ Control de errores y excepciones.
- ✓ Mensajería y localización de cadenas de textos.
- ✓ Librerías de etiquetas o componentes (TagLibs, Widgets, etc...)
- ✓ Componentes de la Interfaz de Usuario, como etiquetado de componentes de formularios, pestañas, controles AJAX, etc...
- ✓ Presentación de información a través de listados y tablas con paginación.
- ✓ Integración con *frameworks* con el patrón Decorador o basados en modelos como Tiles, FreeMarker, Velocity, etc...
- ✓ Acceso datos en diferentes Sistemas de Información: Bases de datos, XML, etc...
- ✓ Abstracción de direcciones URL, Request y sesiones.
- ✓ Autenticación y control de usuarios, roles y filtros.

Entre los *frameworks* que implementan el MVC destaca Apache Jakarta **Struts** (que tiene una evolución en Struts 2.0 al fusionarlo con WebWork), uno de los más empleados en tecnologías JEE y que resulta casi un estándar de facto debido a su integración en otros *frameworks* con más funcionalidades. Se emplea para la implementación de aplicaciones web basadas en Servlets y JSP. Proporciona un conjunto de etiquetas JSP personalizadas (en inglés *Custom Tags*) que permiten encapsular funcionalidades en la vista. Con el modelo de Struts tiene implantación

directa el modelo MVC y otros patrones de diseño pre-construidos, permitiendo la configuración directa de objetos reutilizables ante la configuración de XML. Además proporciona las características anteriormente especificadas: validación, localización, modelo, etc...

Transporta automáticamente los datos insertados polo cliente hasta el controlador a través de Acciones (en inglés *Actions*) mediante formularios ActionForms integrados en el *framework* y viceversa para su presentación. Distingue entre una parte común a cualquier aplicación que haga uso del *framework* que hace de Controlador (ActionServlet) y otra parte configurable a través de archivos de configuración en XML (struts-config.xml, web.xml, ...). Su principal desventaja es no abarcar hasta el nivel de acceso a datos, haciendo que sea necesario el empleo de otros *frameworks* especializados en esta capa para la elaboración de DAO, VO y otras operaciones complementarias.

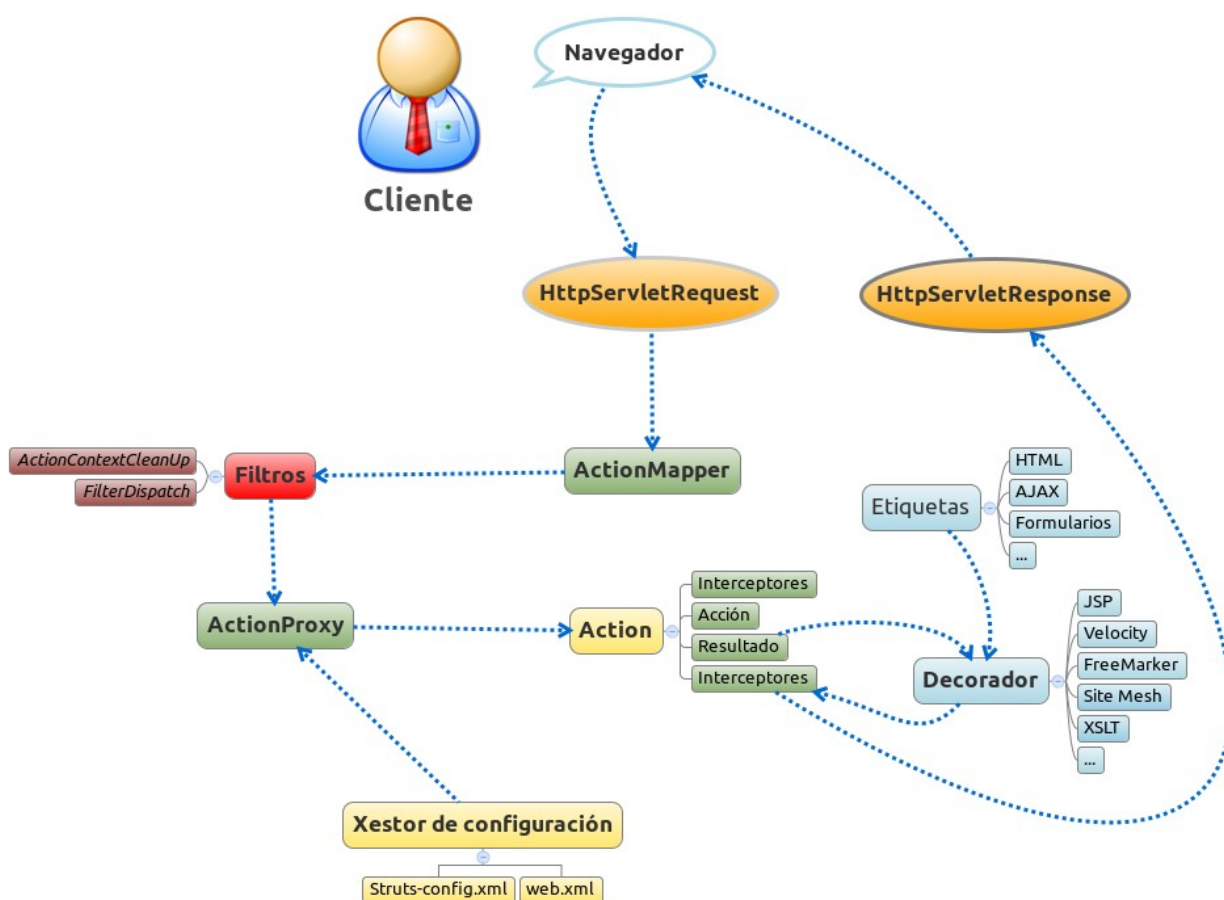


Figura 3: Funcionamiento interno Struts/Struts 2.0.

Legenda : Gestor de configuración

La principal alternativa a Struts sería **Spring** Framework, aunque también permiten integración conjunta y con otros *frameworks* como JSF, Tapestry o WebWork. Aunque su orientación principal sea la plataforma JEE, está disponible en .NET a través del *framework* Spring .NET. Tiene soporte para JTA, JDO, JDBC y ODBC, y permite integración con terceros como Acegi, Hibernate, iBatis y OJB. Como novedad permite programación orientada a aspectos o AOP (en inglés *Aspect-Oriented Programming*) que busca emplear los servicios secundarios como seguridad, registro de log, manejo de transacciones, etc... de las funcionalidades del modelo. Con AOP pueden emplearse los servicios de la aplicación de forma declarativa, o ante archivos XML de configuración o mediante estándares JSR. Asimismo realiza Inversión de Control o IoC, que promueve el bajo acoplamiento a partir de

la inyección de dependencias entre objetos. Las principales desventajas de Spring son que implica una configuración compleja, ya que cada servicio lleva su XML propio, aunque existe la alternativa del JSR. Su contenedor no resulta ligero, lo que impide que tenga aplicación práctica en algunos entornos como pueden ser los dispositivos móviles.

La arquitectura **de Spring** está compuesta por los siguientes componentes:

- ✓ **Core.** El núcleo que aloja el contenedor principal o BeanFactory.
- ✓ **Módulo AOP.** Aporta la implementación de AOP, permitiendo desarrollar interceptores de método y puntos de ruptura para desligar el código del modelo de las funcionalidades transversales.
- ✓ **Módulo DAO.** Aporta la capa de abstracción de acceso a datos y sistemas de información sobre los diferentes conectadores disponibles. Además aporta manejo de transacciones vía AOP y otros servicios.
- ✓ **Módulo ORM.** Aporta integración para las distintas API de correspondencia entre objetos y entidades de bases de datos con soporte de diferentes tecnologías e integración con *frameworks* de terceros.
- ✓ **Módulo JEE.** Integración con aplicaciones y servicios JEE.
- ✓ **Módulo Web.** Aporta componentes especiales orientados a desarrollo web e integración con *frameworks* alternativos como Struts o JSF, además de una implementación del paquete Spring MVC.

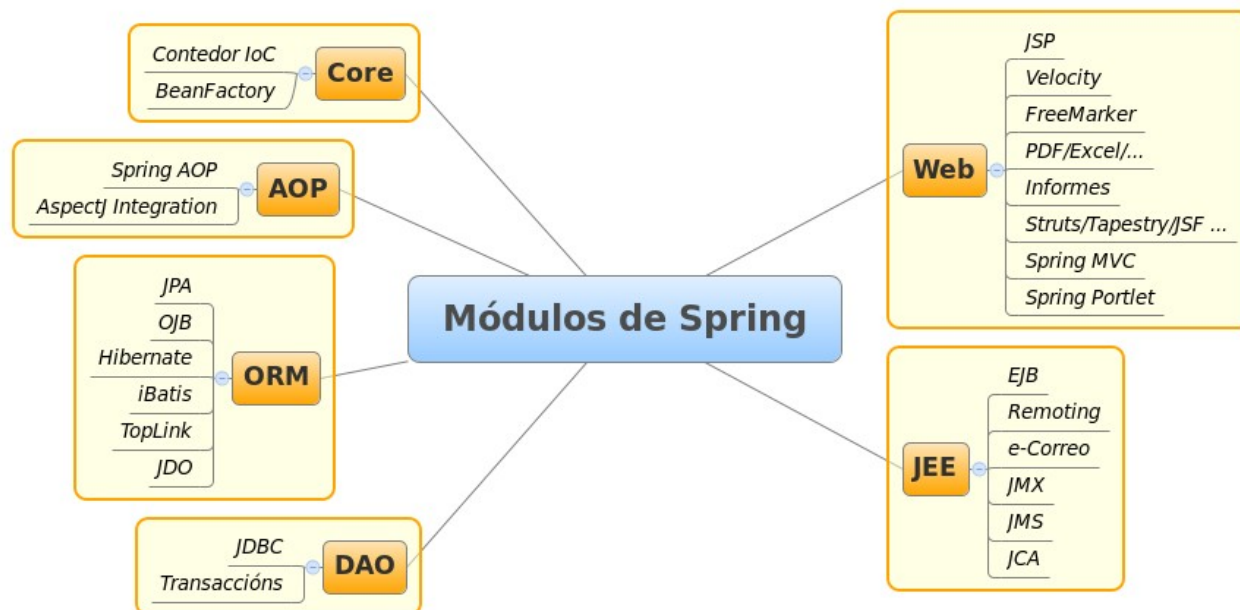


Figura 4: Arquitectura de Spring.

Leyenda: Transacciones

31.4 JSF

La tecnología Java Server Faces proporciona un *framework* de interfaz de componentes de usuarios para el lado del servidor de aplicaciones. En su base emplea JSP pero permite otras tecnologías para interfaces de usuario como XUL. Entre los **componentes** de JSF se encuentran:

- 1) Un conjunto de APIs para representar y manejar componentes de la interfaz de usuario. Entre las opciones que gestionaría se encontrarían control de estado y eventos, validaciones de formularios, conversión de datos, control de navegaciones y soporte de localización y accesibilidad.
- 2) Un conjunto de componentes de la interfaz de usuario reutilizables.
- 3) Dos librerías de etiquetas personalizadas (en inglés *Custom Tags*) para JSP.
- 4) Modelo de eventos para el lado del servidor.
- 5) Soporte para Managed Beans de control de eventos.

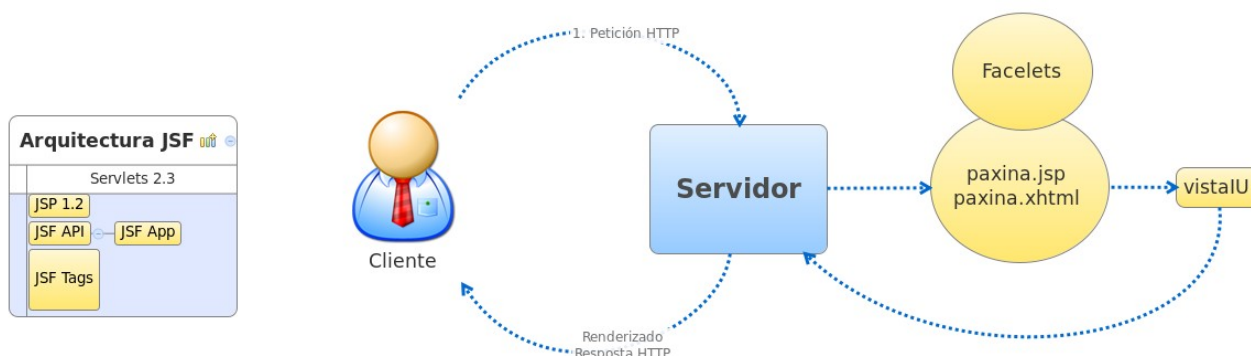


Figura 5: Arquitectura JSF y funcionamiento básico.

LEYENDA: Página / respuesta

Uno de los componentes de JSF es el *framework* JavaServer **Facelets**, destinado a la gestión de modelo (en inglés *templates*). Las principales características de este *framework* son:

- ✓ Coste de tiempo cero para el desarrollo de etiquetas de componentes de la Interfaz de Usuario.
- ✓ Facilidad de creación de modelo de páginas y componentes reutilizables.
- ✓ Soporte para UEL (en inglés *Unified Expression Language*) y validaciones EL.
- ✓ Compatibilidad con cualquiera RenderKit.
- ✓ Se integra plenamente con JSTL, cosa que en JSF puede ocasionar problemas.
- ✓ Compilación más rápida que con JSP.

Actualmente existen numerosas **implementaciones** de JSF que pueden complementar a la especificación oficial JEE. Existe la posibilidad de combinar diferentes implementaciones en una misma aplicación, siendo las más habituales:

- a) **MyFaces Tomahawk/Sandbox.** Desarrollado por Apache, proporciona un conjunto de componentes reutilizables compatibles con las especificaciones JSF 1.1, JSF 1.2 y JSF 2.0.
- b) **Trinidad.** Subproyecto de MyFaces, a partir de la inclusión de los componentes ADF Faces y otros avances. Proporciona los siguientes elementos: Una implementación de JSF, varias librerías de componentes Widgets, la extensión MyFaces Orchestra y módulos de integración para otras tecnologías y estándares como MyFaces Portlet Bridge.
- c) **Tobago.** Otro proyecto basado en MyFaces en una aproximación del diseño de páginas web al de aplicaciones de escritorio. Proporciona una serie de componentes de la Interfaz de Usuario como abstracciones del HTML. Presenta un conjunto de temas para clientes HTML con vistas independientes de HTML/CSS/Javascript.
- d) **ICEfaces.** Contiene diversos componentes de interfaces de usuario enriquecidas basadas en AJAX y compatibles con SSL, como editores de texto, reproductores multimedia, etc... Soporta Facelets y Seam, además de ser compatible con Spring, WebWork y Tomahawk.
- e) **RichFaces.** Otro *framework* AJAX que incluye ciclo de vida, validaciones, conversiones y gestión de recursos en las aplicaciones. Soporta Facelets y Seam, además de ser compatible con Spring y Tomahawk.
- f) **Ajax4JSF.** Otra alternativa más que proporciona un *framework* AJAX que incluye ciclo de vida, validaciones, conversiones y gestión de recursos en las aplicaciones. Soporta Facelets y Seam, además de ser compatible con Spring y Tomahawk. Incluye los siguientes componentes:
 - ✓ *Ajax Filter.* Filtro de peticiones para AJAX.
 - ✓ *Ajax Action Components.* Envían las peticiones desde el cliente.
 - ✓ *Ajax Containers.* Interfaz que describe zonas dentro de las JSP.

- ✓ *Javascript Engine*. Motor en el lado del cliente que actualiza diferentes zonas de las JSP en función de la respuesta AJAX.

31.5 ANTIPATRONES

Contrarios al **concepto** de patrones, los antipatrones representan malos usos habituales, o soluciones que, sobre todo a lo largo del tiempo, presentan más problemas de los que resuelven. Se trata en definitiva de malas prácticas. Existen dos variantes principales: los que describen una mala solución para un problema habitual y que produce consecuencias difíciles de arreglar a lo largo del tiempo; y aquellos que describen cómo poner remedio a un problema y convertirlo en una buena solución. Por norma general los antipatrones se ven como una buena idea al inicio, que falla de mala manera a la hora de su implementación.

Las **motivaciones** o razones para tener en cuenta los antipatrones como caso de estudio atienden a los siguientes puntos:

- ✓ Permiten identificar soluciones de riesgo para problemas habituales.
- ✓ Proporcionan experiencia del mundo real para detectar problemas que se repiten a lo largo del tiempo, ofreciendo posibles soluciones o alternativas para sus implicaciones más habituales.
- ✓ Proporcionan un marco común para la identificación y documentación de los problemas y diseño de las soluciones.

Como sucedía con los patrones, los antipatrones suelen agruparse en diferentes **categorías**, siendo las principales:

- 1) **Antipatrones de desarrollo software**. Definen problemas asociados al desarrollo software a nivel de aplicación, al nivel de los

patrones de diseño.

- 2) **Antipatrones de arquitectura de software.** Se centran en la distribución y relaciones de las aplicaciones, servicios y otros componentes software a nivel de organización.
- 3) **Antipatrones de gestión de proyectos software.** Identifican escenarios críticos sobre la comunicación entre personas y resolución de problemas en equipos, viendo como afectan a un proyecto o proceso software.

Asimismo los antipatrones tienen aplicación en muchas otras áreas como metodología, gestión de la configuración, TDD, diseño web, accesibilidad, usabilidad, etc...

Dentro de los **antipatrones de desarrollo** software nos encontramos entre los más comunes:

- a) **Blob u objeto todopoderoso** (en inglés *God Object*). Se emplea un único objeto, clase o módulo para aglutinar un amplio conjunto de funcionalidades que deberían encontrarse divididas. Con este patrón se cae en un código ampliamente desorganizado y muy acoplado.
- b) **Flujo de lava o lava seca** (en inglés *Lava Flow*). Representa aquellos tipos de programación por impulsos o erupciones de código, de manera desestructurada, desorganizada y con poca documentación. El sistema crece de manera desproporcionada y, pasado un tiempo, los bloques de código más antiguos se consideran metafóricamente solidificados en lo que respecta a la dificultad de solucionar cualquier tipo de problema en el que se encuentren involucrados.
- c) **Descomposición funcional.** Diseño no orientado a objetos, fruto de la migración desde lenguajes estructuradas a POO.

- d) **Poltergeists.** O clases fantasma, debido al desconocimiento dentro de la aplicación de cuál es el objetivo de algunas clases, siendo en muchos casos su única función transmitir información entre clases.
- e) **Martillo dorado.** Emplear la misma solución para cualquier problema que surja, sin contemplar otras posibles alternativas.
- f) **Código spaghetti.** Hace referencia a código de aplicación con una estructura compleja e incomprensible con multitud de tecnologías mezcladas. La analogía se hace a partir de las relaciones entre el código que parecen un gran número de hilos mezclados y enrollados.
- g) **Programación copiar y pegar.** Solución en la que en lugar de crear soluciones genéricas, se copian y se adaptan soluciones ya existentes.

En lo tocante a los **antipatrones de arquitecturas** software destacan por ser los más habituales:

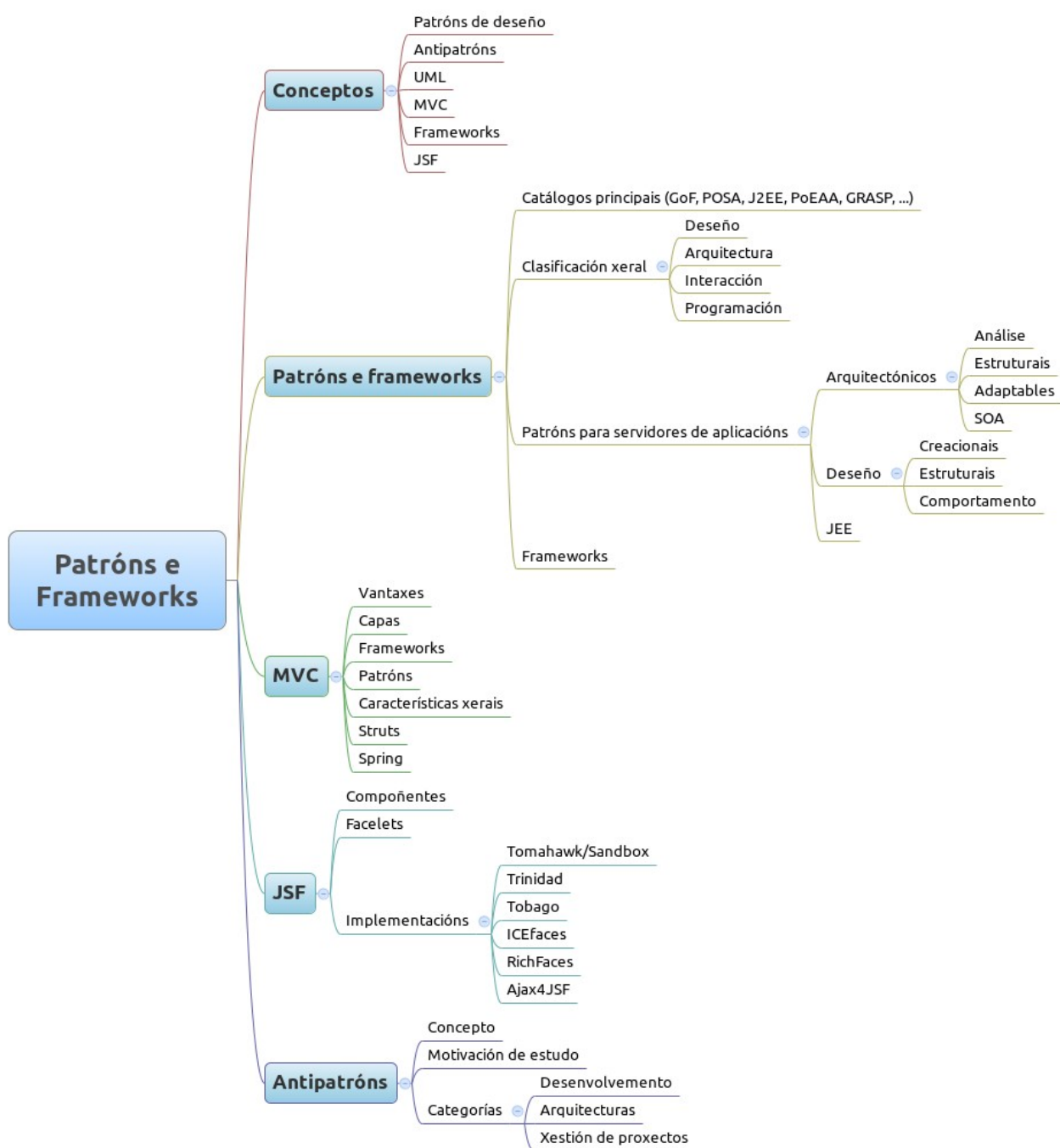
- a) **Reinventar la rueda.** Implementar componentes ya disponibles o que pueden aprovecharse con ligeras modificaciones. Se da por la tendencia a hacer todo uno mismo o por el desconocimiento de la arquitectura y soluciones disponibles en el mercado o alternativas de código abierto.
- b) **Vendor Lock-In.** Construir una arquitectura dependiente de un producto de terceros, en especial cuando se trata de software privativo. Se ponen en peligro la escalabilidad del sistema y aumentan los costes de mantenimiento.
- c) **Aislamiento en la organización.** En una misma organización o conjunto de sistemas se crean diferentes unidades aisladas entre sí que crecen en paralelo solucionando problemas comunes de manera independiente. En este modelo puede crecer sobremanera el coste de integración llegada la necesidad del mismo.

- d) **Diseño por comité.** Demasiadas personas participan de los requisitos del proyecto, dando lugar a un diseño demasiado abstracto y excesivamente complejo por contemplar demasiados puntos de vista particulares. Se complica la toma de decisiones, dando a lugar a demasiadas reuniones de larga duración, que dificultan y provocan errores a lo largo de todo el ciclo de vida del desarrollo.
- e) **Arquitectura por implicación.** No existe documentación de la arquitectura del sistema, ni de los procesos, ni de las tareas automatizadas más habituales.

En lo tocante a los **antipatrones de gestión de proyectos software** destacan por ser los más habituales:

- a) **Parálisis de análisis.** Los procesos de análisis y diseño se prolonga tanto que el proyecto acaba muriendo en él sin llegar a llevarse a cabo. Son desarrollos opuestos a los modelos basados en prototipos e iterativos.
- b) **Muerte por planificación.** Demasiada planificación y reuniones sin llegar a concretar puntos de partida para el desarrollo. De nuevo son desarrollos opuestos a los modelos basados en prototipos e iterativos.
- c) **Personas problemáticas** (en inglés *corncob*). Personas poco aptas para participar en equipos, o con poca capacitación o aptitud, obstruyen, desvían e incluso sabotean el desarrollo.
- d) **Gestión irracional.** La falta de decisión y capacitación sumadas a la nula planificación pueden dar lugar a la toma de decisiones con posterioridad y desarrollos de urgencia.
- e) **Proyectos sin gestión.** No se atiende al análisis y el diseño, solo a implementación. Se van arreglando incidentes según suceden en “modo pila” (las últimas primero).

31.6 ESQUEMA



Leyenda: patrones y frameworks, antipatrones / patrones de diseño, antipatrones / catálogos principales , clasificación general, diseño, patrones para servidores de aplicaciones / ventajas, características generales / Implementaciones / Motivación de estudio, Desarrollo, gestión de proyectos.

31.7 REFERENCIAS

Deepak Alur y otros.

Core J2EE Patterns. Best Practices and Design Strategies. (2003).

William Crawford y Jonathan Kaplan.

J2EE Design Patterns. (2003).

Steven Metsker y William Wake.

Design Patterns in Java. (2006).

Autor: Juan Marcos Filgueira Gomis

Asesor Técnico Consellería de Educación y O. U.

Colegiado del CPEIG



32. APLICACIÓNS DE INTERNET ENRIQUECIDAS (RIA). INGENIERÍA DEL SOFTWARE.

TEMA 32. APLICACIONES DE INTERNET ENRIQUECIDAS (RIA)

32.1 INTRODUCCIÓN Y CONCEPTOS

32.2 AJAX

32.3 RIA PARA MULTIMEDIA Y ANIMACIONES

32.4 OTRAS TECNOLOGÍAS RIA

32.5 ESQUEMA

32.6 REFERENCIAS

32.1 INTRODUCCIÓN Y CONCEPTOS

Las aplicaciones de Internet enriquecidas o **RIA** (en inglés, *Rich Internet Applications*), son un conjunto de tecnologías que buscan acercar las interfaces de las aplicaciones web a las de las aplicaciones de escritorio, dotándolas de nuevas funcionalidades —de ahí la riqueza— y agilizando aspectos como las recargas de datos. Por norma general, necesitan un *framework*, componente adicional o *plug-in* en el navegador que permitan su interpretación. En las aplicaciones RIA, la mayor parte de la comunicación se hace de manera asíncrona en comunicaciones transparentes al usuario que evitan gran parte de las recargas de páginas para realizar actualizaciones de datos. Frente a estas ventajas en lo que respecta a la usabilidad, en cuanto a la mejora de las funcionalidades y actualizaciones de datos, la principal desventaja será la accesibilidad de la página para usuarios que presenten dificultades de acceso a la información en la web.

Muchas de estas **tecnologías** pertenecen al mundo del software propietario, y dependen en gran medida de las compañías que las desarrollan. Las principales tecnologías se encuentran en las plataformas Flash, Flex y AIR de Adobe, Silverlight de Microsoft, OpenLaszlo, incontables *frameworks* AJAX y Javascript, y otras tecnologías, como las ya maduras,

Applets y Java WebStart, y las emergentes como XUL, JavaFX, GWT o Bindows. Cualquiera de estas tecnologías se localiza en la capa de vista, usuario o cliente como complemento a la (X)HTML/CSS y se integran con las tecnologías de servidores de aplicaciones como .NET/JEE.

Dentro de los **casos de éxito** de esta tecnología, en la actualidad la mayor parte de las aplicaciones y servicios web globales de mayor uso dentro de la Web 2.0 hacen uso de tecnologías RIA en sus interfaces, como, por ejemplo, Google Maps, Gmail, Flickr, Meebo, Orkut, y un largo etcétera.

32.2 AJAX

AJAX (en inglés *Asynchronous JavaScript And XML*), Javascript Asíncrono y XML, se origina para aprovechar que la comunicación entre el usuario y la interface no es fluida, permitiendo realizar comunicaciones asíncronas con el servidor y realizar así un mayor aprovechamiento del ancho de banda, obteniendo una mayor velocidad de respuesta. Los datos se cargan en un segundo plano sin afectar a la interface. AJAX no representa una tecnología en sí misma, sino que se trata de la combinación de un grupo de **tecnologías** ya existentes:

- (X)HTML e CSS para el diseño de las páginas web.
- DOM (en inglés *Document Object Model*), o Modelo de Objetos del Documento, API que representa un conjunto de objetos para manipular y modificar dinámicamente documentos (X)HTML e XML a través de lenguajes de Script como Javascript, JScript o ECMAScript.
- Objetos de los tipos Iframe o XMLHttpRequest para intercambiar datos de manera asíncrona con el servidor.
- XML para los formatos de intercambio de datos y comunicaciones a través de JSON o EBML.
- Otras tecnologías para facilitar la implantación de soluciones específicas como XSLT, RSS, PDF o otras tecnologías RIA.
- Javascript para proporcionar el nexo común a todo el conjunto.

Como sucede con las tecnologías RIA en general, es requisito imprescindible que el navegador tenga **soporte** para el conjunto de tecnologías AJAX; de otro modo habría que proporcionar una alternativa HTML básica. Aun así, cada vez se encuentra soportado por un mayor número de navegadores y no requiere la instalación de complementos.

El **funcionamiento básico** de AJAX se basa en el objeto de comunicación asíncrona, como, por ejemplo, el XMLHttpRequest, que se instala con una librería, *framework* o motor AJAX en el lado del cliente. El motor AJAX proporcionará los métodos para permitir la comunicación asíncrona de datos, además de definir los componentes reutilizables AJAX con la definición de su comportamiento y el contenido y estructura general del documento. El hecho de realizar todas estas funciones desde el cliente de manera asíncrona supone el gran avance de rendimiento de AJAX sobre el modelo tradicional de desarrollo web.

Figura 1: Funcionamiento básico de AJAX

TEXTO FIGURA: Lógica / Tecnologías RIA / Tecnologías extendidas / Contenido y estructura.

La **refactorización** de aplicaciones tradicionales al modelo AJAX implica cambios en la estructura interna con la preservación de las funcionalidades. La metodología de refactorización habitual implica una serie de cambios a pequeña escala, para lo cual es ideal la programación orientada a objetos. Estos cambios van desde:

- **Refactorización a nivel de método/clase.** En sistemas con poco acoplamiento, evitando, por ejemplo, que se modifiquen los atributos de las clases entre objetos. Estos accesos múltiples pueden integrarse en un nivel superior una vez resueltas las dependencias del método/clase.
- **Creación de nuevas clases.** Se definen nuevas clases especializadas en la arquitectura AJAX con responsabilidades e interfaces bien definidos.
- **Eliminación de clases intermediarias.** Se eliminan las delegaciones en exceso entre clases del modelo tradicional en aplicación de las consideraciones sobre antipatronos de exceso de capas.
- **Componentes y etiquetado.** Diferentes componentes, sobre todo de la vista, presentan funcionalidades comunes que se pueden factorizar, a través de componentes AJAX y etiquetados, para facilitar el mantenimiento y la reutilización.

En la actualidad existen infinidad de **frameworks** y **librerías AJAX**, que incorporan componentes de la vista, diferentes funcionalidades Javascript, elementos para comunicación asíncrona, tanto en el cliente como en el servidor, y otros elementos para integración con otras tecnologías RILA. El objetivo de estos *frameworks* se resume en facilitar el desarrollo de aplicaciones web basadas en AJAX, haciendo hincapié en aspectos de la

capa de vista o cliente. Los principales *frameworks* en cuanto a su uso más extendido, son:

□ **Prototype.** Puede ser el *framework* de uso más extendido. También de código abierto, dispone de la extensión **Scriptaculous** para añadir animaciones y efectos en los documentos, y JSON para intercambio de datos. Sirve a su vez de base de otros *frameworks* AJAX. Permite una gran integración en aplicaciones desarrolladas con *Ruby on Rails* pero también puede operar de manera independiente. Sus principales características son:

1. **DOM Extendido.** Referencia ágil a objetos DOM, como, por ejemplo, empleando la función `$()` en lugar de `document.getElementById()`.
2. **Scriptaculous.** Aporta al *framework* un constructor de objetos DOM (*builder.js*), un repositorio de efectos visuales (*effects.js*, *slider.js*), funcionalidades de control de elementos (X)HTML (*dragdrop.js*, *controls.js*) y métodos para realizar test de verificación unitarios (*unittest.js*).

□ **Dojo Toolkit.** Proyecto de software libre, actualmente con el soporte de IBM y Sun entre otros, que contiene varias API Javascript modulares y una amplia colecciones de widgets para uso bajo demanda, agrupados en un sistema de paquetes al estilo de JEE. Entre sus principales características están la aportación de:

- a) **Componentes empaquetados en Dijit.** Widgets para la estructura de las páginas como menús, pestañas; específicos para calendarios, relojes, gráficos, vectores 2D/3D, ordenación de tablas y paginación; además de elementos para formularios y su validación, elementos HTML5 y componentes para mejorar la accesibilidad. Asimismo, presenta un editor de texto enriquecido y soporte drag entre sus componentes.

- b) **Comunicación asíncrona.** Provee de una capa de abstracción para la comunicación transparente entre el navegador y el servidor web que hace uso de elementos Iframes ocultos para el refresco de datos.
- c) **Almacenamiento en el servidor.** Implementa diferentes mecanismos de almacenamiento de datos vía CVS, OPML, RDF o el servicio web Del.icio.us.
- d) **Soporte para otras tecnologías.** Permite integración con tecnologías RIA como las aplicaciones AIR basadas en Javascript a través de API y soporte para móviles.

□ **jQuery.** Otro proyecto de software libre, que en este caso busca simplificar el acceso a documento (X)HTML, el modelo DOM, la manipulación de eventos, utilidades, animaciones y efectos. Permite la instalación a través de un paquete básico muy ligero (*jquery.js*), que puede ser ampliado a través de plug-ins como JExpand, para tablas, y JQueryUI para widgets con efectos visuales, entre otros muchos. Entre sus principales características se encuentran:

- a) Integración en la plataforma .NET y con los *frameworks* ASP .NET MVC y ASP .NET AJAX.
- b) Soporte para CSS 3 y XPath.
- c) Soporte para manipulación de (X)HTML y JSON.
- d) Hace uso de programación no intrusiva.
- e) Ligero y extensible.

□ **Qooxdoo.** Colección de librerías Javascript multipropósito de código abierto que, como las vistas anteriormente, permite control ágil a alto nivel de (X)HTML, CSS y DOM, además de proporcionar funcionalidades extendidas. La principal diferencia respecto a las

anteriores es que proporciona widgets de última generación muy similares a los de las aplicaciones de escritorio. Entre sus principales características se encuentran:

- a) **Abstracción del navegador.** Establece una capa intermedia de abstracción del navegador con las especificaciones necesarias para los principales tipos de navegadores, definiendo así una interfaz estándar que mejora la compatibilidad sin necesidad de instalar *plug-ins* adicionales.
- b) **Administración de eventos.** Provee una interfaz propia con métodos para registrar y eliminar eventos.
- c) Herramienta de desarrollo de interfaces de usuario.
- d) Soporte de internacionalización i18n y localización l10n que permite el formato de traducción basado en archivos .po.
- e) Provee *frameworks* para depuración de tests unitarios y simulaciones.

□ **Mootools.** *Framework* de código abierto modular y extensible que permite al desarrollador seleccionar qué componentes emplear para minimizar el peso final de la librería en el cliente. Presenta un componente para la incorporación de efectos avanzados y transiciones, estrechamente relacionados con Flash, siendo un punto fuerte su integración con esta otra tecnología RIA. Provee los siguientes componentes:

- a) **Core.** Núcleo de funciones básicas que emplean todos los demás componentes del *framework*.
- b) **Class.** Librería para instanciación y manipulación de objetos.
- c) **Natives.** Extensiones de funciones básicas Javascript.

- d) **Element y Effects/FX.** API para manejo de documentos HTML y aplicación de efectos sobre sus elementos.
- e) **Remote.** Para intercambio de datos con el servidor a través de peticiones XMLHttpRequest, JSON o Cookies.

□ **ExtJS.** Conjunto de librerías derivadas de la Yahoo! UI; actualmente se emplea como extensión de JQuery y Prototype incorporando *widgets* especializados; en especial, en la representación de gráficas y *grids*. Existe además una adaptación específica para GWT denominada ExtGWT, con muchas optimizaciones para este entorno. Incorpora una capa propia dentro de una arquitectura MVC, lo que le permite proveer de flexibilidad por lo que respecta a los estilos, haciendo uso de la extensión SASS (en inglés *Syntactically Awesome Style Sheets*), una extensión de CSS3. Asimismo, provee de librerías que facilitan la integración con AIR y Spring, como *backend*. Dentro de los componentes de datos, dispone de varios lectores tanto para XML como JSON. La arquitectura general incluye los paquetes Base e Core con las funcionalidades comunes; los Componentes de la interfaz de usuario con los widgets y gadgets; Remoting para la ejecución de métodos en el servidor vía RPC; los Servicios de datos para lectura de vectores, XML y JSON; y el *miniframework Drag and drop* para permitir soporte de arrastre entre los componentes del *framework*.

□ **Rico.** Basado en Prototype y orientado hacia la Web 2.0, las principales aportaciones de este *framework* incluyen efectos de animaciones que permiten realizar transiciones que pueden ser interrumpidas, pausadas o reiniciadas, permitiendo el solapamiento de animaciones. Permite la creación de efectos cinematográficos y otros efectos visuales.

Asimismo, proporciona las funcionalidades básicas para soporte AJAX y amplía parte del repertorio de Prototype con mejoras.

▣ **DWR.** (En inglés, *Direct Web Remoting*). *Framework* de código abierto orientado a la integración de AJAX con aplicaciones JEE a través de mecanismos de RPC como RMI o SOAP. Permite ejecutar código Java en un servidor de aplicaciones como si estuviese en el navegador del cliente, invocando los objetos como si fuesen locales. Consta de dos elementos principales: un *framework* Javascript en el cliente y un Servlet en el servidor para procesar las peticiones y generar las respuestas. El Javascript actuará como proxy de las clases Java, permitiendo que en ese código se incluyan las clases Java en el servidor. En una llamada a un método de una clase, DWR genera dinámicamente una versión Javascript de la clase AjaxService, invocada a través de un manejador de eventos que gestiona la interacción con el servidor. Cuando llega la respuesta al cliente se invoca una función *callback* para actualizar el contenido del documento. Este método se denomina Reverse AJAX, y soporta tres métodos básicos de envío de datos:

- 1) **Polling.** El navegador pregunta al servidor en intervalos regulares si completó la petición.
- 2) **Piggyback.** El servidor espera a la siguiente petición del navegador para darle la respuesta.
- 3) **Comet.** El servidor responde al navegador de manera planificada tipo Streaming en una respuesta Http larga.

Asimismo, provee de dos opciones de comunicación remota:

- 1) **DWR nativo.** Empleando un superconjunto de JSON donde el motor DW (*engine.js*) maneja las peticiones y prepara la ejecución de las llamadas al servidor.
- 2) **JSON/JSONP.** API para JSON que facilita la integración con otros *frameworks* como Dojo, ExtJS o JQuery.

Respecto al tema de la seguridad, DWR contempla protecciones específicas contra ataques XSS (en inglés, *Cross Site Scripting*) y CSRF (en inglés, *Cross Site Request Forgery*).

□ **SAJAX.** (En inglés, *Simple AJAX Toolkit*). Herramienta de código abierto que, de manera análoga, a DRW permite realizar llamadas a métodos del servidor en PHP, ASP, Coldfusion, Ruby, Perl, Python y otros lenguajes desde Javascript en el navegador, sin tener que recargar la página.

Provee de una API para cada lenguaje de servidor, por ejemplo *Sajax.php*, que se incluye en el código de este para permitir la integración con el Javascript del navegador.

□ **GWT.** (En inglés *Google Web Toolkit*). *Framework* de desarrollo AJAX dentro de aplicaciones Java. Este entorno permite que al definir una interface Java se traduzca con el compilador GWT de manera transparente a Javascript y HTML. El principal objetivo de este *framework* es integrar en un mismo IDE el desarrollo de la aplicación y de la parte de interfaces de usuario con AJAX, pero además provee de otras funcionalidades como componentes HTML dinámicos y reutilizables, protocolos de transferencia XML y JSON, internacionalización i18n, integración con Junit, incluso en las llamadas RPC, y con Javascript a través de JSNI. La arquitectura de GWT se estructura en los siguientes elementos:

1. **Compilador Java a Javascript GWT.** Para aplicaciones web genera automáticamente el código Javascript necesario para la interface Java definida.
2. **Hosted Web Browser.** Motor de ejecución de aplicaciones Java sin traducirlas a Javascript a modo de máquina virtual Java.

3. **Librería de Emulación JRE.** Contiene los principales paquetes Java de uso común soportadas por GWT.
4. **Librería de clases de Interfaces de Usuario GWT.** Provee de un conjunto de componentes para interfaces de usuario.

A mayores de estos *frameworks* existen infinidad de alternativas y librerías para temas específicos o versiones más o menos simples de propósito general, como:

- 1) **AjaxAC.** *Framework* PHP que emplea AJAX en el cliente y se orienta a la reutilización por disponer de clases muy simples.
- 2) **AJAX .NET Professional.** Librería AJAX para ASP .NET con funcionalidades básicas para controles de usuario y utilidades de uso general.
- 3) **ATLAS.** También denominado ASP .NET AJAX, integra en un mismo *framework* un conjunto de extensiones para integrar AJAX en .NET, que incluye la Microsoft Ajax Library.
- 4) **BAJAX.** Librería Javascript muy ligera (<6k), para integrar AJAX de la forma más simple posible.
- 5) **Taconite.** *Framework* para desarrollo AJAX, que automatiza tareas para gestionar el objeto XMLHttpRequest o la creación de contenido dinámicamente.
- 6) **Spry Framework for Ajax.** Librería Javascript de Adobe para la integración de AJAX con orígenes de datos XML, JSON y HTML para lenguajes de servidor como Coldfusion, PHP o ASP .NET. Spry ofrece tres componentes principales: Datos, Widgets y Efectos.
- 7) **Tacos.** Librería que proporciona componentes, efectos, validaciones y funcionamiento AJAX para el *framework* Tapestry.

- 8) **XAJAX**. *Framework* AJAX para desarrollo en PHP, que permite desde el navegador llamar a funciones del servidor.
- 9) **Zephyr**. *Framework* AJAX para desarrollo en PHP5 bajo el modelo MVC. Provee de un motor de modelos, soporte para datos adoDB y otras opciones.
- 10) **ZK**. *Framework* para desarrollo de aplicaciones Java que pretende hacer transparente la tecnología Javascript. Los componentes de la interface de usuario se relacionan con componentes POJO en el servidor. Se recomienda la integración con Spring, Toplink o Hibernate y aporta protecciones contra ataques XSS, CSRF y DoS. Se verá con detalle más adelante.

32.3 RIA PARA MULTIMEDIA Y ANIMACIONES

A medida que mejoró el ancho de banda de las conexiones fueron en aumento las tecnologías RIA destinadas a mejorar las funciones multimedia, gráficos vectoriales, animaciones e interactividad. La pionera de estas tecnologías fue Flash para, posteriormente, aparecer Flex, AIR, JavaFX, OpenLaszlo y Silverlight como principales alternativas.

32.3.1 FLASH RIA

La plataforma Flash evolucionó de plug in en el cliente (Flash Player), para la visualización de imágenes vectoriales y animaciones, hacia una arquitectura RIA para dotar de nuevas funcionalidades a las interfaces web. Representa la primera tecnología RIA, y constituye el marco que engloba diferentes tecnologías dentro de lo que se denomina Flash RIA. Dentro de las Flash RIA se encuentran las tres tecnologías principales soportadas por Adobe —y anteriormente Macromedi— cuyo uso es el más extendido:

- 4.1. **Flash.** Empaqueta de aplicaciones en archivos SWF a modo de componentes.
- 4.2. **Flex.** A partir de un servidor de aplicaciones JEE realiza la comunicación con el SWF permitiendo llamar a objetos del servidor.
- 4.3. **AIR.** Para ejecución de aplicaciones Flash en el equipo del cliente sin necesidad de navegadores como intermediarios.

Alternativamente, existen otros proveedores de tecnologías Flash RIA, entre los que se encuentran:

- 4.3.1. **OpenLaszlo.** Muy similar a Flash, pero con un lenguaje de programación propia, LZX.
- 4.3.2. **SnappMX.** Orientada hacia servicios web.
- 4.3.3. **Zulu.** Permite desarrollar aplicaciones conjuntamente con el estándar XUL y Flash
- 4.3.4. **XAMLON.** Permite desarrollar aplicaciones Flash con el lenguaje de marcado XAML dentro de la plataforma .NET.

La orientación principal de Flash, a diferencia de AJAX, es la de ser un complemento de la interfaz de usuario que amplía determinadas funcionalidades, en especial en el campo de las animaciones y de la interacción con el usuario. Los entornos de desarrollo de Flash están más orientados hacia la edición de animaciones que hacia el desarrollo web, pero se fue abriendo camino en el campo de la elaboración de widgets, soporte multilenguaje, efectos 3D, control y validación de formularios. Permite integración con AJAX y Javascript, pero dispone de un lenguaje de *script* propio denominado ActionScript. Este *script* de programación orientado a objetos sigue el estándar ECMA-262, implementando E4X (en

inglés, *ECMAScript for XML*). Opera con un modelo de eventos basado en la especificación DOM, aunque no lo sigue completamente. Se lanza en una máquina virtual específica AMV2 (en inglés, *ActionScript Virtual Machine*), alojada en el entorno de ejecución Flash Player. Por último, destacar que permite conectividad con Servicios web y Bases de datos de manera remota a través de la clase *DataProvider*.

Como sucede con la mayoría de *frameworks* de desarrollo, la plataforma Flash puede ampliarse con paquetes de librerías de terceros; entre estas destacan:

- a) **SPL** (en inglés, *Spelling Plus Library*). Para diseño de editores de texto enriquecido con corrección ortográfica.
- b) **Red5**. Servidor Flash de software libre.
- c) **Papervision3D**. Motor de generación 3D de software libre.
- d) **As3corelib**. Paquete de librerías ActionScript 3 que contiene clases y utilidades de uso común. Incluye codificadores de imagen, serialización JSON, API para fechas, Strings y otros tipos de datos y codificación de llaves MD5 y SHA 1.
- e) **SWFObject**. Javascript para incrustar contenido Flash en documentos (X)HTML.
- f) **Tweener**. Para crear animaciones y transiciones directamente trabajando con ActionScript.
- g) **Gaia**. *Framework* orientado hacia agilización del desarrollo Flash.

32.3.1 FLEX

Flex es la evolución de Flash ampliando el ámbito de desarrollo RIA con nuevas tecnologías y formatos. Se diferencia de Flash en su facilidad de integración con tecnologías de lenguajes de servidor, lo que facilita el uso de patrones de diseño, y en que emplea MXML (en inglés, *Macromedia extensible Markup Language*) para definir el aspecto y comportamiento de

las interfaces de usuario. Como Flash, soporta el lenguaje ActionScript y su plataforma incorpora librerías de componentes para interfaces de usuario específicas. Permite integración con otras tecnologías del lado del servidor, como Servicios Web, REST o AMF. Las aplicaciones Flex pueden integrarse en un documento HTML, de manera que este puede actualizar dinámicamente la vista y enviar y recibir datos asíncronamente con el servidor de fondo, de modo similar a AJAX.

En las **comunicaciones cliente servidor**, Flex en el cliente se comunica con el servidor vía HTTP, y dispone de tres API RPC: HTTPService, WebService y RemoteObject. No acceden directamente a Bases de datos remotas, sino que lo hacen través de capas intermedias. A través de HTTPService solicita archivos JSP o XML con los datos en formato de variables String, formatos de intercambio XML, Y4X u objetos ActionScript. En el caso de devolver JSON Flex dispone de librerías especializadas para serialización así como para SOAP. A través de la API de RemoteObject permite realizar peticiones **Flash Remoting**, que devuelven mensajes binarias **AMF** (en inglés, *Action Message Format*) sobre HTTP. Cuando este formato tiene aplicación se obtiene un mayor rendimiento que en otras tecnologías, como JSON o SOAP.

Figura 2: Integración de Flex en JEE.

TEXTO FIGURA 2: Servicios / otros... / Beans de entidad / Objeto Remoto

Asimismo, Flex permite intercambio de datos en tiempo real ante dos vías: **XML Socket** y **Socket Binario**. Con el XML Socket se crea una conexión que permanece abierta mientras dure la comunicación, o es cerrada explícitamente. En el Socket Binario el funcionamiento es similar, pero cliente e servidor no necesitan intercambiar paquetes XML específicamente, sino que envían los datos como información binaria, o que permite conectar con servidores de correo como POP3, SMTP y IMAP o servidores de noticias como NNTP.

Por lo que respecta a la **seguridad**, a la hora de integrar Flex en una aplicación JEE, será la arquitectura de esta la que imponga el modelo de seguridad, variando desde un *framework* de autenticación/autorización específico a un directorio LDAP, o archivos de configuración XML. La información de seguridad debe añadirse a los servicios BlazeDS y LiveCycle Data, de manera que soliciten credenciales en las comunicaciones con el servidor.

Como en otras tecnologías, en Flex están disponibles una serie de **frameworks** multipropósito. Muchos de ellos también son válidos para AIR. Los más empleados son:

- a) **Cairngorm**. Microarquitectura que aplica un pequeño conjunto de patrones de diseño (Service Locator, Front-Controller...) probados en conjunto. Se centra en tres áreas clave: manejar acciones de usuario, encapsular las interacciones con servidor y la lógica de negocio y gestionar el estado del cliente representándolo en la interfaz de usuario.
- b) **Mate**. *Framework* orientado a eventos basado en etiquetas, implementadas completamente en MXML. Implementa la idea de Inyección de dependencia, construyendo los objetos para, a

continuación, inyectar en las clases os datos. Los objetos no solicitan la información, pero esta les es entregada por el sistema.

- c) **PureMVCFramework**. Como Cairngorm representa también una microarquitectura con un pequeño conjunto de patrones de diseño, con MVC y Fachada como núcleos centrales, cada una a través de un patrón instancia única.
- d) **Swiz**. *Framework* de control de inversión (Ioc), que provee metodologías para simplificar el manejo de eventos y las llamadas asíncronas a procedimientos remotos. Emplea MVC, pero a diferencia de los anteriores, solo en lo que respecta a la estructura de clases y no de directorios.
- e) **Parsley**. Conjunto de librerías ActionScript para correspondencia de objetos y entidades, registro de depuración, inyección de dependencia, mensajería y otras funcionalidades extendidas.

Para la integración con sistemas de información Flex provee del Servicio de gestión de datos dentro del Servicio LiveCycle Data. En este servicio se incluye sincronización de datos en tiempo real entre cliente, servidor y otros clientes, replicación de datos, paginación bajo demanda, y para aplicaciones AIR sincronización de datos locales para conexiones ocasionales de las aplicaciones.

32.3.3 SILVERLIGHT/MOONLIGHT

Complemento para navegadores que permite integrar en la misma extensión elementos multimedia, animaciones e interactividad, de manera similar al WPF. Se basa en XAML para la definición de las interfaces de usuario, a partir de cuales invoca métodos del servidor de aplicaciones .NET. Permite la carga dinámica de XML, con el que se puede operar a

través de DOM a la manera de AJAX. Proporciona extensiones Javascript e. Las principales **características** del *framework* son:

- a) **WPF**. Incluye un subconjunto de WPF que extiende en gran medida elementos de la Interface de Usuario.
- b) **XAML**. Definición de la Interface de Usuario a través de un lenguaje de marcado declarativo.
- c) **Integración** con Javascript y ASP .NET AJAX.
- d) Acceso a **objetos del lado del servidor** .NET.
- e) Conexión con **servicios de red** WCF, SOAP y ASP .NET AJAX, permitiendo orígenes de datos JSON, XML y RSS.
- f) Soporta **LINQ** para implementar el acceso a datos.

La **arquitectura** de Silverlight se compone de 3 partes fundamentales:

- 1) **Framework de presentación básico**. Componentes y servicios orientados a la Interface de usuario y la interacción con el usuario, elementos multimedia y soporte XAML.
- 2) **.NET Framework para Silverlight**. Subconjunto de .NET. *Framework* para Silverlight que contiene componentes y librerías, recolector de basura, WCF y CLR. Asimismo, incluye los controles de la Interfaz de Usuario, XLINQ, RSS/Atom, serialización XML y DLR (en inglés, *Dynamic Language Runtime*).
- 3) **Componente de instalación y actualización**. Control de instalación y actualización de la extensión.

Mención especial merece el apartado de la **seguridad**. Como sucedía con otras tecnologías RIA, Silverlight incorpora políticas de seguridad específicas para:

- a) Seguimiento del Ciclo de vida de seguridad de Microsoft SDL (en inglés, Security Development Lifecycle).
- b) Evitación de ataques XSS.
- c) Aislamiento de código de archivos de configuración XAP.
- d) Proveer acceso seguro a recursos de red.
- e) Servicios criptográficos para protección de datos de usuario.
- f) Firma digital de las aplicaciones.

Figura 2: Arquitectura Silverlight.

Textos Figura 2: Librerías AJAX / Controles / Diseño / Enlace de datos / Colecciones / Motor de ejecución CLR
Ratón / Imágenes / Animaciones

32.3.4 JAVA FX

Java FX es una plataforma que se compone de elementos web, multimedia y scripting junto con tecnologías de servidor JEE para el desarrollo de aplicaciones multiplataforma. Puede funcionar de manera independiente del navegador siempre que el equipo tenga instalada una máquina virtual Java compatible. Promueve el concepto de “Perfil común” para intentar unificar todos los dispositivos que soporten JavaFX, de modo que el mismo modelo de desarrollo se adapte a cualquier entorno.

Los principales **componentes** de Java FX son:

- f.a) **JavaFX Script**. Lenguaje de programación declarativo, con tipos estáticos, que permite invocar métodos de cualquier API de Java de la plataforma.
- f.b) **Entorno de ejecución JavaFX**. Especializado para el dispositivo, Escritorio/Web, Mobile, o TV.
- f.c) **Aplicaciones JavaFX**. Independientes o empaquetadas como archivos JAR.
- f.d) **Herramientas de desarrollo**. Incluye el compilador para JavaFX Script, Plug ins para IDE como Eclipse, y librerías especializadas para gráficos, multimedia o Servicios web, entre otros.

La **arquitectura** de JavaFX presenta en un primer nivel:

1. Las **API públicas** de JavaFX. Las principales funcionalidades de estas API son permitir integración con otros lenguajes como JRuby, Groovy y Javascript, funcionalidades genéricas y extensiones para las interfaces de usuario.
2. **Grafo de Escena**. Este grafo, definido en la API *javafx.scene* se representa en una estructura en árbol con nodos representando todos

los elementos visuales de la interface de usuario. Cada nodo puede llevar sus estilos, además de efectos, manejadores de eventos y control de estado.

Bajo ellos se encuentra el motor de ejecución, compuesto por los siguientes componentes:

f.d.a) **Prism.** Motor gráfico de alto rendimiento que soporta Java2D, OpenGL y DirectX.

f.d.b) **Quantum Toolkit.** Gestiona las reglas de procesos para representación gráfica frente al manejo de eventos.

f.d.c) **Glass Windowing Toolkit.** Sistema de control de ventanas en el nivel más bajo de la arquitectura gráfica de JavaFX. Provee de los servicios operativos nativos del sistema, además de ser responsable de gestionar la cola de eventos.

f.d.d) **Motores web y multimedia.** Incluyen API para soporte de medios visuales y de sonido. Asimismo, el motor web soporta los estándares HTML5, CSS, Javascript, DOM y SVG.

Figura 3: Arquitectura JavaFX.

32.4 OTRAS TECNOLOGÍAS RIA

Si bien las tecnologías vistas con anterioridad representan las soluciones de uso más extendido actualmente, existen otras multipropósito, o más específicas, que quieren hacerse un hueco en el mundo de las RIA. Dentro de estas otras tecnologías, OpenLaszlo merece una mención especial, aun cuando no representa una tecnología en sí, sino un conjunto de tecnologías, con algunas adaptaciones específicas.

32.4.1 OPENLASZLO

OpenLaszlo es un *framework* y plataforma de desarrollo para aplicaciones RIA con licencia GPL que necesita un servidor propio para el alojamiento de las aplicaciones desarrolladas. Una misma aplicación definida a través de un lenguaje de definición propia puede exportarse a diferentes formatos multinavegador y multiplataforma.

Las aplicaciones OpenLaszlo pueden desplegarse en el servidor de aplicaciones de la plataforma, denominado **Despliegue en modo proxy**, o bien en modo **Despliegue “SOLO”** con independencia del servidor, por norma general empaquetada en un archivo SWF. Otra característica peculiar de funcionamiento son las **Librerías dinámicas**, que permiten una descarga “parcial” de la aplicación para obtener una carga inicial más rápida, siendo el resto de la carga de la aplicación bajo demanda. Asimismo, la funcionalidad **Krank** permite cargar las aplicaciones OpenLaszlo más rápidamente, realizando un preprocesamiento de la vista y *scripts* de inicialización.

OpenLaszlo aporta un lenguaje declarativo propio, el LZX, diseñado para describir las interfaces del usuario, al estilo de XUL y XForms. Este lenguaje incorpora un framework de etiquetas dividido en categorías como: elementos de la interfaz, orígenes de datos, efectos multimedia y acciones. Se emplea conjuntamente con Javascript/AJAX, siendo este último el encargado de la interacción con el usuario.

La plataforma OpenLaszlo incorpora los siguientes **componentes**:

- a) **Compilador**. Permite que una aplicación definida ante el lenguaje declarativo LZX pueda transformarse a Flash (SWF) o DHTML-AJAX. Asimismo, presenta una serie de módulos específicos para:
- 1) **Compilación XML IU**. El compilador transforma las definiciones de la interfaz de usuario al formato de salida especificado para la aplicación.
 - 2) **Compilación ECMAScript**. Clases e instancias LZX se traducen a ECMAScript y controladores de eventos, transformándolas a Bytecode.

- 3) **Compilación multimedia.** Se codifican los archivos en formatos de imagen y sonido, así como las fuentes TrueType en ficheros OBJ para SWF o XML.
- b) **Servidor.** Hace las funciones de alojamiento de la aplicación y proxy, manteniendo comunicación bidireccional con los back-ends a través de JAVARPC u otros protocolos de servicios web. Asimismo, proporciona servicios de transformación de formatos, mensajería, *streaming*, encriptación SSL y autenticación.
- c) **Entorno de ejecución o LCF** (en inglés, *Laszlo Foundation Class*). Incluye componentes de la interfaz de usuario, acceso a datos y servicios de red. La LCF se divide en cuatro componentes principales:
- 1) **Data Loader/Binder.** El cargador y encargado de asociar y relacionar los datos. Dirige el tráfico de datos, incluyendo el flujo de datos hacia el cliente.
 - 2) **Sistema de eventos.** Permite una programación basada en eventos al recoger los eventos detectados en el cliente.
 - 3) **Layout & Animation System.** Sistema de animación y escenario de la aplicación que ofrece todos los elementos para la parte gráfica de la aplicación así como animaciones y efectos.
 - 4) **Servicios para las aplicaciones.** Con funcionalidades extra como contadores, sonidos, etc...
- d) **Framework.** Provee de una extensa API para animaciones, estructura de aplicación, acceso a datos, comunicaciones con el servidor y definición de la interfaz de usuario. Estructuralmente sigue un modelo MVC, pero ampliable a las capas que sean necesarias para cada solución.
- e) **Servlet.** Se trata de un componente opcional para la aplicación que permite atender y dirigir peticiones multimedia o para servicios web como SOAP, JavaRPC o XML-RPC. Hace funciones de caché y proxy para

priorización y bloqueo de peticiones, así como de registro de trazas y auditoría.

32.4.2 ZK FRAMEWORK

Se trata de otro *framework* orientado a eventos que, en esencia, se podría incluir con los *frameworks* AJAX, aunque con algunas diferencias. En primer lugar, emplea un lenguaje de marcado propio para las interfaces de usuario denominado ZUML, que puede mezclarse con otros lenguajes de marcado como XUL y XHTML, además de lenguajes de *script* y expresiones EL para manipulación de componentes y datos. Se diseñó para integración con aplicaciones JEE e incorpora las capacidades de AJAX en desarrollos ágiles y reutilizables.

Provee de un *framework* con una implementación de ZK Spring, adaptado del *framework* Spring, y librerías con componentes y etiquetas JSP con soporte para AJAX. En lo que respecta a la seguridad, añade protección para ataques XSS, DoS y CSRF, además de reforzar la autenticación y los permisos con la incorporación de *frameworks* de terceros como Spring Security.

32.5 ESQUEMA

TEXTO ESQUEMA: Tecnologías / Funcionamiento básico /
Otros

RIA MULTIMEDIA Y ANIMACIONES/ Extensión de terceros /
Comunicaciones cliente-servidor / Seguridad /
Componentes
OTRAS RIA / Despliegue Proxy/SOLO / Librerías
Dinámicas / Componentes

32.6 REFERENCIAS

Lee Babin

Beginning Ajax with PHP: from novice to professional (2007).

Rebecca Riordan

Head First Ajax. (2008).

Michael Mahemoff.

Ajax Design Patterns. Creating Web 2.0 Sites with Programming and Usability Patterns. (2006)

Autor: Juan Marcos Filgueira Gomis

Asesor Técnico Consellería de Educación y O. U.

Colegiado del CPEIG



33. INGENIERÍA DEL SOFTWARE. PROCESO SOFTWARE, MODELOS DE PROCESO SOFTWARE. CICLOS DE VIDA. MODELOS DE CICLO DE VIDA. FASES DEL CICLO DE VIDA. MODELOS DE DESARROLLO.

Tema 33. Ingeniería del software. Proceso software, modelos de proceso software. Ciclo de vida. Modelos de ciclo de vida. Fases del ciclo de vida. Modelos de desarrollo.

INDICE

<u>33.1 INGENIERÍA DEL SOFTWARE.....</u>	<u>2</u>
<u>33.1.1 Inicios de la ingeniería del Software.....</u>	<u>2</u>
<u>33.1.2 ¿Qué es la Ingeniería del Software?.....</u>	<u>3</u>
<u>33.2 PROCESO SOFTWARE. MODELOS DE PROCESO SOFTWARE.....</u>	<u>6</u>
<u>33.3 CICLO DE VIDA DEL SOFTWARE.....</u>	<u>10</u>
<u>33.4 MODELOS DE CICLO DE VIDA DEL SOFTWARE.....</u>	<u>12</u>
<u>33.4.1 Modelo Codificar y Corregir (Code and Fix).....</u>	<u>13</u>
<u>33.4.2 Modelo por Etapas.....</u>	<u>13</u>
<u>33.4.3 Modelo en Cascada.....</u>	<u>14</u>
<u>33.4.4 Modelos Evolutivos.....</u>	<u>17</u>
<u>33.4.4.1 Modelo Iterativo Incremental.....</u>	<u>18</u>
<u>33.4.4.2 Modelo en Espiral.....</u>	<u>19</u>
<u>33.4.4.3 Modelos basados en prototipos.....</u>	<u>22</u>
<u>33.4.4.3.1 Prototipado rápido.....</u>	<u>22</u>
<u>33.4.4.3.2 Prototipado evolutivo.....</u>	<u>24</u>
<u>33.4.5 Modelos basados en Transformaciones.....</u>	<u>26</u>
<u>33.4.6 Modelo basado en componentes.....</u>	<u>28</u>
<u>33.5 MODELOS DE DESARROLLO.....</u>	<u>30</u>
<u>33.5.1 Proceso Unificado de Desarrollo de software (PUDS).....</u>	<u>30</u>
<u>33.5.2 Programación Extrema (eXtreme Programming).....</u>	<u>33</u>

33.1 Ingeniería del software

33.1.1 Inicios de la ingeniería del Software.

El auge que se produjo en el ámbito de la informática en los años sesenta, debido en su mayor parte a la aparición de la segunda generación de ordenadores, tuvo como consecuencia que se realizara una masiva escritura incontrolada de líneas de código. Este proceso de creación de software se llevó a cabo sin plantearse ningún tipo de metodología para el diseño y construcción de software, ni ningún método para solventar los problemas relacionados con el mantenimiento, fiabilidad, etc.

Esta expansión sin control tuvo como consecuencia la denominada **crisis del software**, que es el nombre genérico que se ha acuñado para referirse a un conjunto de problemas que se han ido encontrando en el desarrollo del software. Esta problemática no sólo se limita al software que no funciona adecuadamente, sino que abarca otros aspectos como la forma de desarrollar el software, el mantenimiento de un volumen creciente de software existente y la forma de satisfacer la demanda creciente de software.

Los síntomas que hacen palpable la aparición de la crisis del software son, entre otros, los siguientes:

- **Expectativas:** los sistemas no responden a las expectativas que de ellos tienen los usuarios.
- **Fiabilidad:** los programas fallan demasiado a menudo.
- **Costo:** los costos del software son muy difíciles de prever y, frecuentemente, son muy superiores a lo esperado.
- **Plazos:** el software se suele entregar tarde y con menos prestaciones de las ofertadas.
- **Portabilidad:** es difícil cambiar un programa de su entorno hardware, aun cuando las tareas a realizar son las mismas.



- **Mantenimiento:** la modificación del software es una tarea costosa, compleja y propensa a errores.
- **Eficiencia:** los esfuerzos que se hacen para el desarrollo del software no hacen un aprovechamiento óptimo de los recursos disponibles (personas, tiempo, dinero, herramientas, etc.).

La solución a la crisis del software se centra, pues, en abordar y resolver los siguientes problemas principales:

- La planificación del proyecto software y la estimación de los costes de desarrollo, que son muy imprecisos.
- La productividad de las personas, que no se corresponde con la demanda de sus servicios.
- La calidad del producto software, que es, en muchos casos, inadecuada.

33.1.2 ¿Qué es la Ingeniería del Software?

Según Pressman, la Ingeniería del software se puede definir como *el establecimiento y uso de principios de ingeniería robustos, orientados a obtener software económico que sea fiable y funcione de manera eficiente sobre máquinas reales.*

La Ingeniería del Software abarca tres elementos clave:

- **Métodos:** proporcionan la manera de construir técnicamente el software. Abarcan las tareas de planificación y estimación de proyectos, análisis de los requerimientos del sistema y del software, diseño de las estructuras de datos, de la arquitectura de programas y de los procedimientos algorítmicos, y la codificación, pruebas y mantenimiento.
- **Herramientas:** suministran el soporte automático o semiautomático para los métodos; esto es, dan soporte al desarrollo del software.



- **Procedimientos:** definen la secuencia en la que se aplican los métodos, los controles que ayudan a asegurar la calidad y a coordinar los cambios y las guías que facilitan a los gestores del software.

Pressman divide en tres fases el trabajo asociado a la ingeniería del software:

- **La fase de definición** (el *qué*). El que desarrolla el software intenta identificar qué información ha de ser procesada, qué función y rendimiento se desea, qué comportamiento del sistema, qué interfaces van a ser establecidas, qué restricciones de diseño existen, y qué criterios de validación se necesitan para definir un sistema correcto. Por tanto, han de identificarse los requisitos clave del sistema y del software. Aunque los métodos aplicados durante la fase de definición variarán dependiendo del paradigma de ingeniería del software (o combinación de paradigmas) que se aplique, de alguna manera tendrán lugar tres tareas principales: ingeniería de sistemas o de información, planificación del proyecto del software y análisis de los requisitos.
- **La fase de desarrollo** (el *cómo*). Es decir, durante el desarrollo un ingeniero del software intenta definir cómo han de diseñarse las estructuras de datos, cómo ha de implementarse la función dentro de una arquitectura de software, cómo han de implementarse los detalles procedimentales, cómo han de caracterizarse interfaces, cómo ha de traducirse el diseño en un lenguaje de programación (o lenguaje no procedimental) y cómo ha de realizarse la prueba. Los métodos aplicados durante la fase de desarrollo variarán, aunque siempre tendremos: diseño del software, generación de código y prueba del software.
- **La fase de mantenimiento** (el *cambio*). El cambio va asociado a la corrección de errores, a las adaptaciones requeridas a medida que evoluciona el entorno del software y a cambios debidos a las mejoras

producidas por los requisitos cambiantes del cliente. Durante la fase de mantenimiento se encuentran cuatro tipos de cambios:

- o **Corrección.** Incluso llevando a cabo las mejores actividades de garantía de calidad, es muy probable que el cliente descubra los defectos en el software. El *mantenimiento correctivo* cambia el software para corregir los defectos.
- o **Adaptación.** Con el paso del tiempo, es probable que cambie el entorno original para el que se desarrolló el software. El *mantenimiento adaptativo* produce modificaciones en el software para acomodarlo a los cambios de su entorno externo (hardware, sistema operativo, reglas de negocio,...).
- o **Mejora.** Conforme se utilice el software, el cliente/usuario puede descubrir funciones adicionales que van a producir beneficios. El *mantenimiento perfectivo* lleva al software más allá de sus requisitos funcionales originales.
- o **Prevención.** El software de computadora se deteriora debido al cambio. En esencia, el *mantenimiento preventivo* hace cambios en programas de computadora a fin de que se puedan corregir, adaptar y mejorar más fácilmente.

Todas estas fases van acompañadas de un conjunto de actividades que se realizan a lo largo de todo el proceso de creación de software. Estas actividades se denominan actividades protectoras, siendo las más importantes:

- Seguimiento y control del proyecto
- Revisiones técnicas formales
- Garantía de calidad del software
- Gestión de configuración del software

- Preparación y producción de documentos
- Gestión de reutilización
- Mediciones
- Gestión de riesgos

33.2 Proceso software. Modelos de proceso software

Existen diversas definiciones formales para determinar el concepto de *Proceso de Software*:

- *Un proceso del software es un conjunto de actividades que conducen a la creación de un producto software.* Esta es una definición propuesta por Sommerville, en donde estas actividades pueden consistir en el desarrollo de software desde cero, desarrollo de nuevo software ampliando y modificando sistemas existentes o configurando e integrando software comercial o componentes del sistema.
- Desde otro punto de vista, Fugetta determina un proceso software como *un conjunto coherente de políticas, estructuras organizacionales, tecnologías, procedimientos y artefactos que son necesarios para concebir, desarrollar, instalar y mantener un producto software.*

Los procesos del software son complejos y, como todos los procesos intelectuales y creativos, dependen de las personas que toman decisiones y juicios. Debido a la necesidad de juzgar y crear, los intentos para automatizar estos procesos han tenido un éxito limitado.

Las herramientas de ingeniería del software asistida por computadora (CASE) pueden ayudar a algunas actividades del proceso, pero tienen

limitaciones. Una razón por la cual la eficacia de las herramientas CASE está limitada se halla en la inmensa diversidad de procesos del software. No existe un proceso ideal, y muchas organizaciones han desarrollado su propio enfoque para el desarrollo del software. Los procesos han evolucionado para explotar las capacidades de las personas de una organización, así como las características específicas de los sistemas que se están desarrollando. Para algunos sistemas, como los sistemas críticos, se requiere un proceso de desarrollo muy estructurado. Para sistemas de negocio, con requerimientos rápidamente cambiantes, un proceso flexible y ágil probablemente sea más efectivo.

Aunque existen muchos procesos diferentes de software, algunas actividades fundamentales son comunes para todos ellos:

1. **Especificación del software** donde los clientes e ingenieros definen el software a producir y las restricciones sobre su operación.
2. **Desarrollo del software** donde el software se diseña y programa.
3. **Validación del software** donde el software se valida para asegurar que es lo que el cliente requiere.
4. **Evolución del software** donde el software debe evolucionar para cubrir las necesidades cambiantes del cliente.

Diferentes tipos de sistemas necesitan diferentes procesos de desarrollo. Por lo tanto, estas actividades genéricas pueden organizarse de diferentes formas y describirse en diferentes niveles de detalle para diferentes tipos de software. El uso de un proceso inadecuado del software puede reducir la calidad o la utilidad del producto de software que se va a desarrollar y/o incrementar los costes de desarrollo.

Los procesos del software se pueden mejorar con la estandarización. Esto conduce a mejorar la comunicación y a una reducción del tiempo de formación, y hace la ayuda al proceso automatizado más económica. La estandarización también es un primer paso importante para introducir nuevos métodos, técnicas y buenas prácticas de ingeniería del software.

De todos modos, la existencia de un proceso de software no es garantía de que éste será entregado a tiempo, de que satisfará las necesidades del cliente, o de que mostrará las características técnicas que conducirán a características de calidad a largo plazo. El proceso de software debe **evaluarse** para asegurarse de que cumpla una serie de criterios básicos que han demostrado ser esenciales para una ingeniería de software exitosa.

Un **modelo de procesos del software** es una descripción abstracta y simplificada de un proceso del software que presenta una visión de ese proceso. Cada modelo de proceso representa un proceso desde una perspectiva particular y así proporciona sólo información parcial sobre ese proceso. Son abstracciones de los procesos que se pueden utilizar para explicar diferentes enfoques para el desarrollo de software. Puede pensarse en ellos como marcos de trabajo del proceso que pueden ser extendidos y adaptados para crear procesos más específicos de ingeniería del software. Cada modelo describe una sucesión de fases y un encadenamiento entre ellas. Según las fases y el modo en que se produzca este encadenamiento, tenemos diferentes modelos de proceso. Un modelo es más adecuado que otro para desarrollar un proyecto dependiendo de un conjunto de características del proyecto. Los modelos pueden incluir actividades que son parte de los procesos y productos de software y el papel de las personas involucradas en la ingeniería del software. Alternativamente, a veces se usan los términos **ciclo de vida, modelo de ciclo de vida y modelo de desarrollo**.

La mayor parte de los modelos de procesos del software se basan en uno de los tres modelos generales o paradigmas de desarrollo de software:

1. **El enfoque en cascada.** Considera las actividades anteriores y las representa como fases de procesos separados, tales como la especificación de requerimientos, el diseño del software, la implementación, las pruebas, etcétera. Después de que cada etapa



queda definida «se firma» y el desarrollo continúa con la siguiente etapa.

2. **Desarrollo iterativo.** Este enfoque entrelaza las actividades de especificación, desarrollo y validación. Un sistema inicial se desarrolla rápidamente a partir de especificaciones muy abstractas. Éste se refina basándose en las peticiones del cliente para producir un sistema que satisfaga las necesidades de dicho cliente. El sistema puede entonces ser entregado. De forma alternativa, se puede reimplementar utilizando un enfoque más estructurado para producir un sistema más sólido y mantenible.
3. **Ingeniería del software basada en componentes (CBSE).** Esta técnica supone que las partes del sistema ya existen previamente. El proceso de desarrollo del sistema se enfoca en la integración de estas partes más que desarrollarlas desde el principio.

Estos tres modelos de procesos genéricos se utilizan ampliamente en la práctica actual de la ingeniería del software. No se excluyen mutuamente y a menudo se utilizan juntos, especialmente para el desarrollo de sistemas grandes. Los subsistemas dentro de un sistema más grande pueden ser desarrollados utilizando enfoques diferentes. Por lo tanto, aunque es conveniente estudiar estos modelos separadamente, debe entenderse que, en la práctica, a menudo se combinan.

Pressman separa entre el **modelo personal** (modelo utilizado por cada desarrollador) y **modelo en equipo** (cuando el proyecto es dirigido por varios profesionales) para el proceso de software. Ambos destacan la medición, la planeación y la autodirección como ingredientes clave para un proceso de software exitoso.

33.3 Ciclo de vida del software

El ciclo de vida de un sistema de información es *el marco de referencia que contiene los procesos, las actividades y las tareas involucradas en el desarrollo, la explotación y el mantenimiento de un producto de software, abarcando la vida del sistema desde la definición de los requisitos hasta la finalización de su uso.*

También se podría definir el ciclo de vida de un sistema de información como *el conjunto de etapas por las que atraviesa el sistema desde su concepción, hasta su retirada de servicio pasando por su desarrollo y explotación.*

Existen diversos modelos de ciclo de vida, los cuales determinan una serie de etapa, fases o estados por los que ha de pasar un producto software. Esta diversidad es debida en gran medida al hecho de que existen multitud de aplicaciones diferentes y de distinto índole, lo que provoca que existan modelos de ciclo de vida que se ajusten mejor a unos desarrollos que a otros.

Sin embargo, a pesar de esta variedad, todo modelo de ciclo de vida debe cubrir los siguientes objetivos básicos:

- Definir las actividades a realizar y en qué orden, es decir, determinar el orden de las fases del proceso software.
- Establecer los criterios de transición para pasar de una fase a la siguiente.
- Proporcionar puntos de control para la gestión del proyecto, es decir, calendario y organización.
- Asegurar la consistencia con el resto de los sistemas de información de la organización.

Cada proyecto debe seleccionar el modelo de ciclo de vida que sea más apropiado para su caso, el cual se elige en base a considerar una serie de factores como: la cultura de la organización, el deseo de asumir riesgos, el

área de aplicación, la volatilidad de los requisitos, la comprensión de dichos requisitos, etc. En cualquier proyecto software, el modelo de ciclo de vida permite responder a las cuestiones de ¿qué se hará a continuación? y ¿por cuánto tiempo se hará? Dado que cada modelo de ciclo de vida tiene sus ventajas y sus inconvenientes, no se suelen seguir en la práctica los modelos en su forma pura, sino que de acuerdo con las peculiaridades del sistema y la experiencia del personal, se pueden adoptar aspectos de otros modelos que sean más adecuados al caso concreto.

Es importante no confundir el concepto de ciclo de vida con el de metodología. Mientras que el ciclo de vida indica qué actividades hay que realizar y en qué orden, la **metodología** indica cómo avanzar en la construcción del sistema, esto es, con qué técnicas, y entre sus características está la de determinar los recursos a utilizar o las personas implicadas en cada actividad.

33.4 Modelos de ciclo de vida del software

Los distintos modelos de ciclo de vida del software pueden ser clasificados siguiendo diversos criterios. Siguiendo un criterio basándose en la utilización de los mismos existen:

- **Modelos tradicionales:** Son los de más amplia utilización.
 - o Modelo Codificar y Corregir
 - o Modelo por Etapas
 - o Modelo en Cascada.
 - o Modelos Evolutivos
 - Modelo Iterativo incremental
 - Modelo en Espiral
 - Modelos basados en prototipos:
 - Modelo de construcción de prototipos.
 - Modelo de prototipado evolutivo.
- **Modelos alternativos**
 - o Modelos basados en transformaciones: La filosofía general es llegar a generar código a partir de unas especificaciones transformándolas por medio de herramientas. Según usemos unas u otras herramientas tendremos:
 - Las que usan técnicas de cuarta generación (Roger Pressman): lenguajes no procedimentales para consultas a BD; generadores de código, de pantallas, de informes; herramientas de manipulación de datos; facilidades gráficas de alto nivel.
 - Basados en modelos de transformación (Carma McClure)
=> Basados en herramientas CASE que permiten, siguiendo el MCV clásico, pasar de una etapa a otra aplicando las transformaciones que dan las herramientas.
 - o Desarrollo de Software Basado en Componentes (DSBC o CBSB).

33.4.1 *Modelo Codificar y Corregir (Code and Fix)*

Este es un modelo simple, utilizado en los primeros desarrollos de software, el cual se fundamenta en la creación del código y en la corrección y adaptación del mismo. Contiene dos pasos:

- Escribir código.
- Corregir problemas en el código.

Se trata de primero implementar algo de código y luego pensar acerca de requisitos, diseño, validación, y mantenimiento. Este modelo tiene tres problemas principales:

- Después de un número de correcciones, el código puede tener una muy mala estructura, hace que los arreglos sean muy costosos. Esto hizo ver la necesidad de una fase previa de diseño antes de la de codificación.
- Frecuentemente, aún el software bien diseñado, no se ajusta a las necesidades del usuario, por lo que es rechazado o su reconstrucción es muy cara. Esto condujo a la necesidad de introducir una fase de análisis de requerimientos antes del diseño.
- El código es difícil de reparar por su pobre preparación para probar y modificar. Este problema hizo resaltar la necesidad de la planificación y preparación de las distintas tareas en cada fase.

33.4.2 *Modelo por Etapas*

El modelo por etapas nace como respuesta a los problemas que surgen al utilizar el modelo anterior. Como solución se plantea un modelo para la creación de software que se basa en un conjunto de etapas o fases sucesivas que van construyendo el sistema planteado. Las etapas determinadas por este modelo (Stage Wise) son:

- Planificación
- Especificaciones de operación

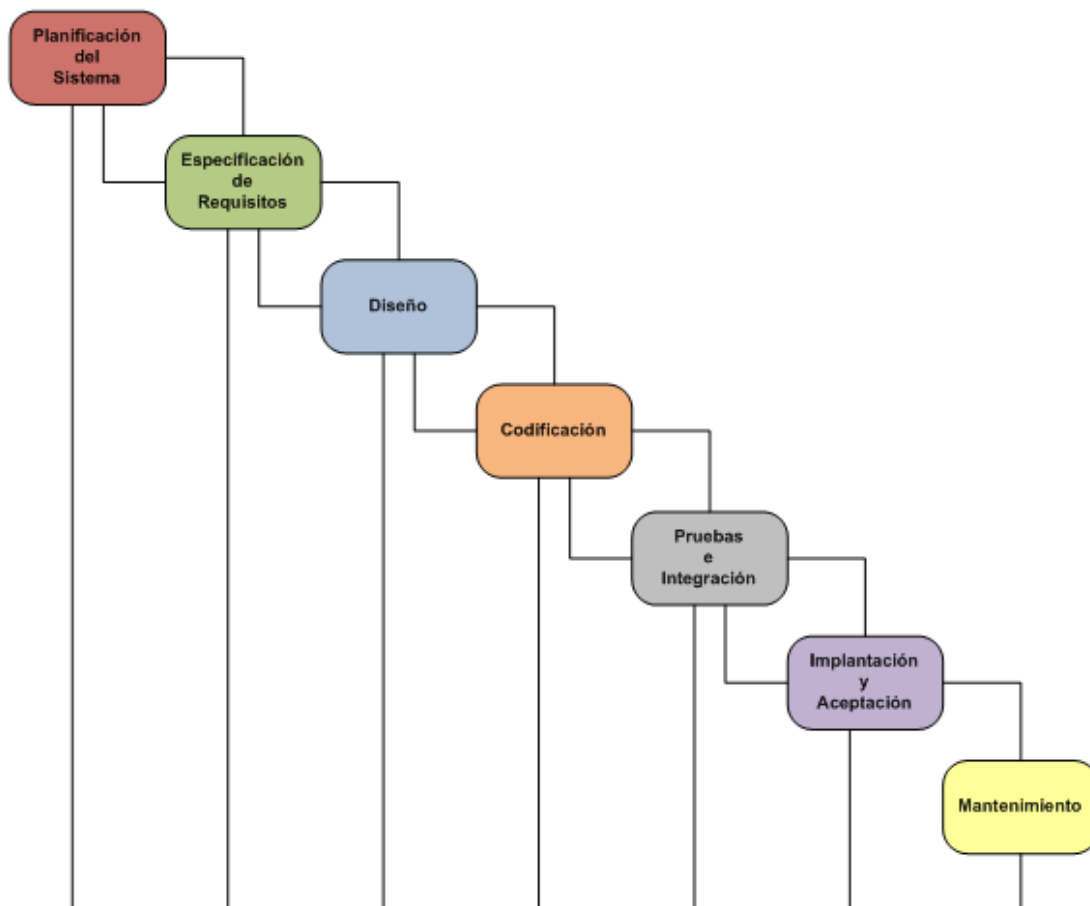
- Especificaciones de codificación
- Codificación
- Prueba de cada unidad
- Prueba de integración
- Eliminación de problemas
- Evaluación del sistema.

33.4.3 *Modelo en Cascada*

Este modelo se fundamenta en el modelo por etapas, al cual incorpora un conjunto de mejoras tales como considerar la realización de bucles de realimentación entre etapas, permitiendo que se puedan resolver los problemas detectados en una etapa, en la etapa anterior y permitir la incorporación inicial del prototipado a fin de captar las especificaciones durante el análisis, o para probar distintas soluciones durante el diseño.

El modelo en cascada se compone de una serie de fases que se suceden secuencialmente, generándose en cada una de ellas unos resultados que serán necesarios para iniciar la fase siguiente. Es decir, la evolución del producto software se produce a través de una secuencia ordenada de transiciones de una fase a la siguiente, según un orden lineal. El número de fases en este modelo es irrelevante, ya que lo que le caracteriza es la *secuencialidad* de las mismas y la *necesidad de completar* cada una de ellas para pasar a la siguiente. El modelo del ciclo de vida en cascada está regido por la documentación, es decir, la decisión del paso de una fase a la siguiente se toma en función de si la documentación asociada a dicha fase está completa o no. Sin embargo, esta forma de proceder no es la más adecuada para algunos tipos de software como el que se usa en las aplicaciones interactivas y de usuario final.

Desde su presentación, el modelo en cascada ha tenido un papel fundamental en el desarrollo de proyectos software. Ha sido, y todavía sigue siendo, el más utilizado, tanto que este modelo se conoce con el nombre de ciclo de vida clásico, si bien incorporando infinidad de



variaciones que eliminan el carácter simplista del mismo. Aun así, existen una serie de limitaciones que justifican la necesidad de definir otros modelos.

Como se ha indicado anteriormente, las fases que comprende el ciclo de vida clásico son irrelevantes, tanto en número, como en cuáles sean esas fases siempre que se produzcan secuencialmente. Posiblemente, el modelo clásico más utilizado sea el modelo de siete fases que son:

- **Planificación del sistema:** En esta fase es necesario fijar el ámbito del trabajo a realizar, los recursos necesarios, las tareas a realizar, las



referencias a tener en cuenta, el coste estimado del proyecto, la composición del equipo de desarrollo y el orden de las actividades.

- **Especificación de requisitos:** En esta fase es preciso analizar, entender y documentar el problema que el usuario trata de resolver con el sistema y se han de especificar con detalle las funciones, objetivos y restricciones del mismo, a fin de que usuarios y desarrolladores puedan tomar éstas como punto de partida para acometer el resto del sistema. Es decir, en la fase de especificación de requisitos se trata de definir **qué** debe hacer el sistema, e identificar la información a procesar, las funciones a realizar, el rendimiento del sistema, las interfaces con otros sistemas y las ligaduras de diseño.
- **Diseño:** Arranca de las especificaciones de la fase anterior. En la fase de diseño, una vez elegida la mejor alternativa, se debe crear la solución al problema descrito atendiendo a aspectos de interfaces de usuario, estructura del sistema y decisiones sobre la implantación posterior. La fase de diseño trata de definir el **cómo**.
- **Codificación:** Esta fase consiste en traducir las especificaciones y representaciones del Diseño a un lenguaje de programación capaz de ser interpretado y ejecutado por el ordenador.
- **Pruebas e integración:** Una vez que se tienen los programas en el formato adecuado al ordenador, hay que llevar a cabo las pruebas necesarias que aseguren la corrección de la lógica interna del programa y que éste cubre las funcionalidades previstas. La integración de las distintas partes que componen la aplicación o el sistema debe garantizar el buen funcionamiento del conjunto.
- **Implantación y aceptación del sistema:** El objetivo de esta fase es conseguir la aceptación del sistema por parte de los usuarios del mismo, y llevar a cabo las actividades necesarias para su puesta en producción.

- **Mantenimiento del sistema:** La fase de mantenimiento comienza una vez que el sistema ha sido entregado al usuario y continúa mientras permanece activa su vida útil. Puede deberse a errores no detectados previamente (correctivo), a modificaciones, mejoras o ampliaciones solicitadas por los usuarios (perfectivo, o aumentativo) o a adaptaciones requeridas por la evolución del entorno tecnológico o cambios normativos (mantenimiento adaptativo).

Las principales **críticas** al modelo se centran en sus características básicas, es decir secuencialidad y utilización de los resultados de una fase para acometer la siguiente de manera que el sistema sólo se puede validar cuando está terminado. En cuanto al flujo secuencial, los proyectos reales raramente siguen el flujo secuencias que propone el modelo. Siempre ocurren interacciones y en las últimas fases sobre todo se pueden realizar en paralelo algunas áreas como por ejemplo codificación y pruebas. Una aplicación del modelo en sentido estricto obligaría a la “congelación” de los requisitos de los usuarios, supuesto este completamente alejado de la realidad. El modelo no contempla la posibilidad de realimentación entre fases. Por otro lado, el modelo no prevé revisiones o validaciones intermedias por parte del usuario, así los resultados de los trabajos sólo se ven al final de una serie de tareas y fases de tal forma que si se ha producido un error en las primeras fases este sólo se detectará al final y su corrección tendrá un costo muy elevado, puesto que será preciso rehacer todo el trabajo desde el principio.

33.4.4 *Modelos Evolutivos*

El software evoluciona con el tiempo. Los requisitos del usuario y del producto suelen cambiar conforme se desarrolla el mismo. Las fechas de mercado y la competencia hacen que no sea posible esperar a poner en el mercado un producto absolutamente completo, por lo que se debe

introducir una versión funcional limitada de alguna forma para aliviar las presiones competitivas.

En esas u otras situaciones similares los desarrolladores necesitan modelos de progreso que estén diseñados para acomodarse a una evolución temporal o progresiva, donde los requisitos centrales son conocidos de antemano, aunque no estén bien definidos a nivel detalle.

Los evolutivos son modelos iterativos, permiten desarrollar versiones cada vez más completas y complejas, hasta llegar al objetivo final deseado; incluso evolucionar más allá, durante la fase de operación.

33.4.4.1 Modelo Iterativo Incremental

El incremental *es un modelo de tipo evolutivo que está basado en varios ciclos cascada realimentados aplicados repetidamente, con una filosofía iterativa*, es decir, consiste en desarrollar un sistema que logré cubrir una parte de los requisitos especificados y luego ir generando nuevas versiones del sistema que incorporen el resto de funcionalidades y requisitos especificados, hasta llegar a un producto final, que se asemeje al sistema planteado.

Con este modelo, se pretende disponer pronto de un sistema que aunque sea incompleto, sea utilizable y satisfaga parte de los requisitos, evitando de paso el efecto big-bang, es decir, que durante un período largo de tiempo no se tenga nada y de repente haya una situación completamente nueva. Por otra parte, también se logra que el usuario se implique estrechamente en la planificación de los pasos siguientes.

El modelo de desarrollo incremental también se utiliza para evitar la demanda de funcionalidades excesivas al sistema por parte de los usuarios, ya que como a éstos les resulta difícil definir sus necesidades reales tienden a pedir demasiado. Actuando con este modelo se atiende primero a

las funcionalidades esenciales y las funcionalidades accesorias sólo se incluyen en las versiones sucesivas cuando realmente son necesarias.

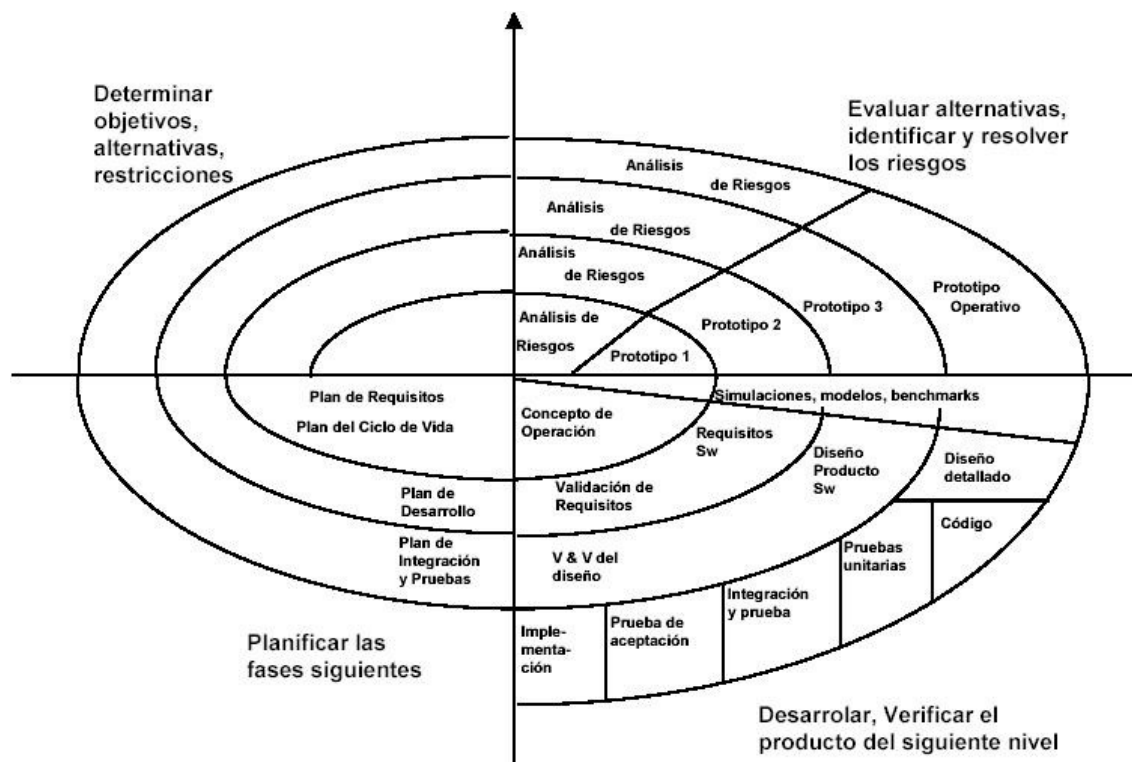
33.4.4.2 *Modelo en Espiral*

Es un modelo de proceso de software evolutivo con las características propias de un desarrollo iterativo mediante el cual se generan distintos prototipos, a las cuales se le suman los aspectos controlados y sistemáticos del modelo en cascada.

Ofrece el potencial para el desarrollo rápido de versiones incrementales del software. En el modelo espiral, el software se desarrolla en una serie de versiones incrementales. Durante las primeras iteraciones, la versión incremental podría ser un modelo en papel o un prototipo. Durante las últimas iteraciones, se producen versiones cada vez más completas del sistema diseñado.

Sus diferencias más importantes con los modelos más clásicos son:

- En el modelo en espiral hay un reconocimiento explícito de las diferentes **alternativas** para alcanzar los objetivos del proyecto.
- El modelo en espiral se centra en la identificación de los **riesgos** asociados a cada alternativa y en la manera de resolver dichos riesgos.
- En el modelo en espiral los proyectos se dividen en ciclos (ciclos de espiral), avanzándose en el desarrollo mediante consensos al final de cada ciclo.
- El modelo en espiral se adapta a cualquier tipo de actividad.



El modelo en espiral refleja la idea de que cada ciclo implica una progresión en el desarrollo del producto software que aplica la misma secuencia de pasos para cada parte del producto y para cada uno de sus niveles de elaboración, desde la concepción global hasta la codificación individual de cada programa.

Esta secuencia de pasos, iterativa en cada fase del desarrollo, se compone de las cuatro actividades siguientes:

- **Planificación:** Este primer paso con el que comienza cada ciclo de espiral consiste en la identificación de los objetivos de la parte del producto que está siendo elaborada (funcionalidad, rendimiento, adaptación a los cambios, etc.), identificación de las alternativas principales para realizar o implementar esta parte del producto, y la identificación de las restricciones impuestas (coste, plazo de realización, interfaces, etc.).
- **Análisis de riesgos:** Comienza con la evaluación de cada alternativa respecto a los objetivos y a las restricciones. Este proceso de evaluación identificará áreas de incertidumbre que son fuentes

significativas de riesgo en el proyecto. Se decidirá como resolver los riesgos asociados a la alternativa elegida.

- **Ingeniería.** Este paso consiste en el desarrollo y verificación del producto objeto de la fase (ciclo de espiral) en que nos encontremos. Como esta implementación está dirigida por el riesgo, el desarrollo podrá seguir las pautas de un prototipado evolutivo, las del ciclo de vida clásico, las orientadas a transformaciones automáticas, o cualquier otro enfoque del desarrollo. En definitiva, esto permite al modelo en espiral acomodarse a cualquier mezcla de estrategias de desarrollo.
- **Evaluación del cliente.** Una característica importante del modelo en espiral es que cada ciclo de espiral se completa con una revisión en la que participan aquellos que tienen relación con el producto (desarrolladores, usuarios, etc.). Esta revisión incluye todos los productos desarrollados durante el ciclo, los planes para el siguiente ciclo y los recursos necesarios para llevarlos a cabo.

Según esto, el modelo se puede representar mediante unos ciclos externos de espiral, que representan las fases en que se ha dividido el desarrollo del proyecto software, normalmente las del modelo clásico, y unos ciclos internos, iterativos para cada fase, en los que se llevan a cabo las cuatro actividades antes citadas. La dimensión radial indica los costes de desarrollo acumulativos, mientras que la dimensión angular indica el progreso hecho en cumplimentar cada fase.

La principal ventaja del modelo en espiral es el amplio rango de opciones a que puede ajustarse y que éstas permiten utilizar los modelos de proceso de construcción de software tradicionales; por otra parte, su orientación al riesgo evita, si no elimina, muchas de las posibles dificultades. Otras **ventajas** son:

- Concentra su atención en opciones que permiten la reutilización de software ya existente.



- Se centra en la eliminación de errores y alternativas poco atractivas.
- No establece procedimientos diferentes para el desarrollo del software y el mantenimiento del mismo.
- Proporciona un marco estable para desarrollos integrados hardware-software.
- Permite preparar la evolución del ciclo de vida del producto software, así como el crecimiento y cambios de éste.
- Permite incorporar objetivos de calidad en el desarrollo de productos software.
- Se adapta muy bien al diseño y programación orientada a objetos. Posiblemente con este método es cuando obtiene mejores resultados.

En cuanto a los **inconvenientes** que plantea la utilización del modelo en espiral, cabe citar:

- Dificultad para adaptar su aplicabilidad al software contratado, debido a la poca flexibilidad y libertad de éste.
- Dependencia excesiva de la experiencia que se tenga en la identificación y evaluación de riesgos.
- Necesidad de una elaboración adicional de los pasos del modelo, lo que depende también, en gran medida, de la experiencia del personal.

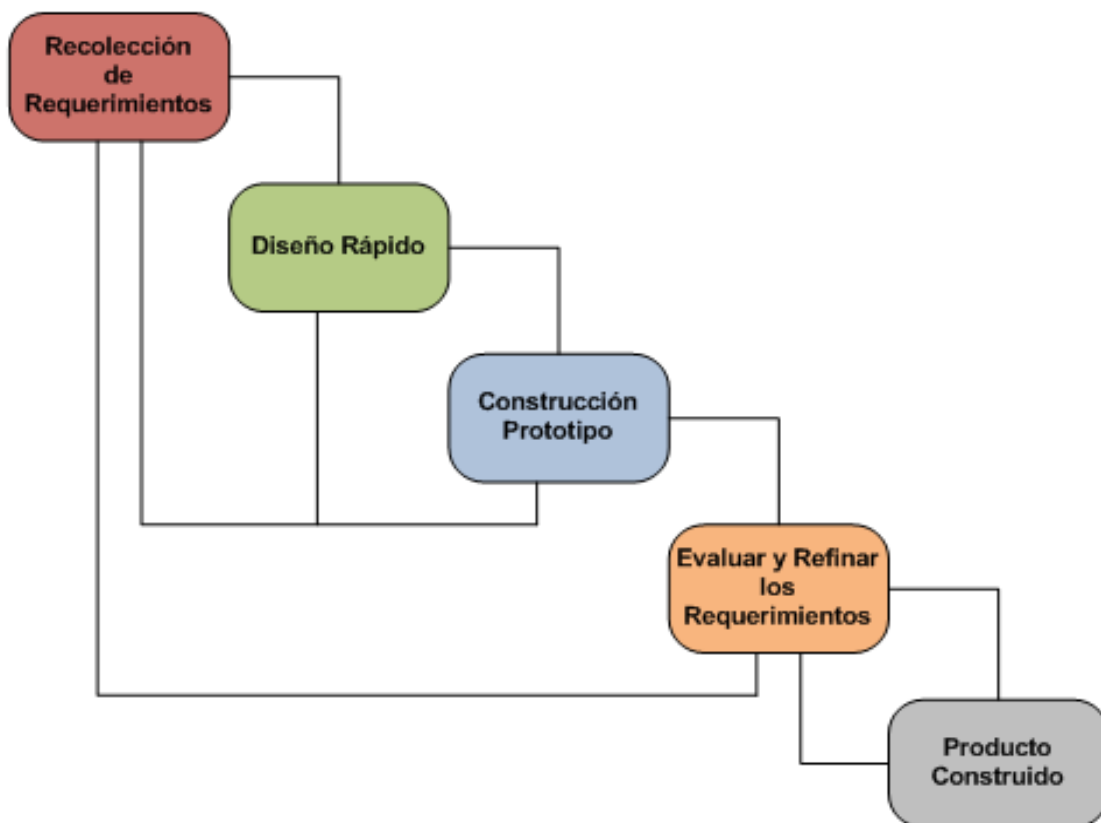
33.4.4.3 *Modelos basados en prototipos*

Los modelos basados en prototipos se centran en la idea de ofrecer una mayor comprensión de los requisitos que el usuario plantea, sobre todo si este no posee una idea clara y concreta de sus pretensiones.

Además, este tipo de modelos puede utilizarse para intentar valorar de una manera temprana la viabilidad de la solución propuesta, cuando no se confía plenamente en ella.

33.4.4.3.1 Prototipado rápido

Este modelo se fundamenta en la construcción de prototipos de una manera fácil, barata y en un reducido período de tiempo, permitiendo así su temprana evaluación. También se denominan de usar y tirar.



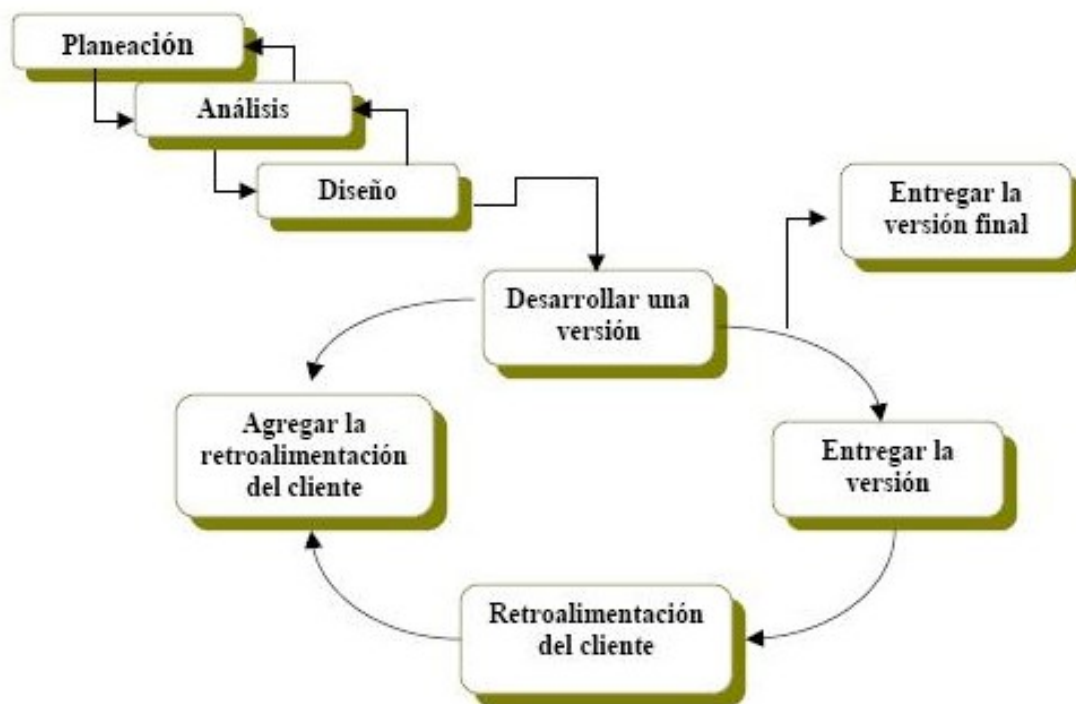
El prototipo sirve para crear y validar la especificación, y para que el usuario tenga una idea de cómo será el software antes de que comience el desarrollo. Es importante precisar que el prototipo se construye sólo para servir como mecanismo de definición de los requerimientos funcionales. Posteriormente ha de desecharse y debe construirse el sistema con los criterios normales de calidad y mantenimiento, siguiendo, por ejemplo, el ciclo de vida clásico, ya que generalmente el prototipo se ha construido tomando decisiones de implementación contrarias al buen criterio de desarrollo de software. Los objetivos del prototipo son:

- Reducir el riesgo de construir un producto que se aleje de las necesidades del usuario
- Reducir el coste de desarrollo al disminuir las correcciones en etapas avanzadas del mismo.
- Aumentar las posibilidades de éxito del producto.

El principal problema de este modelo es que el usuario ve en el prototipo lo que parece ser una versión de trabajo del software, sin saber que con la prisa de hacer que funcione no se ha tenido en cuenta la calidad del software global o la facilidad de mantenimiento a largo plazo. Cuando se informa de que el producto se debe construir otra vez para que se puedan mantener los niveles altos de calidad, el cliente no lo entiende y pide que se apliquen unos pequeños ajustes que puedan hacer del prototipo un producto final.

33.4.4.3.2 Prototipado evolutivo

En este tipo de ciclo de vida se construye una implementación parcial del sistema que satisface los requisitos conocidos, la cual es utilizada por el usuario para llegar a comprender mejor la totalidad de requisitos que desea.



Desde un punto de vista genérico, se puede decir que los modelos evolutivos se encaminan a conseguir un sistema flexible que se pueda expandir, de forma que se pueda realizar rápidamente un nuevo sistema cuando cambian los requisitos. Estos modelos consisten en implementar un producto software operativo y hacerle evolucionar de acuerdo con la propia experiencia operacional. Están especialmente indicados en situaciones en que se utilizan lenguajes de cuarta generación (L4G) y para aquellas otras en que el usuario no puede decir lo que requiere, pero lo reconocerá cuando lo vea. Los modelos evolutivos dan al usuario una rápida capacidad de operación inicial y una buena base para determinar mejoras del sistema. Está relacionado con el concepto de RAD (Rapid Application Development - Desarrollo Rápido de Aplicaciones), que identifica los asistentes, plantillas y entornos de fácil y rápida creación de software.

La *diferencia* fundamental entre el prototipado rápido y el evolutivo estriba en que mientras que en el primer caso se asume que existen una serie de requisitos reales, aunque para establecer lo que el usuario quiere realmente es necesario establecer una serie de iteraciones antes de que

los requisitos se estabilicen al final, en el caso evolutivo se asume desde el principio que los requisitos cambian continuamente.

En el prototipo rápido lo lógico es implementar sólo aquellos aspectos del sistema que se entienden mal, mientras que en el prototipo evolutivo lo lógico es comenzar por los aspectos que mejor se comprenden y seguir construyendo apoyados en los puntos fuertes y no en los débiles. Como resultado de este modo de desarrollo, la solución software evoluciona acercándose cada vez más a las necesidades del usuario; ahora bien, pasado un tiempo el sistema software así construido deberá ser rehecho o sufrir una profunda reestructuración con el fin de seguir evolucionando.

El modelo de prototipado evolutivo (Evolutionary Development model) también tiene sus **dificultades**. Se le puede considerar como una nueva versión, utilizando lenguajes de programación de más alto nivel, del viejo modelo CODE-AND-FIX. Otro inconveniente que presenta es partir de la suposición, muchas veces no realista, de que el sistema operacional del usuario final será lo suficientemente flexible como para poder incorporar caminos de evolución futuros no planificados con anterioridad.

33.4.5 *Modelos basados en Transformaciones*

Surgen como solución al problema que plantean los modelos de desarrollo que producen software con problemas estructurales. Su principal virtud es que ofrecen la posibilidad de convertir de una manera automáticamente una especificación formal de un sistema en un software que cumpla lo establecido en los requisitos.

Los pasos más importantes que siguen este tipo de modelos son:

1. Especificación formal del producto tal como lo permita la comprensión inicial del problema.
2. Transformación automática de la especificación en código.
3. Realizar bucles iterativos para mejorar el rendimiento del código resultante.

4. Probar el producto resultante.
5. Reajustar las especificaciones para dejarlas en concordancia con el resultado de la experiencia operativa y volver a generar el código a partir de las especificaciones, volviendo a optimizar y probar el producto.

El modelo de transformación, por tanto, evita la dificultad de tener que modificar el código poco estructurado (por haber pasado por sucesivas reoptimizaciones), puesto que las modificaciones las aplica sobre la especificación de partida. Esto, también evita el tiempo adicional que se emplearía en los pasos intermedios de diseño, codificación y pruebas.

La dificultad que presentan estos modelos es que las posibilidades de transformación automática generalmente sólo están disponibles para productos relativamente pequeños y aplicados a unas áreas muy limitadas. También comparte algunas de las dificultades del modelo de desarrollo evolutivo tales como, por ejemplo, la suposición de que el sistema operacional del usuario final se prestará a evoluciones no planificadas con anterioridad.

Dentro de este tipo de modelos se encuentran:

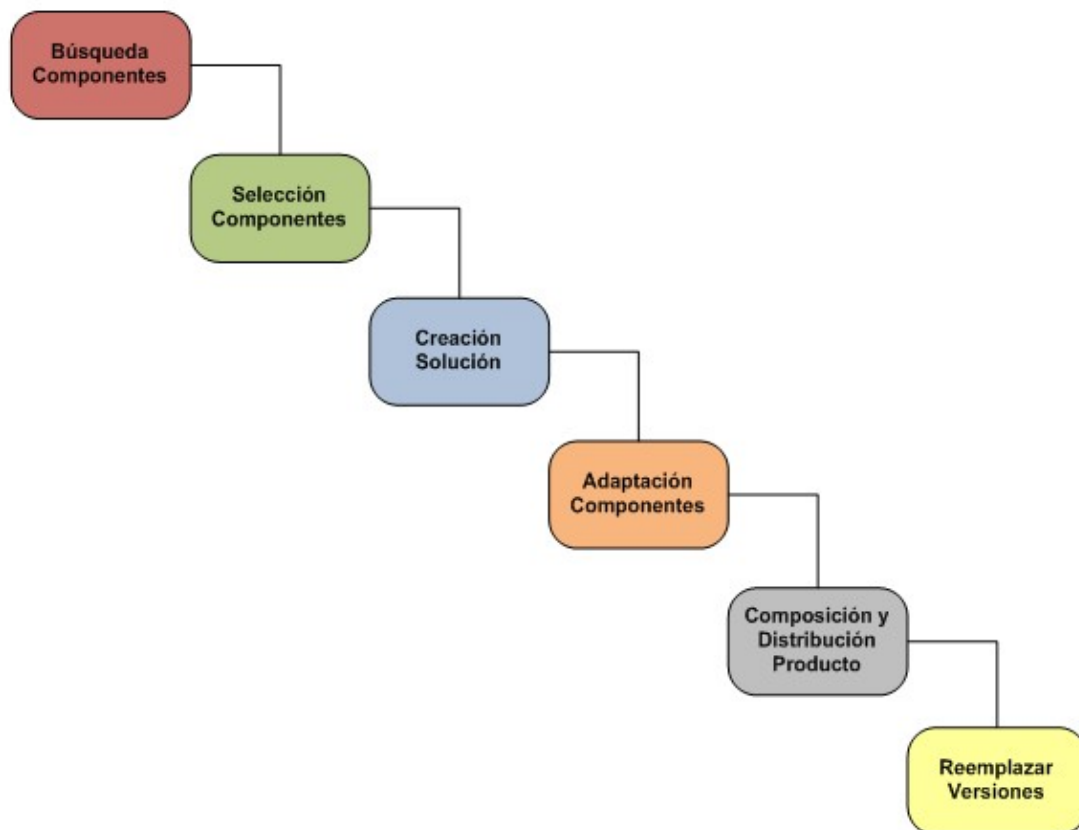
- Los que usan técnicas de cuarta generación (Roger Pressman): Suelen estar basados en herramientas de cuarta generación. Estos permiten la generación de código rápido. En ellos se indica qué se quiere obtener, no cómo.
- Basados en modelos de transformación (Carma McClure) => Basados en herramientas CASE que permiten, siguiendo el MCV clásico, pasar de una etapa a otra aplicando las transformaciones que dan las herramientas.

En ambos casos, la filosofía general es llegar a generar código a partir de unas especificaciones transformándolas por medio de herramientas.

33.4.6 Modelo basado en componentes

El modelo basado en componentes surge de la necesidad de reutilización que los complejos sistema actuales precisan para acelerar su desarrollo. Este modelo posibilita que ciertas piezas de código preelaboradas puedan ser reutilizadas en otras partes del sistema o incluso en otros sistemas para llevar a cabo diversas tareas, conllevando a diversos beneficios como las mejoras a la calidad, la reducción del ciclo de desarrollo y el mayor retorno sobre la inversión.

Un componente es una pieza de código preelaborado que encapsula alguna funcionalidad expuesta a través de interfaces estándar. Los componentes son los "ingredientes de las aplicaciones", que se juntan y combinan para llevar a cabo una tarea. El paradigma de ensamblar componentes y escribir código para hacer que estos componentes funcionen se conoce como Desarrollo de Software Basado en Componentes.



Los pasos de que consta el ciclo de desarrollo para un sistema basado en componentes son:

1. Buscar componentes, tanto COTS (Comercial Off-The-Shelf) como no COTS.
2. Seleccionar los componentes más adecuados para el sistema.
3. Crear una solución compuesta que integre la solución previa.
4. Adaptar los componentes seleccionados de forma que se ajusten al modelo de componentes o a los requisitos de la aplicación.
5. Componer y distribuir el producto.
6. Reemplazar versiones anteriores o mantener las partes COTS y no COTS del sistema.

Además de los problemas inherentes a la reutilización del software, los productos COTS presentan problemas específicos como incompatibilidad, inflexibilidad (no existe código fuente), complejidad (esfuerzo de aprendizaje) o cambio de versiones, por lo que el establecimiento de

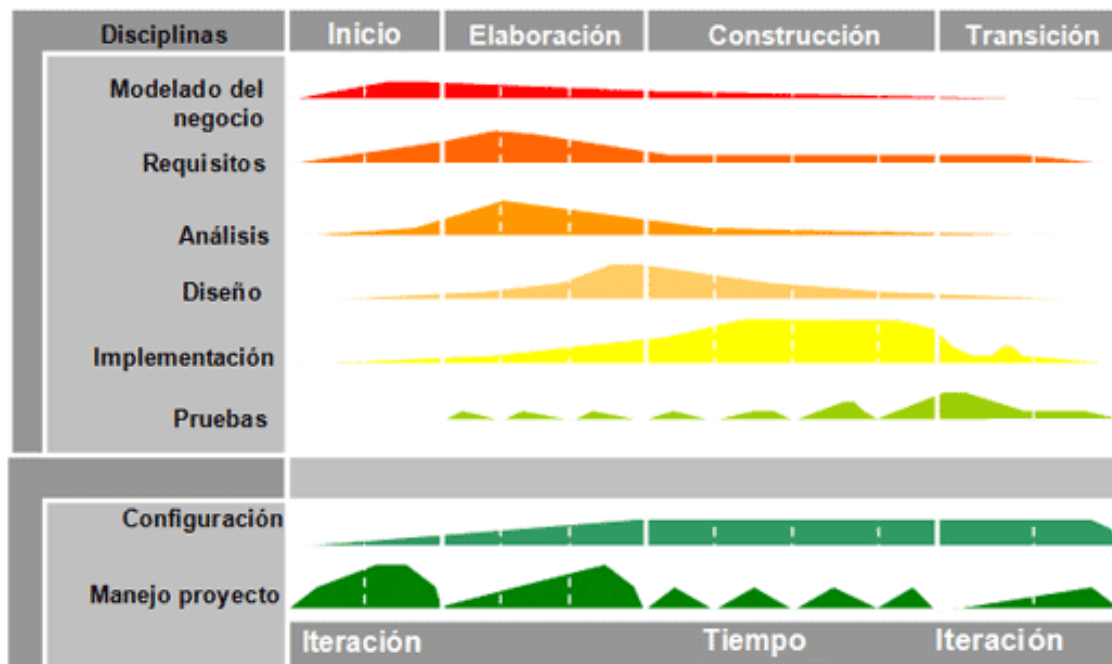
métodos sistemáticos y repetibles para evaluar y seleccionar dichos componentes es un aspecto importante para el desarrollo del software basado en componentes y, en general, para la Ingeniería del Software Basada en Componentes (ISBC).

Entre las ventajas del Desarrollo basado en componentes tenemos que se reducen tiempos y costes de desarrollo y se aumenta la fiabilidad. Entre los inconvenientes, tendremos la dificultad para reconocer los componentes potencialmente reutilizables, dificultad de catalogación y recuperación y los problemas de gestión de configuración.

33.5 Modelos de Desarrollo

33.5.1 *Proceso Unificado de Desarrollo de software (PUDS)*

En realidad es una metodología que propone un modelo de ciclo de vida. Está desarrollada por tres padres de la IS moderna: Yourdon, Booch y Rumbaugh. Plantea un modelo de ciclo de vida iterativo e incremental, centrado en una arquitectura que guía el desarrollo del sistema, cuyas actividades están dirigidas por casos de uso y soporta las técnicas orientadas a objetos. PUDS impulsa un control de calidad y una gestión de riesgos objetivos y continuos.



El PUDS se compone de fases, iteraciones y ciclos. Una fase es el intervalo de tiempo entre dos hitos importantes del proceso durante la cual se cumple un conjunto bien definido de objetivos, se completan entregables y se toman las decisiones sobre si pasar o no a la siguiente fase. Las **fases** son:

1. **Iniciación.** En esta fase se establece la visión del negocio, que incluye el contexto del negocio, los factores de éxito, y la previsión económica. Para completar la visión del negocio se genera un plan del proyecto, una descripción de los posibles riesgos y del propio proyecto (requisitos principales del proyecto, restricciones y características claves)
2. **Elaboración.** Es donde el proyecto comienza a tomar forma. En esta fase se hace el análisis del dominio del problema y se obtiene una idea básica de la arquitectura del sistema, además de revisarse los riesgos. En esta fase el proyecto todavía puede cancelarse o rediseñarse.
3. **Construcción.** En esta fase el enfoque se traslada al desarrollo de componentes y otras características del sistema que está siendo diseñado. Aquí se realiza el grueso de las tareas de codificación. En

proyectos grandes, se puede dividir la fase en varias iteraciones para dividir los casos de uso en segmentos manejables que produzcan prototipos funcionales.

4. **Transición.** El producto se implanta en la organización del usuario final. Aquí se lleva a cabo la formación de los usuarios finales y las pruebas de aceptación del sistema para validarlo contra las expectativas del usuario.

En cada fase hay una o varias iteraciones. Una **iteración** ofrece como resultado un incremento del producto desarrollado que añade o mejora las funcionalidades del sistema en desarrollo. Cada fase e iteración se centra en disminuir algún riesgo y concluye con un hito bien definido. El paso a través de las 4 fases constituye un **ciclo** de desarrollo y produce una generación de software. El primer ciclo es el inicial y después serán ciclos de evolución del sistema.

Los flujos de trabajo del proceso son los siguientes:

- Modelado del negocio. El objetivo es establecer una mejor comprensión y un mejor canal de comunicación entre los clientes y los expertos en sistemas.
- Requisitos. El objetivo es describir lo que el sistema debe hacer.
- Análisis y diseño. Aquí se muestra la forma que tendrá el sistema en la fase de implementación.
- Implementación. Codificar y realizar pruebas unitarias.
- Pruebas. Se realizan pruebas de integración.
- Despliegue. Incluye una amplia variedad de actividades como la generación de versiones estables o la distribución e instalación del software.
- Configuración y gestión de cambios.
- Gestión del proyecto. Se realiza a 2 niveles, un nivel de grano grueso que trata la planificación de las fases y otro nivel de grano fino que trata la planificación de las iteraciones.

- Entorno.

33.5.2 Programación Extrema (eXtreme Programming)

En la programación extrema, todos los requerimientos se expresan como escenarios (llamados historias de usuario), los cuales se implementan directamente como una serie de tareas. Los programadores trabajan en parejas y desarrollan pruebas para cada tarea antes de escribir el código. Todas las pruebas se deben ejecutar satisfactoriamente cuando el código nuevo se integre al sistema. Existe un pequeño espacio de tiempo entre las entregas del sistema. La programación extrema implica varias prácticas, que se ajustan a los principios de los métodos ágiles:

1. El desarrollo incremental se lleva a cabo través de entregas del sistema pequeñas y frecuentes y por medio de un enfoque para la descripción de requerimientos basado en las historias de cliente o escenarios que pueden ser la base para el proceso de planificación.
2. La participación del cliente se lleva a cabo a través del compromiso a tiempo completo del cliente en el equipo de desarrollo. Los representantes de los clientes participan en el desarrollo y son los responsables de definir las pruebas de aceptación del sistema.
3. El interés en las personas, en vez de en los procesos, se lleva a cabo a través de la programación en parejas, la propiedad colectiva del código del sistema, y un proceso de desarrollo sostenible que no implique excesivas jornadas de trabajo.
4. El cambio se lleva a cabo a través de las entregas regulares del sistema, un desarrollo previamente probado y la integración continua.
5. El mantenimiento de la simplicidad se lleva a cabo a través de la refactorización constante para mejorar la calidad del código y la utilización de diseños sencillos que no prevén cambios futuros en el sistema.

Los clientes del sistema son parte del equipo de desarrollo y discuten escenarios con otros miembros del equipo. Desarrollan conjuntamente una «tarjeta de historias» (story card) que recoge las necesidades del cliente. El equipo de desarrollo intentará entonces implementar ese escenario en una entrega futura del software. Una vez que se han desarrollado las tarjetas de historias, el equipo de desarrollo las divide en tareas y estima el esfuerzo y recursos requeridos para su implementación. El cliente establece entonces la prioridad de las historias a implementar.

El problema con la implementación de cambios imprevistos es que tienden a degradar la estructura del software, por lo que los cambios se hacen cada vez más difíciles de implementar. La programación extrema aborda este problema sugiriendo que se debe refactorizar constantemente el software. Esto significa que el equipo de programación busca posibles mejoras del software y las implementa inmediatamente. Por lo tanto, el software siempre debe ser fácil de entender y cambiar cuando se implementen nuevas historias.

Otra práctica innovadora que se ha introducido es que los programadores trabajan en parejas para desarrollar el software. Las ventajas de esto son que apoya la idea de la propiedad y responsabilidad comunes del sistema, actúa como un proceso de revisión informal del código y ayuda en la refactorización.

Bibliografía

- Ingeniería del Software. Un enfoque práctico. ROGER S. PRESSMAN.
Ed. McGraw Hill
- Ingeniería de Software 7 Edición - Ian Sommerville
- Ingeniería de Sistemas de Software – Gonzalo León Serrano. Ed.
Isdefe.
- Metodologías para la gestión y desarrollo de software

Autor: Francisco Javier Rodríguez Martínez.

Subdirector de la Escuela Superior de Ingeniería Informática.

Universidad de Vigo.

34. METODOLOGÍAS DE DESARROLLO DE SISTEMAS DE INFORMACIÓN. MÉTRICA 3. RUP. METODOLOGÍAS ÁGILES.

Tema 34. Metodologías de desarrollo de sistemas de información.

Métrica 3. RUP. Metodologías ágiles.

INDICE

34.1 Metodologías de desarrollo de sistemas de información.

34.2 Métrica Versión 3

34.2.1 Procesos Principales de Métrica Versión 3

34.2.2 Planificación de Sistemas de Información

34.2.3 Desarrollo de Sistemas de Información

34.2.3.1 Estudio de Viabilidad del Sistema (EVS)

34.2.3.2 Análisis del Sistema de Información (ASI)

34.2.3.3 Diseño del Sistema de Información (DSI)

34.2.3.4 Construcción del Sistema de Información (CSI)

34.2.3.5 Implantación y Aceptación del Sistema (IAS)

34.2.4 Mantenimiento de Sistemas de Información

34.2.5 Interfaces de Métrica Versión 3

34.3 RUP

34.3.1 Fases del ciclo de desarrollo

34.3.2 Flujos de trabajo

34.4 Metodologías Ágiles

34.4.1 SCRUM

34.4.2 DSDM

34.4.3 Extreme Programming (XP)

34.4.4 FCC

34.4.5 Agile Modeling (AM)

34.4.6 Familia Crystal

34.1 Metodologías de desarrollo de sistemas de información.

Desde que el desarrollo de software se comenzó a considerar como un proceso de ingeniería, se han ido definiendo diferentes marcos de trabajo orientados a estructurar, planificar y controlar el proceso de desarrollo en los sistemas de información. El proceso detallado y completo de desarrollo de software suele denominarse “Metodología”. Las metodologías se basan en una combinación de los modelos de procesos genéricos (cascada, evolutivo, incremental, etc.).

Las metodologías deben definir con precisión los productos, roles y actividades involucrados, junto con prácticas y técnicas recomendadas, guías de adaptación de la metodología al proyecto, guías para uso de herramientas de apoyo, etc. Las técnicas, notaciones y guías asociadas que se aplican a las diferentes actividades del proceso de desarrollo son lo que se conoce como "métodos".

La comparación y/o clasificación de metodologías no es una tarea sencilla debido a la diversidad de propuestas y diferencias en el grado de detalle, información disponible y alcance de cada una de ellas. A grandes rasgos, si tomamos como criterio las notaciones utilizadas para especificar productos producidos en actividades de análisis y diseño, podemos clasificar las metodologías en dos grupos: Metodologías Estructuradas y Metodologías Orientadas a Objetos. Por otra parte, considerando su filosofía de desarrollo, aquellas metodologías con mayor énfasis en la planificación y control del proyecto, en especificación precisa de requisitos y modelado, reciben el apelativo de Metodologías Tradicionales (o peyorativamente denominada Metodologías Pesadas, o Peso Pesado). Otras metodologías, denominadas Metodologías Ágiles, están más orientadas a la generación de código con ciclos muy cortos de desarrollo, se dirigen a equipos de desarrollo pequeños, hacen especial hincapié en aspectos humanos asociados al trabajo en equipo e involucran activamente al cliente en el

proceso. A continuación se revisan brevemente algunas de estas categorías de metodologías.

- **Metodologías estructuradas:** Los métodos estructurados comenzaron a desarrollarse a fines de los 70's con la Programación Estructurada. A mediados de los 70's aparecieron técnicas para el Diseño (por ejemplo: el diagrama de Estructura) primero y posteriormente para el Análisis (por ejemplo: Diagramas de Flujo de Datos). Estas metodologías son particularmente apropiadas en proyectos que utilizan para la implementación lenguajes de 3ra y 4ta generación. Ejemplos de metodologías estructuradas de ámbito gubernamental: MERISE (Francia), MÉTRICA (España), SSADM (Reino Unido). Ejemplos de propuestas de métodos estructurados en el ámbito académico: Gane & Sarson, Ward & Mellor, Yourdon & DeMarco e Information Engineering.
- **Metodologías orientadas a objetos:** Su historia va unida a la evolución de los lenguajes de programación orientada a objetos. A fines de los 80's comenzaron a consolidarse algunos métodos Orientados a Objetos. En 1995 Booch y Rumbaugh proponen el Método Unificado con la ambiciosa idea de conseguir una unificación de sus métodos y notaciones, que posteriormente se reorienta a un objetivo más modesto, para dar lugar al Unified Modeling Language (UML), la notación OO más popular en la actualidad. Algunos métodos OO con notaciones predecesoras de UML son: OOAD (Booch), OOSE (Jacobson), Coad & Yourdon, Shaler & Mellor y OMT (Rumbaugh). Algunas metodologías orientadas a objetos que utilizan la notación UML son: Rational Unified Process (RUP), OPEN, MÉTRICA (que también soporta la notación estructurada).
- **Metodologías tradicionales (no ágiles):** Las metodologías no ágiles son aquellas que están guiadas por una fuerte planificación durante todo el proceso de desarrollo; llamadas también metodologías tradicionales o clásicas, donde se realiza una intensa

etapa de análisis y diseño antes de la construcción del sistema. Todas las propuestas metodológicas antes indicadas pueden considerarse como metodologías tradicionales..

- **Metodologías ágiles:** Un proceso es ágil cuando el desarrollo de software es **incremental** (entregas pequeñas de software, con ciclos rápidos), **cooperativo** (cliente y desarrolladores trabajan juntos constantemente con una cercana comunicación), **sencillo** (el método en sí mismo es fácil de aprender y modificar, bien documentado), y **adaptable** (permite realizar cambios de último momento). Algunas de las metodologías ágiles identificadas son Extreme Programming, Scrum, Familia de Metodologías Crystal, Feature Driven Development, Proceso Unificado Rational, Dynamic Systems Development Method, Adaptive Software Development. Se verán con más detalle en un apartado posterior.
- **Proceso Unificado de Rational:** Es un proceso de desarrollo de software y junto con el Lenguaje Unificado de Modelado UML, constituye la metodología estándar más utilizada para el análisis, implementación y documentación de sistemas orientados a objetos. El RUP no es un sistema con pasos firmemente establecidos, sino un conjunto de metodologías adaptables al contexto y necesidades de cada organización. Se verá en un apartado posterior.
- **Métrica V3:** La metodología MÉTRICA Versión 3 ofrece a las Organizaciones un instrumento útil para la sistematización de las actividades que dan soporte al ciclo de vida del software. Se verá en un apartado posterior.
- **Open Source Development Software:** Open Source es software desarrollado con la falta de coordinación, donde los programadores colaboran libremente, utilizando el código fuente distribuido y la infraestructura de comunicaciones de Internet. El código abierto se basa en la filosofía del software libre, sin embargo, extiende esta ideología ligeramente para presentar un enfoque más comercial que

incluye tanto un modelo de negocio como una metodología de desarrollo.

34.2 Métrica Versión 3.

Métrica Versión 3 es una evolución de la metodología Métrica promovida por el Ministerio de Administraciones Públicas del Gobierno de España. Métrica consiste en una metodología para la planificación, desarrollo y mantenimiento de los sistemas de información, orientada a la sistematización de las actividades del ciclo de vida de los proyectos software en el ámbito de las administraciones públicas. La metodología MÉTRICA Versión 3 ofrece a las Organizaciones un instrumento útil para la sistematización de las actividades que dan soporte al ciclo de vida del software dentro del marco que permite alcanzar los siguientes objetivos:

- Proporcionar o definir Sistemas de Información que ayuden a conseguir los fines de la Organización mediante la definición de un marco estratégico para el desarrollo de los mismos.
- Dotar a la organización de productos software que satisfagan las necesidades de los usuarios dando una mayor importancia al análisis de requisitos.
- Mejorar la productividad de los departamentos de Sistemas y Tecnologías de la Información y las Comunicaciones, permitiendo una mayor capacidad de adaptación a los cambios y teniendo en cuenta la reutilización en la medida de lo posible.
- Facilitar la comunicación y entendimiento entre los distintos participantes en la producción de software a lo largo del ciclo de vida del proyecto, teniendo en cuenta su papel y responsabilidad, así como las necesidades de todos y cada uno de ellos.
- Facilitar la operación, mantenimiento y uso de los productos software obtenidos.

En la elaboración de MÉTRICA Versión 3 se han tenido en cuenta los métodos de desarrollo más extendidos, así como los últimos estándares de ingeniería del software y calidad, además de referencias específicas en cuanto a seguridad y gestión de proyectos. En una única estructura, la metodología MÉTRICA Versión 3 cubre distintos tipos de desarrollo: estructurado y orientado a objetos, facilitando a través de interfaces la realización de los procesos de apoyo u organizativos: Gestión de Proyectos, Gestión de Configuración, Aseguramiento de Calidad y Seguridad.

En lo que se refiere a estándares se ha tenido en cuenta como referencia el Modelo de Ciclo de Vida de Desarrollo propuesto en la norma ISO/IEC 12207 "Information technology - Software life cycle processes". Siguiendo este modelo se ha elaborado la estructura de MÉTRICA Versión 3 en la que se distinguen procesos principales (Planificación, Desarrollo y Mantenimiento) e interfaces (Gestión de Proyectos, Aseguramiento de la Calidad, Seguridad y Gestión de Proyectos) cuyo objetivo es dar soporte al proyecto en los aspectos organizativos. Además de la norma ISO/IEC 12207, entre los estándares de referencia hay que destacar las normas ISO/IEC TR 15.504/SPIICE "Software Process Improvement and Assurance Standards Capability Determination", UNE-EN-ISO 9001:2000 Sistemas de Gestión de la Calidad. Requisitos, UNE-EN-ISO 9000:2000 Sistemas de Gestión de la Calidad. Fundamentos y Vocabulario y el estándar IEEE 610.12-1.990 "Standard Glossary of Software Engineering Terminology". Igualmente se han tenido en cuenta otras metodologías como SSADM, Merise, Information Engineering, MAGERIT. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información promovida por el Consejo Superior de Informática y EUROMÉTODO.

Se ha diferenciado entre la aplicación de Técnicas, como conjunto de heurísticas y procedimientos apoyados en estándares que utilizan notaciones específicas en términos de sintaxis y semántica, y de Prácticas cuya utilización no conlleva reglas preestablecidas con la misma rigidez.

Las nuevas técnicas están ampliamente soportadas por herramientas comerciales.

34.2.1 Procesos Principales de Métrica Versión 3

MÉTRICA Versión 3 tiene un enfoque orientado al ciclo de vida de software y por ello se ha enmarcado dentro de la norma ISO/IEC 12207, que se centra en la clasificación y definición de los procesos del ciclo de vida del software, cubriendo el Proceso de Desarrollo y el Proceso de Mantenimiento de Sistemas de Información.

MÉTRICA Versión 3 ha sido concebida para abarcar el desarrollo completo de Sistemas de Información sea cual sea su complejidad y magnitud, por lo cual su estructura responde a desarrollos máximos y deberá adaptarse y dimensionarse en cada momento de acuerdo a las características particulares de cada proyecto. La metodología descompone cada uno de los procesos en actividades, y éstas a su vez en tareas. Para cada tarea se describe su contenido haciendo referencia a sus principales acciones, productos, técnicas, prácticas y participantes. El orden asignado a las actividades no debe interpretarse como secuencia en su realización, ya que éstas pueden realizarse en orden diferente a su numeración o bien en paralelo. Sin embargo, no se dará por acabado un proceso hasta no haber finalizado todas las actividades del mismo determinadas al inicio del proyecto.

Así los procesos de la estructura principal de MÉTRICA Versión 3 son los siguientes:

- PLANIFICACIÓN DE SISTEMAS DE INFORMACIÓN.
- DESARROLLO DE SISTEMAS DE INFORMACIÓN.
- MANTENIMIENTO DE SISTEMAS DE INFORMACIÓN.

34.2.2 Planificación de sistemas de información

Los planes estratégicos de sistemas de información pretenden abordar el estudio de los sistemas y recursos informáticos para conseguir unos objetivos determinados dentro de las organizaciones. El objetivo principal de un Plan de Sistemas de Información es proporcionar un marco estratégico de referencia para los Sistemas de Información de un determinado ámbito de la Organización. El resultado del Plan de Sistemas debe, por tanto, orientar las actuaciones en materia de desarrollo de Sistemas de Información con el objetivo básico de apoyar la estrategia corporativa, elaborando una arquitectura de información y un plan de proyectos informáticos para dar apoyo a los objetivos estratégicos. Por este motivo es necesario un proceso como el de Planificación de Sistemas de Información, en el que participen, por un lado los responsables de los procesos de la organización con una visión estratégica y por otro, los profesionales de SI capaces de enriquecer dicha visión con la aportación de ventajas competitivas por medio de los sistemas y tecnologías de la información y comunicaciones.

Como productos finales de este proceso se obtienen los siguientes:

- Catálogo de requisitos de PSI que surge del estudio de la situación actual en el caso de que sea significativo dicho estudio, del diagnóstico que se haya llevado a cabo y de las necesidades de información de los procesos de la organización afectados por el plan de sistemas.
- Arquitectura de información que se compone de los siguientes productos: modelo de información, modelo de sistemas de información, arquitectura tecnológica, plan de proyectos y plan de mantenimiento del PSI.

Este nuevo enfoque de alineamiento de los sistemas de información con la estrategia de la organización, la implicación directa de la alta dirección y la propuesta de solución presenta como ventajas:

- La implicación de la alta dirección facilita que se pueda desarrollar con los recursos necesarios y el calendario establecido.
- La perspectiva horizontal de los procesos dentro de la Organización facilita que se atienda a intereses globales y no particulares de unidades organizativas que puedan desvirtuar los objetivos del Plan.
- La prioridad del desarrollo de los sistemas de información de la organización por objetivos estratégicos.
- La propuesta de Arquitectura de Información que se hace en el plan es más estratégica que tecnológica.

34.2.3 Desarrollo de Sistemas de Información

El proceso de Desarrollo de MÉTRICA Versión 3 contiene todas las actividades y tareas que se deben llevar a cabo para desarrollar un sistema, cubriendo desde el análisis de requisitos hasta la instalación del software. Además de las tareas relativas al análisis, incluye dos partes en el diseño de sistemas: arquitectónico y detallado. También cubre las pruebas unitarias y de integración del sistema. Este proceso es, sin duda, el más importante de los identificados en el ciclo de vida de un sistema y se relaciona con todos los demás.

En MÉTRICA Versión 3 se han abordado los dos tipos de desarrollo: estructurado y orientado a objeto, por lo que ha sido necesario establecer actividades a realizar en función del tipo de desarrollo elegido. Se han definido 5 subprocesos para este apartado:

- Estudio de Viabilidad del Sistema (EVS)
- Análisis Del Sistema De Información (ASI).
- Diseño Del Sistema De Información (DSI).

- Construcción Del Sistema De Información (CSI).
- Implantación Y Aceptación Del Sistema (IAS).

34.2.3.1 Estudio de Viabilidad del Sistema (EVS)

Consiste en analizar un conjunto de necesidades concreto y definido, para elaborar una solución inicial abaricable a corto plazo. Los criterios con los que se hace esta propuesta no serán estratégicos sino tácticos y relacionados con aspectos económicos, técnicos, legales y operativos. Los resultados del Estudio de Viabilidad del Sistema constituirán la base para tomar la decisión de seguir adelante o abandonar. Si se decide seguir adelante pueden surgir uno o varios proyectos que afecten a uno o varios sistemas de información. Se considerarán alternativas de solución basadas en soluciones "a medida", soluciones basadas en la adquisición de productos software del mercado o soluciones mixtas. Para valorar las alternativas planteadas y determinar una única solución, se estudiará el impacto en la organización de cada una de ellas, la inversión y los riesgos asociados. El resultado final de este proceso son los productos relacionados con la solución que se propone para cubrir la necesidad concreta que se planteó en el proceso, y que depende de si la solución conlleva desarrollo a medida o no.

34.2.3.2 Análisis del Sistema de Información (ASI)

Durante esta fase inicial del proceso, el objetivo consiste en recopilar de forma detallada, concreta y específica todos los aspectos referentes al sistema de información. El resultado obtenido deberá presentarse en forma de especificación de un catálogo de requisitos que cubren las necesidades de información de los usuarios finales hacia quiénes va dirigido el sistema. Dicha especificación representa la salida del proceso ASI y representa la entrada para el proceso de Diseño del Sistema de Información (DSI).

En primer lugar se describe inicialmente el sistema de información, a partir de los productos generados en el proceso Estudio de Viabilidad del Sistema (EVS). Se delimita su alcance, se genera un catálogo de requisitos generales y se describe el sistema mediante unos modelos iniciales de alto nivel. Se recogen de forma detallada los requisitos funcionales que el sistema de información debe cubrir, catalogándolos, lo que permite hacer la traza a lo largo de los procesos de desarrollo. Además, se identifican los requisitos no funcionales del sistema, es decir, las facilidades que ha de proporcionar el sistema, y las restricciones a que estará sometido, en cuanto a rendimiento, frecuencia de tratamiento, seguridad, etc. Para facilitar el análisis del sistema se identifican los subsistemas de análisis, y se elaboran los modelos de Casos de Uso y de Clases, en desarrollos orientados a objetos, y de Datos y Procesos en desarrollos estructurados. Se especificarán todas las interfaces entre el sistema y el usuario, como formatos de pantallas, diálogos, formatos de informes y formularios de entrada. Finalizados los modelos, se realiza un análisis de consistencia. Una vez realizado dicho análisis de consistencia se elabora el producto **Especificación de Requisitos Software**, que constituye un punto de referencia en el desarrollo del software y la línea base de referencia para las peticiones de cambio sobre los requisitos inicialmente especificados. En este proceso se inicia también la especificación del Plan de Pruebas, que se completará en el proceso Diseño del Sistema de Información (DSI). En este proceso es muy importante la participación de los usuarios, a través de técnicas interactivas, como diseño de diálogos y prototipos, que permiten al usuario familiarizarse con el nuevo sistema y colaborar en la construcción y perfeccionamiento del mismo.

34.2.3.3 Diseño del Sistema de Información (DSI)

El propósito del Diseño del Sistema de Información (DSI) es obtener la definición de la arquitectura del sistema y del entorno tecnológico que le va

a dar soporte, junto con la especificación detallada de los componentes del sistema de información. A partir de dicha información, se generan todas las especificaciones de construcción relativas al propio sistema, así como la especificación técnica del plan de pruebas, la definición de los requisitos de implantación y el diseño de los procedimientos de migración y carga inicial, éstos últimos cuando proceda.

Este proceso consta de un primer bloque de actividades, que se realizan en paralelo, y cuyo objetivo es obtener el diseño de detalle del sistema de información que comprende la partición física del sistema de información, independiente de un entorno tecnológico concreto, la organización en subsistemas de diseño, la especificación del entorno tecnológico sobre el que se despliegan dichos subsistemas y la definición de los requisitos de operación, administración del sistema, seguridad y control de acceso. En el caso de diseño orientado a objetos, conviene señalar que se ha contemplado que el diseño de la persistencia se lleva a cabo sobre bases de datos relacionales.

Un segundo bloque de actividades complementa el diseño del sistema de información, en el que se generan todas las especificaciones necesarias para la construcción del sistema de información.

34.2.3.4 Construcción del Sistema de Información (CSI)

La construcción del Sistema de Información (CSI) tiene como objetivo final la construcción y prueba de los distintos componentes del sistema de información, a partir del conjunto de especificaciones lógicas y físicas del mismo, obtenido en el Proceso de Diseño del Sistema de Información (DSI). Se desarrollan los procedimientos de operación y seguridad y se elaboran los manuales de usuario final y de explotación, estos últimos cuando proceda. Para conseguir dicho objetivo, se recoge la información relativa al producto del diseño Especificaciones de construcción del sistema de

información, se prepara el entorno de construcción, se genera el código de cada uno de los componentes del sistema de información y se van realizando, a medida que se vaya finalizando la construcción, las pruebas unitarias de cada uno de ellos y las de integración entre subsistemas. Si fuera necesario realizar una migración de datos, es en este proceso donde se lleva a cabo la construcción de los componentes de migración y procedimientos de migración y carga inicial de datos.

34.2.3.5 Implantación y Aceptación del Sistema (IAS)

Este proceso tiene como objetivo principal, la entrega y aceptación del sistema en su totalidad, que puede comprender varios sistemas de información desarrollados de manera independiente, según se haya establecido en el proceso de Estudio de Viabilidad del Sistema (EVS), y un segundo objetivo que es llevar a cabo las actividades oportunas para el paso a producción del sistema. Se establece el plan de implantación, una vez revisada la estrategia de implantación y se detalla el equipo que lo realizará. Para el inicio de este proceso se toman como punto de partida los componentes del sistema probados de forma unitaria e integrados en el proceso Construcción del Sistema de Información (CSI), así como la documentación asociada. El Sistema se someterá a las Pruebas de Implantación con la participación del usuario de operación cuya responsabilidad, entre otros aspectos, es comprobar el comportamiento del sistema bajo las condiciones más extremas. También se someterá a las Pruebas de Aceptación cuya ejecución es responsabilidad del usuario final. En este proceso se elabora el plan de mantenimiento del sistema de forma que el responsable del mantenimiento conozca el sistema antes de que éste pase a producción. También se establece el acuerdo de nivel de servicio requerido una vez que se inicie la producción.

34.2.4 Mantenimiento de Sistemas de Información (MSI)

El objetivo de este proceso es la obtención de una nueva versión de un sistema de información desarrollado con MÉTRICA, a partir de las peticiones de mantenimiento que los usuarios realizan con motivo de un problema detectado en el sistema o por la necesidad de una mejora del mismo. Sólo se considerarán en MÉTRICA Versión 3 los tipos de Mantenimiento **Correctivo** y **Evolutivo**. Ante una petición de cambio de un sistema de información ya en producción, se realiza un registro de las peticiones, se diagnostica el tipo de mantenimiento y se decide si se le da respuesta o no, en función del plan de mantenimiento asociado al sistema afectado por la petición, y se establece con qué prioridad. La definición de la solución al problema o necesidad planteada por el usuario que realiza el responsable de mantenimiento, incluye un estudio del impacto, la valoración del esfuerzo y coste, las actividades y tareas del proceso de desarrollo a realizar y el plan de pruebas de regresión.

34.2.5 Interfaces De Métrica Versión 3

La estructura de MÉTRICA Versión 3 incluye también un conjunto de interfaces que definen una serie de actividades de tipo organizativo o de soporte al proceso de desarrollo y a los productos, que en el caso de existir en la organización se deberán aplicar para enriquecer o influir en la ejecución de las actividades de los procesos principales de la metodología y que si no existen habrá que realizar para complementar y garantizar el éxito del proyecto desarrollado con MÉTRICA Versión 3. Son cuatro:

- **Gestión de Proyectos:** Tiene como finalidad principal la planificación, el seguimiento y control de las actividades y de los recursos humanos y materiales que intervienen en el desarrollo de un Sistema de Información. Como consecuencia de este control es posible conocer en

todo momento qué problemas se producen y resolverlos o paliarlos lo más pronto posible, lo cual evitará desviaciones temporales y económicas. Las actividades de la Interfaz de Gestión de Proyectos son de tres tipos:

- o *Actividades de Inicio del Proyecto*, que permiten estimar el esfuerzo y establecer la planificación del proyecto.
 - o *Actividades de Seguimiento y Control*, supervisando la realización de las tareas por parte del equipo de proyecto y gestionando las incidencias y cambios en los requisitos que puedan presentarse y afectar a la planificación del proyecto.
 - o *Actividades de Finalización del Proyecto*, cierre y registro de la documentación de gestión.
- **Seguridad:** La interfaz de Seguridad hace posible incorporar durante la fase de desarrollo las funciones y mecanismos que refuerzan la seguridad del nuevo sistema y del propio proceso de desarrollo, asegurando su consistencia y seguridad, completando el plan de seguridad vigente en la organización o desarrollándolo desde el principio, utilizando MAGERIT como metodología de análisis y gestión de riesgos en el caso de que la organización no disponga de su propia metodología. Contempla dos tipos de actividades diferenciadas: las relacionadas con la seguridad intrínseca del sistema de información, y las que velan por la seguridad del propio proceso de desarrollo del sistema de información. Además se hace especial hincapié en la formación en materia de seguridad. Al ser finitos los recursos, no pueden asegurarse todos los aspectos del desarrollo de los sistemas de información, por lo que habrá que aceptar un determinado nivel de riesgo concentrándose en los aspectos más comprometidos o amenazados.
- **Gestión de la Configuración:** La interfaz de gestión de la configuración consiste en la aplicación de procedimientos administrativos y técnicos durante el desarrollo del sistema de

información y su posterior mantenimiento. Su finalidad es identificar, definir, proporcionar información y controlar los cambios en la configuración del sistema, así como las modificaciones y versiones de los mismos. Este proceso permitirá conocer el estado de cada uno de los productos que se hayan definido como elementos de configuración, garantizando que no se realizan cambios incontrolados y que todos los participantes en el desarrollo del sistema disponen de la versión adecuada de los productos que manejan. La gestión de configuración facilita además el mantenimiento del sistema, aportando información precisa para valorar el impacto de los cambios solicitados y reduciendo el tiempo de implementación de un cambio, tanto evolutivo como correctivo.

- **Aseguramiento de la Calidad:** El objetivo de la interfaz de Aseguramiento de la Calidad es proporcionar un marco común de referencia para la definición y puesta en marcha de planes específicos de aseguramiento de calidad aplicables a proyectos concretos. Las actividades están orientadas a verificar la calidad de los productos. Son actividades que evalúan la calidad y que son realizadas por un grupo de Asesoramiento de la Calidad independiente de los responsables de la obtención de los productos. Las actividades contempladas permitirán reducir, eliminar y prevenir las deficiencias de calidad de los productos a obtener, así como alcanzar una razonable confianza en que las prestaciones y servicios esperados por el cliente o el usuario queden satisfechas.

34.3 RUP (Rational Unified Process)

Es una de las metodologías más extendidas y conocidas por su amplia difusión comercial que intenta integrar todos los aspectos a tener en cuenta durante todo el ciclo de vida del software, con el objetivo de hacer abarcables tanto pequeños como grandes proyectos software. Fue definido

por los creadores del UML unificando los métodos de Jacobson, Booch y Rumbaugh cuando trabajaban en la empresa Rational. Además, Rational proporciona herramientas para todos los pasos del desarrollo así como documentación en línea para sus clientes. Las **características principales** de RUP son:

- **Guiado/Manejado por casos de uso:** un caso de uso es una facilidad que el software debe proveer a sus usuarios. Los casos de uso reemplazan la antigua especificación funcional tradicional y constituyen la guía fundamental establecida para las actividades a realizar durante todo el proceso de desarrollo incluyendo el diseño, la implementación y las pruebas del sistema.
- **Centrado en arquitectura:** La arquitectura involucra los elementos más significativos del sistema y está influenciada entre otros por plataformas software, sistemas operativos, manejadores de bases de datos, protocolos, consideraciones de desarrollo como sistemas heredados y requerimientos no funcionales. Los casos de uso guían el desarrollo de la arquitectura y la arquitectura se realimenta en los casos de uso, los dos juntos permiten conceptualizar, gestionar y desarrollar adecuadamente el software.
- **Iterativo e Incremental:** Para hacer más manejable un proyecto se recomienda dividirlo en ciclos. Para cada ciclo se establecen fases de referencia, cada una de las cuales debe ser considerada como un miniproyecto cuyo núcleo fundamental está constituido por una o más iteraciones de las actividades principales básicas de cualquier proceso de desarrollo.
- **Desarrollo basado en componentes:** La creación de sistemas intensivos en software requiere dividir el sistema en componentes con interfaces bien definidas, que posteriormente serán ensamblados para generar el sistema. Esta característica en un proceso de desarrollo permite que el sistema se vaya creando a medida que se obtienen o que se desarrollan y maduran sus componentes.

- **Utilización de un único lenguaje de modelado:** UML es adoptado como único lenguaje de modelado para el desarrollo de todos los modelos.
- **Proceso Integrado:** Se establece una estructura que abarque los ciclos, fases, flujos de trabajo, mitigación de riesgos, control de calidad, gestión del proyecto y control de configuración; el proceso unificado establece una estructura que integra todas estas facetas. Además esta estructura cubre a los vendedores y desarrolladores de herramientas para soportar la automatización del proceso, soportar flujos individuales de trabajo, para construir los diferentes modelos e integrar el trabajo a través del ciclo de vida y a través de todos los modelos.

La **estructura estática** del proceso unificado se define en base a cuatro elementos

- **Roles:** Un rol define el comportamiento y responsabilidades de un individuo, o de un grupo de individuos trabajando juntos como un equipo. Una persona puede desempeñar diversos roles, así como un mismo rol puede ser representado por varias personas. Las responsabilidades de un rol son tanto el llevar a cabo un conjunto de actividades como el ser el 'dueño' de un conjunto de productos. Responde a la pregunta **¿quién?**
- **Actividades:** Una actividad de un trabajador en concreto es una unidad de trabajo que una persona que desempeñe ese rol puede ser solicitado a que realice. Las actividades tienen un objetivo concreto, normalmente expresado en términos de crear o actualizar algún producto. Responden a la pregunta **¿cómo?**
- **Productos:** Un producto o artefacto es un trozo de información que es producido, modificado o usado por un proceso. Los productos son los resultados tangibles del proyecto, las cosas que va creando y usando hasta obtener el producto final. Responden a la pregunta **¿qué?**
- **Flujos de trabajo:** La mera enumeración de roles, actividades y productos no define un proceso, necesitamos definir la secuencia de

actividades realizadas por los diferentes roles, así como la relación entre los mismos, que nos producen unos resultados observables. Las distintas iteraciones a realizar consistirá en la ejecución de estos flujos de trabajo con una mayor o menos intensidad dependiendo de la fase e iteración en la que nos encontremos. Responden a la pregunta **¿cuándo?**

34.3.1 Fases del ciclo de desarrollo.

Este proceso de desarrollo considera que cualquier desarrollo de un sistema software debe pasar por cuatro **fases**:

- **Fase 1: Inicio.** Su objetivo principal es establecer los objetivos para el ciclo de vida del producto. En esta fase se establece el caso del negocio con el fin de delimitar el alcance del sistema, saber qué se cubrirá y delimitar el alcance del proyecto. Los productos de esta fase son:

- o Alcance del Sistema
 - Lista de Características
 - Modelo del Dominio o Modelo del Negocio (1ª. versión)
 - Modelo de Casos de Uso, Modelo de Análisis y Modelo de Diseño (1ª. versión)
 - Requerimientos Suplementarios (1ª. Versión)
- o Arquitectura Inicial (propuesta)
- o Lista Inicial de Riesgos (riesgos críticos más importantes) y Lista Priorizada de los Casos de Uso
- o Prototipo para Validación de Conceptos (prototipo de descarte)
- o Entorno de Desarrollo Configurado (proceso y herramientas) (configuración inicial)
- o Plan Inicial del Proyecto
- o Caso Inicial del Negocio (1ª. versión) (contexto del negocio y criterios de éxito) (costo, tiempos, calidad, utilidades)

- **Fase 2: Elaboración.** Su objetivo principal es plantear la arquitectura para el ciclo de vida del producto. En esta fase se realiza la captura de la mayor parte de los requerimientos funcionales, manejando los riesgos que interfieran con los objetivos del sistema, acumulando la información necesaria para el plan de construcción y obteniendo suficiente información para hacer realizable el caso del negocio. Al terminar tendremos los siguientes productos:
 - o Contexto del Sistema (Modelo del Dominio o Modelo del Negocio preferiblemente completo)
 - o Captura del 80% de los Requerimientos Funcionales
 - Modelo de Casos de Uso (aprox. el 80%) y Modelo de Análisis (realización de los casos de uso más significativos)
 - Modelo de Diseño, Modelo de Despliegue y Modelo de Implementación (menos del 10%)
 - Niveles para los Atributos de Calidad y Requerimientos Suplementarios Actualizados
 - Manual Preliminar de Usuario
 - o Arquitectura de Referencia (línea de base) (descripción de las vistas arquitecturales de los modelos del sistema)
 - o Lista Actualizada de Riesgos (críticos y significativos) y Riesgos Críticos Mitigados
 - o Plan del Proyecto para las fases de Construcción y Transición
 - o Entorno de Desarrollo Adecuado (proceso y herramientas)
 - o Caso del Negocio Completo (y “Contrato” o declaración del negocio)
- **Fase 3: Construcción.** Su objetivo principal es alcanzar la capacidad operacional del producto. En esta fase a través de sucesivas iteraciones e incrementos se desarrolla un producto software, listo para operar, éste es frecuentemente llamado versión beta. Los productos obtenidos serán:

- o Modelos Completos (Casos de Uso, Análisis, Diseño, Despliegue e Implementación)
 - o Arquitectura Íntegra (mantenida y mínimamente actualizada)
 - o Riesgos Presentados Mitigados
 - o Plan del Proyecto para la fase de Transición
 - o Manual Inicial de Usuario (con suficiente detalle)
 - o Prototipo Operacional – beta
 - o Caso del Negocio Actualizado
- **Fase 4: Transición.** Su objetivo principal es realizar la entrega del producto operando, una vez realizadas las pruebas de aceptación por un grupo especial de usuarios y habiendo efectuado los ajustes y correcciones que sean requeridos. Los productos obtenidos serán:
 - o Prototipo Operacional
 - o Documentos Legales
 - o Caso del Negocio Completo
 - o Línea de Base del Producto completa y corregida que incluye todos los modelos del sistema
 - o Descripción de la Arquitectura completa y corregida
 - o Manuales para Usuario Final, Operador y Administrador del Sistema, y Materiales para Entrenamiento

34.3.2 Flujos de trabajo.

En RUP se definen nueve **flujos de trabajo** distintos, separados en dos grupos: ingeniería (2, 3, 4, 5, 6, 9) y de apoyo (1, 7, 8).

- 1- **Administración del Proyecto.** El flujo de trabajo se centra en tres aspectos: Planificar un proyecto iterativo y cada iteración particular, administrar el riesgo y monitorizar el progreso del proyecto a través de métricas. La planificación de un proyecto debe acometerse en dos niveles de abstracción: un plan de “grano grueso” para las fases y un

plande “grano fino” para cada iteración. El plan de desarrollo (o plan de fases) debe contener las fechas esperadas para los hitos principales. También debería tener una previsión de las necesidades de personal y medios.

- 2- **Modelado del negocio.** Con este flujo de trabajo pretendemos llegar a un mejor entendimiento de la organización donde vamos a implantar nuestro producto. Este flujo de trabajo no será siempre necesario.
- 3- **Requisitos.** Se establece *QUÉ* es lo que tiene que hacer exactamente el sistema que construyamos. En este flujo de trabajo hay que analizar el problema, comprender las necesidades de los interesados y expresarlas en forma de requisitos, construir diagramas de casos de uso para los requisitos funcionales, los no funcionales describirlos textualmente en especificaciones suplementarias. Además hay que gestionar los cambios en los requisitos a lo largo de todo el proceso.
- 4- **Análisis y diseño.** El objetivo de este flujo de trabajo es traducir los requisitos a una especificación que describe cómo implementar el sistema. El **análisis** consiste en obtener una visión del sistema que se preocupa de ver *QUÉ* hace, de modo que sólo se interesa por los requisitos funcionales. Por otro lado el **diseño** es un refinamiento del análisis que tiene en cuenta los requisitos no funcionales, en definitiva *CÓMO* cumple el sistema sus objetivos. El resultado final más importante de este flujo de trabajo será el modelo de diseño. Consiste en colaboraciones de clases, que pueden ser agregadas en paquetes y subsistemas.
- 5- **Implementación.** En este flujo de trabajo se implementan las clases y objetos en ficheros fuente, binarios, ejecutables y demás. Además se deben hacer las pruebas unitarias: cada implementador es responsable de testear las unidades que produzca. El resultado final de este flujo de trabajo es un sistema ejecutable.

- 6- **Test.** Este flujo de trabajo es el encargado de evaluar la calidad del producto que estamos desarrollando. “El papel del testeo no es asegurar la calidad, pero sí evaluarla, y proporcionar una realimentación a tiempo, de forma que las cuestiones de calidad puedan resolverse de manera efectiva en tiempo y coste. Los principales aspectos a ser evaluados en un producto software son la *Fiabilidad* (resistente a fallos), la *Funcionalidad* (hace lo que debe) y el *Rendimiento* (lleva a cabo su trabajo de manera efectiva).
- 7- **Configuración y gestión de cambios.** La finalidad de este flujo de trabajo es mantener la integridad de todos los productos que se crean en el proceso, así como de mantener información del proceso evolutivo que han seguido. Cubre tres funciones interdependientes como son la **gestión de la configuración**, la **gestión de las peticiones de cambio**, y la **Realización de métricas**.
- 8- **Entorno.** La finalidad de este flujo es dar soporte al proyecto con las adecuadas herramientas, procesos y métodos. Es decir tener a punto las herramientas que se vayan a necesitar en cada momento, así como definir la instancia concreta de proceso unificado que se va a seguir.
- 9- **Despliegue.** El objetivo de este flujo de trabajo es producir con éxito distribuciones del producto y distribuirlo a los usuarios.

34.4 Metodologías Ágiles.

En las **metodologías ágiles**, la creación de valor mediante la adaptación a las necesidades cambiantes aparece en un primer plano frente a la tradicional idea de diseñar un plan y cumplir unos calendarios/requerimientos estáticos. Los proyectos gestionados con metodologías ágiles se inician sin un detalle cerrado de lo que va a ser construido. A nivel comercial, los proyectos pueden ser vendidos como servicios y no como productos. Las características básicas de los proyectos gestionados con metodologías ágiles son las siguientes:



- **Incertidumbre:** la dirección indica la necesidad estratégica que se desea cubrir (sin entrar en detalles), ofreciendo máxima libertad al equipo de trabajo.
- **Equipos auto-organizados:** no existen roles especializados
 - o Autonomía: libertad para la toma de decisiones.
 - o Auto-superación: de forma periódica se evalúa el producto que se está desarrollando.
 - o Auto-enriquecimiento: transferencia del conocimiento.
- **Fases de desarrollo solapadas:** Las fases no existen como tal sino que se desarrollan tareas/actividades en función de las necesidades cambiantes durante todo el proyecto. De hecho, en muchas ocasiones no es posible realizar un diseño técnico detallado antes de empezar a desarrollar y ver algunos resultados. Por otra parte, las fases tradicionales efectuadas por personas diferentes no favorece el trabajo en equipo y pueden llegar a generar más inconvenientes que ventajas (por ej. un retraso en una fase, afecta a todo el proyecto).
- **Control sutil:** establecimientos de puntos de control para realizar un seguimiento adecuado sin limitar la libertad y creatividad del equipo. Así mismo, se recomienda:
 - o Evaluar el ambiente laboral, siendo fundamental la elección de personas que no generen conflictos.
 - o Reconocer los méritos mediante un sistema de evaluación justo y entender los errores como puntos de mejora y aprendizaje.
 - o Potenciar la interacción entre el equipo y el negocio, para que puedan conocer las necesidades de primera mano.
- **Difusión y transferencia del conocimiento:** alta rotación de los miembros de los equipos entre diferentes proyectos. Por otra parte, potenciar el acceso libre a la información y documentación.

Algunas de las metodologías ágiles más conocidas las veremos en los apartados siguientes.

34.4.1 Scrum

Scrum es un proceso de desarrollo de software en el que se aplican de manera regular un conjunto de buenas prácticas para trabajar colaborativamente, en equipo, y obtener el mejor resultado posible de un proyecto. En Scrum se realizan entregas parciales y regulares del producto final, priorizadas por el beneficio que aportan al receptor del proyecto. Por ello, Scrum está especialmente indicado para proyectos en entornos complejos, donde se necesita obtener resultados pronto, donde los requisitos son cambiantes o poco definidos, donde la innovación, la competitividad, la flexibilidad y la productividad son fundamentales.

Scrum representa un marco de trabajo para la gestión y desarrollo de software basado en procesos iterativo e incremental utilizado comúnmente en entornos basados en la metodología Agile de desarrollo de software. Es un modelo de referencia que incluye un conjunto de prácticas y roles predefinidos. Los roles principales en Scrum son el ScrumMaster, que mantiene los procesos y trabaja de forma similar al director de proyecto, el ProductOwner, que representa a los stakeholders (clientes externos o internos), y el Team que incluye a los desarrolladores. Durante cada sprint, un periodo entre 15 y 30 días (la longitud es definida por el equipo), el equipo crea un incremento de software potencialmente entregable (utilizable). El conjunto de características que forma parte de cada sprint viene del **product backlog**, que es un conjunto de requisitos de alto nivel priorizados que dan forma al trabajo a realizar. Los elementos del backlog que forman parte del sprint se determinan durante la reunión de **sprint planning**. Durante esta reunión, el Product Owner informa al equipo de los elementos en el product backlog que quiere ver completados. El equipo entonces determina la cantidad de ese trabajo que puede comprometerse a completar durante el siguiente sprint. Durante el sprint, nadie puede cambiar el sprint backlog, lo que significa que los requisitos están congelados durante el sprint. Existen varias implementaciones de sistemas para gestionar el proceso de Scrum, que van desde notas amarillas "post-it" y pizarras hasta paquetes de software. Una de las mayores ventajas de

Scrum es que es muy fácil de aprender, y requiere muy poco esfuerzo para comenzarse a utilizar.

A modo de resumen, podemos establecer que la metodología Scum se basa en:

- Desarrollo incremental de los requisitos del proyecto en bloques temporales cortos y fijos.
- La priorización de los requisitos por valor para el cliente y coste de desarrollo en cada iteración.
- El control empírico del proyecto. Al final de cada iteración se demuestra al cliente el resultado real obtenido, de manera que pueda tomar las decisiones necesarias en función de lo que observa y del contexto del proyecto en ese momento. Por otro lado, el equipo se sincroniza diariamente y realiza las adaptaciones necesarias.
- La potenciación del equipo, que se compromete a entregar unos requisitos y para ello se le otorga la autoridad necesaria para organizar su trabajo.
- La sistematización de la colaboración y la comunicación tanto entre el equipo y como con el cliente.
- El timeboxing de las actividades del proyecto, para ayudar a la toma de decisiones y conseguir resultados.

34.4.2 Dynamic Systems Development Method (DSDM)

Provee un framework para el [desarrollo ágil de software](#), apoyado por la continua implicación del usuario en un [desarrollo iterativo y creciente](#). DSDM fue desarrollado en el [Reino Unido](#) en los [años 90](#). Como extensión del [Desarrollo rápido de aplicaciones](#) (RAD), DSDM se centra en los proyectos de sistemas de información que son caracterizados por presupuestos y agendas apretadas. DSDM trata los problemas que ocurren con frecuencia en el desarrollo de los sistemas de información en lo que respecta a pasar sobre tiempo y presupuesto y otras razones comunes para la falta en el proyecto tal como falta de implicación del usuario y de la comisión superior de la gerencia. DSDM consiste en 3 fases: fase del pre-proyecto, fase del ciclo de vida del proyecto, y fase del post-proyecto. La fase del ciclo de vida del proyecto se subdivide en 5 etapas: estudio de viabilidad, estudio de la empresa, iteración del modelo funcional, diseño e iteración de la estructura, e implementación. Tiene 9 principios fundamentales:

- **Involucrar al cliente** es la clave para llevar un proyecto eficiente y efectivo, donde ambos, cliente y desarrolladores, comparten un entorno de trabajo para que las decisiones puedan ser tomadas con precisión.
- **El equipo del proyecto debe tener el poder** para tomar decisiones que son importantes para el progreso del proyecto, sin esperar aprobación de niveles superiores.
- DSDM se centra en la **entrega frecuente de productos**, asumiendo que entregar algo temprano es siempre mejor que entregar todo al final. Al entregar el producto frecuentemente desde una etapa temprana del proyecto, el producto puede ser verificado y revisado allí donde la documentación de registro y revisión puede ser tomada en cuenta en la siguiente fase o iteración.

- El principal **criterio de aceptación** de entregables reside en entregar un sistema que satisface las actuales necesidades de negocio.
- El **desarrollo** es **iterativo e incremental**, guiado por la realimentación de los usuarios para converger en una solución de negocio precisa.
- Todos los **cambios** durante el desarrollo son reversibles.
- Requerimientos globales antes de comenzar el proyecto.
- Las pruebas son realizadas durante todo el ciclo vital del proyecto.
- La comunicación y cooperación entre todas las partes interesadas.

34.4.3 Extreme Programming(XP)

La programación extrema, o Extreme Programming, es una de las metodologías ágiles de desarrollo de software más existosas de los últimos tiempos. La programación extrema se diferencia de las metodologías tradicionales principalmente en que pone más énfasis en la adaptabilidad que en la previsibilidad. Los defensores de XP consideran que los cambios de requisitos sobre la marcha son un aspecto natural, inevitable e incluso deseable del desarrollo de proyectos. Creen que ser capaz de adaptarse a los cambios de requisitos en cualquier punto de la vida del proyecto es una aproximación mejor y más realista que intentar definir todos los requisitos al comienzo del proyecto e invertir esfuerzos después en controlar los cambios en los requisitos. XP construye un proceso de diseño evolutivo que se basa en refactorizar un sistema simple en cada iteración. Todo el diseño se centra en la iteración actual y no se hace nada anticipadamente para necesidades futuras. Los Valores originales de la programación extrema son: **simplicidad**(de diseño, código y documentación), **comunicación**(la comunicación con el cliente es fluida ya que el cliente forma parte del equipo de desarrollo. El cliente decide que características tienen prioridad y siempre debe estar disponible para solucionar dudas), **retroalimentación** (*feedback*). Al estar el cliente integrado en el proyecto, su opinión sobre el

estado del proyecto se conoce en tiempo real.), y **coraje** (Se requiere coraje para implementar las características que el cliente quiere ahora sin caer en la tentación de optar por un enfoque más flexible que permita futuras modificaciones). Un quinto valor, **respeto**(los miembros del equipo respetan el trabajo del resto no haciendo menos a otros, sino orientándolos a realizarlo mejor, obteniendo como resultado una mejor autoestima en el equipo y elevando el ritmo de producción en el equipo), fue añadido posteriormente.

Las características fundamentales de esta metodología son:

- Desarrollo iterativo e incremental
- Pruebas unitarias continuas
- Programación en parejas
- Integración del equipo de programación con el cliente
- Corrección de todos los errores
- Refactorización del código
- Propiedad del código compartida
- Simplicidad en el código

34.4.4 Feature Driven Development (FDD)

Se basa en un proceso iterativo con iteraciones cortas que producen un software funcional que el cliente y la dirección de la empresa pueden ver y monitorizar. Las iteraciones se deciden en base a funcionalidades, que son pequeñas partes del software con significado para el cliente. **No** cubre todo el ciclo de vida sino sólo las fases de diseño y construcción. No requiere un modelo específico de proceso y se complementa con otras metodologías. FDD consiste en cinco procesos secuenciales durante los cuales se diseña y construye el sistema:

- **Desarrollo de un modelo general:** Cuando comienza esta fase, los expertos del dominio ya tienen una idea del contexto y los requerimientos del sistema. El dominio global es dividido en

diferentes áreas y se realiza informe detallado para cada una de ellas por parte de los expertos del dominio.

- **Construcción de la lista de funcionalidades** Los ensayos, modelos de objetos y documentación de requerimientos proporcionan la base para construir una amplia lista de funcionalidades. Estas funcionalidades son pequeños ítems útiles a los ojos del cliente. La lista de funcionalidades es revisada por los usuarios y patrocinadores para asegurar su validez. Las funcionalidades que requieran de más de diez días se descomponen en otras más pequeñas.
- **Planeamiento por funcionalidades:** En esta etapa se incluye la creación de un plan de alto nivel, en el cual la lista de funcionalidades es ordenada en base a la prioridad y a la dependencia entre cada funcionalidad. Además, las clases identificadas en la primera etapa son asignadas a cada programador.
- **Diseño y construcción por funcionalidades:** El diseño y construcción de la funcionalidad es un proceso iterativo durante el cual las funcionalidades seleccionadas son producidas. Una iteración puede llevar desde unos pocos días a un máximo de dos semanas. Este proceso iterativo incluye tareas como inspección del diseño, codificación, pruebas unitarias, integración e inspección del código.

34.4.5 Agile Modeling (AM)

Se puede describir como una metodología basada en la práctica para el modelado efectivo de sistemas de software. No define procedimientos detallados de cómo crear un tipo de modelo dado. En lugar de eso, sugiere prácticas para que los modelos y documentación sean efectivos. Su secreto no está en las técnicas de modelado a usar, sino en cómo se aplican. No es un desarrollo de software completo ya que no cubre actividades de programación, prueba, gestión de proyectos, implementación, soporte u otros elementos de la realización de proyectos que no sean la

documentación y el modelado. Es necesario, por lo tanto, combinarlo con otras metodologías como pueden ser XP, DSDM, SCRUM o RUP. Los valores de esta metodología son la **comunicación** (entre participantes del equipo de trabajo, desarrolladores y analistas, etc.), **simplicidad**, **coraje** (para tomar decisiones importantes y ser capaces de cambiar de dirección cuando el camino tomado no es el correcto) y **humildad** (todos los interesados en el proyecto pueden contribuir en algo para la mejor realización).

34.4.6 Crystal

Crystal es una metodología de desarrollo de Software Ágil. Más que una metodología, Crystal se la considera una familia de metodologías, dado a que se subdivide en varios tipos de metodologías en función a la cantidad de personas que vayan a participar el proyecto.

Alistair Cockburn es el propulsor de esta serie de metodologías. El desarrollo de esta familia de metodologías está fundamentado en el análisis de distintos proyectos de desarrollo de SW y su propia experiencia. Se habla de familia de metodologías porque según el propio autor los tipos diferentes de proyectos requieren tipos diferentes de metodologías. La óptica bajo la cuál recoge esta perspectiva se presenta fundamentada en dos ejes: el número de personas en el proyecto, y las consecuencias de los errores. Dispone un código de color para marcar la complejidad de cada metodología. Comparte con la XP una orientación humana, pero esta centralización en la gente se hace de una manera diferente. Alistair considera que las personas encuentran difícil seguir un proceso disciplinado, así que más que seguir la alta disciplina de la XP, Alistair explora la metodología menos disciplinada que aun podría tener éxito, intercambiando conscientemente productividad por facilidad de ejecución. Él considera que aunque Crystal es menos productivo que la XP, más personas serán capaces de seguirlo. Alistair también pone mucho



peso en las revisiones al final de la iteración, animando al proceso a ser “automejorable”. Defiende que el desarrollo iterativo está para encontrar los problemas temprano, y entonces permitir corregirlos. Esto pone más énfasis en la gente supervisando su proceso y afinándolo conforme desarrollan.

BIBLIOGRAFÍA:

- http://administracionelectronica.gob.es/archivos/pae_000001027.pdf
Introducción a Métrica Versión 3. Ministerio de Administraciones Públicas
- <http://atenea.ucauca.edu.co/~gramirez/archivos/AnotacionesRUP.pdf>
Ramírez González, Gustavo A., *Laboratorio III de Electrónica, Anotaciones RUP*, 2001.
- Guía a Rational Unified Process. Alejandro Martínez y Raúl Martínez. Escuela Politécnica Superior de Albacete – Universidad de Castilla la Mancha.
- Rational Unified Process: Best Practices for Software Development Teams. Rational Software White Paper.
http://www.ibm.com/developerworks/rational/library/content/03July/1000/1251/1251_bestpractices_TP026B.pdf
- Análisis, Diseño y Mantenimiento del Software. José Ramón Álvarez Sánchez y Manuel Arias Calleja. Dpto. de Inteligencia Artificial - ETSI Informática - UNED
- <http://www.marblestation.com/?p=661>. Metodologías ágiles de gestión de proyectos. Sergi Blanco Cuaresma.
- Agile Project Management With SCRUM. Ken Schwaber, Microsoft, 2004.
- <http://www.proyectosagiles.org>
- Agile Modeling: Effective Practices for eXtreme Programming and the Unified Process. Scoot Ambler. 2002.
- <http://es.wikipedia.org/wiki/DSDM>
- Agile Modeling (AM) Felipe Ferrada.
- http://www.ort.edu.uy/fi/publicaciones/ingsoft/investigacion/ayudantias/metodologia_FDD.pdf. Metodología FDD. Cátedra de Ingeniería de Software. Luis Calabria. Universidad ORT Uruguay
- <http://www.programacionextrema.org/articulos/newMethodology.es.html> La Nueva Metodología. [Martin Fowler](#)
- I. Jacobson, G. Booch, J. Rumbaugh. The Unified Software Development

Process. Ed. Addison-Wesley, 1999.

Autor: Francisco Javier Rodríguez Martínez.
Subdirector de la Escuela Superior de Ingeniería Informática.
Universidad de Vigo.

35. INGENIERÍA DE REQUISITOS. VERIFICACIÓN. VALIDACIÓN. ESPECIFICACIÓN DE REQUISITOS. GESTIÓN DE REQUISITOS.

Tema 35- Ingeniería de requisitos. Verificación. Validación. Especificación de requisitos. Gestión de requisitos.

INDICE

- 35.1 Ingeniería de requisitos
 - 35.1.1 Tipos de requisitos
- 35.2 Identificación de los requisitos del software
 - 35.2.1 Entrevistas
 - 35.2.2 JAD (Joint Application Design)
 - 35.2.3 Prototipos
 - 35.2.4 Análisis de factores críticos de éxito
 - 35.2.5 Brainstorming
 - 35.2.6 Escenarios y casos de uso
 - 35.2.7 Etnografía
- 35.3 Verificación - Validación
- 35.4 Especificación de Requisitos
 - 35.4.1 IEEE/ANSI 830-1998
- 35.5 Gestión de requisitos
 - 35.5.1 Planificación de la gestión requisitos.
 - 35.5.2 Gestión del cambio.

35.1 Ingeniería de requisitos

La Ingeniería de requisitos forma parte de la Ingeniería del software y comprende todas las tareas relacionadas con la determinación de las necesidades o de las condiciones a satisfacer para un software nuevo o modificado, tomando en cuenta los diversos requisitos de los usuarios. Así, los requisitos se generan a partir de la interacción entre los usuarios y los

ingenieros del software, representando las características del sistema a construir, es decir, las necesidades de los usuarios.

Hay múltiples definiciones del término requisito, algunas de ellas son:

- Según la sociedad IEEE un **requisito** es:
 - o Una condición o capacidad que necesita un usuario para resolver un problema o alcanzar un objetivo.
 - o Una condición o capacidad que debe cumplir o poseer un sistema o un componente del mismo para satisfacer un contrato, un estándar, una especificación, u otro documento impuesto de una manera formal.
 - o Una representación documentada de una condición o capacidad tal como las expresadas en los dos puntos anteriores.

En resumen, los requisitos son las características que debe cumplir el sistema para que cubra las necesidades de los usuarios. Muchas veces se habla de requerimientos en vez de requisitos. Esto se debe a una mala traducción del inglés. La palabra *requirement* debe ser traducida como requisito, mientras que requisito se traduce al inglés como *request*.

Sommerville divide el proceso de Ingeniería de requisitos en cuatro subprocesos que son (1) la evaluación de si el sistema es útil para el negocio (**estudio de viabilidad**); (2) el **descubrimiento de requisitos** (obtención y análisis); (3) la transformación de estos requisitos en formularios estándar (**especificación**), y la (4) verificación de que los requisitos realmente definen el sistema que quiere el cliente (**validación**).

Para Thayer, *“La ingeniería de requisitos proporciona el mecanismo apropiado para entender lo que el cliente quiere, analizar las necesidades, evaluar la factibilidad, negociar una solución razonable, especificar la solución sin ambigüedades, validar la especificación, y administrar los*

requisitos conforme se transforman en un sistema operacional” y establece las siguientes fases para el proceso:

- **Inicio.** Se establece una comprensión básica del problema por parte de los analistas.
- **Obtención.** Se obtienen los requisitos del software mediante la interacción entre los analistas y el cliente.
- **Elaboración.** Se refina la información obtenida en el paso anterior y se enfoca a la construcción de un modelo de análisis que represente al sistema a construir.
- **Negociación.** Hay requisitos que no son implementables o son difíciles de trasladar al sistema. Por esta razón los analistas negocian estos requisitos para llegar a un entendimiento y lograr un sistema factible de desarrollarse en un plazo y coste determinado.
- **Especificación.** Se confecciona un conjunto de documentos (descripciones en lenguaje natural, diagramas, etc.) que definan lo que el sistema debe hacer.
- **Validación.** Se examina la especificación para asegurar que todos los requisitos software se han establecido de una manera precisa, que no hay inconsistencias, omisiones ni errores, además de cumplirse los estándares de calidad establecidos para el proyecto.
- **Gestión de Requisitos.** Esta actividad permite tratar con el inevitable problema de los cambios de especificaciones, identificando, controlando y determinando el impacto del cambio de requisitos en el resto.

Otros autores modifican el número de etapas y las dividen en:

- **Educción de Requisitos.** En ella los analistas obtienen las necesidades del cliente a partir de todas las fuentes de información que tienen disponibles (documentación, entrevistas, estudio de los procesos de la organización, etc.). Términos equivalentes usados por los ingenieros de software para esta actividad son Extracción de



Requisitos, Identificación de Requisitos, Determinación de Requisitos, etc. Vemos que estas se corresponderían con las dos primeras fases del modelo anterior.

- **Análisis de Requisitos:** se procede a trabajar sobre los requisitos educidos en el paso anterior. Se estudian estos requisitos en busca de conflictos e incoherencias, implicaciones, información no obtenida y aspectos no resueltos. Después se clasifican, se evalúa su viabilidad y se integran los nuevos requisitos con los ya existentes. El objetivo final es lograr una lista de requisitos que defina las necesidades del cliente. Corresponderían con las fases de Elaboración y Negociación del modelo anterior.
- **Representación de los Requisitos.** Actividad en la que se representan los requisitos de una o más formas, utilizando para ello diferentes técnicas como por ejemplo el lenguaje formal, el lenguaje natural, representaciones gráficas, etc. Para la representación existen múltiples técnicas, las más usadas son, entre otras, los Diagramas de Flujo de Datos, Modelo Entidad Relación, Casos de Uso o Diagramas de Clases. Una vez que están los requisitos representados, es necesario que se reúnan los diversos participantes en el desarrollo para revisarlos y aprobarlos. El producto final con el que culmina esta fase es la Especificación de Requisitos Software, en donde está descrito con exactitud todo lo que el sistema debe hacer. Corresponde a las fases de Especificación y Validación del modelo anterior.
- **Validación de Requisitos** Se procede a definir una serie de criterios y técnicas que permitirán, cuando el sistema esté construido, comprobar que éste cumple los requisitos.

Independientemente del modelo que usemos, lo importante es tener claro que el objetivo de la ingeniería de requisitos es determinar con claridad y precisión qué es lo que hay que hacer y para ello será necesario identificar los requisitos clave.



Los factores principales que conducen al fracaso en los proyectos software y que tienen que ver con los requisitos son: la falta de comunicación con los usuarios, los requisitos incompletos y los cambios en los requisitos. La evidencia demuestra que los requisitos contienen demasiados errores, que muchos de estos errores no se detectan al principio, pero podrían ser detectados, y que no detectar estos errores incrementa los costes del proyecto y su duración. La consecuencia es que el sistema no satisfará a los usuarios, se producirán desacuerdos entre usuarios y desarrolladores, y se gastará tiempo y dinero en construir un sistema equivocado.

35.1 Tipos de requisitos

La mayoría de los autores distinguen entre:

- **Requisitos funcionales:** Son declaraciones de los servicios que debe proporcionar el sistema, de la manera en que éste debe reaccionar a entradas particulares y de cómo se debe comportar en situaciones concretas. En algunos casos, los requisitos funcionales de los sistemas también pueden declarar explícitamente lo que el sistema no debe hacer. Los requisitos funcionales de un sistema describen lo que el sistema debe hacer.
- **Requisitos no funcionales:** Son restricciones de los servicios o funciones ofrecidos por el sistema. Incluyen restricciones de tiempo, sobre el proceso de desarrollo y estándares. Como su nombre sugiere, no se refieren directamente a las funciones específicas que proporciona el sistema, sino a las propiedades de éste como la fiabilidad, el tiempo de respuesta y la capacidad de almacenamiento. Pueden venir de las características requeridas del software (requisitos del producto), de la organización que desarrolla el software (requisitos organizacionales) o de fuentes externas. Ejemplos:
 - o **Requisitos del producto.** Estos requisitos especifican el comportamiento del producto. Algunos ejemplos son los



requisitos de rendimiento en la rapidez de ejecución del sistema y cuánta memoria se requiere; los requisitos de fiabilidad que fijan la tasa de fallos para que el sistema sea aceptable; los requisitos de portabilidad, y los requisitos de usabilidad.

- o **Requisitos organizacionales.** Estos requisitos se derivan de políticas y procedimientos existentes en la organización del cliente y en la del desarrollador. Algunos ejemplos son los estándares en los procesos que deben utilizarse; los requisitos de implementación, como los lenguajes de programación o el método de diseño a utilizar, y los requisitos de entrega que especifican cuándo se entregará el producto y su documentación.
- o **Requisitos externos.** Este gran apartado incluye todos los requisitos que se derivan de los factores externos al sistema y de su proceso de desarrollo. Éstos pueden incluir los requisitos de interoperabilidad que definen la manera en que el sistema interactúa con sistemas de otras organizaciones; los requisitos legislativos que deben seguirse para asegurar que el sistema funcione dentro de la ley, y los requisitos éticos. Estos últimos son puestos en un sistema para asegurar que será aceptado por sus usuarios y por el público en general.

Sommerville distingue entre **requisitos del usuario**, que son declaraciones, en lenguaje natural y en diagramas, de los servicios que se espera que el sistema proporcione y de las restricciones bajo las cuales debe funcionar, y **requisitos del sistema**, que establecen con detalle las funciones, servicios y restricciones operativas del sistema. Estos diferentes niveles de especificación serían de utilidad debido a que comunican la información del sistema a diferentes tipos de lectores.

35.2 Identificación de los requisitos del software

La educación, identificación o determinación de requisitos es el paso durante el cual los requisitos del software son obtenidos de fuentes tales como: la gente implicada (usuarios, clientes, expertos en la materia, etc.), las necesidades que ha de satisfacer el sistema, el entorno físico que rodea al sistema, el entorno organizacional, etc.

Los problemas de la obtención de requisitos se pueden agrupar en tres categorías:

- 1- Problemas de alcance, ya que los requisitos pueden implicar demasiada o muy poca información.
- 2- Problemas de comprensión, como consecuencia de una pobre comunicación entre usuario y analista. En este caso los requisitos obtenidos son ambiguos, incompletos, inconsistentes e incorrectos, porque no responden a las verdaderas necesidades de los usuarios.
- 3- Problemas de volatilidad, ya que los requisitos evolucionan con el tiempo. En efecto, a medida que avanza el desarrollo del sistema, las necesidades del usuario pueden madurar a causa del conocimiento adicional fruto del desarrollo, o de necesidades del entorno o de la organización no previstas.

La solución al primer problema pasa por determinar claramente el contexto del sistema, es decir, los límites y objetivos del mismo. Si no se contempla el contexto donde va a funcionar el sistema, se puede llegar a requisitos incompletos, no verificables, innecesarios y no utilizables. La solución del segundo es que exista una buena comunicación entre usuarios, desarrolladores y clientes, a fin de que los requisitos se puedan escribir de manera que permitan, tanto que el desarrollador pueda distinguir si dichos requisitos se pueden implementar, como que el personal de control pueda comprobar si la implementación cumple con los requisitos. Por último la solución al tercer problema es incorporar estos cambios a los requisitos

originales, pues si no, éstos serán incompletos e inconsistentes con la nueva situación.

Son numerosas las estrategias y técnicas que se han desarrollado para la obtención de los requisitos. Las más importantes las veremos a continuación.

35.2.1 Entrevista

Se entiende por entrevista el encuentro que se realiza “cara a cara” entre un usuario y la persona responsable de obtener la información (analista). Para realizar la entrevista solo es necesario designar a las personas que deben participar en ella y determinar el lugar en el que poder llevarla a cabo. Es importante identificar a qué tipo de perfil va dirigida la entrevista, a quiénes se va a entrevistar y cuál es el momento más oportuno, con el fin de evitar situaciones embarazosas y conseguir que la entrevista sea eficaz y productiva.

Como paso previo a la realización de la entrevista se deben tener en cuenta una serie de reglas generales o directrices básicas:

- Desarrollar un plan global de la entrevista.
- Asegurarse de que se cuenta con la aprobación para hablar con los usuarios.
- Preparar la entrevista previamente.
- Realizar la entrevista.
- Consolidar el resultado de la entrevista.

Además, es conveniente planificar las entrevistas estudiando la secuencia en que se van a llevar a cabo, en función de los distintos perfiles implicados y las relaciones existentes entre los entrevistados. Según la información a obtener y dependiendo de las distintas fuentes que pueden proporcionarla, puede ser necesario realizar una entrevista conjunta con varias personas.

Durante la preparación de la entrevista es imprescindible remitir al usuario un guión previo sobre los puntos a tratar, para que pueda estudiarlo con tiempo y solicitar la información que estime conveniente para la entrevista. Se debe pensar bien el tipo de guión, según el perfil y las responsabilidades del entrevistado y su extensión, de forma que se pueda conseguir la suficiente información, sin provocar rechazo en el entrevistado. Si se considera apropiado se pueden utilizar herramientas automatizadas.

Una vez que se dispone de la aprobación para hablar con los usuarios, se hace la convocatoria de la entrevista enviando la información oportuna y fijando los objetivos, el método de trabajo que se va a seguir y el tiempo del que se dispone.

Para realizar la entrevista, es importante hacer un resumen general de los temas a tratar, utilizar un estilo apropiado y crear desde su inicio un clima de confianza entre los asistentes. Es posible que el entrevistado se resista a aportar información, siendo útil en estos casos utilizar técnicas específicas de comunicación.

Antes de finalizar la entrevista es importante que el entrevistador sintetice las conclusiones y compruebe que todos los asistentes están de acuerdo, dejando siempre abierta la posibilidad de volver a contactar para aclarar temas que surjan al estudiar la información recopilada.

Finalmente, el responsable depura y consolida el resultado de las entrevistas, elaborando un informe de conclusiones. En algunos casos puede ser conveniente elaborar un acta que refleje estas conclusiones y remitirla a los entrevistados con el objetivo de asegurar que se han comprendido bien las especificaciones dadas.

35.2.2 JAD (Joid Application Design)

Las características de una sesión de trabajo tipo JAD se pueden resumir en los siguientes puntos:

- Se establece un equipo de trabajo cuyos componentes y responsabilidades están perfectamente identificados teniendo en cuenta que el fin de la sesión es conseguir el consenso entre las necesidades de los usuarios y los servicios del sistema en producción.
- Se llevan a cabo pocas reuniones, de larga duración y muy bien preparadas.
- Durante la propia sesión se elaboran los modelos empleando diagramas fáciles de entender y mantener, directamente sobre herramientas CASE.
- Al finalizar la sesión se obtienen un conjunto de modelos que deberán ser aprobados por los participantes.

Es importante definir claramente el perfil y las responsabilidades de los participantes de una sesión JAD. Se pueden distinguir los siguientes perfiles:

- Moderador (líder) con amplios conocimientos de la metodología de trabajo, dinámica de grupos, psicología del comportamiento, así como de los procesos de la organización objeto del estudio.
- Promotor, persona que ha impulsado el desarrollo.
- Jefe de proyecto, responsable de la implantación del proyecto.
- Especialista en modelización, responsable de la elaboración de los modelos en el transcurso de la sesión.
- Desarrolladores, aseguran que los modelos son correctos y responden a los requisitos especificados.
- Usuarios, responsables de definir los requisitos del sistema y validarlos.

Para llevar a cabo una sesión JAD, es necesario realizar una serie de actividades antes de su inicio, durante el desarrollo y después de su finalización. Estas actividades se detallan a continuación:

- **Inicio:** se define el ámbito y la estructura del proyecto, los productos a obtener, se prepara el material necesario para la sesión, se determina el lugar donde se van a llevar a cabo, se seleccionan los participantes y se sugiere una agenda de trabajo.
- **Desarrollo:** se identifican las salidas del proyecto y se debe conseguir el consenso entre los participantes de modo que se materialice en los modelos.
- **Finalización:** se valida la información de la sesión y se generan los productos de la metodología de trabajo propuesta. Si fuera necesario se integran los productos de salida.

35.2.3 Prototipado

Los prototipos son sistemas software que sólo implementan una parte del sistema. Normalmente, los prototipos se emplean para obtener requisitos del usuario cuando éstos no están completamente claros. Es mucho más fácil que el usuario entienda y apruebe un sistema viendo una versión reducida pero operativa y puede interaccionar con él, a revisar una larga lista de texto con los requisitos que describen dicho sistema. Al fin y al cabo, como se suele decir, el prototipo permite salvar la situación siguiente: “No se lo que quiero, pero lo sabré cuando lo vea”. Y en efecto, será mucho más fácil para un usuario saber si lo que quiere es lo que tiene delante y que puede interaccionar con él, que si es un montón de hojas con todos los requisitos escritos uno a uno.

La aplicación de la técnica del prototipado consta de los siguientes pasos:

- 1- Estudio preliminar de los requisitos del usuario.
- 2- Proceso iterativo consistente en:
 - a. Construir un prototipo.
 - b. Evaluarlo con los usuarios.
 - c. Formular nuevos requisitos.

d. Desechar el prototipo.

Los aspectos clave en el diseño de prototipos son: la identificación de los usuarios a los que va dirigido, teniendo en cuenta que debe responder a diferentes individualidades, con distintos conocimientos y habilidades, qué funciones tienen asignadas, y qué tipo de información requerirán para llevar a cabo dichas funciones.

35.2.4 Análisis de factores críticos de éxito.

Esta técnica consistente en identificar y concentrarse en un pequeño conjunto de factores críticos de los que depende el éxito y efectividad del sistema. Aunque la identificación de los factores críticos correctos es, a veces, una labor compleja, esta técnica es bastante útil cuando el sistema es técnicamente complejo.

35.2.5 Brainstorming

Esta técnica se usa principalmente para la generación de ideas en los casos en los que la generación de éstas no es obvia. Se trata de una técnica sencilla en la que se reúnen en grupo de 4 a 10 personas para generar ideas, sin restricciones, en un ambiente libre de críticas. Uno de los principales puntos fuertes de la técnica es que ideas que en un principio pueden ser descabelladas tienen cabida. Primero se proporcionan las ideas y en una segunda vuelta se refinan. El Brainstorming permite aportar a la obtención de requisitos los siguientes aspectos:

- **Genera múltiples puntos de vista de un problema.** Cada uno da su visión del problema, que no tiene porqué ser la misma. Una vez vistos todos los puntos de vista se puede atacar el problema de una forma más efectiva.

- **Formular un problema de distintas formas.** Cada participante puede ver el problema desde una óptica distinta, por lo que a la hora de formularlo lo hará de una forma distinta. Estas diferencias pueden aportar gran valor a la hora del estudio del problema, identificando los puntos clave del problema de cada participante.

La técnica de Brainstorming, para que sea efectiva, debe ser previamente preparada. Las fases por las que pasa la ejecución de la técnica son:

- 1- **Fase de Preparación:** Se identifican los participantes de la sesión (clientes, usuarios, analistas, etc.), se designa un líder que lleva la sesión, se planifica la sesión y se busca una sala adecuada.
- 2- **Fase de Generación:** Se comienza exponiendo las ideas de forma libre, por turnos o espontáneamente. Las ideas se van apuntando en una pizarra que todos puedan ver.
- 3- **Fase de Consolidación:** Se revisan las ideas obtenidas en el paso anterior, se clarifican si no están claras, se rescriben si es necesario, se descartan las que no son utilizables, se discuten las restantes y se priorizan.

35.2.6 Escenarios y Casos de uso

Normalmente, las personas encuentran más fácil dar ejemplos de la vida real que descripciones abstractas. Los **escenarios** pueden ser especialmente útiles para agregar detalle a un esbozo de la descripción de requisitos. Son descripciones de ejemplos de las sesiones de interacción. Cada escenario abarca una o más posibles interacciones. El escenario comienza con un esbozo de la interacción y, durante la obtención se agregan detalles para crear una descripción completa de esta interacción. De forma general, un escenario puede incluir:

- 1- Una descripción de lo que esperan el sistema y los usuarios cuando el escenario comienza.

- 2- Una descripción del flujo normal de eventos en el escenario.
- 3- Una descripción de lo que puede ir mal y cómo manejarlo.
- 4- Información de otras actividades que se podrían llevar a cabo al mismo tiempo.
- 5- Una descripción del estado del sistema cuando el escenario termina.

Los escenarios se pueden redactar como texto, complementados por diagramas, fotografías de las pantallas, etcétera. De forma alternativa, se puede adoptar un enfoque más estructurado, como los escenarios de evento o los casos de uso.

Los casos de uso son una técnica que se basa en escenarios para la obtención de requisitos. En su forma más simple, un caso de uso identifica el tipo de interacción y los actores involucrados. Los actores en el proceso se representan como figuras delineadas, y cada clase de interacción se representa como una elipse con su nombre. El conjunto de casos de uso representa todas las posibles interacciones a representar en los requisitos del sistema. Actualmente se han convertido en una característica fundamental de la notación de UML, que se utiliza para describir modelos de sistemas orientados a objetos.

Los escenarios y los casos de uso son técnicas eficaces para obtener requisitos para los puntos de vista de los interactuadores, donde cada tipo de interacción se puede representar como un caso de uso. Sin embargo, debido a que se centran en las interacciones, no son tan eficaces para obtener restricciones y requisitos de negocio y no funcionales de alto nivel de puntos de vista indirectos o para descubrir requisitos del dominio.

35.2.7 Observación directa e investigación contextual (Etnografía)

La **etnografía** es una técnica de observación que se puede utilizar para entender los requisitos sociales y organizacionales. Un analista se sumerge

por sí solo en el entorno laboral donde se utilizará el sistema. Observa el trabajo diario y anota las tareas reales en las que los participantes están involucrados. El valor de la etnografía es que ayuda a los analistas a descubrir los requisitos implícitos que reflejan los procesos reales más que los formales en los que la gente está involucrada.

La etnografía es especialmente efectiva para descubrir dos tipos de requisitos:

- Los requisitos que se derivan de la forma en la que la gente trabaja realmente más que de la forma en la que las definiciones de los procesos establecen que debería trabajar.
- Los requisitos que se derivan de la cooperación y conocimiento de las actividades de los demás.

Los estudios etnográficos pueden revelar los detalles de los procesos críticos que otras técnicas de obtención de requisitos a menudo olvidan. Sin embargo, puesto que se centran en el usuario final, este enfoque no es apropiado para descubrir los requisitos organizacionales o del dominio. Los estudios etnográficos no siempre pueden identificar nuevas propiedades que se deban agregar al sistema. Por lo tanto, la etnografía no es un enfoque completo para la obtención de requisitos por sí mismo, y debe utilizarse para complementar otros enfoques, como el análisis de casos de uso.

35.3 Verificación - Validación

La **validación** de requisitos trata de mostrar que éstos realmente definen el sistema que el cliente desea. La validación de requisitos es importante debido a que los errores en los requisitos pueden conducir a importantes costes al repetir el trabajo cuando son descubiertos durante el desarrollo o después de que el sistema esté en uso. El coste de arreglar un problema en

los requisitos haciendo un cambio en el sistema es mucho mayor que reparar los errores de diseño o los de codificación.

La razón de esto es que un cambio en los requisitos normalmente significa que el diseño y la implementación del sistema también deben cambiar y que éste debe probarse nuevamente.

Durante el proceso de validación de requisitos, se deben llevar a cabo las siguientes **verificaciones**:

- 1- **Verificaciones de validez.** Un usuario puede pensar que se necesita un sistema para llevar a cabo ciertas funciones. Sin embargo, el razonamiento y el análisis pueden identificar que se requieren funciones adicionales o diferentes. También se deben tener en cuenta que en un mismo sistema suele haber diferentes usuarios, con diferentes puntos de vista, algunas veces contrapuestos, y que éstos deben llegar a un compromiso a la hora de definir los requisitos del sistema.
- 2- **Verificaciones de consistencia.** Los requisitos no deben contradecirse. Esto es, no debe haber restricciones o descripciones contradictorias de la misma función del sistema.
- 3- **Verificaciones de completitud.** Los requisitos deben definir todas las funciones y restricciones propuestas por el usuario del sistema.
- 4- **Verificaciones de realismo.** Utilizando el conocimiento de la tecnología existente, los requisitos deben verificarse para asegurar que se pueden implementar. Estas verificaciones también deben tener en cuenta el presupuesto y la confección de agendas para el desarrollo del sistema.
- 5- **Verificabilidad.** Para reducir la posibilidad de discusiones entre el cliente y el desarrollador, los requisitos del sistema siempre deben redactarse de tal forma que sean verificables. Esto significa que debe poder escribir un conjunto de pruebas que demuestren que el sistema a entregar cumple cada uno de los requisitos especificados.

Pueden utilizarse, en conjunto o de forma individual, varias técnicas de validación de requisitos:

- 1- **Revisiones de requisitos.** Los requisitos son analizados manual y sistemáticamente por un equipo de revisores formado por personas tanto de la organización del cliente como de la desarrolladora. Se verifican los requisitos en cuanto a anomalías y omisiones. Pueden ser informales o formales. Las informales sencillamente implican que los desarrolladores deben tratar los requisitos con tantos usuarios del sistema como sea posible. En la revisión formal de requisitos, el equipo de desarrollo debe «conducir» al cliente a través de los requisitos del sistema, explicándole las implicaciones de cada requisito. Los revisores deben comprobar la:
 - a. **Verificabilidad.** ¿Puede probarse el requisito de modo realista?
 - b. **Comprensibilidad.** ¿Las personas que adquieren el sistema o los usuarios finales comprenden correctamente el requisito?
 - c. **Rastreabilidad.** ¿Está claramente establecido el origen del requisito? Puede tener que volver a la fuente del requisito para evaluar el impacto del cambio. La rastreabilidad es importante ya que permite evaluar el impacto del cambio en el resto del sistema.
 - d. **Adaptabilidad.** ¿Es adaptable el requisito? Es decir, ¿puede cambiarse el requisito sin causar efectos de gran escala en los otros requisitos del sistema?

Los conflictos, contradicciones, errores y omisiones en los requisitos deben ser señalados por los revisores y registrarse formalmente en el informe de revisión. Queda en los usuarios, la persona que adquiere el sistema y el desarrollador de éste negociar una solución para estos problemas identificados.

- 2- **Construcción de prototipos** En este enfoque de validación, se muestra un modelo ejecutable del sistema a los usuarios finales y a los clientes. Éstos pueden experimentar con este modelo para ver si cumple sus necesidades reales.
- 3- **Generación de casos de prueba.** Los requisitos deben poder probarse. Si las pruebas para éstos se conciben como parte del proceso de validación, a menudo revela los problemas en los requisitos. Si una prueba es difícil o imposible de diseñar, normalmente significa que los requisitos serán difíciles de implementar y deberían ser considerados nuevamente.

Es difícil demostrar que un conjunto de requisitos cumple las necesidades del usuario. Como consecuencia, rara vez se encuentran todos los problemas en los requisitos durante el proceso de validación de éstos. Es inevitable que haya cambios adicionales de requisitos para corregir las omisiones y las malas interpretaciones después de que el documento de requisitos haya sido aprobado.

35.4 Especificación de requisitos

El **documento de requisitos del software** (algunas veces denominado *especificación de requisitos del software* o **ERS**) es la declaración oficial de qué deben implementar los desarrolladores del sistema. Tiene un conjunto diverso de usuarios que va desde los altos cargos de la organización que pagan por el sistema, hasta los ingenieros responsables de desarrollar el software. Los objetivos que pretende el ERS son los siguientes:

- Proporcionar los medios de comunicación entre todas las partes implicadas en el sistema: clientes, usuarios, analistas y diseñadores.
- Servir como base para las actividades de prueba y verificación.
- Ayudar al control de la evolución del sistema software.

El documento ERS debe incluir una descripción completa y concisa de toda la interfaz externa del sistema con su entorno, incluido el resto del software, puertos de comunicación, hardware y usuarios. Es decir, debe incluir tanto los requisitos de comportamiento del sistema (funcionales), que son aquellos que definen lo que hace éste y la información que maneja, como los requisitos que no son de comportamiento, esto es, aquellos que definen los atributos del sistema según realiza su trabajo (eficiencia, fiabilidad, seguridad, etc.).

Por contra, un documento ERS no debe incluir los elementos de gestión del proyecto (planificaciones, hitos, etc.), ni el diseño, ni los planes de control del producto (gestión de configuración, garantía de calidad, etc.). Un documento ERS debe reunir las siguientes características:

- **Correcto.** Cada requisito establecido debe representar algo requerido para el sistema.
- **No Ambiguo.** Cada requisito establecido tiene una sola interpretación.
- **Completo.** Debe incluir todo lo que el software tiene que hacer.
- **Verificable.** Se ha de poder comprobar, mediante un proceso efectivo y de coste limitado, que el producto reúne cada requisito establecido.
- **Consistente.** Cada requisito no puede estar en conflicto con otros requisitos.
- **Modificable.** La estructura y estilo del documento debe hacer fáciles los cambios.
- **Conciso,** comprensible por el usuario y organizado.
- **Referenciado.** Cada requisito debe estar calificado y debidamente referenciado.

35.4.1 IEEE/ANSI 830-1998

Varias organizaciones grandes, como el Departamento de Defensa de los Estados Unidos y el IEEE, han definido estándares para los documentos de requisitos. El estándar más ampliamente conocido es el IEEE/ANSI 830-1998 (IEEE, 1998). Este estándar IEEE sugiere la siguiente estructura para los documentos de requisitos:

1. Introducción

- 1.1 Propósito del documento de requisitos: Propósito y a quién va dirigido.
- 1.2 Alcance del producto
- 1.3 Definiciones, acrónimos y abreviaturas
- 1.4 Referencias
- 1.5 Descripción del resto del documento

2. Descripción general

- 2.1 Perspectiva del producto
- 2.2 Funciones del producto
- 2.3 Características del usuario
- 2.4 Restricciones generales
- 2.5 Suposiciones y dependencias

3. Requisitos específicos. Este será el grueso del documento.

3.1. Interfaces Externas: Se describirán los requisitos que afecten a la interfaz de usuario, interfaz con otros sistemas (hardware y software) e interfaces de comunicaciones.

3.2. Funciones: Esta subsección (quizá la más larga del documento) deberá especificar todas aquellas acciones (funciones) que deberá llevar a cabo el software. Si se considera necesario, podrán utilizarse notaciones gráficas y tablas, pero siempre supeditadas al lenguaje natural, y no al revés. El estándar permite organizar esta subsección de múltiples formas, y sugiere, entre otras, las siguientes:

- **Por tipos de usuario:** Distintos usuarios poseen distintos requisitos. Para cada clase de usuario que exista en la

organización, se especificarían los requisitos funcionales que le afecten o tengan mayor relación con sus tareas.

- **Por objetos:** Los objetos son entidades del mundo real que serán reflejadas en el sistema. Para cada objeto, se detallarán sus atributos y sus funciones. Los objetos pueden agruparse en clases. Esta organización de la ERS no quiere decir que el diseño del sistema siga el paradigma de Orientación a Objetos.
- **Por objetivos:** Un objetivo es un servicio que se desea que ofrezca el sistema y que requiere una determinada entrada para obtener su resultado. Para cada objetivo o subobjetivo que se persiga con el sistema, se detallarán las funciones que permitan llevarlo a cabo.
- **Por estímulos:** Se especificarían los posibles estímulos que recibe el sistema y las funciones relacionadas con dicho estímulo.
- **Por jerarquía funcional:** Si ninguna de las anteriores alternativas resulta de ayuda, la funcionalidad del sistema se especificaría como una jerarquía de funciones que comparten entradas, salidas o datos internos. Se detallarían las funciones (entrada, proceso, salida) y las subfunciones del sistema. Esto no implica que el diseño del sistema deba realizarse según el paradigma de Diseño Estructurado.

3.3. Requisitos de Rendimiento: Se detallarían los requisitos relacionados con la carga que se espera tenga que soportar el sistema. Por ejemplo, el número de terminales, el número esperado de usuarios simultáneamente conectados, número de transacciones por segundo que deberá soportar el sistema, etc. También, si es necesario, se especificarían los requisitos de datos, es decir, aquellos requisitos que afecten a la información que se guardará en la base de datos. Por ejemplo, la frecuencia de uso, las capacidades de acceso y la cantidad de registros que se espera almacenar (decenas, cientos, miles o millones).

3.4. Restricciones de Diseño: Todo aquello que restrinja las decisiones relativas al diseño de la aplicación: Restricciones de otros estándares, limitaciones del hardware, etc.

3.5. Atributos del Sistema: Se detallaran los atributos de calidad del sistema: Fiabilidad, mantenibilidad, portabilidad, y, muy importante, la seguridad. Debería especificarse que tipos de usuario están autorizados, o no, a realizar ciertas tareas, y como se implementarían los mecanismos de seguridad

3.6. Otros Requisitos

4. Apéndices

5. Índice

El estándar IEEE es un marco general que se puede transformar y adaptar para definir un estándar ajustado a las necesidades de una organización en particular. La información que se incluya en un documento de requisitos debe depender del tipo de software a desarrollar y del enfoque de desarrollo que se utilice.

35. 5 Gestión de requisitos

Los requisitos para sistemas software grandes son siempre cambiantes. Debido a que el problema no puede definirse completamente, es muy probable que los requisitos del software sean incompletos. Durante el proceso del software, la comprensión del problema por parte de los clientes cambia, y los requisitos deben entonces evolucionar para reflejar esto. Además, una vez que un sistema se ha instalado, inevitablemente surgen nuevos requisitos. Cuando los usuarios finales trabajan con un sistema, descubren nuevas necesidades y prioridades debidas a:

- Normalmente, los sistemas grandes tienen una comunidad de usuarios diversa donde los estos tienen diferentes requisitos y

prioridades. Los que se usaron para definir el sistema pudieron no ser los mejores.

- Las personas que pagan por el sistema y los usuarios de éste raramente son la misma persona. Los clientes del sistema imponen requisitos debido a las restricciones organizacionales y de presupuesto. Éstos pueden estar en conflicto con los requisitos de los usuarios finales y, después de la entrega, pueden tener que añadirse nuevas características de apoyo al usuario si el sistema tiene que cumplir sus objetivos.
- El entorno de negocios y técnico del sistema cambia después de la instalación, y estos cambios se deben reflejar en el sistema. Se puede introducir nuevo hardware, puede ser necesario que el sistema interactúe con otros sistemas, las prioridades de negocio pueden cambiar con modificaciones consecuentes en la ayuda al sistema, y puede haber una nueva legislación y regulaciones que deben ser implementadas por el sistema.

La **gestión de requisitos** es el proceso de comprender y controlar los cambios en los requisitos del sistema. Es necesario poder evaluar el impacto de los cambios en los requisitos. Hay que establecer un proceso formal para implementar las propuestas de cambios. El proceso de gestión de requisitos debería empezar en cuanto esté disponible una versión preliminar del documento de requisitos, pero se debería empezar a planificar cómo gestionar los requisitos que cambian durante el proceso de obtención de requisitos.

Existen **requisitos duraderos**, que son requisitos relativamente estables que se derivan de la actividad principal de la organización y que están relacionados directamente con el dominio del sistema. Estos requisitos se pueden derivar de los modelos del dominio que muestran las entidades y relaciones que caracterizan un dominio de aplicación. Por otro lado, existen **requisitos volátiles**, que son requisitos que probablemente cambian

durante el proceso de desarrollo del sistema o después de que éste se haya puesto en funcionamiento, debido a cambios del entorno, legislación,...

35.5.1 Planificación de la gestión requisitos.

Para cada proyecto, la etapa de planificación establece el nivel de detalle necesario en la gestión de requisitos. Habrá que decidir sobre:

1. **La identificación de requisitos.** Cada requisito se debe identificar de forma única de tal forma que puedan ser remitidos por otros requisitos de manera que pueda utilizarse en las evaluaciones de rastreo.
2. **Un proceso de gestión del cambio.** Éste es el conjunto de actividades que evalúan el impacto y coste de los cambios. Lo veremos en un apartado posterior.
3. **Políticas de rastreo o trazabilidad.** Estas políticas definen las relaciones entre los requisitos, y entre éstos y el diseño del sistema que se debe registrar y la manera en que estos registros se deben mantener.
4. **Selección de herramientas CASE.** La gestión de requisitos comprende el procesamiento de grandes cantidades de información sobre los requisitos. Las herramientas que se pueden utilizar van desde sistemas de gestión de requisitos especializados hasta hojas de cálculo y sistemas sencillos de bases de datos.

El concepto de trazabilidad hace referencia a la posibilidad de determinar cómo se ha llegado a un cierto elemento del software a partir de otros. Para poder llevar a cabo esta trazabilidad es especialmente importante el poder relacionar unos requisitos con otros y también relacionar requisitos con elementos del sistema a los que da lugar. Se habla de trazabilidad *hacia delante* cuando partiendo de un requisito se llega a todos los

elementos que materializan dicho requisito, o *hacia atrás*, cuando partiendo de un elemento del sistema se llega al requisito que lo generó.

Un requisito se debe poder relacionar con otros requisitos similares para así evitar repeticiones en los mismos. Además, cuando se hace un cambio en uno, es más fácil localizar aquellos requisitos en los que hay relación, para ver el impacto del cambio. Por otro lado, es útil poder relacionar un requisito con los elementos del sistema a los que éste da lugar, por si hay que cambiar un elemento del sistema, o simplemente, para poder saber qué requisitos dieron lugar a un determinado componente del sistema. Esta relación no sólo debe ser entre requisitos, sino también entre cualquier elemento que se haya derivado posteriormente, ya sea del análisis, del diseño, de la construcción, de pruebas, etc.

La gestión de requisitos necesita ayuda automatizada. Las herramientas CASE para esto deben elegirse durante la fase de planificación. Se precisan herramientas de ayuda para:

1. **Almacenar requisitos.** Los requisitos deben mantenerse en un almacén de datos seguro y administrado que sea accesible a todos los que estén implicados en el proceso de ingeniería de requisitos.
2. **Gestionar el cambio.**
3. **Gestionar el rastreo.** Las herramientas de ayuda para el rastreo permiten que se descubran requisitos relacionados. Algunas herramientas utilizan técnicas de procesamiento del lenguaje natural para ayudarle a descubrir posibles relaciones entre los requisitos.

Para sistemas pequeños, es posible que no sea necesario utilizar herramientas de gestión de requisitos especializadas, pero si es muy conveniente para sistemas grandes.

35.5.2 Gestión del cambio

La ventaja de utilizar un proceso formal para gestionar el cambio es que todos los cambios propuestos son tratados de forma consistente y que los cambios en los requisitos se hacen de forma controlada. Existen varias etapas principales en un proceso de gestión de cambio:

- **Propuesta de Cambios.** El afectado por un requisito que no le satisface debe rellenar un formulario de propuesta de cambio indicando cual es el cambio que hay que realizar. Este cambio se remitirá al equipo de gestión de requisitos para que lo estudie.
- **Análisis de Impactos.** La propuesta de cambio se evalúa para determinar el impacto del cambio en el resto de los requisitos. Hay propuestas cuyo impacto es mínimo, y otras cuyo impacto hace que se deba modificar una parte sustancial del sistema. Además del impacto se deberá estudiar la oportunidad o necesidad del cambio. Ocurre muchas veces que a un usuario no le parece bien un determinado aspecto del sistema pero a otros si les satisface. En estos casos se debe llegar a un consenso entre todas las partes. Otras veces el cambio es interesante pero se considera que no es oportuno hacerlo en dicho momento, quizás porque se quiera lanzar el sistema cuanto antes o porque el cambio es considerable y sería mejor atacarlo en una fase posterior de desarrollo.
- **Toma de Decisiones.** Dependiendo del impacto, de la necesidad u oportunidad del cambio y de otras cuestiones específicas que puedan surgir alrededor del cambio, se debe determinar si el cambio debe ser realizado o no. Si se decide realizarlo se deben hacer las modificaciones pertinentes en el sistema para integrar el cambio con el resto, empezando por los requisitos y finalizando por las partes más avanzadas del sistema. Si por el contrario se decide no hacerlo se puede optar por dos soluciones:
 - o Rechazar el cambio, porque se considera que no tiene sentido.

- o Posponer su realización para un futuro, se considera el cambio necesario pero el momento no es oportuno. Se pospone para cuando se pueda acometer.
- **Comunicación.** Tanto si se acepta como si no, se debe notificar los efectos de la propuesta de cambio a todos los afectados.
- **Incorporación.** Se hacen las modificaciones pertinentes que se identificaron en el análisis de impacto en los diferentes elementos afectados por el cambio.
- **Medición de la Estabilidad de los Requisitos.** Se evalúan los parámetros que definen la estabilidad de los requisitos tras las modificaciones que se hayan realizado.

Bibliografía:

Ian Sommerville – “Ingeniería de Software” 7 Edición. Editorial Prentice Hall, 2005

Jacobson, I., Booch, G., Rumbaugh, J. El Proceso Unificado de Desarrollo de Software”. Editorial Addison-Wesley, 2000

Piattini, M. G., Calvo-Manzano, J. A., Cervera, J., Fernández, L. “Análisis y Diseño de Aplicaciones Informáticas de Gestión. Una perspectiva de Ingeniería del Software”. Editorial Ra-ma. 2004

Métrica 3 – Técnicas y Prácticas. Ministerio de Administraciones Públicas

Especificación de Requisitos según el estándar de IEEE 830

<http://www.fdi.ucm.es/profesor/gmendez/docs/is0809/ieee830.pdf>

Pohl, K. “Requirements Engineering: An Overview”. En M. Dekker (Ed.), Encyclopedia of Computer Science and Technology, 36. 1997.
disponible en <ftp://sunsite.informatik.rwth-aachen.de/pub/CREWS/CREWS-96-02.pdf>

Autor: Francisco Javier Rodríguez Martínez.

Subdirector de la Escuela Superior de Ingeniería Informática.

Universidad de Vigo.



36. ANÁLISIS ORIENTADO A OBJETOS. LENGUAJE UNIFICADO DE MODELADO (UML).

Tema 36. Análisis orientado a objetos. Lenguaje Unificado de modelado (UML)

INDICE:

36.1 Análisis orientado a objetos

36.1.1 Introducción a la orientación a objetos

36.1.2 Elementos de la orientación a objetos

36.1.3 Propiedades de la orientación a objetos

36.1.4 Análisis orientado a objetos

36.1.5 Modelado de Clases-Responsabilidades-Colaboraciones (CRC)

36.2 Lenguaje Unificado de modelado (UML)

36.2.1 Introducción

36.2.2 Elementos de construcción

36.2.3 Relaciones

36.2.4 Diagramas

36.1 Análisis orientado a objetos.

36.1.1 Introducción a la orientación a objetos

El principal objetivo de la orientación a objetos es reducir la complejidad del desarrollo y mantenimiento del software y puede describirse como el conjunto de disciplinas que desarrollan y modelan software que facilitan la construcción de sistemas complejos a partir de componentes. Los conceptos de orientación a objetos datan de los años 60, pero dado que la tecnología no estaba acorde con su implementación, se mantuvo sólo como concepto hasta su gran expansión a mediados de los 80.

El Análisis Orientado a Objetos "es un método de análisis que examina los requisitos desde la perspectiva de las clases y objetos encontrados en el

vocabulario del dominio del problema"(Booch 94). El modelo del Análisis debe incluir información significativa desde la perspectiva del mundo real, debe presentar una vista externa del sistema definiendo los objetos en el dominio del problema. Debe ser comprendido por el cliente y servir de ayuda para encontrar los verdaderos requerimientos del sistema.

El ciclo de desarrollo del software orientado a objetos comienza, en primer lugar construyendo en el **Análisis** un modelo que abstrae los aspectos esenciales del dominio del problema, sin tener en cuenta en esta etapa la implementación concreta. Este modelo conceptual contendrá objetos encontrados en el dominio de la aplicación y describirá las propiedades y comportamiento de aquéllos. En segundo lugar, el **Diseño** añadirá detalles y tomará decisiones que optimicen la implementación. En el diseño, los objetos se describen en términos del dominio del ordenador. Finalmente, el modelo obtenido en el diseño se **implementa** en un lenguaje de programación, una base de datos y un hardware concretos.

36.1.2 Elementos de la orientación a objetos.

- **Objetos:** Los objetos son módulos que contienen los datos y las instrucciones que manipulan esos datos, poseen una funcionalidad porque pueden reaccionar ante una serie de mensajes y procesar una serie de peticiones. Dicho de otra forma, los objetos son entidades que tienen atributos (datos) y formas de comportamiento (procedimientos) particulares. Dentro de un sistema orientado a objetos se representarán todos aquellos relevantes para el Universo de Discurso sobre el que trate el sistema.
- **Clases:** Una clase describe un conjunto de objetos diferentes con propiedades (atributos) similares y un comportamiento común, podemos verlo como una plantilla que define las variables y métodos que son comunes para los objetos de cierto tipo. Cada uno de los objetos individuales pertenecientes a una clase se denomina

instancia de dicha clase. Una clase que no tenga instancias se denomina clase abstracta. Una clase abstracta puede servir para declarar las propiedades o comportamiento de un conjunto determinado de clases que derivarán de ella. Las clases son un concepto **estático** definido en el programa fuente, son una abstracción de la esencia de un objeto, mientras que los objetos son entes **dinámicos** que existen en tiempo y espacio y que ocupan memoria en la ejecución de un programa.

- **Atributos:** representan los datos asociados a los objetos instanciados por esa clase, es decir, son las propiedades o características de un objeto.
- **Operaciones o métodos:** representan las funciones o procesos propios de los objetos de una clase, caracterizando a dichos objetos. Los métodos de un objeto se invocan exclusivamente con el mensaje adecuado, y al ser invocado un método de un objeto, sólo se referirá a la estructura de datos de ese objeto y no a la de otros, aunque sean de la misma clase. La interfaz de la clase estará definida por el conjunto de métodos que soporta y los mensajes que es capaz de tratar.
- **Mensajes.** Los objetos tienen la posibilidad de actuar. La actuación sucede cuando un objeto recibe un mensaje, que no es más que una solicitud que le pide que se comporte de alguna forma determinada. El mensaje contiene el nombre del objeto al que va dirigido, el nombre de una operación y, en ocasiones, un grupo de parámetros.

36.1.3 Propiedades de la orientación a objetos

Los principios del modelo orientado a objetos son:

- **Identidad:** Cada objeto tiene su propia identidad inherente, es decir, dos objetos son distintos aunque tengan todas sus propiedades iguales.
- **Clasificación.** Se refiere a que los objetos que tienen la misma estructura de datos (atributos), y el mismo comportamiento (operaciones), están agrupados en una clase.
- **Herencia.** La herencia es el mecanismo mediante el cual una clase (subclase) adquiere las propiedades de otra clase jerárquicamente superior (superclase, clase base). La herencia proporciona el mecanismo para compartir automáticamente métodos y datos entre clases, subclases y objetos, y puede ser simple o múltiple, según que una subclase herede los datos y métodos de una sola clase o de más de una. Una clase se puede definir de manera muy amplia y después refinarla en sucesivas subclases. Cada subclase incorpora o “hereda” todas las propiedades de su superclase y añade sus propiedades únicas, lo que reduce en gran medida la repetición en el diseño y la programación y es una de las principales ventajas de la Orientación a Objetos. La herencia proporciona relaciones entre clases del tipo “es-un”. La herencia permite que las clases derivadas proporcionen comportamientos específicos, manteniendo una clases base común.
- **Abstracción:** Es una descripción simplificada de un sistema que enfatiza algunos de los detalles o propiedades del mismo, mientras suprime otros. Consiste en la generalización conceptual del comportamiento de un determinado grupo de objetos y de sus atributos. Se trata de abstraer los datos y métodos comunes a un conjunto de objetos para almacenarlos en una clase. La orientación a objetos hace que los programadores y usuarios piensen sobre las aplicaciones en términos abstractos, prestando atención a lo que un objeto es y hace antes de decidir cómo será implementado.
- **Encapsulación:** Es el término que se utiliza para expresar que los datos de un objeto sólo pueden ser manipulados mediante los

mensajes y métodos predefinidos. Es decir, los datos relativos a algún objeto están almacenados junto con el proceso que crea y manipula esos datos. De esta forma, quedan escondidos los detalles de implementación de un objeto que no contribuyen a definir sus características esenciales.

Los objetos restringen la visibilidad de sus recursos (atributos y métodos) al resto de usuarios. Cada objeto posee una interface que determina la manera de interactuar con él. La implementación del objeto (su interior) es encapsulada, lo que quiere decir que desde fuera el objeto es invisible, simplemente se usa.

- **Polimorfismo:** Es la propiedad por la cual un mismo mensaje puede originar conductas diferentes al ser recibido por objetos diferentes. Es decir, la misma operación puede comportarse de manera diferente para clases diferentes. El polimorfismo es consecuencia de la herencia. Las funciones de una clase base pueden ser sustituidas en una clase derivada mediante la redefinición de su declaración en la clase hija. Por lo tanto, los objetos de las dos clases pueden reaccionar ambos a los mismos mensajes pero lo harán de diferentes maneras. También hablamos de polimorfismo cuando tenemos distintos métodos que tienen un comportamiento distinto en función del número o tipo de parámetros que reciben. En este caso hablamos de **métodos polimórficos**.

El polimorfismo es posible gracias a las interfaces que permiten acceder a métodos con el mismo nombre en diferentes clases. Dentro de cada clase particular se puede redefinir el método obteniendo distintos métodos con el mismo nombre. Así es que un método no se define exactamente con su nombre, si no con su nombre y el nombre de la clase a la que pertenece.

- **Reusabilidad:** Es la capacidad de producir componentes reutilizables para otros diseños o aplicaciones, es decir, permite reutilizar parte del código para el desarrollo de una aplicación similar. En la Orientación a objetos se consigue de una forma natural mediante el diseño de componentes.
- **Persistencia:** Un objeto en software ocupa un determinado espacio de memoria y existe durante una cierta cantidad de tiempo: es un concepto dinámico. La persistencia es la cualidad que se refiere a la permanencia del objeto, es decir, al tiempo durante el cual se le asigna espacio y permanece accesible en la memoria del ordenador (principal o secundaria).
- **Extensibilidad:** Es la capacidad de un programa para ser fácilmente alterado de forma que pueda tratar con nuevas clases de entrada. Mediante esta propiedad, los objetos pueden ser usados para almacenar y procesar muchos tipos diferentes de datos simplemente añadiendo clases que traten los tipos de datos que sean necesarios.

36.1.4 Análisis orientado a objetos

El Análisis Orientado a Objetos enfatiza la construcción de modelos basados en el mundo real, utilizando una perspectiva del mismo basada en las clases y objetos encontrados en el dominio del problema. Firesmith describe el **análisis del dominio** como *“la identificación, análisis y especificación de requisitos comunes en un dominio de aplicación específico, normalmente para su reutilización en múltiples proyectos dentro del mismo dominio de aplicación. El análisis orientado a objetos del dominio es la identificación, análisis y especificación de capacidades comunes y reutilizables dentro de un dominio de aplicación específico, en términos de objetos, clases, submontajes y marcos de trabajo comunes”*. Al igual que en los métodos estructurados tradicionales, en la etapa Análisis hay que establecer qué es lo que debe hacerse, dejando para etapas posteriores los detalles. El resultado del análisis debe ser una

completa comprensión del problema. Las dos grandes etapas de que consta el Análisis son las siguientes:

1. La descripción o especificación del problema. Esta descripción no debe considerarse inmutable, sino más bien como la base para ir refinando las especificaciones reales. La especificación del problema debe establecer el ámbito del problema, describir las necesidades y requisitos, el contexto de la aplicación, los supuestos de que se parte o las necesidades de rendimiento del sistema. En estas especificaciones, el usuario del sistema debe indicar cuáles son obligadas y cuáles se pueden considerar opcionales. Asimismo, otros puntos a tratar pueden ser los estándares de Ingeniería del Software, diseño de las pruebas a efectuar, previsión de futuras extensiones, etc.
2. La modelización del Análisis: Las características esenciales deben abstraerse en un modelo. Las especificaciones expresadas en lenguaje natural tienden a ser ambiguas, incompletas e inconsistentes, sin embargo, el Modelo de Análisis es una representación precisa y concisa del problema, que permite construir una solución. La etapa siguiente de diseño se remitirá a este modelo, en lugar de a las vagas especificaciones iniciales. El Modelo de Análisis se construye identificando las clases y objetos del dominio del problema (estructura estática), las interacciones entre los objetos y su secuenciamiento (estructura dinámica), y las acciones a realizar por el sistema que producen un resultado observable y valioso para los usuarios (estructura funcional).

36.1.5 Modelado de Clases-Responsabilidades-Colaboraciones (CRC)

El modelado de Clases-Responsabilidades-Colaboraciones (CRC) aporta un medio sencillo de identificar y organizar las clases que resulten relevantes

al sistema o requisitos del producto. Este modelo parte de los casos de uso (una secuencia de acciones realizadas por el sistema, que producen un resultado observable y valioso para un usuario en particular, es decir, representa el comportamiento del sistema con el fin de dar respuestas a los usuarios) que se utilizaron para modelar el sistema desde el punto de vista del usuario. Una vez desarrollados los escenarios de uso básicos, se identifican las clases candidatas, sus responsabilidades y sus colaboraciones. “Un modelo CRC es una colección de tarjetas que representan clases. Las tarjetas están divididas en tres secciones. A lo largo de la cabecera de la tarjeta usted escribe el nombre de la clase. En el cuerpo se listan las responsabilidades de la clase a la izquierda y a la derecha los colaboradores.”

Para identificar las **clases y objetos**, se parte de un análisis léxico-gramatical lo más preciso posible de la descripción del problema. Los **sustantivos** se convierten en clases/objetos candidatos. Un objeto/clase potencial debe satisfacer estas características para poder ser considerado como posible miembro del modelo:

- Retener información: el objeto potencial será útil durante el análisis si la información sobre el mismo debe guardarse para que el sistema funcione.
- Debe tener un conjunto de operaciones que permitan cambiar los valores de sus atributos.
- Atributos comunes: el conjunto de atributos definido para la clase debe ser aplicable a todas las ocurrencias del objeto.
- Operaciones comunes: la clase potencial debe definir un conjunto de operaciones aplicables, al igual que antes, a todos los objetos de la clase.

Las **responsabilidades** estarían formadas por los atributos y operaciones de las clases. Los **atributos** representan características o propiedades de

una clase, es decir, información sobre la clase. Las **operaciones** también se pueden extraer del análisis léxico-gramatical de la descripción del problema. Los **verbos** se transforman en candidatos a operaciones. Cada operación elegida para una clase exhibe un comportamiento de la clase.

Las clases cumplen con sus responsabilidades de dos formas: O bien una clase puede usar sus propias operaciones para manipular sus propios atributos, cumpliendo por lo tanto con una responsabilidad particular, o puede colaborar con otras clases.

Decimos que un objeto **colabora** con otro, si para ejecutar una responsabilidad necesita enviar algún mensaje al otro objeto. Una colaboración simple fluye en una dirección, representando una solicitud del cliente al servidor. Desde el punto de vista del cliente, cada una de sus colaboraciones está asociada con una responsabilidad particular implementada por el servidor.

Cada tarjeta del modelo CRC contiene una clase con una lista de responsabilidades. El siguiente paso es definir aquellas clases colaboradoras que ayudan en la realización de cada responsabilidad. Esto establece las **conexiones o relaciones** entre clases. Las **relaciones** deben derivarse a partir del examen de los verbos en la descripción del problema. Una vez conectadas las clases con sus colaboradores, etiquetamos cada una de estas conexiones, les añadimos una dirección, en función de qué clase llama a qué otra y por último se evalúa cada extremo de la conexión para determinar la cardinalidad. Este modelo de clases conectadas da lugar al **modelo Objeto-Relación**.

El modelo CRC y el modelo Objeto-Relación representan elementos estáticos. Para tener un modelo dinámico, debemos introducir el comportamiento del sistema, como una función de sucesos específicos y tiempo. Se identifican los sucesos que dirigen las secuencias de interacción entre objetos, se crea una traza de sucesos para cada caso de

uso, y se construye un diagrama de transición de estados para el sistema. Una vez terminada esta tarea tendríamos el **modelo Objeto-Comportamiento**.

36.2 Lenguaje Unificado de Modelado (UML)

36.2.1 Introducción

UML (Unified Modeling Language) es un lenguaje que permite modelar, construir y documentar los elementos que forman un sistema software orientado a objetos. Se ha convertido en el estándar de facto de la industria, debido a que ha sido impulsado por los autores de los tres métodos más usados de orientación a objetos: Grady Booch, Ivar Jacobson y Jim Rumbaugh. Es el estándar actual del llamado Object Management Group (OMG). Uno de los objetivos principales de la creación de UML era posibilitar el intercambio de modelos entre las distintas herramientas CASE orientadas a objetos del mercado. Para ello era necesario definir una notación y semántica común.

Hay que tener en cuenta que el estándar UML no define un proceso de desarrollo específico, tan solo se trata de una notación. UML sirve para *especificar*, modelos concretos, no ambiguos y completos. Un modelo de UML representa a un sistema software desde una perspectiva específica. Cada modelo nos permite fijarnos en un aspecto distinto del sistema. Debido a su estandarización y su definición completa no ambigua, y aunque no sea un lenguaje de programación, UML se puede conectar de manera directa a lenguajes de programación como Java, C++ o Visual Basic, esta correspondencia permite lo que se denomina como ingeniería directa (obtener el código fuente partiendo de los modelos) pero además es posible reconstruir un modelo en UML partiendo de la implementación, o sea, la ingeniería inversa.

UML se expresa a través de **elementos de construcción**, de **relaciones** y de **diagramas** que contienen elementos y relaciones

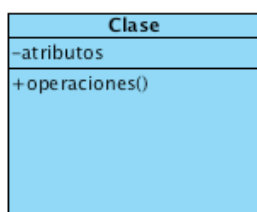
36.2.2 Elementos de construcción

Llamamos elementos a los bloques básicos de construcción. Son de cuatro tipos:

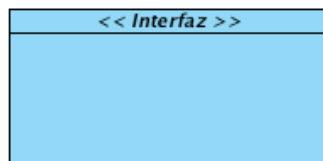
36.2.2.1 Elementos estructurales

En su mayoría son las partes estáticas del modelo. Son siete:

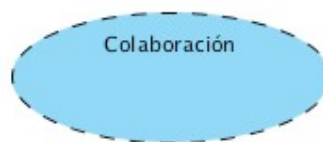
- **Clase:** Descripción de un conjunto de objetos que comparten los mismos atributos, operaciones, relaciones y semántica. Una clase se representa mediante una caja subdividida en tres partes: En la superior se muestra el nombre de la clase, en la media los atributos y en la inferior las operaciones. Una clase puede representarse de forma esquemática, con los detalles como atributos y operaciones suprimidos, siendo entonces tan solo un rectángulo con el nombre de la clase.



- **Interfaz:** colección de operaciones que especifican un servicio de una clase o componente, mostrando el comportamiento visible externamente de ese elemento. Una interfaz contiene sólo las especificaciones de las operaciones, es decir su signatura, pero no la implementación.



- **Colaboración:** define una interacción y representa un conjunto de elementos del modelo que colaboran para proporcionar un comportamiento cooperativo mayor que la suma de los comportamientos de sus elementos. Por lo tanto, las colaboraciones tienen tanto dimensión estructural como de comportamiento



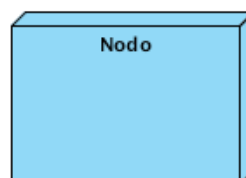
- **Caso de uso:** descripción de un conjunto de secuencias de acciones que un sistema ejecuta y que produce un resultado observable de interés para un usuario particular. Un caso de uso se utiliza para estructurar los aspectos de comportamiento en un modelo. Un caso de uso es realizado por una colaboración.



- **Clase activa:** Clase cuyos objetos tienen uno o más procesos o hilos de ejecución, y por lo tanto pueden dar origen a actividades de control.
- **Componente:** Parte física y reemplazable de un sistema que representa típicamente el empaquetamiento físico de diferentes elementos lógicos, como clases, interfaces y colaboraciones.



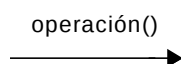
- **Nodo:** Elemento físico que existe en tiempo de ejecución y representa un recurso computacional que generalmente dispone de memoria y capacidad de procesamiento. (Impresoras, PCs, ...)



36.2.2.2 Elementos de comportamiento

Los elementos de comportamiento son las partes dinámicas de los modelos. Representan comportamiento en el tiempo y en el espacio. Hay dos tipos de elementos de comportamiento:

- **Interacciones:** una interacción es un comportamiento que comprende un conjunto de mensajes intercambiados entre un conjunto de objetos, dentro de un contexto particular para alcanzar



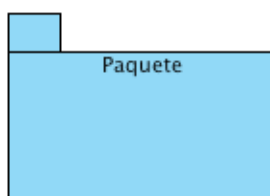
un propósito específico. El comportamiento de una sociedad de objetos o una operación individual puede especificarse mediante una interacción. Una interacción involucra otros elementos, incluyendo mensajes, secuencias de acción (el comportamiento invocado por un mensaje) y enlaces (conexiones entre objetos).

- **Máquinas de estados:** una máquina de estados especifica las secuencias de estados por las que pasa un objeto o una interacción durante su vida en respuesta a eventos. El comportamiento de una clase individual o una colaboración de clases puede especificarse con una máquina de estados. Una máquina de estados involucra otros elementos, incluyendo estados, transiciones (el flujo de un estado a otro), eventos (que disparan una transición) y actividades (la respuesta a una transición).



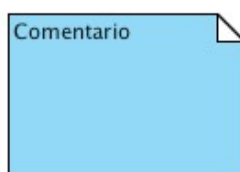
36.2.2.3 Elementos de agrupación

Los elementos de agrupación son las partes organizativas de los modelos de UML. Sólo hay un elemento de agrupación: el **paquete**, que es un mecanismo para organizar los elementos en grupos. Puede contener elementos estructurales, elementos de comportamiento e incluso otros paquetes.



36.2.2.4 Elementos de anotación

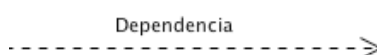
Los elementos de anotación son la parte explicativa de los modelos de UML. Son comentarios que se pueden aplicar para describir, clarificar y hacer observaciones sobre cualquier elemento de un modelo. El principal elemento de anotación es la nota, que es simplemente un símbolo para mostrar restricciones y comentarios junto a un elemento o una colección de elementos.



36.2.3 Relaciones

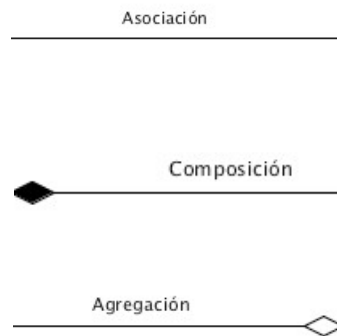
Hay cuatro tipos de relaciones en UML:

- **Dependencia:** es una relación semántica entre dos elementos, en la cual un cambio a un elemento (el elemento independiente) puede afectar a la semántica del otro elemento (el elemento dependiente).

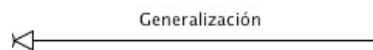


- **Asociación:** Una **asociación** es una relación estructural que describe un conjunto de enlaces, los cuales son conexiones entre objetos. La **agregación** es un tipo especial de asociación, que representa una relación estructural entre un todo y sus partes. Gráficamente, una asociación se representa como una línea continua, posiblemente dirigida, que a veces incluye una etiqueta, y a menudo incluye otros adornos, como la multiplicidad y los nombres de rol. La agregación se representa mediante un rombo situado en la parte del todo. La **composición** es un tipo de agregación en el que cada parte

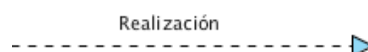
solo puede pertenecer a un todo y no puede existir la parte sin el todo. Se representa igual que la agregación, solo que el rombo está relleno.



- **Generalización:** Una generalización es una relación de especialización /generalización en la cual los objetos del elemento especializado (el hijo) pueden sustituir a los objetos del elemento general (el padre). De esta forma, el hijo comparte la estructura y el comportamiento del padre.



- **Realización:** Una realización es una relación semántica entre clasificadores, en donde un clasificador especifica un contrato que otro clasificador garantiza que cumplirá. Se pueden encontrar relaciones de realización en dos sitios: entre interfaces y las clases y componentes que las realizan, y entre los casos de uso y las colaboraciones que los realizan.



36.2.4 Diagramas

Un diagrama es la representación gráfica de un conjunto de elementos, en general visualizado como un grafo conexo de nodos (elementos) y arcos

(relaciones). Los diagramas se dibujan para visualizar un sistema desde diferentes perspectivas. Se pueden agrupar en dos bloques en función de si vemos el modelo de forma estática (estructural) o de forma dinámica (comportamiento). La primera incluye los diagramas de despliegue, componentes, clases y objetos, mientras que la segunda incluye los diagramas de estados, actividades, secuencia, colaboración y casos de uso. Pasamos a ver cada uno de ellos.

36.2.4.1 Diagrama de casos de uso.

Un Diagrama de Casos de Uso muestra la relación entre los actores y los casos de uso del sistema y representa la funcionalidad que ofrece el sistema en lo que se refiere a su interacción externa. Un caso de uso es una secuencia de acciones realizadas por el sistema, que producen un resultado observable y valioso para un usuario en particular, es decir, representa el comportamiento del sistema con el fin de dar respuestas a los usuarios y sirve para describir ante los usuarios dicho sistema.

La especificación de un caso de uso recoge, en un primer momento, una descripción general. Esta descripción reflejará posiblemente uno o varios requisitos funcionales del sistema o formará parte de algún requisito. Se puede completar la descripción definiendo cuáles son las precondiciones y postcondiciones. También se pueden enumerar los diferentes escenarios del caso de uso si los tuviese y dar una breve descripción de ellos. Los escenarios son los distintos caminos por los que puede evolucionar un caso de uso, dependiendo de las condiciones que se van dando en su realización.

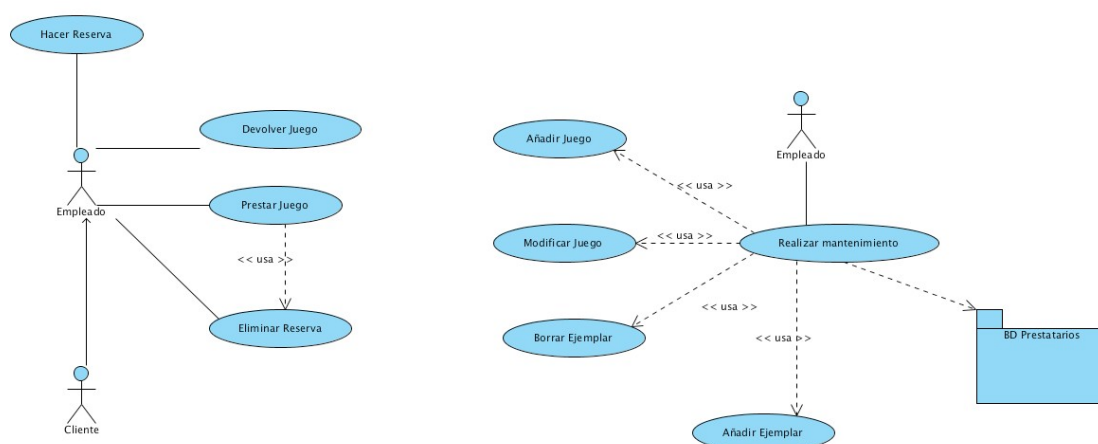
Están formados por dos elementos: **actores**, que es algo o alguien que se encuentra fuera del sistema y que interactúa con él y puede referirse tanto a actores que sean personas como a otro tipo de actores (otros sistemas, sensores, etc), y **casos de uso**, que representa el comportamiento que ofrece el sistema de información desde el punto de vista del usuario,

además se representan las relaciones entre los casos de uso. Opcionalmente también podría incluir paquetes que agruparían otras partes del sistema.

Entre los elementos de un diagrama de casos de uso se pueden dar tres tipos de relaciones:

- **Comunica:** Es la relación entre un actor y un caso de uso, que denota la participación del actor en dicho caso de uso.
- **Usa:** Relación de dependencia entre dos casos de uso que denota la inclusión del comportamiento de un escenario en otro. Se usa cuando se quiere reflejar un comportamiento común en varios casos de uso.
- **Extiende:** Relación de dependencia entre dos casos de uso en el que uno es una especialización del otro, existiendo en este caso una extensión de la funcionalidad.

Se representan como una línea que une a los dos casos de uso relacionados, con una flecha en forma de triángulo y con una etiqueta <<extiende>>, <<usa>> o <<comunica>> según sea el tipo de relación.



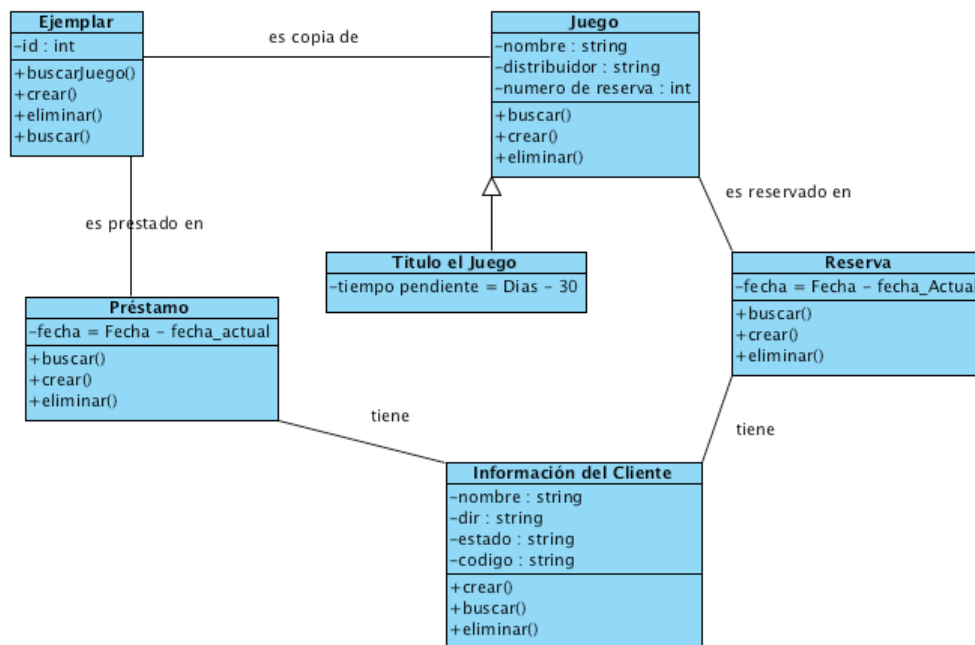
36.2.4.2 Diagrama de clases

El objetivo principal de este modelo es la representación de los aspectos estáticos del sistema, utilizando diversos mecanismos de abstracción

(clasificación, generalización, agregación). Recoge las clases de objetos y sus asociaciones. En este diagrama se representa la estructura y el comportamiento de cada uno de los objetos del sistema y sus relaciones con los demás objetos, pero no muestra información temporal. Nos sirve para visualizar las relaciones entre las clases que involucran el sistema, las cuales pueden ser asociativas, de herencia y de uso.

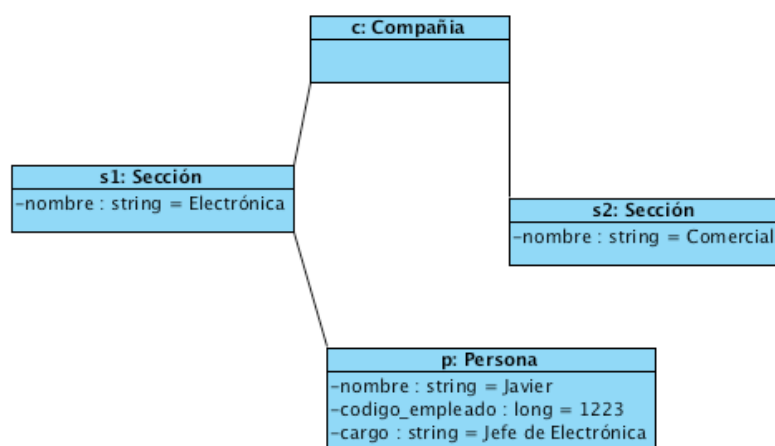
El modelo está formado por:

- **Clases:** Se representa como una caja dividida en tres zonas. En la zona superior se pone el nombre de la clase. En el centro se colocan los atributos (características) de la clase con el formato: *“visibilidad nombre : tipo = valor-inicial { propiedades }”*. La visibilidad será en general publica (+), privada (-) o protegida. En la zona inferior se incluye una lista con las operaciones que proporciona la clase. Cada operación aparece en una línea con formato: *“visibilidad nombre (lista-de-parámetros): tipo-devuelto { propiedad }”*
- **Relaciones:** Asociaciones, agregaciones, composiciones, dependencias o herencia. Se pueden documentar con una descripción de su propósito, su multiplicidad, navegabilidad o rol de cada una de las clases en la relación.
- **Interfaces**
- **Paquetes**



36.2.4.3 Diagrama de objetos.

Modelan las instancias de elementos contenidos en los diagramas de clases. Muestra un conjunto de objetos y sus relaciones en un momento concreto. Para mostrar el estado de un objeto, se indica el valor de sus atributos y sus objetos agregados. Los diagramas de objetos no muestran multiplicidad ni roles, aunque su notación es similar a la de los diagramas de clase.



36.2.4.4 Diagramas de Interacción.

Los **diagramas de interacción** se utilizan para modelar los aspectos dinámicos del sistema y mostrar un patrón de interacción entre objetos. Mientras que un diagrama de casos de uso presenta una visión externa del sistema, la funcionalidad de dichos casos de uso se recoge como un flujo de eventos. Por otra parte los diagramas de clases y los de objeto representan información estática, no obstante en un sistema funcional los objetos interactúan entre sí y tales eventos o interacciones suceden en el tiempo. Este flujo de eventos puede recogerse en una especificación texto acompañada de distintos escenarios especificados mediante diagramas de interacción donde cada diagrama será una visión gráfica de un escenario. Existen dos tipos de diagramas de interacción: **secuencia** y **colaboración**. Ambos son equivalentes. La diferencia entre ellos está en los aspectos que resaltan. Los diagramas de secuencia destacan el orden temporal de los mensajes, mientras que los diagramas de colaboración destacan la organización estructural de los objetos.

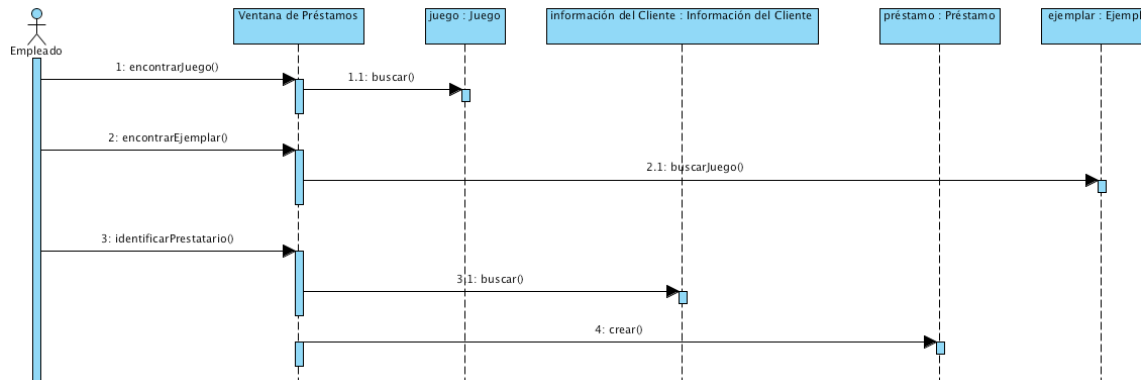
36.2.4.4.1 Diagramas de secuencia

Muestran las interacciones entre objetos ordenadas en **secuencia temporal**. Muestra los objetos que se encuentran en el escenario y la secuencia de mensajes intercambiados entre los objetos para llevar a cabo la funcionalidad descrita por el escenario. Se hace un diagrama de secuencia por cada caso de uso o para una parte del mismo.

El eje vertical representa el tiempo, y en el eje horizontal se colocan los objetos y actores participantes en la interacción, sin un orden prefijado. Cada objeto o actor tiene una línea vertical, y los mensajes se representan mediante flechas entre los distintos objetos. El tiempo fluye de arriba abajo. Se pueden emplear etiquetas para especificar restricciones de tiempo, descripciones de acciones, etc; bien en el margen izquierdo o junto al mensaje o activación a la que se refiera.

Los conceptos más importantes relacionados con los diagramas de secuencia son:

- **Línea de vida** de un objeto: representa la vida del objeto durante la interacción. El objeto se representa como una línea vertical punteada con un rectángulo de encabezado con el nombre del objeto y de su clase.
- **Activación:** Muestra el período de tiempo durante el cual el objeto se encuentra desarrollando alguna operación. Se denota por un rectángulo sobre la línea de vida del objeto.
- **Mensaje:** Se muestra mediante una línea sólida dirigida desde el objeto que emite el mensaje hacia el que lo ejecuta.
- **Caminos alternativos** de ejecución y concurrencia: Pueden representar condiciones en la ejecución o diferentes hilos de ejecución (threads)

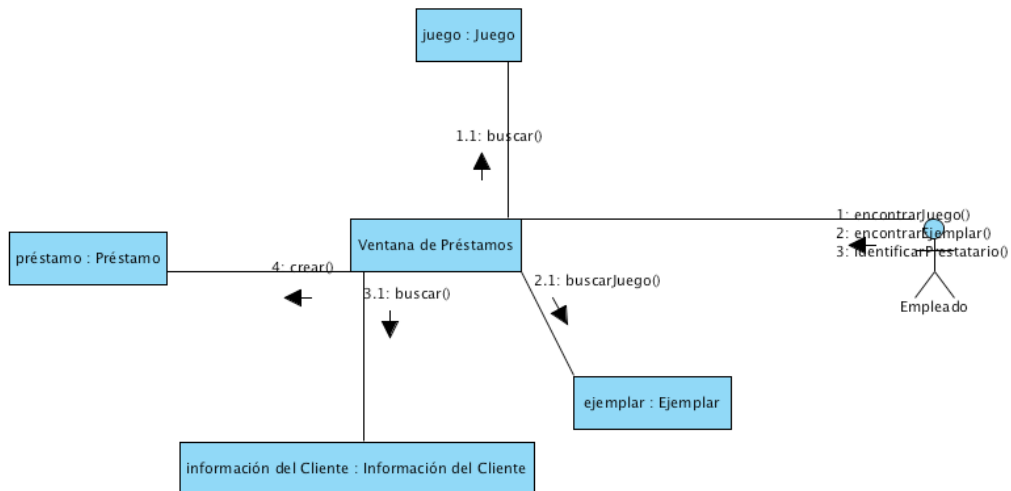


36.2.4.4.2 Diagramas de colaboración

Los diagramas de colaboración suponen una forma alternativa al diagrama de secuencia para mostrar un escenario. Muestra la misma información que un diagrama de secuencia pero de forma diferente. En los diagramas de colaboración no existe una secuencia temporal. Los elementos de un sistema trabajan en conjunto para cumplir con los objetivos del sistema y es esta colaboración la que se refleja. Este diagrama resalta la **organización estructural** de los objetos que envían y reciben los mensajes. Este tipo de diagrama muestra un conjunto de objetos, enlaces entre ellos y los mensajes que intercambian.

A diferencia de los Diagramas de Secuencia, los Diagramas de Colaboración muestran

las relaciones entre los roles de los objetos. La secuencia de los mensajes debe determinarse explícitamente mediante números de secuencia.



36.2.4.5 Diagramas de estados.

Representan los estados que puede tomar un componente o un sistema y muestra los eventos que implican el cambio de un estado a otro. Los diagramas de estado son útiles, entre otras cosas, para indicar los eventos del sistema en los casos de uso y para ilustrar qué eventos pueden cambiar el estado de los objetos de una clase. Los dos elementos principales en estos diagramas son los estados y las posibles transiciones entre ellos.

- El **estado** de un componente o sistema representa algún comportamiento que es observable externamente y que perdura durante un periodo de tiempo finito, podemos verlo también como un periodo en el que se satisface una condición. Viene dado por el valor de uno o varios atributos que lo caracterizan en un momento dado.
- Una **transición** es un cambio de estado producido por un evento y refleja los posibles caminos para llegar a un estado final desde un estado inicial. Refleja que un objeto en el primer estado puede entrar al segundo y ejecutar ciertas operaciones, cuando un evento ocurre y si ciertas condiciones son satisfechas.

Una transición se representa gráficamente como una línea continua dirigida desde el estado origen hasta el estado destino. Puede venir acompañada por un texto con el siguiente formato:

nombre-evento ‘(‘lista-argumentos‘)’ ‘[‘guard-condition‘] ‘/’
expresión-acción ‘^’ cláusula-envío

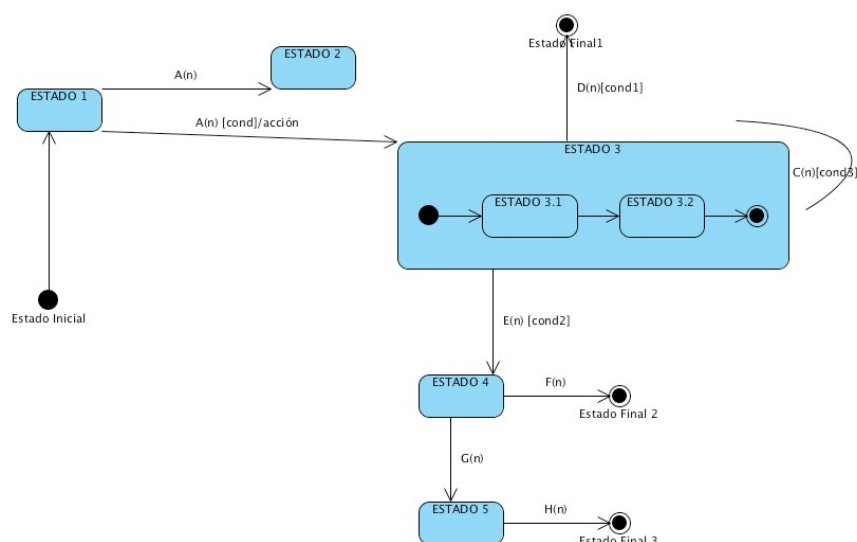
- *nombre-evento* y *lista-argumentos* describen el evento que da lugar a la transición y forman lo que se denomina event-signature.
- *guard-condition* es una condición (expresión booleana) adicional al evento y necesaria para que la transición ocurra. Si la guard-condition se combina con una event-signature, entonces para que la transición se dispare tienen que suceder dos cosas: debe ocurrir el evento y la condición booleana debe ser verdadera.
- *expresión-acción* es una expresión procedimental que se ejecuta cuando se dispara la transición. Es posible tener una o varias expresión-acción en una transición de estado, las cuales se delimitan con el carácter “/”.
- *cláusula-envío* es una acción adicional que se ejecuta con el cambio de estado, por ejemplo, el envío de eventos a otros paquetes o clases. Este tipo especial de acción tiene una sintaxis explícita para enviar un mensaje durante la transición entre dos estados. La sintaxis consiste de una expresión de destino y de un nombre de evento, separados por un punto.

Desde un estado pueden surgir varias transiciones en función del evento que desencadena el cambio de estado, teniendo en cuenta que, las transiciones que provienen del mismo estado no pueden tener el mismo evento, salvo que exista alguna condición que se aplique al evento. Un diagrama de estados puede representar ciclos continuos o bien una vida

finita, en la que hay un estado inicial de creación y un estado final de destrucción (del caso de uso o del objeto).

Un sistema sólo puede tener un **estado inicial**, que se representa mediante una transición sin etiquetar al primer estado normal del diagrama. En ningún caso puede haber una transición dirigida al estado inicial. El **estado final** representa que un componente ha dejado de tener cualquier interacción o actividad. No se permiten transiciones que partan del estado final. Puede haber varios estados finales en un diagrama.

Otros dos elementos que ayudan a clarificar estos diagramas son las acciones y las actividades. Una acción es una operación instantánea asociada a un evento, cuya duración se considera no significativa y que se puede ejecutar: dentro de un estado, al entrar en un estado o al salir del mismo. Una actividad es una operación asociada a un estado que se ejecuta durante un intervalo de tiempo hasta que se produce el cambio a otro estado.



36.2.4.6 Diagrama de actividades.

Las actividades que ocurren dentro de un caso de uso dentro del comportamiento de un objeto se dan, normalmente, en secuencia. Este tipo de diagrama puede considerarse un caso especial del diagrama de estados en el cual casi todos los estados son estados acción (identifican una acción que se ejecuta al entrar en él) y casi todas las transiciones evolucionan al término de dicha acción. La interpretación de un diagrama de actividades depende de la perspectiva considerada: en un diagrama conceptual, la actividad es alguna tarea que debe ser realizada; en un diagrama de especificación o de implementación, la actividad es un método de una clase. Se suelen utilizar para modelar los pasos de un algoritmo.

Los diagramas de actividad pueden visualizar, especificar y documentar la dinámica de un conjunto de objetos. También se pueden usar para modelar el flujo de control de una operación. Mientras que los diagramas de interacción enfatizan el flujo de control de un objeto a otro, los diagramas de actividad subrayan el flujo de control de una actividad a otra.

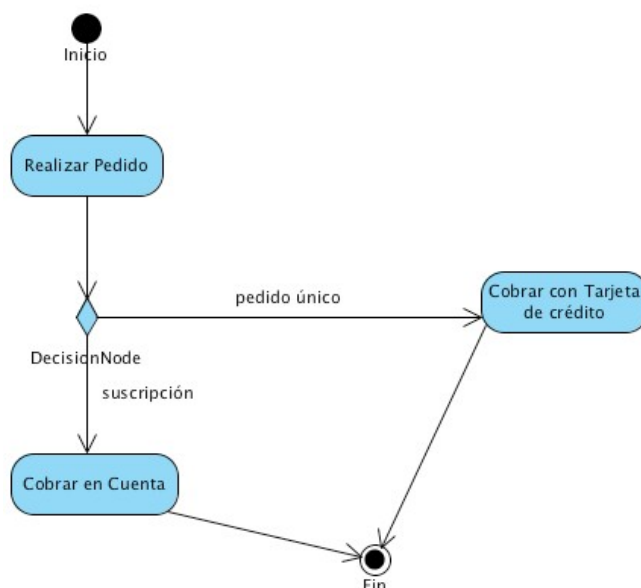
El principal inconveniente de los diagramas de actividad es que no indican explícitamente qué objetos ejecutan qué actividades ni tampoco la forma en que el servicio de mensajería trabaja entre ellos. Para mostrar tales interacciones de forma clara son necesarios los diagramas de interacción, los cuales son más utilizados en la práctica.

En los diagramas de actividad, las decisiones se representan mediante una transición múltiple que sale de un estado donde cada camino tiene una etiqueta distinta. Se presenta mediante un rombo al cual llega la transición del estado origen y del cual salen las múltiples transiciones de los estados destino. Los diagramas de actividad son útiles cuando queremos describir un comportamiento paralelo, o cuando queremos mostrar qué comportamientos interactúan en varios casos de uso.

Un diagrama de actividades contiene:



- *Estados de actividad y Estados de acción:* La representación de ambos es un rectángulo con las puntas redondeadas, en cuyo interior se representa bien una actividad o bien una acción.
 - o Un estado que represente una acción es atómico, lo que implica que la ejecución puede considerarse instantánea y no se puede interrumpir.
 - o Un estado actividad puede descomponerse en más sub-actividades representadas a través de otros diagramas de actividades. Además estos estados pueden ser interrumpidos y tardan cierto tiempo en completarse.
 - o En los estados de actividad podemos encontrar otros elementos adicionales como son: acciones de entrada y de salida del estado en cuestión.
- *Transiciones:* Reflejan el paso de un estado a otro, bien sea de actividad o de acción. Esta transición se produce como resultado de la finalización del estado del que parte el arco dirigido que marca la transición.



36.2.4.7 Diagramas de implementación.

Un diagrama de implementación muestra las dependencias entre las partes de código del sistema (**diagrama de componentes**) o la estructura del sistema en ejecución (**diagrama de despliegue**). Los diagramas de componentes se utilizan para modelar la vista de implementación estática de un sistema, mientras que los diagramas de despliegue se utilizan para modelar la vista de despliegue estática.

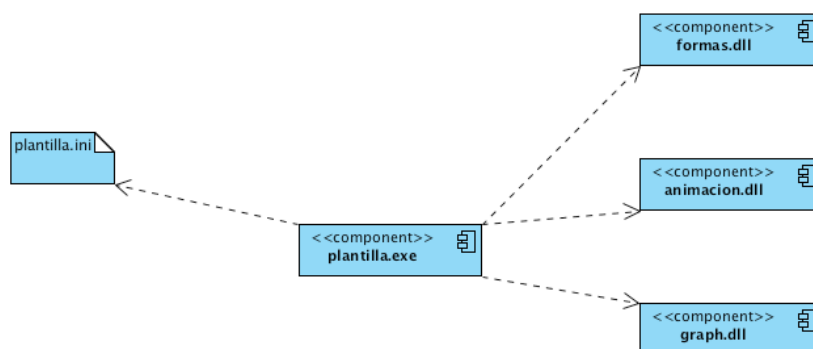
36.2.4.7.1 Diagrama de componentes.

Muestra las organizaciones y dependencias lógicas entre componentes software, sean éstos componentes de código fuente, binarios, documentos, archivos o ejecutables. Los diagramas de componentes representan cualquier tipo de elemento software que participe en el desarrollo de un sistema informático y pueden ser simples archivos, librerías, etc. Los diagramas de componentes pueden contener paquetes para organizar los elementos.

Dado que los diagramas de componentes muestran los componentes software que constituyen una parte reusable, sus interfaces, y sus interrelaciones, en muchos aspectos se puede considerar como un diagrama de clases a gran escala. Cada componente del diagrama debe ser documentado con un diagrama de componentes más detallado, un diagrama de clases, o un diagrama de casos de uso.

Tipos de componentes:

- *Componentes de despliegue:* componentes necesarios y suficientes para formar un sistema ejecutable, como pueden ser las bibliotecas dinámicas y ejecutables.
- *Componentes producto del trabajo:* estos componentes son básicamente productos que quedan al final del proceso de desarrollo. Consisten en cosas como archivos de código fuente y de datos a partir de los cuales se crean los componentes de despliegue.
- *Componentes de ejecución:* son componentes que se crean como consecuencia de un sistema en ejecución.



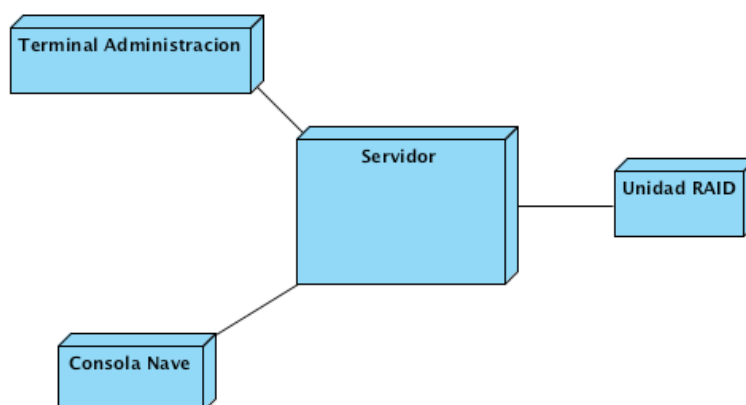
36.2.4.8 Diagrama de despliegue

Muestra las relaciones físicas (arquitectura física) entre los componentes hardware y software en el sistema final, es decir, la configuración de los

elementos de procesamiento en tiempo de ejecución y los componentes software (proceso y objetos que se ejecutan en ellos). Muestran la configuración en funcionamiento del sistema, incluyendo hardware y software. Cubre principalmente la distribución, entrega e instalación de las partes que configuran el sistema físico, y se suelen utilizar para modelar sistemas empotrados, sistemas cliente-servidor y sistemas distribuidos.

En un diagrama de despliegue un nodo representa un elemento físico que existe en tiempo de ejecución y que representa un recurso computacional. Los nodos se conectan mediante asociaciones de comunicación, tales como enlaces de red, conexiones TCP/IP, etc.

Los diagramas de despliegue son los complementos de los diagramas de componentes que, unidos, proveen la vista de implementación del sistema.



BIBLIOGRAFÍA:

- Ingeniería del Software. Un enfoque práctico. ROGER S. PRESSMAN. Ed. McGraw Hill
- Aprendiendo UML en 24 horas. Joseph Schmuller
- Systems analysis and design with UML: an object-oriented approach. Alan Dennis.
- Utilización de UML en ingeniería del software con objetos y componentes. Perdita Stevens.
- Análisis y diseño orientado a objetos con UML y el proceso unificado. Stephen Schach.
- Learning UML. Sinan Si Alhir.
- Métrica 3 - Técnicas y Prácticas. Ministerio de Administraciones Públicas
- Resumen de términos de UML - Desconocido.
- Curso de OO dirigido por la introducción a la ambigüedad. Anexo 1 : UML
http://is.ls.fi.upm.es/docencia/proyecto/docs/curso/12Anexo_1_UML.doc
- Temario de las pruebas selectivas para ingreso en el Cuerpo Superior de Sistemas y Tecnologías de la Información de la Administración del Estado. ASTIC.

Autor: Francisco Javier Rodríguez Martínez

Subdirector de la Escuela Superior de Ingeniería Informática.

Universidad de Vigo.

37. TÉCNICAS DE PROGRAMACIÓN. PROGRAMACIÓN ESTRUCTURADA. PROGRAMACIÓN ORIENTADA A OBJETOS. INGENIERÍA INVERSA Y REINGENIERÍA.

Tema 37. Técnicas de programación. Programación Estructurada. Programación orientada a objetos. Ingeniería inversa y reingeniería.

INDICE

- 37.1 Técnicas de programación
 - 37.1.1 Clasificación y evolución de los lenguajes de programación
- 37.2 Programación Estructurada
 - 37.2.1 Recursos abstractos
 - 37.2.2 Diseño descendente
 - 37.2.3 Estructuras básicas
- 37.3 Programación orientada a objetos
- 37.4 Ingeniería inversa
 - 37.4.1 Modelo cíclico
 - 37.4.2 Modelo de herradura
 - 37.4.3 Modelo del IEEE
 - 37.4.4 Método Análisis de Opciones para Reingeniería (OAR)

37.1 Técnicas de programación

Un **lenguaje de programación** es un lenguaje artificial diseñado para representar expresiones e instrucciones de forma que las entienda un ordenador. Aunque los lenguajes de programación son más sencillos que los lenguajes naturales, poseen también un alfabeto (símbolos básicos) con los que se construye el vocabulario (tokens, palabras reservadas), que se combinan según unas reglas sintácticas formando expresiones y sentencias, cuyo significado viene dado por la semántica del lenguaje. Se llama **programa** al conjunto de instrucciones escritas en un lenguaje de programación, destinadas a realizar una tarea. De forma general, un programa, tomará unos datos de entrada y devolverá unos datos de salida. Se dice que lo que hace el programa es implementar un **algoritmo**, que es un conjunto finito de instrucciones que se deben seguir para realizar una determinada tarea.

Entendemos la **programación** como *la planificación, proyección, desarrollo e implementación de la resolución de un problema*, la que abarca obviamente a la creación del algoritmo. Un profesional en la

programación debe encarar la solución del problema de forma tal que su producto sea útil ahora y en el futuro, estando o no él en el centro de desarrollo. Para lograr esto, se debe tener muy presentes las posibles modificaciones futuras del mismo.

Las características que debe tener un programa son:

- 1) **Claridad algorítmica:** Que sea claro significa, que su resolución algorítmica sea sencilla, que esté correctamente estructurado, y que resulte de fácil comprensión.
- 2) **Legibilidad:** Que sea legible significa que cuando se codificó se eligieron bien los nombres de los objetos utilizados, se agregaron comentarios para indicar lo que se iba haciendo y se estructuró bien el código para resaltar el contenido semántico sobre lo sintáctico.
- 3) **Modificabilidad:** Que sea fácilmente modificable, implica que cualquier modificación del problema que genere una agregación, supresión o cambio de alguna de sus partes, no debe obligar a cambiar todo el programa, sino sólo esa parte.

En sus inicios la programación no seguía ninguna metodología, y teníamos cientos o miles de líneas de código, hechas por un programador, y que solo él modificaba. En esta época los profesionales programadores solían estar vinculados a la empresa y no era frecuente que abandonaran la misma. Los programas no tenían estructura definida. Las modificaciones en el programa suponían un coste importante ya que había que revisar el código casi línea a línea para buscar donde hacer las modificaciones. Además, estos cambios no dejaban de ser un riesgo importante debido a los posibles efectos colaterales. Esto derivó en lo que se denominó crisis del software.

Para tratar de dar respuesta a la crisis del software, en los años 60 surgieron técnicas de programación como la **programación modular** y la **programación estructurada**. Ambas técnicas parten de la idea del diseño descendente (también llamado refinamiento sucesivo), que consiste en dividir un problema complejo en varios problemas mas

pequeños y más sencillos de resolver. Se comienza planteando el problema y su solución a un nivel alto y luego se sigue descomponiendo el problema general en otros problemas más sencillos de resolver. Este proceso continua hasta que llegamos a pequeños problemas, fácilmente implementables en código llamados módulos. Un módulo es un conjunto de acciones (un bloque del código del algoritmo total) junto a un conjunto de especificaciones de datos para realizar una tarea específica. Cuando se utiliza esta técnica, la solución queda dividida en varias partes: un algoritmo principal y uno o varios subalgoritmos (los módulos). La ejecución se inicia en el algoritmo principal y desde este se invoca a los módulos. La programación estructurada hace uso de la programación modular, además de otras características que se verán en un apartado posterior.

También como respuesta a la crisis del software surgieron en los años 60 los conceptos de la orientación a objetos, que tenían como principal objetivo reducir la complejidad del desarrollo y mantenimiento del software. Dado que la tecnología no estaba acorde con su implementación, se mantuvo sólo como concepto hasta su gran expansión a finales de los 80. La **programación orientada a objetos** no supone una ruptura radical frente al paradigma de la programación estructurada / imperativa predominante hasta su aparición, sino que supone una evolución. Frente a la programación estructurada, cuyos programas separan datos y estructuras de datos de funciones y procedimientos, la programación orientada a objetos encapsula en una misma abstracción estos dos elementos clásicos de los sistemas de información: datos y los procesos. Esto lo hace a través de una nueva abstracción: el objeto. La orientación a objetos consiste en una visión de los objetos como entidades activas que ejecutan acciones sobre sus propios datos en respuesta a peticiones externas. Además, no considera a unos y a otros (datos y procesos) como realidades aisladas susceptibles de analizarse e implantarse por separado. Los objetos tratan de abstraer características comunes que podrán compartirse entre varias aplicaciones y reutilizarse todo lo posible. La

creación de un nuevo sistema consiste esencialmente en una labor de ensamblado de objetos preexistentes, completada con el desarrollo de un porcentaje reducido de nuevos objetos, que a su vez alimentarían las correspondientes librerías para poder ser utilizados en los próximos sistemas.

El paradigma de ensamblar componentes y escribir código para hacer que estos componentes funcionen se conoce como **Desarrollo de Software Basado en Componentes**. Un componente es una pieza de código preelaborado que encapsula alguna funcionalidad expuesta a través de interfaces estándar. Cada componente es diseñado para acoplarse perfectamente con sus pares, las conexiones son estándar y el protocolo de comunicación está ya preestablecido. Al unirse las partes, obtenemos un sistema completo.

Por último, la **programación orientada a aspectos** surge para resolver el problema de la "dispersión de código" existente en la programación orientada a objetos para aquellos aspectos de un programa que no tienen que ver directamente con el dominio de negocio del problema como por ejemplo, la gestión de conexiones, logs, trazas de mensajes, sincronización y concurrencia, manejo de errores y excepciones, etc. Este código está disperso a lo largo de diferentes objetos del programa (siendo buena parte de las veces el mismo código repetido) lo que dificulta su mantenimiento. Esta metodología de programación intenta separar los componentes y los aspectos unos de otros, proporcionando mecanismos que hagan posible abstraerlos y componerlos para formar todo el sistema. Es un desarrollo que sigue al paradigma de la orientación a objetos, y como tal, soporta la descomposición orientada a objetos, además de la procedimental y la descomposición funcional. Pero, a pesar de esto, no se puede considerar como una extensión de la programación orientada a objetos POO, ya que puede utilizarse con los diferentes estilos de programación ya mencionados.

37.1.1 Clasificación y evolución de los lenguajes de programación

Para explicar la evolución de los lenguajes de programación hablamos de generaciones:

- **Primera generación.** Lenguaje máquina. Empieza en los años 1940-1950. Los programas están hechos de secuencias de unos y ceros que el computador es capaz de interpretar. Es el único que es directamente entendible por el ordenador, sin necesidad de traducción. Estos se consideran como de bajo nivel por que no existe un [programa](#) de [codificación](#) menos complicado que el que utiliza los símbolos binarios 1 y 0.
- **Segunda generación.** Ensamblador. Fines de los años 50. Se usan nemotécnicos que sustituyen los unos y ceros. Siguen siendo dependientes de la máquina. El código fuente es traducido al lenguaje máquina mediante traductores. Aún se utilizan estos lenguajes cuando interesa un nivel máximo de eficiencia en la ejecución o cuando se requieren manipulaciones intrincadas. Al igual que los lenguajes máquina, los lenguajes ensambladores son únicos para una computadora particular. Esta dependencia de la computadora los hace ser lenguajes de bajo nivel.
- **Tercera generación.** Lenguajes de alto nivel. Años 60. Lenguajes estructurados con comandos cercanos al lenguaje natural. Fueron creados para facilitar el proceso de programación. Los comandos se asemejan a palabras de uso común. Los lenguajes de esta generación se dividen en tres categorías, según se orienten a:
 - o *procedimientos*: Requieren que la codificación de las instrucciones se haga en la secuencia en que se deben ejecutar para solucionar el problema. A su vez se clasifican en:
 - científicos (FORTRAN), empresariales (COBOL), y de uso general (BASIC).

- Todos estos lenguajes permiten señalar cómo se debe efectuar una tarea a un nivel mayor que en los lenguajes ensambladores. Hacen énfasis los procedimientos o las matemáticas implícitas, es decir en lo que se hace (la acción).
 - o *problemas*: Están diseñados para resolver un conjunto particular de problemas y no requieren el detalle de la programación que los lenguajes orientados a procedimientos. Hacen hincapié en la entrada y la salida deseadas.
 - o *objetos*: El énfasis se hace en el objeto de la acción. Los beneficios que aportan estos lenguajes incluyen una mayor productividad del programador y claridad de la lógica, además de ofrecer la flexibilidad necesaria para manejar problemas abstractos de programación.
-
- **Cuarta generación:** Nacen los lenguajes 4G. Son lenguajes de propósito específico, orientados a resolver problemas específicos, como generación de informes, pantallas, consultas de bases de datos,... Se caracterizan por tener una mayor facilidad de programación comparados con los de tercera generación, permitiendo la creación de prototipos rápidamente puesto que generan el código fuente automáticamente a través de asistentes, plantillas, etc. Su característica distintiva es el énfasis en especificar qué es lo que se debe hacer, en vez de cómo ejecutar una tarea. Las especificaciones de los programas se desarrollan a un nivel más alto que en los lenguajes de la generación anterior. La característica distintiva es ajena a los procedimientos, y el programador no tiene que especificar cada paso para terminar una tarea o procesamiento. Las características generales de los lenguajes de cuarta generación son:

- o Uso de frases y oraciones parecidas al inglés para emitir instrucciones;
- o No operan por procedimientos, por lo que permiten a los usuarios centrarse en lo que hay que hacer, no en cómo hacerlo;
- o Al hacerse cargo de muchos de los detalles de cómo hacer las cosas, incrementan la productividad.

Hay dos tipos de lenguajes de cuarta generación, según se orienten:

- o A la producción: Diseñados sobre todo para profesionales en la computación.
 - o Al usuario: Diseñados sobre todo para los usuarios finales, que pueden escribir programas para hacer consultas en una base de datos y para crear sistemas de información.
- **Quinta generación:** Lenguajes Naturales. Son lenguajes orientados a la inteligencia artificial y los sistemas expertos. En lugar de sólo ejecutar órdenes, el objetivo de los sistemas es anticipar las necesidades de los usuarios. Están aún en desarrollo.

Los lenguajes de programación se pueden clasificar según muchos criterios:

- Según el **nivel de abstracción**:
 - o **Lenguajes máquina y de bajo nivel:** el lenguaje o código máquina está formado por cadenas binarias entendibles directamente por la máquina. No necesitan traducción y son muy rápidos. El lenguaje ensamblador permite al menos escribir las instrucciones utilizando una notación simbólica, utilizar direcciones de memoria relativas y no absolutas, insertar comentarios. Necesitan de un traductor para convertir a código máquina, traducción que resulta casi trivial debido a su bajo nivel. Estos lenguajes son completamente dependientes de la máquina. En general se utiliza este tipo de lenguaje para programar controladores (drivers).

- **Ventajas:**
 - Mayor adaptación al equipo.
 - Posibilidad de obtener la máxima velocidad con mínimo uso de memoria.
- **Inconvenientes:**
 - Imposibilidad de escribir código independiente de la máquina.
 - Mayor dificultad en la programación y en la comprensión de los programas.
- o **Lenguajes de medio nivel:** aquí se encontraría el lenguaje C. El lenguaje C permite un manejo abstracto e independiente de la máquina (lo que lo acercaría al alto nivel), pero sin perder su característica de potencia, eficiencia y cercanía a la máquina (uso directo de punteros, etc.).

Estos lenguajes son clasificados muchas veces de alto nivel, pero permiten ciertos manejos de bajo nivel. Son precisos para ciertas aplicaciones como la creación de sistemas operativos, ya que permiten un manejo abstracto (independiente de la máquina, a diferencia del ensamblador), pero sin perder mucho del poder y eficiencia que tienen los lenguajes de bajo nivel.
- o **Lenguajes de alto nivel:** son independientes de la arquitectura de la máquina y se aproximan al lenguaje natural, disponen de gran diversidad de instrucciones potentes, y usan una sintaxis similar al lenguaje natural lo que facilita su comprensión. Aquí estarían básicamente el resto de los lenguajes conocidos, de hecho, se puede decir que el principal problema que presentan los lenguajes de alto nivel es la gran cantidad de ellos que existen actualmente en uso.

- Según la **forma de ejecución**



- o **Compilados:** una vez escrito el programa, éste se traduce a partir de su código fuente por medio de un compilador en un archivo ejecutable para una determinada plataforma, este archivo se llama ejecutable. El compilador lee el código fuente y almacena el ejecutable resultado de la traducción para posibles ejecuciones futuras. Un programa escrito en un lenguaje compilado posee la ventaja de no necesitar un programa anexo para ser ejecutado una vez que ha sido compilado. Además, como sólo es necesaria una traducción, la ejecución se vuelve más rápida. Sin embargo, no es tan flexible como un programa escrito en lenguaje interpretado, ya que cada modificación del archivo fuente (el archivo comprensible para los seres humanos: el archivo a compilar) requiere de la compilación del programa para aplicar los cambios. Ejemplos: C, C++, Pascal, Kilix, Delphi, ...
- o **Interpretados:** necesitan de un intérprete para ejecutar el código escrito en los programas. Las instrucciones se traducen o interpretan una a una en tiempo de ejecución a un lenguaje intermedio o lenguaje máquina. En la ejecución de un lenguaje interpretado se van leyendo las líneas del código fuente y traduciéndolas a medida que va siendo necesario. Cada vez que se lee una instrucción se interpreta y se ejecuta, generando su código máquina “al vuelo”. Ejemplos: Java, JavaScript, PHP, lenguajes de .NET,...
- Según el **paradigma de programación:** Con esto nos referimos al enfoque a la hora de afrontar el problema que tratamos de programar.
 - o **Imperativos:** se fundamentan en la utilización de variables para almacenar valores y en la realización de instrucciones para operar con los datos almacenados. Aparece el concepto de

algoritmo, el CÓMO conseguir el objetivo. Dentro de los lenguajes imperativos, podemos clasificarlos en:

- **Procedurales o procedimentales:** agrupan código en subprogramas que pueden llamarse desde distintos puntos del programa. Ej. C, Pascal, Fortran, Basic, etc.
- **Orientados a objetos:** ven el programa como una colección de objetos que interactúan los unos con los otros a través de mensajes. Es el más utilizado en la actualidad. Ej. Smalltalk, C++, Java, C#, Visual Basic.NET, Eiffel, etc.

En la actualidad, casi todas las nuevas versiones de los lenguajes incorporan características de orientación a objetos. De hecho, muchos autores proponen el paradigma orientado a objetos como paradigma propio, evolución del paradigma imperativo.

- o **Declarativos:** se declara o se describe las propiedades o características del problema, dejando que la solución la encuentre la máquina. Realmente se declaran condiciones, proposiciones, hechos, reglas, afirmaciones, restricciones, ecuaciones, transformaciones, etc. que debe cumplir el conjunto de valores que constituyen la solución. Dentro de este tenemos tres tipos:
 - **Funcional o aplicativo:** Todas las construcciones son funciones matemáticas. No hay instrucciones, y tampoco hay instrucción de asignación. El programa se define por composición de funciones más simples. Para ejecutarlo, se llama a una función con los datos de entrada y se obtiene un resultado. Ej. Haskell, LISP, CAML, etc.
 - **Lógico:** Se basa en la definición de reglas lógicas para luego interrogar al sistema y resolver problemas. La programación lógica trata con relaciones (predicados)

entre objetos (datos), en lugar de hacerlo con funciones.
Ej. Prolog

- **Algebraicos o Relacionales:** Algunos autores hablan de este paradigma para clasificar el SQL, que es el lenguaje utilizado para interrogar BBDD relacionales. Especificamos el resultado que queremos y la ejecución del SQL nos lo proporciona.

Hay que decir que algunos lenguajes son **multiparadigma**. Por ejemplo el C++ es un lenguaje orientado a objetos, pero también podemos usarlo como lenguaje imperativo, sin hacer uso de la orientación a objetos, o el Prolog, que es lógico, pero también cuenta con estructuras repetitivas propias del paradigma imperativo.

37.2 Programación Estructurada.

La programación estructurada es un concepto que surge como repuesta a la crisis del software de los años 60, cuando el coste en el desarrollo de programas era cada vez mayor, y el mantenimiento de los mismos se hacía cada vez menos manejable.

Fue desarrollada en sus principios por Edsgar W. Dijkstra en su libro “Notes on Structures Programming” y se basa en el denominado Teorema de la Estructura o de *Böhm-Jacopini* en honor de Corrado Böhm y Giuseppe Jacopini.

Edsgar Dijkstra definió la programación estructurada como *“aquella que utiliza recursos abstractos, se basa en el diseño descendente y respeta un conjunto de estructuras básicas llamadas Estructuras de Control: Estructura secuencial, estructuras selectivas y estructuras repetitivas”*.

37.2.1 Recursos abstractos

Todos los lenguajes de programación poseen un conjunto de recursos que podríamos denominar recursos concretos: instrucciones, palabras reservadas, tipos de datos, funciones, reglas, etc. Sin embargo, estos recursos no son suficientes para escribir programas para distintas aplicaciones, por lo tanto, el programador deberá valerse de artificios (recursos abstractos) para implementar sus algoritmos utilizando solo los recursos concretos.

Según Dijkstra, *escribir un programa en términos de recursos abstractos consiste en descomponer las acciones complejas en acciones simples, capaces de ser ejecutadas por una máquina*. Esto significa que es posible escribir programas complejos utilizando un conjunto limitado de instrucciones muy simples.

37.2.2 Diseño Descendente

Existen dos técnicas para escribir los algoritmos: el diseño ascendente y el diseño descendente.

Cuando se utiliza diseño ascendente, se parte desde los detalles particulares de implementación de la solución hacia la solución general del problema. La solución del problema se logra con la integración de todas las soluciones particulares planteadas al principio. Esto significa que primero se resuelven partes particulares del problema y por último el problema en sí. Esta técnica presenta dos dificultades: lograr que las soluciones particulares funcionen en conjunto y lograr que varios programadores trabajen en coordinación.

El diseño descendente consiste en comprender el problema a solucionar y luego descomponerlo en un conjunto de problemas menores. Cuando se usa esta técnica, primero se plantea la solución de forma general para luego pasar a los detalles particulares. Esto se realiza en varios pasos llamados refinamientos. Pueden existir varios niveles de refinamiento hasta llegar a los detalles de implementación de la solución

(subalgoritmos independientes llamados módulos). Una ventaja de esta técnica es que permite la división de tareas entre varios programadores donde cada uno podrá escribir un algoritmo que obtenga una parte de la solución.

La programación estructurada hace pues uso de la **programación modular**. Un módulo es un conjunto de acciones que realiza una tarea específica. Puede realizar las mismas acciones que un programa: aceptar datos, realizar cálculos y devolver resultados. Sin embargo los módulos se utilizan para un fin específico. Cuando se utiliza esta técnica, toda la solución (el algoritmo) queda dividida en varias partes: un algoritmo principal y uno o varios subalgoritmos (los módulos). La ejecución se inicia en el algoritmo principal y desde este se invoca a los módulos. Los módulos también pueden ser invocados desde otros módulos y el control de la ejecución siempre se retorna al punto desde donde se lo invocó por última vez.

37.2.3 Estructuras básicas

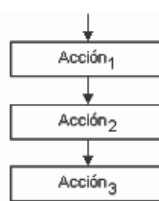
Bohm y Jacopini demostraron que es posible resolver problemas escribiendo programas denominados **propios**. Un programa se define como propio si cumple con:

- tiene un solo punto de entrada y uno solo de salida (inicio y fin),
- todas las acciones del algoritmo son accesibles, es decir, para cada acción existe un conjunto de datos que hará que ésta sea accesible desde el inicio y además se podrá llegar al fin.
- no posee lazos o bucles infinitos.

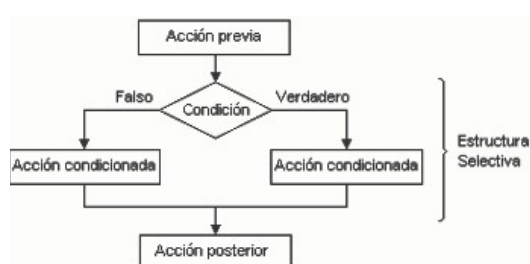
Pues bien, el **teorema de la estructura** establece que *cualquier programa propio puede ser escrito utilizando solamente las siguientes estructuras lógicas de control: secuencia, selección e iteración*. Un

algoritmo correctamente implementado poseerá un único punto de entrada, un único punto de salida, y permitirá la ejecución de todas sus instrucciones en función de los parámetros de entrada. La programación estructurada se basa en el concepto de programa propio y utiliza solamente estas tres estructuras básicas:

- **Estructura Secuencial:** Se caracteriza porque una acción se escribe y ejecuta a continuación de otra. Está representada por una sucesión de operaciones que se ejecutan secuencialmente.

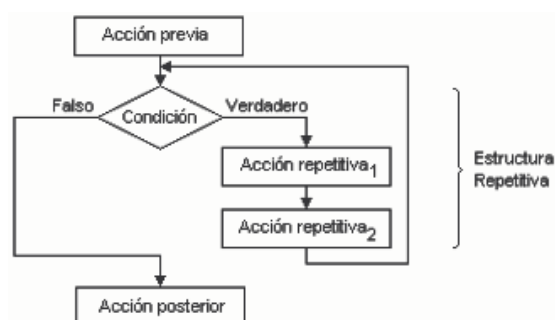


- **Estructura selectiva:** Se caracteriza porque existen dos o más secuencias alternativas de acciones en el programa. La selección de una u otra se realiza de acuerdo a una *condición* que se debe cumplir para que el conjunto de acciones sea ejecutado. Se dice que las estructuras selectivas *bifurcan* la ejecución del programa. Una instrucción de bifurcación evalúa una *condición* y, en función del resultado de esa evaluación, la ejecución se bifurca a un determinado punto. Una *condición* se construye con *expresiones lógicas*.



- **Estructura repetitiva o bucle:** Se caracteriza porque existe un conjunto de acciones cuya ejecución se debe repetir un determinado número de veces llamado bucle (o lazo). La implementación del bucle debe ser tal que sea posible acceder a él y también salir de él. No deben existir lazos de ejecución infinita. Para que un bucle cumpla

con las condiciones mencionadas (poder acceder y poder salir de él) es necesario el uso de una condición que lo controle. En cada ciclo de ejecución del bucle se deberá evaluar la condición para decidir si se vuelve a ejecutar o si se sale de él, así, todo bucle deberá poseer un controlador (un contador o un centinela), una decisión (una condición para decidir la repetición o la salida del bucle) y un cuerpo (conjunto de acciones que se repiten). Un contador es una variable numérica entera cuyo contenido se incrementa o se decrementa sucesivamente con un valor constante. En un proceso de introducción de datos, el centinela es el valor que indica la finalización del bucle.



Como ejemplos de lenguajes de programación estructurados tenemos FORTRAN, PASCAL, MODULA, ADA, C, etc.

37.3 Programación orientada a objetos

La programación orientada a objetos es lo que se conoce como un paradigma o modelo de programación. Esto significa que no es un lenguaje específico, o una tecnología, sino una forma de programar, una manera de plantearse la programación. Lo que caracteriza a la programación orientada a objetos es que intenta llevar al mundo del código lo mismo que encontramos en el mundo real. Cuando miramos a nuestro alrededor ¿qué vemos? pues, cosas, objetos, y podemos reconocer estos objetos porque cada objeto pertenece a una clase de objeto. Eso nos permite distinguir, por ejemplo, un perro de un coche (porque son de clases diferentes) y

también un televisor de otro (porque, aunque sean iguales, cada uno es un objeto distinto). Éste es el modelo que la programación orientada a objetos intenta seguir para estructurar un sistema.

La construcción de software orientado a objetos es el método de desarrollo de software que basa la arquitectura de cualquier sistema software en módulos deducidos de los tipos de objetos que manipula (en lugar de basarse en la función o funciones a las que el sistema está destinado a asegurar). Los desarrolladores analizarán los tipos de los objetos del sistema y el diseño irá pasando por las sucesivas mejoras de su comprensión de estas clases de objetos. Es un proceso ascendente, frente a la programación estructurada que era descendente, de construcción de soluciones robustas y extensibles para ciertas partes del problema, y de combinación de esas soluciones en montajes cada vez más potentes, hasta que el montaje final da una solución del problema original; además, los mismos componentes ensamblados de manera diferente y combinados posiblemente con otros, deberán ser lo suficientemente generales para producir también otros subproductos software, es decir, deben ser reutilizables.

Así, un sistema se concibe como un conjunto de objetos, pertenecientes a alguna clase, que se comunican entre sí mediante mensajes. Los objetos se distinguen por:

- Poseer un estado que puede cambiar,
- tener una identidad única,
- soportar interrelaciones con otros objetos,
- poseer un comportamiento,
- poder recibir y emitir mensajes.

Un **objeto** se describe por sus propiedades, también llamadas atributos (definen la estructura del objeto), y por los servicios (métodos u operaciones) que puede proporcionar (comportamiento del objeto). El

estado de un objeto viene determinado por los valores que toman sus atributos. El objeto es la unidad fundamental de descomposición en la programación orientada a objetos.

Además, todo objeto es una instancia de alguna **clase**. Todos los objetos se crean de acuerdo a una definición de clase de objetos. Dicha clase incluye declaraciones de todos los atributos y operaciones que deberían asociarse con un objeto de dicha clase. Una clase es una abstracción de las propiedades comunes y comportamiento de un conjunto de objetos.

Así pues, un programa orientado a objetos consta de una o más clases interdependientes. Las clases permiten describir las propiedades (atributos o campos) y habilidades (métodos) de los objetos con los que el programa tiene que tratar. El conjunto de atributos y métodos de una clase reciben también el nombre de **miembros** de esa clase.

La definición de los miembros pueden ir precedidas de un **modificador de acceso**, que es algo que indica desde que puntos del código es accesible ese miembro. Los tres principales modificadores de acceso son:

- **Public:** Se puede acceder desde cualquier punto.
- **Protected:** Es accesible desde los métodos de su clase y de las clases que de ella pudieran derivarse.
- **Private:** Solo se puede utilizar desde los métodos de la propia clase.

Estos son los modificadores de acceso más comunes, aunque dependiendo del lenguaje podríamos tener otros modificadores que varían los accesos en función de si las clases están en el mismo paquete, etc.

El **comportamiento** de un objeto viene determinado por el conjunto de métodos que éste proporciona. Nos referiremos indistintamente a ellos como **métodos, servicios u operaciones**. Un método está formado por un conjunto de sentencias (acciones) que deben llevarse a cabo para hacer efectivo un comportamiento de un objeto. Un objeto proporciona un

conjunto de métodos que pueden utilizarse desde otros objetos. Dicho conjunto de métodos constituye lo que se denomina **interfaz** del objeto. Mediante la interfaz de un objeto podremos acceder a los valores de sus atributos (estado) para su consulta y/o modificación y activar un comportamiento del mismo. Cuando se hace una llamada a un método de la interfaz de un objeto decimos que estamos enviando un mensaje a dicho objeto. Así, un **mensaje** se puede definir como una petición a un objeto para la obtención de algún comportamiento deseado del mismo. Una llamada a un método puede contener **parámetros**, o conjunto de datos de entrada del método. Los métodos pueden devolver valores, objetos o nada (void en algunos lenguajes).

Se dice que la información acerca de un objeto está **encapsulada** por su comportamiento. A un objeto se le deben pedir sus datos, o pedir que los cambie con un mensaje. Al encapsular u ocultar información se separan los aspectos externos de un objeto (los accesibles para todos) de los detalles de implementación (los accesibles para nadie). Con esto se trata de lograr que al tener algún cambio en la implementación de un objeto no se tengan que modificar los programas que utilizan tal objeto.

Una de las propiedades más característica de la orientación a objetos es la **herencia**, que es la capacidad de crear nuevas clases (subclases) a partir de otra clase ya existente, especificando únicamente las diferencias con la clase padre. Aunque algunos lenguajes permiten la herencia múltiple (una clase que deriva de más de una clase), en general, la mayoría de ellos no lo hacen y sólo permiten que se herede de una clase. Para simular la herencia múltiple se utilizan los interfaces, que si son soportados por todos los lenguajes orientados a objetos. Los interfaces especifican (no implementan) conjuntos de métodos y atributos para que las clases los implementen. Una clase que implementa un interfaz está obligada a tener una implementación para cada método definido en el interfaz.

Cuando se diseña un modelo orientado a objetos, es útil introducir clases a cierto nivel que pueden no existir en realidad, pero que permiten actuar como un depósito de métodos y atributos compartidos para las subclases de nivel inferior. Estas clases se denominan **clases abstractas**, y no pueden tener ninguna instancia. No se pueden crear objetos de dicha clase. También tenemos **métodos abstractos**, que son aquellos en los que no se especifica ninguna implementación. Son las clases derivadas las que tienen que hacerlo. Una **clase** se dice que es **sellada** (sealed) cuando no puede tener clases derivadas. Igualmente, un **método sellado** es aquel que no puede ser redefinido en las clases derivadas. Se utilizan para poder optimizar su ejecución a nivel de código, ya que el implementador sabe que no se puede utilizar como clase base de otras.

Los atributos de objeto son aquellos que almacenan un valor para cada objeto de la clase. Los atributos de clase son aquellos que almacenan un valor accesible para todos los objetos de la clase. Los métodos de objeto son aquellos que acceden al estado de un objeto concreto, mientras que los métodos de clases no necesitan acceder a ningún atributo de ningún objeto. Los miembros (atributos y métodos) de clase también son llamados estáticos o compartidos.

Un **constructor** es un método especial que se ejecuta automáticamente cuando se crea el objeto. Su propósito es inicializar el objeto con, al menos, los datos mínimos que necesita. Igual que para el resto de métodos, puede haber varios constructores sobrecargados. Es decir, podemos crear objetos de distintas formas. Se llama constructor por defecto a aquel que no tiene argumentos. Un **destructor** es un método especial que suele liberar la memoria y otros recursos cuando un objeto deja de ser usado. Puede ser llamado automáticamente, liberando así de la responsabilidad al programador.

Por último hablaremos de otra de las características fundamentales de la programación orientada a objetos, el **polimorfismo**. El polimorfismo se

refiere a dos aspectos diferentes: por un lado la sobrecarga de métodos y operadores (métodos polimórficos) y por otro lado, la ligadura dinámica. El primero es la capacidad de tener distintos métodos en la misma clase con el mismo nombre, aunque con distinta firma (número de argumentos, tipos de los argumentos, orden). Lo que no pueden es devolver un resultado de distinto tipo. El otro aspecto, la ligadura dinámica, se refiere a que cuando se envía un mensaje a un objeto, el código que se llama no se determina hasta el momento de la ejecución. El compilador asegura que la función existe, pero no conoce el código exacto a ejecutar. Para ello, el compilador inserta un código especial en lugar de una llamada absoluta. Este código calcula en tiempo de ejecución la dirección real del método que hay que ejecutar utilizando la información almacenada en el propio objeto. Esta ligadura dinámica está relacionada con la herencia. En términos prácticos, el polimorfismo permite definir una referencia a una clase padre, que en tiempo de ejecución apuntará a un objeto concreto de alguna clase hija (no conocida en tiempo de compilación). La llamada a los métodos virtuales (los métodos de la clase padre que serán redefinidos en la clase hija) a través de dicha referencia se ejecutarán correctamente, pues durante la ejecución se verifica el tipo del objeto almacenado y se llama a la versión correcta del método.

Ejemplos de lenguajes de programación orientados a objetos son: C++, Objective C, Java, Smalltalk, Eiffel, Ruby, Python, OCAML, Object Pascal, CLIPS, Actionscript, Perl, C#, Visual Basic.NET, PHP, Simula, Delphi, PowerBuilder

37.4 Ingeniería inversa y reingeniería

La Ingeniería Inversa se ocupa de estudiar un sistema de información en el orden inverso establecido en el ciclo de vida habitual; esto es, partiendo del código fuente, se trata de identificar los componentes del sistema y las relaciones existentes entre ellos. Hasta su llegada, el ciclo de vida del

software era, en teoría, en una sola dirección; ahora, se puede hablar de dos direcciones: forward o hacia adelante, que es la tradicional, y reverse o hacia atrás, que es la de la Ingeniería Inversa. La Ingeniería Inversa también es conocida como modernización de caja blanca (White-Box Modernization).

Daremos un par de definiciones de ingeniería inversa:

“El análisis de un sistema para identificar sus componentes actuales y las dependencias que existen entre ellos, para extraer y crear abstracciones de dicho sistema e información de su diseño” [Chifofsky, 1990].

“El proceso de analizar el código, documentación y comportamiento de un sistema para identificar sus componentes actuales y sus dependencias para extraer y crear una abstracción del sistema e información de diseño. El sistema en estudio no es alterado, sino que se produce conocimiento adicional acerca del sistema” [SEI, 2004].

A partir de estas definiciones podemos declarar que la ingeniería inversa tiene la misión de desentrañar los misterios y secretos de los sistemas en uso. Consiste principalmente en recuperar el diseño de una aplicación a partir del código. Esto se realiza principalmente mediante herramientas que extraen información de los datos, procedimientos y arquitectura del sistema existente. El objetivo primordial es proporcionar una base para el mantenimiento y futuros desarrollos. Este objetivo general se puede traducir en los siguientes objetivos parciales:

- Reducir los errores y los costes del mantenimiento.
- Hacer los sistemas más fáciles de entender, cambiar y probar.
- Proteger y extender la vida del sistema.
- Facilitar la reutilización de componentes del sistema existentes.
- Proporcionar documentación que no existe, o actualizar la existente.
- Migrar a otra plataforma hardware o software, cuando sea necesario.

- Llevar el sistema bajo el control de un entorno CASE.

A la vista de estos objetivos, los sistemas candidatos a aplicarles la Ingeniería Inversa reúnen algunas de las siguientes características:

- Las especificaciones de diseño y la documentación, no existen o están incompletas.
- El código no es estructurado.
- Inexistencia de documentación interna en los programas, o bien ésta es incomprensible o está desfasada.
- El sistema necesita un excesivo mantenimiento correctivo.
- Algunos módulos se han hecho excesivamente complejos debido a los sucesivos cambios realizados en ellos.
- Se necesita una migración hacia una nueva plataforma de hardware o de software.
- La aplicación está sujeta a cambios frecuentes, que pueden afectar a parte del diseño.
- Se prevé que la aplicación pueda tener aún larga vida.

Aplicar la Ingeniería Inversa supone un enorme esfuerzo y, por tanto, se hace necesario evaluar exhaustivamente y siendo muy realistas los casos en los que es rentable su aplicación. Su resultado varía fuertemente en función de los siguientes elementos:

- **El nivel de abstracción** del proceso de Ingeniería Inversa, y de las herramientas que se usen. Esto alude a la sofisticación de la información de diseño que se puede extraer del código fuente. El nivel de abstracción ideal deberá ser lo más alto posible. Esto es, el proceso de ingeniería inversa deberá ser capaz de derivar sus representaciones de diseño de procedimientos (con un bajo nivel de abstracción); y la información de las estructuras de datos y de programas (un nivel de abstracción ligeramente más elevado); modelos de flujo de datos y de control (un nivel de abstracción

relativamente alto); y modelos de entidades y de relaciones (un elevado nivel de abstracción). A medida que crece el nivel de abstracción se proporciona al ingeniero del software información que le permitirá comprender más fácilmente estos programas.

- **La completitud** del proceso. La completitud de un proceso de ingeniería inversa alude al nivel de detalle que se proporciona en un determinado nivel de abstracción. En la mayoría de los casos, la completitud decrece a medida que aumenta el nivel de abstracción. Por ejemplo, dado un listado del código fuente, es relativamente sencillo desarrollar una representación de diseño de procedimientos completa. También se pueden derivar representaciones sencillas del flujo de datos, pero es mucho más difícil desarrollar un conjunto completo de diagramas de flujo de datos o un diagrama de transición de estados. La completitud mejora en proporción directa a la cantidad de análisis efectuado por la persona que está efectuando la ingeniería inversa.
- **La interactividad del proceso.** La interactividad alude al grado con el cual el ser humano se “integra” con las herramientas automatizadas para crear un proceso de ingeniería inversa efectivo. En la mayoría de los casos, a medida que crece el nivel de abstracción, la interactividad deberá incrementarse, o sino la completitud se verá reducida.
- **La direccionalidad** del proceso. Si la direccionalidad del proceso de ingeniería inversa es monodireccional, toda la información extraída del código fuente se proporcionará a la ingeniería del software que podrá entonces utilizarla durante la actividad de mantenimiento. Si la direccionalidad es bidireccional, entonces la información se suministrará a una herramienta de reingeniería que intentará reestructurar o regenerar el viejo programa.

La Ingeniería inversa no implica la modificación del sistema, ni la generación de nuevos sistemas, sin embargo, existen una serie de técnicas intrínsecamente relacionadas con ella:

- **Redocumentación:** es la producción de una representación semántica de un sistema a cualquier nivel de abstracción que se requiera. Las herramientas usadas parten del código fuente existente, para producir diagramas de flujo de datos, modelos de datos, etc. Si la redocumentación toma la forma de modificación de comentarios en el código fuente, puede ser considerada una forma suave de reestructuración. Si se piensa en ella como una transformación desde el código fuente a pseudocódigo y/o prosa, esta última es considerada como de más alto nivel de abstracción que la primera.
- **Recuperación del diseño:** es un subconjunto de la ingeniería inversa, en el cual, aparte de las observaciones del sistema, se añaden conocimientos sobre su dominio de aplicación, información externa, y procesos deductivos con el objeto de identificar abstracciones significativas a un mayor nivel.
- **Reestructuración:** La transformación desde una forma de representación a otra en el mismo nivel de abstracción, preservando las características externas del sistema (funcionalidad y semántica). [Chifofsky, 1990]. La reestructuración del software modifica el código fuente y/o los datos en un intento de adecuarlo a futuros cambios. En general, la reestructuración no modifica la arquitectura global del programa. Tiene a centrarse en los detalles de diseño de módulos individuales y en estructuras de datos locales definidas dentro de los módulos. Si el esfuerzo de la reestructuración se extiende más allá de los límites de los módulos y abarca la arquitectura del software, la reestructuración pasa a ser ingeniería directa (forward engineering). Arnold indica que los beneficios que se pueden lograr con la reestructuración del software son el obtener programas de mayor

calidad, mejorar la productividad de los ingenieros del software, reducir el esfuerzo requerido para llevar a cabo actividades de mantenimiento, y hacer que el software sea más sencillo de comprobar y de depurar.

- **Reingeniería:** La reingeniería parte de los resultados obtenidos en la ingeniería inversa para reconstruir el sistema mediante ingeniería hacia adelante. La Reingeniería no sólo recupera la información de diseño de un software existente, sino que usa ésta para alterar o reconstruir el sistema existente, en un esfuerzo por mejorar la calidad general.

Chikofsky define la **reingeniería** como el *examen y alteración de un sistema para reconstruirlo de una nueva forma y la subsiguiente implementación de esta nueva forma*». Arnold, por su parte, señala que reingeniería es *cualquier actividad que mejore nuestro entendimiento sobre el software y prepare o mejore el propio software, normalmente para su facilidad de mantenimiento, reutilización o evolución*. La definición dada por el Reengineering Center del Software Engineering Institute es *la transformación sistemática de un sistema existente a una nueva forma para realizar mejoras de la calidad en operación, capacidad del sistema, funcionalidad, rendimiento o capacidad de evolución a bajo coste, con un plan de desarrollo corto y con bajo riesgo para el cliente*.

La importancia de las técnicas de reingeniería del software estriban en que reducen los riesgos evolutivos de una organización, ayudan a las organizaciones a recuperar sus inversiones en software, hacen el software más fácilmente modificable, amplían la capacidad de las herramientas CASE y son un catalizador para la automatización del mantenimiento del software.

Para algunos autores, la reingeniería de sistemas puede clasificarse según los niveles de conocimientos requeridos para llevar a cabo el proyecto. La reingeniería que requiere conocimientos a bajos niveles de abstracción

(código fuente) se llama **Ingeniería Inversa o Modernización de Caja Blanca** y aquella que sólo requiere el conocimiento de las interfaces del sistema se llama **Reingeniería** propiamente dicha o **Modernización de Caja Negra**.

Para realizar la reingeniería en los sistemas existentes (también llamados **legacy systems** o **sistemas heredados**) se emplean técnicas métricas, de visualización de programas, de abstracción y reformulación del código. Tanto para reingeniería como para ingeniería inversa, se crean patrones para la resolución de problemas relacionados con estas técnicas. En base al conocimiento del sistema, los datos, las funcionalidades y las interfases, se desarrollan nuevas técnicas de reingeniería no basadas en el conocimiento del código sino en el examen del comportamiento de las entradas y salidas del sistema, desarrollando nuevos patrones de reingeniería y sentando las bases de la reingeniería basada en wrapping. Idealmente, **wrapping** es una reingeniería en la que sólo se analizan las interfases (las entradas y salidas) del sistema existente ignorando los detalles internos. Esta solución no es aplicable siempre y a veces requiere el concurso de la ingeniería inversa para el conocimiento interno del sistema.

Veremos en los siguientes apartados distintos modelos de reingeniería:

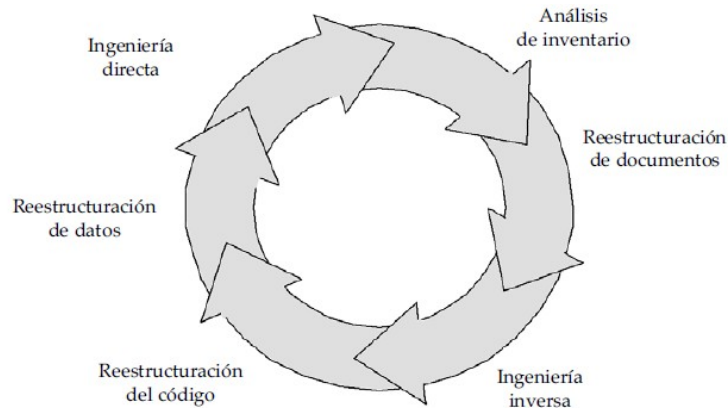
37.4.1 Modelo Cíclico

El modelo cíclico, debido a Pressman, concibe la reingeniería como un proceso compuesto por seis actividades las cuales se producen, generalmente, de forma secuencial y lineal. Las actividades que se definen en el modelo cíclico son:

- **Análisis de inventario.** Todas las organizaciones de software deberán disponer de un inventario de todas sus aplicaciones, a fin de poder identificar los candidatos a la reingeniería.

- **Reestructuración de documentos.** Una documentación escasa es la marca de muchos sistemas de información heredados. Ante ello será necesario, o bien crear la documentación, o actualizar la existente o hacerla nueva por completo.
- **Ingeniería Inversa.** La Ingeniería Inversa del software es el proceso de análisis de un programa con el fin de crear una representación de programa con un nivel de abstracción más elevado que el código fuente. La Ingeniería Inversa se extraerá del programa existente información del diseño arquitectónico y de proceso, e información de los datos.
- **Reestructuración del código.** El tipo más común de reingeniería es la reestructuración del código. Algunos sistemas heredados tienen una arquitectura de programa relativamente sólida, pero los módulos individuales han sido codificados de una forma que hace difícil comprenderlos, comprobarlos y mantenerlos. En estos casos, se puede reestructurar el código ubicado dentro de los módulos sospechosos.
- **Reestructuración de datos.** Un programa que posea una estructura de datos débil será difícil de adaptar y de mejorar. De hecho, para muchas aplicaciones, la arquitectura de datos tiene más que ver con la viabilidad a largo plazo del programa que el propio código fuente. A diferencia de la reestructuración de código, que se produce en un nivel relativamente bajo de abstracción, la estructuración de datos es una actividad de reingeniería a gran escala.
- **Ingeniería directa (forward engineering).** La ingeniería directa no solamente recupera la información de diseño de un software ya existente, sino que, además, utiliza esta información en un esfuerzo por mejorar su calidad global. En la mayoría de los casos, el software procedente de una reingeniería vuelve a implementar la

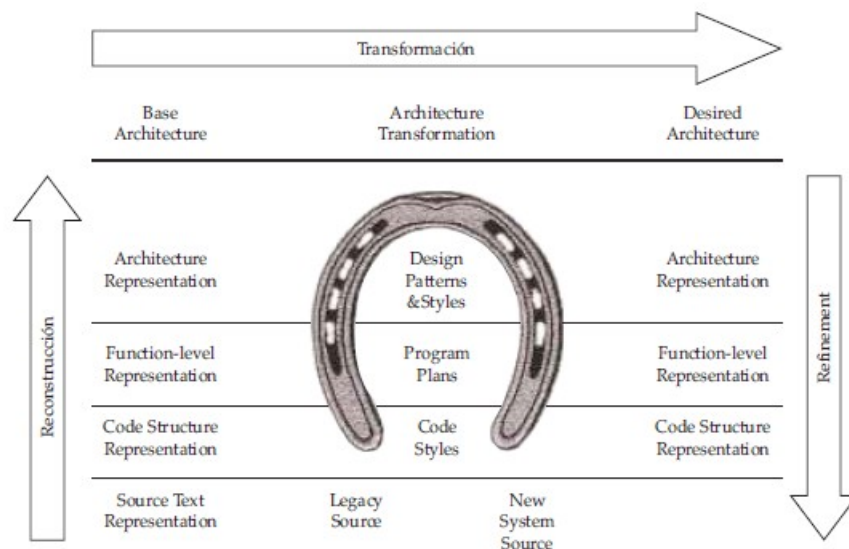
funcionalidad del sistema existente, y añade además nuevas funciones y/o mejora el rendimiento global.



37.4.2 El modelo de herradura

El modelo de herradura se fundamenta en considerar tres niveles de abstracción en todo sistema y que la reingeniería está formada por tres procesos básicos:

- **Análisis de un sistema existente:** sube el extremo izquierdo de la herradura, y recupera la arquitectura por medio de la extracción de artefactos desde el código fuente.
- **Transformación lógica:** cruza la parte superior y es la transformación de arquitectura. La arquitectura antes construida es recuperada y se reingenieriza para hacer la nueva arquitectura deseable
- **Desarrollo de un nuevo sistema:** baja por el extremo derecho de la herradura, y construye la nueva arquitectura deseable.



La riqueza del modelo de herradura son los tres niveles de abstracción que pueden ser adoptados para las descripciones lógicas, las cuales pueden ser artefactos tan concretos y simples como el código fuente del sistema o tan complejos y abstractos como la arquitectura del sistema. Los tres niveles que adopta el modelo de herradura son:

- **Representación de la estructura de código**, el cual incluye código fuente y artefactos tales como árboles de sintaxis abstractos y diagramas de flujo.
- **Representación del nivel funcional**, el cual describe la relación entre las funciones del programa (llamadas), datos (funciones y relaciones de datos), y archivos (agrupamiento de funciones y datos).
- **Nivel conceptual**, el cual representa grupo tanto de funciones y artefactos del nivel de código que son ensamblados dentro de subsistemas de componentes relacionados o conceptos.

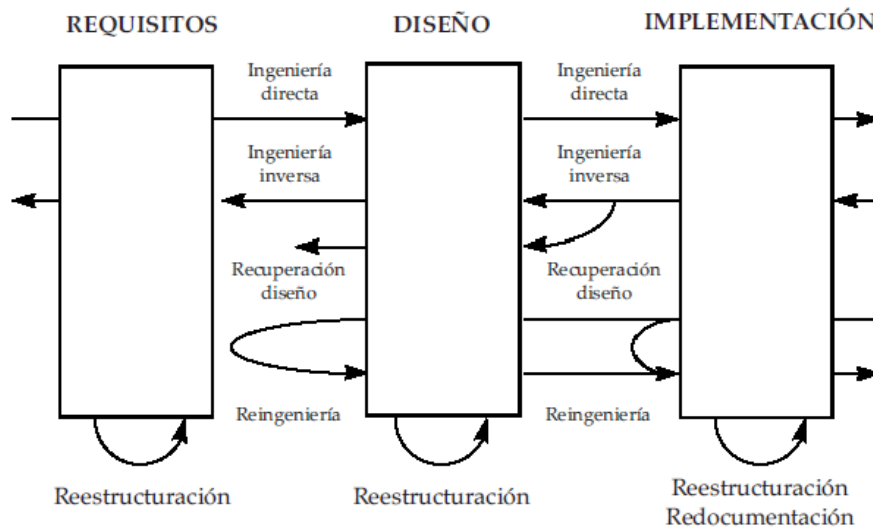
37.4.3 El modelo del IEEE

Este modelo se basa en considerar tres niveles de abstracción en todo sistema, el nivel requisitos, el nivel diseño y el nivel implementación, y en

fijar una terminología. Los conceptos que define el IEEE, basados en las definiciones de Chifofsky y Cross, son los siguientes:

- **Ingeniería Inversa (Reverse Engineering):** es el proceso de analizar un sistema para identificar los componentes y las interrelaciones entre ellos, creando representaciones del sistema en otra forma distinta a la original o bien a un nivel superior de abstracción.
- **Reingeniería (Reengineering):** es el examen y modificación de un sistema para ser reconstruido de una forma nueva y además realizar la implantación derivada de esa nueva forma. La Reingeniería normalmente incluye alguna forma de Ingeniería Inversa y va seguida de alguna forma de Ingeniería «hacia adelante» o también de una Reestructuración.
- **Reestructuración (Restructuring):** es la transformación de una forma de representación del sistema en otra distinta, pero del mismo nivel de abstracción, sin modificar el comportamiento externo del sistema.
- **Ingeniería Hacia Adelante (Forward Engineering):** es el proceso que va desde un alto nivel de abstracción, que es independiente de la implementación concreta, hasta la propia implementación física del sistema. Es decir, es la Ingeniería del Software en su vertiente restringida al nuevo desarrollo.
- **Reingeniería de Empresas (Business Process Reengineering):** es la aplicación del concepto de Reingeniería al campo económico, y se desarrolla alrededor de tres actividades clave: rediseñando los procesos básicos de trabajo para alcanzar los objetivos del negocio; utilizando las nuevas tecnologías para concebir, diseñar y poner en marcha nuevas actividades; y cambiando la forma en la que trabajan los empleados.

Las relaciones entre las definiciones y los niveles de abstracción son los que se ven en la figura.



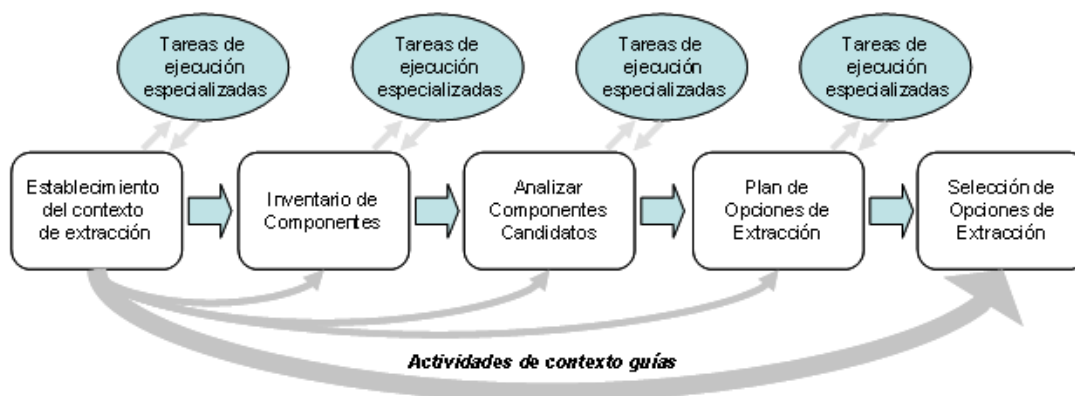
37.4.4 El método *Análisis de Opciones para Reingeniería* ("Options Analysis for Reengineering" (OAR))

Es un método sistemático para la identificación y extracción de componentes dentro de grandes y complejos sistemas de software. OAR identifica componentes de arquitectura potencialmente relevantes y analiza los cambios requeridos para usarlos en una línea de producción de software o nuevas arquitecturas de software. En esencia, OAR proporciona un conjunto de opciones de extracción junto con estimación de costos, esfuerzo y riesgos asociados con estas opciones. El método OAR consiste en cinco actividades principales:

- **Establecimiento del contexto de extracción:** consiste en entrevistar a los accionistas y estudiar la línea de producción de la organización o nuevos requerimientos de sistema, base heredada y expectativas para la extracción de componentes heredados. Estos esfuerzos establecen una línea base de un conjunto de metas, expectativas y necesidades de componentes.
- **Inventario De Componentes:** el equipo OAR identifica los componentes del sistema heredado que potencialmente pueden ser extraídos para usarlos en una línea de producción o en una nueva

arquitectura de software. Esta actividad resulta en un inventario de los componentes heredados candidatos.

- **Análisis de componentes candidatos:** El siguiente paso de los miembros del equipo es analizar el conjunto de candidatos de componentes heredados para extraer los tipos de cambios que son requeridos.
- **Plan de opciones de extracción:** Dado el conjunto de componentes candidatos analizados, el equipo desarrollará alternativas para la extracción basada en consideraciones de calendario, costo, esfuerzo, riesgo y recursos. El equipo OAR también filtra una vez más los componentes candidatos y analiza el impacto de agregación de diferentes componentes.
- **Selección de opciones de extracción:** Finalmente, los miembros del equipo seleccionan la mejor opción de extracción o combinación de opciones. Después de evaluar cada opción de extracción, ellos preparan un resumen en el que presentan y justifican sus elecciones.



Bibliografía

- Ingeniería del Software. Un enfoque práctico.
- Algoritmos y estructuras de datos.
- Estructuras de datos, algoritmos y programación orientada a objetos. Gregory L. Heileman.
- Reverse engineering and design recovery: A taxonomy. E. Chikofsky y J. Cross. Ed. IEEE Software.



- Programación orientada a objetos. Luis Joyanes Aguilar
- Software Reengineering. R. S. Arnold. Ed. IEEE Computer Society Press.
- Técnicas de programación. Instituto nacional de estadística e informática.
- <http://www.authorstream.com/Presentation/verarex-33544-evolucion-de-los-lenguajes-programaci-evolucionlp-education-ppt-powerpoint/>. Evolución de los lenguajes de programación. Denis Cedeño.

Reconstrucción de la arquitectura: Una actividad de la reingeniería de software. Flores Carmona Nicolás Johnatan

Introducción a la programación orientada a objetos. Timothy Budd

http://www.cybertesis.edu.pe/sisbib/2007/acevedo_rj/pdf/acevedo_rj.pdf. Ingeniería inversa aplicado a sistemas desarrollados con programación orientada a objetos para obtener la documentación. Jessica Jahany Acevedo Ricse

Autor: Francisco Javier Rodríguez Martínez

Subdirector de la Escuela Superior de Ingeniería Informática.

Universidad de Vigo.



38. MÉTODOS DE PRUEBA DEL SOFTWARE. FUNDAMENTOS. CAJA NEGRA Y CAJA BLANCA. ESTRATEGIAS DE PRUEBA DEL SOFTWARE.

Tema 38: Métodos de prueba del software. Fundamentos. Caja negra y caja blanca. Estrategias de prueba del software.

ÍNDICE

38.1 Métodos de prueba del software. Fundamentos.

38.2 Pruebas de Caja negra y Caja blanca

38.2.1 Pruebas de Caja blanca

38.2.1.1 Prueba del camino básico

38.2.1.2 Prueba de la estructura de control

38.2.2 Pruebas de Caja Negra

38.2.2.1 Partición equivalente

38.2.2.2 Análisis de valores límite

38.2.2.3 Valores típicos de error y valores imposibles

38.2.2.4 Basados en grafos

38.2.2.3 Tabla Ortogonal

38.2.2.4 Prueba de comparación

38.3 Estrategias de prueba del software.

38.3.1 Pruebas de Unidad

38.3.2 Pruebas de integración

38.2.3 Pruebas del sistema

38.2.4 Pruebas de implantación

38.2.5 Pruebas de aceptación.

38.1 Fundamentos de las pruebas del software

La prueba del software es un elemento de un tema más amplio que, a menudo, es conocido como **verificación** y **validación** (V&V). La **verificación** se refiere al conjunto de actividades que aseguran que el software implementa correctamente una función específica. La **validación**

se refiere a un conjunto diferente de actividades que aseguran que el software construido se ajusta a los requisitos del cliente.

- **Verificación:** ¿Estamos construyendo el producto correctamente?
- **Validación:** ¿Estamos construyendo el producto correcto?

La prueba presenta una anomalía para el ingeniero del software, ya que, mientras en las fases anteriores de definición y desarrollo, el ingeniero intenta construir, al llegar las pruebas, el ingeniero diseña una serie de casos de prueba que pretenden “demoler” lo construido. Por eso los autores dicen que la prueba se puede ver como destructiva, en lugar de constructiva.

El proceso de pruebas del software tiene dos objetivos distintos:

- Para demostrar al desarrollador y al cliente que el software satisface sus requerimientos. Para el software a medida, esto significa que debería de haber al menos una prueba para cada requerimiento de los documentos de requerimientos del sistema y del usuario. Para productos de software genéricos, significa que debería de haber pruebas para todas las características del sistema que se incorporarán en la entrega del producto.
- Para descubrir errores en el software en que el comportamiento de éste es incorrecto, no deseable o no cumple su especificación. La prueba de errores está relacionada con la eliminación de todos los tipos de comportamientos del sistema no deseables, tales como caídas del sistema, interacciones no permitidas con otros sistemas, cálculos incorrectos y corrupción de datos.

De las muchas definiciones válidas de la “prueba del software” podemos quedarnos con:

- La prueba es el proceso de ejecución de un programa con la intención de descubrir errores (Glenford Myers).

- La prueba es cualquier actividad dirigida a evaluar la capacidad de un programa y determinar que alcanza los resultados requeridos.

38.1.1 Principios de las pruebas

Conocida la definición de prueba, algunos de los principios que les afectan son:

- La prueba es el proceso de ejecutar un programa con la intención de descubrir errores, por lo que un buen caso de prueba es aquel que tiene una alta probabilidad de descubrir un error no encontrado hasta entonces.
- Las pruebas deben planificarse antes de que se empiece a codificar. Así la planificación comienza con el modelo de requisitos, y la definición detallada de los casos de prueba una vez que el diseño del sistema está consolidado.
- El 80% de los errores estarán localizados en el 20% de los módulos.
- La prueba completa es imposible.
- Para ser más eficaces, las pruebas deberían ser hechas por un equipo independiente.
- La probabilidad de la existencia de más errores en una parte del software es proporcional al número de errores ya encontrados en dicha parte.

38.2 Pruebas de Caja Negra y Caja Blanca.

Cualquier producto de ingeniería se puede probar de una de estas dos formas:

- Conociendo la función específica para la que fue diseñado el producto, se pueden llevar a cabo pruebas que demuestren que cada función es completamente operativa.

- Conociendo el funcionamiento del producto, se pueden desarrollar pruebas que aseguren que “todas las piezas encajan”, o sea, que las operaciones internas se ajustan a las especificaciones y que todos los componentes internos se han comprobado de forma adecuada.

El primer enfoque de prueba se denomina prueba de **caja negra** y el segundo, prueba de **caja blanca**.

La prueba de **caja negra** se refiere a las pruebas que se llevan a cabo sobre la interfaz del software. O sea, los casos de prueba pretenden demostrar que las funciones del software son operativas, que la entrada se acepta de forma adecuada y que se produce un resultado correcto, así como que la integridad de la información externa (por ejemplo, archivos de datos) se mantiene. Una prueba de caja negra examina algunos aspectos del modelo fundamental del sistema sin tener en cuenta la estructura lógica interna del software.

La prueba de **caja blanca** del software se basa en el minucioso examen de los detalles procedimentales. Se comprueban los caminos lógicos del software proponiendo casos de prueba que ejerciten conjuntos específicos de condiciones y/o bucles. Se puede examinar el “estado del programa” en varios puntos para determinar si el estado real coincide con el esperado o mencionado.

38.2.1 Pruebas de caja blanca

El enfoque de la estrategia de pruebas conocido por el nombre de método de **caja blanca** o, también, **conducido por la lógica** o “**logic driven**”, se centra en probar el comportamiento interno y la estructura del programa, examinando la lógica interna del mismo y sin considerar los aspectos de rendimiento. El objetivo de este enfoque es ejecutar, al menos una vez, todas las sentencias y ejecutar todas las condiciones tanto en su vertiente verdadera como falsa, teniendo en cuenta que la única información de entrada con que se cuenta es el diseño del programa y el código fuente.

Las técnicas específicas más usuales que siguen el método de caja blanca son:

- Prueba del camino básico
- Prueba de la estructura de control
 - o Prueba de condiciones
 - o Prueba de flujo de datos
 - o Prueba de bucles

38.2.1.1. Prueba del camino básico

La prueba del camino básico fue propuesta inicialmente por Thomas J. McCabe. También propuso el término complejidad ciclomática, muy relacionado con el camino básico y que veremos más adelante.

Esta prueba del camino básico permite al diseñador de casos de prueba obtener una medida de la complejidad lógica de un diseño procedimental y usar esa medida como guía para la definición de un conjunto básico de caminos de ejecución. Los casos de prueba obtenidos del conjunto básico garantizan que durante la prueba se ejecuta por lo menos una vez cada sentencia del programa.

De la técnica del camino básico se derivan dos pruebas complementarias y no excluyentes:

- *Prueba de cobertura de sentencias.* Consiste en generar casos de prueba que permitan probar todas y cada una de las sentencias de un módulo una vez. Esta prueba es necesaria pero no es suficiente.
- *Prueba de cobertura de condiciones.* Consiste en diseñar juegos de prueba que consideren todos los valores posibles de cada una de las condiciones. Esta prueba también es necesaria pero no es suficiente ya que no garantiza que todos los caminos sean cubiertos, por lo que debe ser complementada con la anterior.

La técnica de prueba del camino básico utiliza una convención de representación denominada “grafos de flujo” para la determinación de caminos y para ello se apoya en el concepto de “complejidad ciclomática”.

La notación de “**grafo de flujo**” se utiliza para simplificar el desarrollo del conjunto básico de caminos de ejecución. Su objetivo es ejemplificar el flujo de control del módulo que se está probando y para ello utiliza tres elementos:

- **Nodos** o tareas de procesamiento (N). Representan cero, una o varias sentencias procedimentales. Cada nodo comprende como máximo una sentencia de decisión (bifurcación). Cada nodo que contiene una condición se denomina **nodo predicado** y está caracterizado porque dos o más aristas emergen de el.
- **Aristas**, flujo de control o conexiones (A). Unen dos nodos, incluso aunque el nodo no represente ninguna sentencia procedimental.
- **Regiones** (R). Son las áreas delimitadas por las aristas y nodos. Cuando se contabilizan las regiones debe incluirse el área externa como una región más.

La **complejidad ciclomática** es una métrica del software basada en la teoría de grafos, que proporciona una medición cuantitativa de la complejidad lógica de un programa. Cuando se usa en el contexto del método de prueba del camino básico, el valor calculado como complejidad ciclomática define el número de caminos independientes del conjunto básico de un programa y nos da un límite superior para el número de pruebas que se deben realizar para asegurar que se ejecuta cada sentencia al menos una vez. Un camino independiente es cualquier camino del programa que introduce, por lo menos, un nuevo conjunto de sentencias de proceso o una nueva condición. En términos del grafo de flujo, un camino independiente está constituido por lo menos por una arista que no haya sido recorrida anteriormente a la definición del camino. El valor de la complejidad se puede obtener de tres formas:

- 1- El número de regiones del grafo. (R)
- 2- El número de aristas menos el número de nodos + 2. ($A - N + 2$.)
- 3- Número de nodos predicado + 1. ($P + 1$)

La prueba del camino básico nos permite obtener los casos de prueba de la siguiente forma:

- 1- Usando el diseño o el código como base, dibujamos el correspondiente grafo de flujo.
- 2- Determinamos la complejidad ciclomática del grafo de flujo resultante.
- 3- Determinamos un conjunto básico de caminos linealmente independientes.
- 4- Preparamos los casos de prueba que forzarán la ejecución de cada camino del conjunto básico.

38.2.1.2 Pruebas de la estructura de control

Dentro de éste tipo de pruebas se contempla el método del camino básico mencionado anteriormente pero además se complementa con otras pruebas asociadas que permiten ampliar la cobertura de la prueba y mejorar su calidad.

38.2.1.2.1 Prueba de condición.

Es un método de diseño de casos de prueba que ejercita las condiciones lógicas contenidas en el módulo de un programa. Algunos conceptos empleados alrededor de esta prueba son los siguientes:

- *Condición simple:* es una variable lógica o una expresión relacional ($E_1 < operador - relacional > E_2$).
- *Condición compuesta:* esta formada por dos o más condiciones simples, operadores lógicos y paréntesis.

En general los tipos de errores que se buscan en una prueba de condición, son los siguientes:

- *Error en operador lógico* (existencia de operadores lógicos incorrectos, desaparecidos, sobrantes).
- *Error en variable lógica.*
- *Error en paréntesis lógico.*
- *Error en operador relacional.*
- *Error en expresión aritmética.*

38.2.1.2.2 Prueba del flujo de datos.

Selecciona caminos de prueba de un programa de acuerdo con la ubicación de las definiciones y los usos de las variables del programa.

38.2.1.2.3. Prueba de bucles

La prueba de bucles es una técnica de prueba de caja blanca que se centra exclusivamente en la validez de las construcciones de bucles. Se pueden definir cuatro clases diferentes de bucles:

- **Bucles simples.** A los bucles simples se les debe aplicar el siguiente conjunto de pruebas, donde ***n*** es el número máximo de pasos permitidos por el bucle:
 1. pasar por alto totalmente el bucle
 2. pasar una sola vez por el bucle
 3. pasar dos veces por el bucle
 4. hacer *m* pasos por el bucle con $m < n$
 5. hacer $n - 1$, n y $n+1$ pasos por el bucle

- **Bucles anidados.** Si extendiéramos el enfoque de prueba de los bucles simples a los bucles anidados, el número de posibles pruebas aumentaría geométricamente a medida que aumenta el nivel de anidamiento. Esto llevaría un número impracticable de pruebas. Se sugiere un enfoque que ayuda a reducir el número de pruebas:
 1. Comenzar por el bucle más interior. Establecer o configurar los demás bucles con sus valores mínimos.
 2. Llevar a cabo las pruebas de bucles simples para el bucle más interior, mientras se mantienen los parámetros de iteración (por ejemplo, contador del bucle) de los bucles externos en sus valores mínimos. Añadir otras pruebas para valores fuera de rango o excluidos.
 3. Progresar hacia fuera, llevando a cabo pruebas para el siguiente bucle, pero manteniendo todos los bucles externos en sus valores mínimos y los demás bucles anidados en sus valores «típicos».
 4. Continuar hasta que se hayan probado todos los bucles.
- **Bucles concatenados.** Los bucles concatenados se pueden probar mediante el enfoque anteriormente definido para los bucles simples, mientras cada uno de los bucles sea independiente del resto. Sin embargo, si hay dos bucles concatenados y se usa el controlador del bucle 1 como valor inicial del bucle 2, entonces los bucles no son independientes. Cuando los bucles no son independientes, se recomienda usar el enfoque aplicado para los bucles anidados.
- **Bucles no estructurados.** En este caso, ante la complejidad que puede representar la comprensión del flujo de control, es más práctico rediseñar el módulo a probar de forma que se codifique mediante bucles estructurados.

38.2.2 Pruebas de caja negra.

El enfoque de la estrategia de pruebas conocido por el nombre de método de **caja negra** o, también, “**conducido por los datos**” (**data driven**) o “**conducido por la entrada/salida**” (**input-output driven**), o también **pruebas de comportamiento**, no considera el detalle procedimental de los programas y se centra en buscar situaciones donde el programa no se ajusta a su especificación, utilizando ésta como entrada para derivar los casos de prueba.

Si por las especificaciones funcionales se sabe lo que tiene que hacer un módulo, es más sencillo comprobarlo que desmenuzarlo y examinarlo internamente en todas las circunstancias posibles. Por ello, las pruebas de «caja negra» son el enfoque más simple de prueba del software. Los casos de prueba se diseñan a partir de las especificaciones funcionales.

En este tipo de pruebas los casos de prueba consisten en conjuntos de datos de entrada que deberán generar una salida acorde con la especificación. La atención se centra, pues, en los datos de entrada y salida ignorando intencionadamente el conocimiento del código del programa. Si con esta técnica se quisieran encontrar todos los errores del programa, habría que recurrir a probar todas las posibles combinaciones de casos de entrada, lo que supondría generar todas las posibles combinaciones de valores para todas las posibles variables de entrada, y ello, en la realidad, es imposible. De esta imposibilidad se pueden extraer la conclusión de que mediante el método de la caja negra no es posible asegurar que un programa esté libre de errores.

Dado que no se pueden probar todos los casos posibles, el método de caja negra contempla una serie de técnicas encaminadas a simplificar los casos de prueba. Éstas son:

- Partición equivalente
- El análisis de valores límite.

- Los valores típicos de error y los valores imposibles.
- Métodos de prueba basados en grafos.
- Prueba de la tabla ortogonal
- Las pruebas de comparación.

38.2.2.1 Partición equivalente.

La **partición equivalente** es un método de prueba de caja negra que divide el campo de entrada de un programa en clases de datos de los que se pueden derivar casos de prueba. Un caso de prueba ideal descubre de forma inmediata una clase de errores (por ejemplo, proceso incorrecto de todos los datos de carácter) que, de otro modo, requerirían la ejecución de muchos casos antes de detectar el error genérico. La partición equivalente se dirige a la definición de casos de prueba que descubran clases de errores, reduciendo así el número total de casos de prueba que hay que desarrollar.

El diseño de casos de prueba para la partición equivalente se basa en una evaluación de las clases de equivalencia para una condición de entrada. Una **clase de equivalencia** representa un conjunto de estados válidos o no válidos para condiciones de entrada. Típicamente, una condición de entrada es un valor numérico específico, un rango de valores, un conjunto de valores relacionados o una condición lógica. Las clases de equivalencia se pueden definir de acuerdo con las siguientes directrices:

- 1- Si una condición de entrada especifica un rango, se define una clase de equivalencia válida y dos no válidas.
- 2- Si una condición de entrada requiere un valor específico, se define una clase de equivalencia válida y dos no válidas.
- 3- Si una condición de entrada especifica un miembro de un conjunto, se define una clase de equivalencia válida y una no válida.

- 4- Si una condición de entrada es lógica, se define una clase de equivalencia válida y una no válida.

38.2.2.2 Análisis de valores límite.

El **análisis de valores límite** AVL es una técnica de diseño de casos de prueba que complementa a la partición de equivalencia y se justifica en la constatación de que para una condición de entrada que admite un rango de valores, es más fácil que existan errores en los límites que en el centro. Por tanto, la diferencia entre esta técnica y la partición de equivalencia estriba en que en el análisis de valores límite no se selecciona un elemento representativo de la clase de equivalencia, sino que se seleccionan uno o más elementos de manera que los límites de cada clase de equivalencia son objeto de prueba. Otra diferencia es que con esta técnica también se derivan casos de prueba para las condiciones de salida.

Al igual que en el caso anterior, la técnica de análisis de valores límite no asegura la prueba completa, ya que es imposible probar exhaustivamente todos los conjuntos de datos de entrada tanto en su vertiente válida como inválida. Sin embargo, la ventaja que presenta esta técnica es que maximiza el número de errores encontrados con el menor número de casos de prueba posibles, lo que rentabiliza la inversión efectuada en la prueba.

Las directrices de AVL son similares en muchos aspectos a las que proporciona la partición equivalente:

- 1- Si una condición de entrada especifica un rango delimitado por los valores a y b , se deben diseñar casos de prueba para los valores a y b , y para los valores justo por debajo y justo por encima de a y b , respectivamente.
- 2- Si una condición de entrada especifica un número de valores, se deben desarrollar casos de prueba que ejerciten los valores máximo

y mínimo. También se deben probar los valores justo por encima y justo por debajo del máximo y del mínimo.

- 3- Aplicar las directrices 1 y 2 a las condiciones de salida.
- 4- Si las estructuras de datos internas tienen límites preestablecidos (por ejemplo, una matriz que tenga un límite definido de 100 entradas), hay que asegurarse de diseñar un caso de prueba que ejerce la estructura de datos en sus límites.

38.2.2.3. Valores típicos de error y valores imposibles.

Un buen complemento de las dos técnicas fundamentales de pruebas tipo «caja negra» (particiones de equivalencia y análisis de valores límite) consiste en incluir en los casos de prueba ciertos valores de los datos de entrada susceptibles de causar problemas, esto es, valores típicos de error, y valores especificados como no posibles, es decir, valores imposibles.

La determinación de los valores típicos de error se realiza en función de la naturaleza y funcionalidad del programa a probar, por lo que depende en buena medida de la experiencia del diseñador de la prueba.

Asimismo, dentro de las especificaciones del sistema o del programa a probar puede haber valores de datos especificados como no posibles. El hecho de probar estos valores imposibles se debe a que dichos valores podrían haber sido generados internamente por el sistema o el programa provocando un mal funcionamiento del mismo. La prueba de valores imposibles debe realizarse siempre que dichos valores puedan ser detectados y el programa pueda manejarlos adecuadamente sin provocar errores irreparables.

38.2.2.4 Métodos de prueba basados en grafos.

En este método se debe entender los objetos (objetos de datos, objetos de programa tales como módulos o colecciones de sentencias del lenguaje de programación) que se modelan en el software y las relaciones que conectan a estos objetos. Una vez que se ha llevado a cabo esto, el siguiente paso es definir una serie de pruebas que verifiquen que todos los objetos tienen entre ellos las relaciones esperadas. En este método:

1. Se crea un grafo de los objetos importantes y sus relaciones.
2. Se diseña una serie de pruebas que cubran el grafo de manera que se ejerciten todos los objetos y sus relaciones para descubrir errores.

Boris Beizer describe una serie de modelados para pruebas de comportamiento que pueden hacer uso de los grafos:

- *Modelado del flujo de transacción.* Los nodos representan los pasos de alguna transacción y los enlaces representan las conexiones lógicas entre esos pasos.
- *Modelado de estado finito.* Los nodos representan diferentes estados del software observables por el usuario, y los enlaces representan las transiciones que ocurren para moverse de estado a estado.
- *Modelado de flujo de datos.* Los nodos objetos de datos y los enlaces son las transformaciones que ocurren para convertir un objeto de datos en otro.
- *Modelado de planificación.* Los nodos son objetos de programa y los enlaces son las conexiones secuenciales entre esos objetos. Los pesos de enlace se usan para especificar los tiempos de ejecución requeridos al ejecutarse el programa.
- *Gráfica Causa-efecto.* Un gráfico de causa-efecto es un lenguaje formal al cual se traduce una especificación permitiendo seleccionar un gran conjunto de casos de prueba. El gráfico es realmente un circuito de lógica digital (una red combinatoria de lógica), pero en vez

de la notación estándar de la electrónica, se utiliza una notación algo más simple. No es preciso tener conocimientos de electrónica con excepción de una comprensión de la lógica booleana (entendiendo los operadores de la lógica y, o, y no). Tiene un efecto secundario beneficioso ya que permite precisar estados incompletos y ambigüedades en la especificación.

38.2.2.5 Prueba de tabla ortogonal

Hay aplicaciones donde el número de parámetros de entrada es pequeño y los valores de cada uno de los parámetros están claramente delimitados. Cuando estos números son muy pequeños (por ejemplo, 3 parámetros de entrada tomando 3 valores diferentes), es posible considerar cada permutación de entrada y comprobar exhaustivamente el proceso del dominio de entrada. En cualquier caso, cuando el número de valores de entrada crece y el número de valores diferentes para cada elemento de los datos se incrementa, la prueba exhaustiva se hace impracticable.

La prueba de la **tabla ortogonal** puede aplicarse a problemas en que el dominio de entrada es relativamente pequeño pero demasiado grande para posibilitar pruebas exhaustivas. El método de prueba de la tabla ortogonal es particularmente útil al encontrar errores asociados con fallos localizados -una categoría de error asociada con defectos de la lógica dentro de un componente software-. La prueba de tabla ortogonal permite proporcionar una buena cobertura de pruebas con bastantes menos casos de prueba que en la estrategia exhaustiva.

38.2.2.6 Prueba de comparación.

Hay situaciones en las que la fiabilidad del software es algo absolutamente crítico. En ese tipo de aplicaciones, a menudo se utiliza hardware y software redundante para minimizar la posibilidad de error. Cuando se

desarrolla software redundante, varios equipos de ingeniería del software separados desarrollan versiones independientes de una aplicación, usando las mismas especificaciones. En esas situaciones, se deben probar todas las versiones con los mismos datos de prueba, para asegurar que todas proporcionan una salida idéntica. Luego, se ejecutan todas las versiones en paralelo y se hace una comparación en tiempo real de los resultados, para garantizar la consistencia.

Esas versiones independientes son la base de una técnica de prueba de caja negra denominada ***prueba de comparación o prueba mano a mano***.

38.3 Estrategias de prueba del software.

Una estrategia de prueba del software integra las técnicas de diseño de casos de prueba en una serie de pasos bien planificados que dan como resultado una correcta construcción del software. La estrategia proporciona un mapa que describe los pasos que hay que llevar a cabo como parte de la prueba, cuándo se deben planificar y realizar esos pasos, y cuánto esfuerzo, tiempo y recursos se van a requerir. Por tanto, cualquier estrategia de prueba debe incorporar la planificación de la prueba, el diseño de casos de prueba, la ejecución de las pruebas y la agrupación y evaluación de los datos resultantes.

Una estrategia de prueba del software debe ser suficientemente flexible para promover la creatividad y la adaptabilidad necesarias para adecuar la prueba a todos los grandes sistemas basados en software. Al mismo tiempo, la estrategia debe ser suficientemente rígida para promover un seguimiento razonable de la planificación y la gestión a medida que progresa el proyecto.

Se han propuesto varias estrategias de prueba del software con distintos autores. Todas estas estrategias proporcionan al ingeniero del software una plantilla para la prueba y todas tienen las siguientes características generales:

- Las pruebas comienzan a nivel de módulo y trabajan “hacia fuera”, hacia la integración de todo el sistema.
- Según el momento, son apropiadas diferentes técnicas de prueba.
- La prueba la lleva a cabo el responsable del desarrollo del software y (para grandes proyectos) un grupo independiente de pruebas.
- La prueba y la depuración son actividades diferentes, pero la depuración se debe incluir en cualquier estrategia de prueba.

Una estrategia de prueba del software debe incluir pruebas de bajo nivel que verifiquen que todos los pequeños segmentos de código fuente se han implementado correctamente, así como pruebas de alto nivel que validen las principales funciones del sistema frente a los requisitos del cliente. Una estrategia debe proporcionar una guía al profesional y proporcionar un conjunto de hitos para el jefe de proyecto.

Se deben abordar los siguientes puntos si se desea implementar con éxito una estrategia de prueba del software:

- Especificar los requisitos del producto de manera cuantificable mucho antes de que comiencen las pruebas.
- Establecer los objetivos de la prueba de manera explícita.
- Comprender qué usuarios van a manejar el software y desarrollar un perfil para cada categoría de usuario.
- Desarrollar un plan de prueba que haga hincapié en la “prueba de ciclo rápido”
- Construir un software “robusto” diseñado para probarse a sí mismo
- Usar revisiones técnicas formales efectivas como filtro antes de la prueba.

- Llevar a cabo revisiones técnicas formales para evaluar la estrategia de prueba y los propios casos de prueba.
- Desarrollar un enfoque de mejora continua al proceso de prueba

Si consideramos el proceso desde el punto de vista procedimental, la prueba, en el contexto de la ingeniería del software, realmente es una serie de cinco pasos que se llevan a cabo secuencialmente. Inicialmente, la prueba se centra en cada módulo individualmente, asegurando que funcionan adecuadamente como una unidad. De ahí el nombre de *prueba de unidad*. La prueba de unidad hace un uso intensivo de las técnicas de prueba de caja blanca, ejercitando caminos específicos de la estructura de control del módulo para asegurar un alcance completo **y** una detección máxima de errores. A continuación, se deben ensamblar o integrar los módulos para formar el paquete de software completo.

La *prueba de integración* se dirige a todos los aspectos asociados con el doble problema de verificación **y** de construcción del programa. Durante la integración, las técnicas que más prevalecen son las de diseño de casos de prueba de caja negra, aunque se pueden llevar a cabo algunas pruebas de caja blanca con el fin de asegurar que se cubren los principales caminos de control. Después de que el software se ha integrado (construido), se dirigen un conjunto de *pruebas de alto nivel*. Se debe comprobar que el software, al combinarlo con otros elementos del sistema (por ejemplo, hardware, gente, bases de datos), cada elemento encaja de forma adecuada y que se alcanza la funcionalidad y el rendimiento exigido. Esta es la base de la *prueba de sistemas*.

Posteriormente se asegurará mediante la *prueba de implantación* el funcionamiento correcto del sistema integrado de hardware y software en el entorno de operación, y permitir al usuario que, desde el punto de vista de operación, realice la aceptación del sistema una vez instalado en su entorno real y en base al cumplimiento de los requisitos no funcionales especificados. La *prueba de aceptación* proporciona una seguridad final de

que el software satisface todos los requisitos funcionales, de comportamiento y de rendimiento. Durante las últimas tres pruebas (*sistemas, implantación y aceptación*) se usan exclusivamente técnicas de prueba de caja negra.

38.3.1 Pruebas de Unidad

Las pruebas de unidad tienen como objetivo verificar la funcionalidad y estructura de cada componente individualmente una vez que ha sido codificado.

La **prueba de unidad** es un proceso para probar los subprogramas, las subrutinas, los procedimientos individuales o las clases en un programa. Es decir, es mejor probar primero los bloques desarrollados más pequeños del programa, que inicialmente probar el software en su totalidad. Las motivaciones para hacer esto son tres. (1) Las pruebas de unidad son una manera de manejar los elementos de prueba combinados, puesto que se centra la atención inicialmente en unidades más pequeñas del programa. (2) La prueba de una unidad facilita la tarea de eliminar errores (el proceso de establecer claramente y de corregir un error descubierto), puesto que, cuando se encuentra un error, se sabe que existe en un módulo particular. Finalmente, (3) las pruebas de unidad introducen paralelismo en el proceso de pruebas del software presentándose la oportunidad de probar los múltiples módulos simultáneamente.

Se necesitan dos tipos de información al diseñar los casos de prueba para una prueba de unidad: la especificación para el módulo y el código fuente del módulo. La especificación define típicamente los parámetros de entrada y de salida del módulo y su función.

Las pruebas de unidad son en gran parte orientadas a caja blanca. Una razón es que como en pruebas de entidades más grandes tales como

programas enteros (es el caso para los procesos de prueba subsecuentes), la prueba de caja blanca llega a ser menos factible. Una segunda razón es que los procesos de prueba subsecuentes están orientados a encontrar diversos tipos de errores. Por lo tanto, el procedimiento para el diseño de casos de prueba para una prueba de unidad es la siguiente: analizar la lógica del módulo usando uno o más de los métodos de caja blanca y después completar los casos de prueba aplicando métodos de caja negra a la especificación del módulo.

38.3.2 Pruebas de integración

El objetivo de las **pruebas de integración** es verificar el correcto ensamblaje entre los distintos componentes una vez que han sido probados unitariamente con el fin de comprobar que interactúan correctamente a través de sus interfaces, tanto internas como externas, cubren la funcionalidad establecida y se ajustan a los requisitos no funcionales especificados en las verificaciones correspondientes.

En las pruebas de integración se examinan las interfaces entre grupos de componentes o subsistemas para asegurar que son llamados cuando es necesario y que los datos o mensajes que se transmiten son los requeridos. Debido a que en las pruebas de unidad es necesario crear módulos auxiliares que simulen las acciones de los componentes invocados por el que se está probando y a que se han de crear componentes "conductores" para establecer las precondiciones necesarias, llamar al componente objeto de la prueba y examinar los resultados de la prueba, a menudo se combinan los tipos de prueba de unidad y de integración.

Los tipos fundamentales de integración son los siguientes:

- *Integración incremental*: se combina el siguiente componente que se debe probar con el conjunto de componentes que ya están probados

y se va incrementando progresivamente el número de componentes a probar. Con el tipo de prueba incremental lo más probable es que los problemas que surjan al incorporar un nuevo componente o un grupo de componentes previamente probado, sean debidos a este último o a las interfaces entre éste y los otros componentes.

- *Integración no incremental:* se prueba cada componente por separado y posteriormente se integran todos de una vez realizando las pruebas pertinentes. Este tipo de integración se denomina también **Big-Bang**.

Dentro de la *integración incremental*, tenemos tres tipos de estrategias:

- *Estrategia Descendente (top-down):* El primer componente que se prueba es el primero de la jerarquía. Los componentes de nivel más bajo se sustituyen por componentes auxiliares llamados **resguardos** para simular a los componentes invocados. Luego se van sustituyendo los resguardos subordinados por los componentes reales. Ventajas: Las interfaces entre los distintos componentes se prueban en una fase temprana y con frecuencia. Verifica los puntos de decisión o de control principales al principio del proceso de prueba.
- *Estrategia Ascendente (bottom-up):* En este caso se crean primero los componentes de más bajo nivel y se crean componentes **controladores** para simular a los componentes que los llaman. A continuación se sustituyen los controladores por los módulos desarrollados de más alto nivel y se prueban.
- *Estrategia combinada:* A menudo es útil aplicar las estrategias anteriores conjuntamente. De este modo, se prueban las partes principales del sistema con un enfoque **top-down**, mientras que las

partes de nivel más bajo se prueban siguiendo un enfoque **bottom-up**.

Cada vez que se añade un nuevo módulo como parte de una prueba de integración, el software cambia. Se establecen nuevos caminos de flujo de datos, pueden ocurrir nuevas E/S y se invoca una nueva lógica de control. Estos cambios pueden causar problemas con funciones que antes trabajaban perfectamente. En este contexto, la **prueba de regresión** es volver a ejecutar un subconjunto de pruebas que se han llevado a cabo anteriormente para asegurarse de que los cambios no han propagado efectos colaterales no deseados.

38.3.3 Pruebas de sistema

Las pruebas del sistema tienen como objetivo validar el sistema comprobando la integración del sistema de información globalmente, verificando el funcionamiento correcto de las interfaces entre los distintos subsistemas que lo componen y con el resto de sistemas de información con los que se comunica.

Una vez que se han probado los componentes individuales y se han integrado, se prueba el sistema de forma global. En esta etapa pueden distinguirse los siguientes tipos de pruebas, cada uno con un objetivo claramente diferenciado:

- **Pruebas funcionales.** Dirigidas a asegurar que el sistema de información realiza correctamente todas las funciones que se han detallado en las especificaciones dadas por el usuario del sistema.
- **Pruebas de comunicaciones.** Determinan que las interfaces entre los componentes del sistema funcionan adecuadamente, tanto a través de

dispositivos remotos, como locales. Asimismo, se han de probar las interfaces hombre/máquina.

- **Pruebas de rendimiento.** Consisten en determinar que los tiempos de respuesta están dentro de los intervalos establecidos en las especificaciones del sistema.
- **Pruebas de volumen.** Consisten en examinar el funcionamiento del sistema cuando está trabajando con grandes volúmenes de datos, simulando las cargas de trabajo esperadas.
- **Pruebas de sobrecarga.** Consisten en comprobar el funcionamiento del sistema en el umbral límite de los recursos, sometiéndole a cargas masivas. El objetivo es establecer los puntos extremos en los cuales el sistema empieza a operar por debajo de los requisitos establecidos.
- **Pruebas de disponibilidad de datos.** Consisten en demostrar que el sistema puede recuperarse ante fallos, tanto de equipo físico como lógico, sin comprometer la integridad de los datos.
- **Pruebas de facilidad de uso.** Consisten en comprobar la adaptabilidad del sistema a las necesidades de los usuarios, tanto para asegurar que se acomoda a su forma habitual de trabajo, como para determinar las facilidades que aporta al introducir datos en el sistema y obtener los resultados.
- **Pruebas de operación.** Consisten en comprobar la correcta implementación de los procedimientos de operación, incluyendo la planificación y control de trabajos, arranque y re arranque del sistema, etc.
- **Pruebas de entorno.** Consisten en verificar las interacciones del sistema con otros sistemas dentro del mismo entorno.

- **Pruebas de seguridad.** Consisten en verificar los mecanismos de control de acceso al sistema para evitar alteraciones indebidas en los datos.
- **Pruebas de configuración.** Programas tales como sistemas operativos, sistemas de gestión de base de datos, y programas de conmutación de mensajes soportan una variedad de configuraciones de hardware, incluyendo varios tipos y números de dispositivos de entrada-salida y líneas de comunicaciones, o diversos tamaños de memoria. A menudo el número de configuraciones posibles es demasiado grande para probar cada uno de los dispositivos, pero en lo posible, se debe probar el programa con cada tipo de dispositivo de hardware y con la configuración mínima y máxima. Si el programa por sí mismo se puede configurar para omitir componentes, o si puede funcionar en diversas computadoras, cada configuración posible de este debe ser probada.
- **Pruebas de instalación.** Un funcionamiento incorrecto del programa de instalación generaría una experiencia negativa en el usuario siendo una de las primeras experiencias del usuario con la aplicación. Si esta fase se realiza mal, entonces el usuario/el cliente puede buscar otro producto o tener poca confianza en la validez de la aplicación.
- **Pruebas de documentación.** La documentación del usuario debe ser inspeccionada, comprobando esta para saber si hay exactitud y claridad. Cualquiera de los ejemplos ilustrados en la documentación se deben probar y hacer parte de los casos de uso y se deben introducir en el programa.

38.3.4 Prueba de implantación

El objetivo de las **pruebas de implantación** es comprobar el funcionamiento correcto del sistema integrado de hardware y software en

el entorno de operación, y permitir al usuario que, desde el punto de vista de operación, realice la aceptación del sistema una vez instalado en su entorno real y en base al cumplimiento de los requisitos no funcionales especificados.

Una vez que hayan sido realizadas las pruebas del sistema en el entorno de desarrollo, se llevan a cabo las verificaciones necesarias para asegurar que el sistema funcionará correctamente en el entorno de operación. Debe comprobarse que responde satisfactoriamente a los requisitos de rendimiento, seguridad, operación y coexistencia con el resto de los sistemas de la instalación para conseguir la aceptación del usuario de operación.

Las pruebas de **seguridad** van dirigidas a verificar que los mecanismos de protección incorporados al sistema cumplen su objetivo; las de **rendimiento** a asegurar que el sistema responde satisfactoriamente en los márgenes establecidos en cuanto tiempos de respuesta, de ejecución y de utilización de recursos, así como los volúmenes de espacio en disco y capacidad; por último con las pruebas de **operación** se comprueba que la planificación y control de trabajos del sistema se realiza de acuerdo a los procedimientos establecidos, considerando la gestión y control de las comunicaciones y asegurando la disponibilidad de los distintos recursos.

Asimismo, también son llevadas a cabo las pruebas **de gestión de copias de seguridad y recuperación**, con el objetivo de verificar que el sistema no ve comprometido su funcionamiento al existir un control y seguimiento de los procedimientos de salvaguarda y de recuperación de la información, en caso de caídas en los servicios o en algunos de sus componentes. Para comprobar estos últimos, se provoca el fallo del sistema, verificando si la recuperación se lleva a cabo de forma apropiada. En el caso de realizarse de forma automática, se evalúa la inicialización, los mecanismos de recuperación del estado del sistema, los datos y todos aquellos recursos que se vean implicados.

Las verificaciones de las pruebas de implantación y las pruebas del sistema tienen muchos puntos en común al compartir algunas de las fuentes para su diseño como pueden ser los casos para las pruebas de rendimiento (pruebas de sobrecarga o de stress).

El responsable de implantación junto al equipo de desarrollo determina las verificaciones necesarias para realizar las pruebas así como los criterios de aceptación del sistema. Estas pruebas las realiza el equipo de operación, integrado por los técnicos de sistemas y de operación que han recibido previamente la formación necesaria para llevarlas a cabo.

38.3.6 Pruebas de aceptación

El objetivo de las **pruebas de aceptación** es validar que un sistema cumple con el funcionamiento esperado y permitir al usuario de dicho sistema que determine su aceptación desde el punto de vista de su funcionalidad y rendimiento.

Las pruebas de aceptación son definidas por el usuario del sistema y preparadas por el equipo de desarrollo, aunque la ejecución y aprobación final corresponden al usuario. Estas pruebas van dirigidas a comprobar que el sistema cumple los requisitos de funcionamiento esperado, recogidos en el catálogo de requisitos y en los criterios de aceptación del sistema de información, y conseguir así la aceptación final del sistema por parte del usuario.

El responsable de los usuarios debe revisar los criterios de aceptación que se especificaron previamente en el plan de pruebas del sistema y, posteriormente, dirigir las pruebas de aceptación final. La validación del sistema se consigue mediante la realización de pruebas de caja negra que demuestran la conformidad con los requisitos y que se recogen en el plan de pruebas, el cual define las verificaciones a realizar y los casos de prueba asociados. Dicho plan está diseñado para asegurar que se satisfacen todos los requisitos funcionales especificados por el usuario teniendo en cuenta

también los requisitos no funcionales relacionados con el rendimiento, seguridad de acceso al sistema, a los datos y procesos, así como a los distintos recursos del sistema.

La formalidad de estas pruebas dependerá en mayor o menor medida de cada organización, y vendrá dada por la criticidad del sistema, el número de usuarios implicados en las mismas y el tiempo del que se disponga para llevarlas cabo, entre otros.

Si el software se desarrolla como un producto que va a ser usado por muchos clientes, no es práctico realizar pruebas de aceptación formales para cada uno de ellos. La mayoría de los desarrolladores de productos de software llevan a cabo un proceso denominado prueba alfa y beta para descubrir errores que parezca que sólo el usuario final puede descubrir.

La **prueba alfa** se lleva a cabo, por un cliente, en el lugar de desarrollo. Se usa el software de forma natural con el desarrollador como observador del usuario y registrando los errores y los problemas de uso. Las pruebas alfa se llevan a cabo en un entorno controlado.

La **prueba beta** se lleva a cabo por los usuarios finales del software en los lugares de trabajo de los clientes. A diferencia de la prueba alfa, el desarrollador no está presente normalmente. Así, la prueba beta es una aplicación «en vivo» del software en un entorno que no puede ser controlado por el desarrollador. El cliente registra todos los problemas (reales o imaginarios) que encuentra durante la prueba beta e informa a intervalos regulares al desarrollador. Como resultado de los problemas informados durante la prueba beta, el desarrollador del software lleva a cabo modificaciones y así prepara una versión del producto de software para toda la clase de clientes.

Bibliografía



Pressman, R. "Software Engineering" Editorial McGraw-Hill. 2009

Ian Sommerville - "Ingeniería de Software" 7 Edición. Editorial Prentice Hall, 2005

Carlo Ghezzi, Mehdi Jazayeri, Dino Mandrioli. "Fundamentals of Software Engineering". Ed. Prentice-Hall. 2002

Métrica 3 - Técnicas y Prácticas. Ministerio de Administraciones Públicas

Autor: Francisco Javier Rodríguez Martínez.

Subdirector de la Escuela Superior de Ingeniería Informática.

Universidad de Vigo.

39. MODELOS DE CALIDAD. INGENIERÍA DE PROCESOS DE SOFTWARE: CMMI, ISO 15504, ISO 9000-3. MODELOS ÁGILES. SEGURIDAD EN LOS SISTEMAS DE INFORMACIÓN.

Tema 39: Modelos de calidad. Ingeniería de procesos de software: CMMI, ISO 15504, ISO 9000-3. Modelos ágiles.

INDICE

- 1- Introducción al concepto de calidad
 - 1.1 Calidad del software
- 2- Modelos de Calidad
 - 2.1 Modelo de calidad clásico de McCall
 - 2.2 CMM- CMMI
 - 2.3 SPICE y la norma ISO 15504
 - 2.4 ISO 9000-3
 - 2.5 Modelos Ágiles.

1. Introducción al concepto de calidad

A lo largo del tema vamos a tratar la calidad como un elemento básico que nos va a permitir valorar de una manera objetiva determinados sistemas de información. Antes de entrar en detalle acerca de qué representa la calidad en el ámbito de los sistemas de información, y que mecanismos existen a nuestra disposición para garantizar un alcance mínimo de esta medida cualitativa, se necesita inicialmente acordar qué entendemos por calidad.

La calidad, a nivel general, podemos definirla como una propiedad intrínseca de cualquier cosa, que nos va a permitir poder comprarla con otra entidad de su misma especie, con objeto de determinar para ciertos aspectos cuál presenta un mejor grado de satisfacción para un propósito determinado. El concepto actual de **calidad** procede del mundo empresarial y, más concretamente, del de los procesos productivos. En el mundo empresarial es relativamente frecuente encontrar el término calidad asociado a otros conceptos tales como eficacia, eficiencia o productividad. Se pueden encontrar múltiples definiciones del concepto de calidad, casi tantas como autores hablan sobre la materia:

- *“Propiedad o conjunto de propiedades inherentes a algo, que permiten juzgar su valor”*. Real Academia Lengua.
- *“El conjunto de todas aquellas propiedades y características de un producto o servicio que se refieren a su capacidad para satisfacer unas necesidades implícitas ó explícitas”*. ISO. Aquí observamos que está orientada a satisfacer al cliente, más que a obtener un producto bien hecho.
- *“Un modelo sistemático y planificado de todas las acciones necesarias para proporcionar la adecuada confianza que el proyecto precisa para los requerimientos establecidos”* IEEE
- *“El conjunto de acciones que permite asegurar que el producto responde a las necesidades expresadas por el usuario”*. Marta D’Amore.



- “*Consiste en diseñar, producir y servir un bien o un servicio que sea útil, lo máseconómico posible y siempre satisfactorio para el usuario*”. Ishikawa

Las definiciones anteriores plantean la idea de satisfacción de necesidades. Se fundamentan en que un componente básico de la calidad es la percepción que tienen los clientes del producto en función de lo que esperan de él. De forma sencilla, la satisfacción del cliente se puede definir como la diferencia entre las expectativas y la percepción del cliente respecto del producto o servicio. La interpretación del término calidad ha venido cambiando progresivamente, desde el concepto inicial de calidad aplicado al producto hasta llegar al actual de calidad aplicado a toda la organización. Esta evolución ha ido pasando por las siguientes etapas:

- *Orientada al producto: **Inspección*** después de la producción, auditoría sobre productos acabados y actividades de resolución de problemas. Es la fase inicial que algunas empresas aún hoy no han superado.
- *Orientada al proceso: **Control de la Calidad*** durante la fabricación, incluyendo el Control Estadístico del Proceso.
- *Orientada al sistema: **Aseguramiento de la Calidad***, involucrando a todos los departamentos y, en cierta manera, también a los proveedores.
- *Orientada hacia la gestión: **Gestión de la Calidad***, enfocada al cliente, considerando la participación del personal, basada en el desarrollo de los procesos y en la mejora continua.
- *Orientada hacia la excelencia empresarial o hacia las personas: Corresponde a la llamada **Calidad Total***, y apunta más allá de la calidad de los productos y de la eficiencia de los procesos para fijarse en la organización en su globalidad.

Estas etapas no están enfrentadas, sino que cada vez son más amplias de modo que cada etapa engloba a la anterior.

La **Gestión de la Calidad** representa la función dentro de una organización que determina y aplica las políticas de calidad. En términos más normalizados, la gestión de la calidad aparece definida por las normas UNE-EN ISO 9000:2000 como las actividades coordinadas para dirigir y controlar una organización en lo relativo a la calidad. Incluye actuaciones como el establecimiento de la política de la calidad y los objetivos de la calidad, la planificación de la calidad, el control de la calidad y la mejora de la calidad.

La **calidad total** (Total Quality Management, TQM) representa al conjunto de principios y métodos en una estrategia global para conseguir la dinamización de la organización y la satisfacción del cliente. La calidad total se gestiona mediante un modelo de Gestión de Calidad Total (TQM) que representa la propia estrategia orientada a crear una conciencia de calidad en todos los procesos de la organización. La norma ISO 8402 la define como *“Forma de gestión de una organización centrada en la calidad, basada en la participación de todos sus miembros y que pretende un éxito a largo plazo mediante la satisfacción del cliente y beneficios para todos los miembros de la organización y para la sociedad”*. Los aspectos más relevantes que lo identifican son:

1. La participación de todos los profesionales en el proceso de mejora continua. Todo el personal de la organización es agente y responsable de la calidad.
2. Todas las actividades de la organización están implicadas en la obtención de la calidad.
3. La implicación de la dirección en la planificación, organización y asignación de recursos para la calidad, tomando el papel de verdaderos motores del cambio cultural de su organización.
4. Una cultura basada en considerar al cliente como centro de nuestra actividad. Una forma de hacer en positivo, exenta de mecanismos de control punitivos, enfocada a la superación de metas, tanto profesionales como personales.

5. El concepto cliente, desarrollado en su doble versión de clientes internos y externos.
6. La prevención como un fin, el lema debe ser hacerlo bien a la primera. Empezando por el reconocimiento del error, rompiendo la permanente situación de negación de las equivocaciones y la detección de problemas como método de mejora.
7. El costo de la no-calidad. El planteamiento de que la calidad va ligada al binomio coste-eficacia, y que los errores suponen costes adicionales.

1.1 Calidad del software

La calidad en el software es una preocupación actual a la que cada vez se dedican más esfuerzos. La dependencia tecnológica actual en todos los sectores hace necesario establecer sistemas operativos que proporcionen alto rendimiento y fiabilidad para el control de tareas que pueden abarcar lo más sencillo hasta lo más crítico. Es por ello que el concepto de calidad tiene un peso específico, debido a que está ligado a todo un conjunto de procedimientos que permiten, además de ponderarla, asegurar que se alcanzan unos mínimos razonables de calidad que permiten garantizar que se cumplen determinadas expectativas para los usuarios. En cualquier caso, es necesario poner de manifiesto que el software casi nunca es perfecto, sin embargo todo proyecto de software debe plantearse como objetivo el producir software de la mejor calidad posible.

En el caso del software, la calidad del producto software se diferencia de la calidad de otros productos de fabricación industrial debido a las características especiales que tiene el propio software, tales como :

- Es un producto abstracto, no restringido por las leyes de la Física o por los límites de los procesos de fabricación, y su calidad también lo es.



- Se desarrolla, no se fabrica; por tanto, el coste y los errores se generan fundamentalmente en la fase de diseño y no en la de producción.
- No se deteriora con el tiempo. Los problemas que surgen durante el mantenimiento estaban allí desde el principio, es decir, no se generan nuevos errores.
- El software con errores no se rechaza. Se asume que es inevitable que el software presente errores.

También es importante destacar que la calidad de un producto software debe considerarse en todos sus estados de evolución (especificaciones, diseño, código...) y no basta con tener en cuenta sólo la calidad del producto una vez finalizado. Es decir, como primera aproximación al concepto de calidad del software, es importante diferenciar entre la calidad del producto y la calidad del proceso de desarrollo. No obstante, las metas que se fijen para la primera van a determinar las que se establezcan para la segunda, ya que la calidad del producto va a estar en función de la calidad del proceso de desarrollo.

Simplificando, podríamos definir la **calidad del software** como la “creación de productos software que, tanto eficaz como eficientemente, den completa satisfacción al usuario”. Esta definición merece algunos comentarios:

- 1- La calidad debe supeditarse al **grado** en el cual un cliente o usuario percibe que el software cumple sus expectativas. La palabra "grado" implica una valoración cuantitativa. En este sentido, las métricas constituyen una herramienta que ayuda a cuantificar aspectos de la calidad, de forma que ésta sea medible.
- 2- En la calidad intervienen los conceptos de **eficiencia** y de **eficacia**. Eficiencia es la capacidad para hacer las cosas bien (“do things right”). Por ejemplo, los desarrolladores realizan sus actividades correctamente, cometiendo pocos errores. Eficacia, o efectividad, es

la capacidad para hacer las cosas adecuadas (“do the right things”). Por ejemplo, los desarrolladores llevan a cabo las tareas adecuadas.

- 3- La calidad tiene un enfoque dirigido a las **características del producto**. Como consecuencia de ello, en primer lugar hay que documentar, luego discutir, ya que puede haber distintos puntos de vista en cuanto a las percepciones y las expectativas de cada usuario, y por último, consensuar. Estos pasos dan lugar a un proceso iterativo hasta llegar al consenso, que pasa por determinar los factores y criterios que intervienen en la calidad del software, y por cuantificar esos factores y criterios.

Otros autores han dado definiciones distintas para el concepto de calidad del software. Así, por ejemplo, el IEEE define la calidad del software como el “grado con el cual un cliente o usuario percibe que el software satisface sus expectativas”. JONES, señala que la calidad del software es la “ausencia de defectos o errores, siendo éstos las desviaciones respecto al comportamiento esperado”. Por último PRESSMAN señala que “Calidad es la conformidad con los requisitos que se hayan declarado explícitamente sobre funcionalidad y rendimiento, cumplimiento de estándares o normas documentadas que se hayan establecido, y existencia de otras características implícitas que son de esperar en un producto desarrollado en un contexto de práctica profesional”.

En cualquier caso, los principales problemas a los que nos enfrentamos a la hora de hablar de la calidad de un producto software son:

- **La definición misma de la calidad del software.** ¿Es realmente posible encontrar un conjunto de propiedades en un producto software que nos den una indicación de su calidad? Para ello se definen los **factores** y los **criterios** de calidad.
- **La comprobación de la calidad.** ¿Cómo medir el grado de calidad de un producto software en función de sus propiedades? Para ello se definen las **métricas** de calidad.

- **La mejora de la calidad del software.** ¿Cómo utilizar la información disponible sobre la calidad del producto software para mejorar su calidad a lo largo del ciclo de vida de desarrollo? Para ello se definen las actividades constructivas de la garantía de calidad del software.

39.2 Modelos de calidad

La consecuente preocupación derivada de la necesidad de elevar el control de la calidad en las organizaciones ha servido para impulsar la aparición de varios modelos y sistemas de potenciación de dicha calidad, modelos con los que se pretende estimar o valorar en qué grado la organización en cuestión alcanza el nivel de calidad acorde con el modelo aplicado.

Por tanto podemos definir, a grandes rasgos, un **modelo de calidad** como el conjunto de herramientas que guían a las Organizaciones a la Mejora Continua y la Competitividad dando las especificaciones de que tipo de requisitos deben de implementar para poder brindar productos y servicios de alto nivel.

Como ya se ha comentado, existen una gran cantidad de modelos de calidad que establecen mecanismos y procedimientos de implantación y valoración de característica. Los más conocidos y aplicados internacionalmente son los correspondientes a las normas **ISO**. Sin embargo, existen también otras alternativas como el Modelo Deming en Japón, el Modelo Malcolm Baldrige en Estados Unidos, y al Modelo de Excelencia de la EFQM, en Europa.

El modelo de Excelencia de la EFQM (Fundación Europea para la Gestión de la Calidad) se introdujo en 1991 como el marco de trabajo para la autoevaluación de las organizaciones y como base para juzgar a los concursantes por el Premio Europeo de la Calidad. Este modelo es el más

ampliamente utilizado en Europa en materia de calidad, y está orientado a ayudar a crear organizaciones fuertes que practiquen los principios de la administración de la calidad total (TQM) en sus procesos de negocio y relaciones con clientes, empleados, accionistas y comunidades en las que operan.

*Esquema de ponderación propuesto por el Modelo de Excelencia de la
EFQM*

La gestión de la calidad (*conjunto de actividades y medios necesarios para definir e implementar un sistema de la calidad y responsabilizarse de su control, aseguramiento y mejora continua*) a nivel de las empresas u organizaciones de software ha seguido dos líneas que pueden perfectamente complementarse entre sí. Por una parte, se ha seguido la línea marcada por las entidades internacionales de estandarización para todos los productos y servicios a través de las normas ISO 9000 y por otra, el mundo del software ha creado su propia línea de trabajo en la gestión de la calidad, trabajando sobre los procesos de producción de software como medio de asegurar la calidad del producto final.

Cuando los estándares de calidad se orientaban sobre todo al control, en las organizaciones dedicadas al software aparecen un grupo de modelos específicos con ese fin (modelos de calidad tradicionales), como: el Modelo FCM (*Factors /Criteria /Metrics*) de McCall (1.977), el Modelo de Boehm (1.978), el Marco ISO 9126 (ISO/IEC, 1991), el Paradigma GQM (*Goal-Question-Metric*) de Basili y Rombach (1.988), el Modelo de Gilb (1.988), etc.

En los últimos años en que los estándares de calidad internacionales han evolucionado hacia el aseguramiento de la calidad, primeramente, y hacia la calidad total, definitivamente, han aparecido en la industria del software dos importantes modelos de referencia que tienen en común la evaluación

de la capacidad de los procesos en niveles de desarrollo o madurez: el Modelo CMM - CMMI(*Capability Maturity Model - Capability Maturity Model Integration*) (Paulk, 1993), y el Modelo SPICE (*Software Process Improvement and Capability determination*) (Rout, 1995), (SPICE, 1999), que veremos en apartados posteriores.

2.1 Modelo de calidad clásico de McCall

El modelo de Jim McCall es un modelo de calidad clásico desarrollado inicialmente para la fuerza aérea de los EEUU en 1977. Es uno de los modelos de calidad del software de gestión más difundidos y ha servido como base para otros modelos como el de Boehm o el Software Quality Management -SQM- de Murine. Este modelo busca reducir la brecha entre usuarios y desarrolladores enfocándose en un número de factores de calidad que reflejen las prioridades de ambos.

El modelo de calidad McCall está organizado sobre tres tipos de Características de Calidad:

- **Factores** (especificar): Describen la visión externa del software, como es visto por los usuarios.
- **Criterios** (construir): Describen la visión interna del software, como es visto por el desarrollador.
- **Métricas** (controlar): Se definen y se usan para proveer una escala y método para la medida.

El modelo nos describe 11 factores de calidad del software, para los cuales establece 23 criterios y 41 métricas.

Los **factores de calidad** representan la calidad desde el punto de vista del usuario. Son, pues, elementos externos, y hacen referencia, según el Modelo de McCall (o **Modelo FCM**) al comportamiento actual del software (operación del producto), a la facilidad de cambio del software (revisión del

producto) y a la facilidad de conversión del software (transición del producto). Los once factores son:

- 1- **Corrección:** Mide hasta qué punto un producto software cumple sus especificaciones y satisface los objetivos requeridos por el usuario.

Se valora según los siguientes aspectos:

- 1.1. **Compleitud:** Atributos del software que proporcionan la implementación completa de todas las funciones requeridas.
- 1.2. **Consistencia:** Atributos del software que proporcionan uniformidad en las técnicas y notaciones de diseño e implementación.
- 1.3. **Trazabilidad o rastreabilidad:** Atributos del software que proporcionan una traza desde los requisitos a la implementación con respecto a un entorno operativo concreto.

- 2- **Fiabilidad:** Mide hasta qué punto un producto software realiza las funciones previstas en su diseño, con la precisión necesaria. Es decir, hasta qué punto se puede confiar en el funcionamiento sin errores del software. Factores:

- 2.1. **Precisión:** Atributos del software que proporcionan el grado de precisión requerido en los cálculos y los resultados.
- 2.2. **Consistencia.**
- 2.3. **Tolerancia a fallos:** Atributos del software que posibilitan la continuidad del funcionamiento bajo condiciones no usuales.
- 2.4. **Modularidad:** Atributos del software que proporcionan una estructura de módulos altamente independientes.
- 2.5. **Simplicidad:** Atributos del software que posibilitan la implementación de funciones de la forma más comprensible posible.

- 2.6. Exactitud: La precisión de los cálculos y del control.
- 3- **Eficiencia:** Mide el grado de optimización con el que el software utiliza los recursos informáticos para realizar la función que le ha sido asignada (¿Consume los recursos Hw y Sw de forma óptima?)
- 4- **Integridad** (seguridad): Mide hasta qué punto se pueden controlar los accesos ilegales (por personas no autorizadas) a los programas y a los datos. Factores:
- 4.1. Control de accesos. Atributos del software que proporcionan control de acceso al software y los [datos](#) que maneja.
 - 4.2. Facilidad de [auditoría](#): Atributos del software que facilitan la auditoría de los accesos al software.
 - 4.3. [Seguridad](#): La disponibilidad de mecanismos que controlen o protejan los programas o los datos.
- 5- **Usabilidad, facilidad de uso ó disponibilidad**): Mide el esfuerzo y coste necesario para aprender, operar, preparar la entrada e interpretar la salida de un producto software. Esto es, para aprender a manejar el producto.(¿Es cómodo y fácil de usar?)
- 6- **Mantenibilidad** (facilidadde mantenimiento):Mide el esfuerzo y coste necesario para localizar y corregir un error enun producto software que esté operativo. (¿Es susceptible de corregirse?)
- 7- **Verificabilidad (facilidad de prueba)**:Mide el esfuerzo y coste necesario para verificar un producto softwarecon el fin de garantizar que realiza la función prevista. Esto es, el esfuerzo y coste de probar un programa para comprobar que satisface sus requisitos.(¿Se puede probar?)
- 8- **Flexibilidad**:Mide el esfuerzo y coste necesario para modificar un producto softwareoperativo.(¿Se puede modificar?)



- 9- **Portabilidad:** Mide el esfuerzo y coste necesario para transferir un producto software de una configuración y/o entorno de hardware a otro. (¿Se puede utilizar en otro equipo?)
- 10- **Reusabilidad (reutilizabilidad):** Mide hasta qué punto puede utilizarse un producto software en otras aplicaciones. Es decir, hasta qué punto se puede transferir un módulo o programa a otra aplicación, y con qué esfuerzo. (¿Se puede rentabilizar total o parcialmente en otras aplicaciones?)
- 11- **Interoperabilidad:** Mide el esfuerzo y coste necesario para acoplar un sistema a otro. Es decir, para conectar dos productos entre sí. (¿Puede colaborar con otros productos software?)

Estos factores se pueden agrupar en tres grupos:

- Los factores de calidad que hacen referencia al comportamiento actual del software (operación o explotación del producto): Corrección, Fiabilidad, Eficiencia, Integridad y Usabilidad.
- Los que hacen referencia a la facilidad de cambio del producto (revisión): Mantenibilidad, Verificabilidad y Flexibilidad.
- Los que se refieren a la facilidad de conversión del software (transición del producto): Portabilidad, Reusabilidad e Interoperabilidad

Cada uno de los factores de calidad se descompone en un conjunto de **criterios** o atributos internos de calidad que, cuando están presentes, contribuyen al aspecto de la calidad que el factor asociado representa. Se trata, pues, de una visión de la calidad desde el punto de vista del producto software. Por tanto, los criterios de calidad son elementos internos o de los realizadores del software, y hacen referencia a la forma y estructura de los programas, los datos y los documentos. La relación entre los factores de calidad y los criterios se puede ver en la siguiente tabla:

factores de calidad	criterios de calidad
corrección	trazabilidad, completitud, coherencia
fiabilidad	coherencia, precisión, tolerancia a errores, simplicidad
eficiencia	eficiencia de memoria, eficiencia de ejecución
integridad	confidencialidad, control de accesos
usabilidad	operatividad, facilidad de aprendizaje, comunicabilidad
mantenibilidad	coherencia, simplicidad, modularidad, autodescripción, concisión
verificabilidad	simplicidad, modularidad, instrumentación, autodescripción
flexibilidad	modularidad, generalidad, expandibilidad, autodescripción
portabilidad	modularidad, autodescripción, independencia del entorno hardware, independencia del entorno software
reusabilidad	modularidad, generalidad, autodescripción, independencia del entorno hardware, independencia del entorno software
interoperabilidad	modularidad, estandarización de interfaces, estandarización de datos

Por último, al planificar la calidad de un producto hay que especificar para cada criterio el nivel de calidad que se considera aceptable; es decir, el valor mínimo o máximo aceptable. Por tanto, para cada uno de los criterios de calidad es necesario definir un conjunto de **métricas**, que son medidas cuantitativas de ciertas características del producto que, cuando están

presentes, dan una indicación del grado en que dicho producto posee un determinado atributo de calidad.

Las **métricas de calidad**, en su mayor parte medidas subjetivas, permiten la cuantificación de los factores y los criterios de calidad. Fundamentan su evaluación en la medida de los factores de calidad del software, a través de los criterios de calidad, y se basan en el examen detallado de los productos ya en proceso, si bien, también requieren un análisis estático de las especificaciones, diseño y programación de las aplicaciones.

2.2 CMM-CMMI

El modelo CMM inicial representa un modelo para la evaluación de los procesos de una organización, desarrollado inicialmente para los procesos relativos al desarrollo e implementación de software por la Universidad Carnegie-Mellon. El modelo CMM permite definir el grado de madurez de las prácticas de gestión y reingeniería de software de dichas organizaciones y determinar cuales son las acciones de mejora prioritarias para sus procesos de software.

El modelo CMM se compone de **cinco niveles de madurez** de acuerdo con la capacidad del proceso de software, definidos por los objetivos de los procesos que, cuando son satisfechos, permiten evolucionar al próximo nivel, ya que uno o más componentes importantes del proceso de software han sido estabilizados.

En cada nivel, se definen un conjunto de **áreas clave del proceso** que describen las funciones de ingeniería del software que deben llevarse a cabo para el desarrollo de una buena práctica. Mediante un amplio conjunto de métricas se determina la calidad de cada una de las áreas clave, obteniéndose una visión precisa del rigor, la eficacia y la eficiencia

de la metodología de desarrollo de una organización productora de software.

Cada una de las áreas está organizada en cinco secciones, denominadas **características comunes**. Estas son las siguientes:

- **Compromiso.** Es el conjunto de acciones que la organización debe realizar para poder asegurar que el proceso es repetible y duradero. Normalmente está relacionado con las políticas de la organización y el liderazgo de la dirección.
- **Capacidad.** Describe las precondiciones que deben darse en un proyecto o en la organización para implantar de forma efectiva los procesos de software. Habitualmente afecta a los recursos, a la estructura y a la formación.
- **Actividades.** Describen los roles y los procedimientos necesarios para implantar un área clave de proceso. Habitualmente incluyen procedimientos relacionados con la planificación y el seguimiento del trabajo, así como las acciones correctivas necesarias.
- **Medidas y análisis.** Describen la necesidad de realizar mediciones de los procesos y analizan dichas medidas. Suelen incluir ejemplos de las medidas tomadas para determinar el estado y la eficacia de las actividades realizadas.
- **Verificación.** Describe los pasos que deben llevarse a cabo para asegurar que las actividades se realizan según los procesos establecidos. Habitualmente incluye revisiones y auditorías por parte de la dirección y del grupo de aseguramiento de la calidad.

A su vez, en cada característica común se especifican unas **prácticas clave**, que son normas, procedimientos y actividades cuya realización lleva a la consecución de los objetivos del área. En algunos casos se detallan subprácticas más específicas, guías e interpretaciones de la práctica y, cuando procede, ejemplos y referencias cruzadas a otras prácticas. Asimismo, el modelo define **indicadores clave**, que son aquellas prácticas

clave o componentes de prácticas clave que ofrecen una visión mayor de la consecución de los objetivos de un área clave de proceso.

Los cinco niveles de madurez, representados en la imagen anterior, que forman parte del modelo son:

- 1- **Inicial:** el proceso de software es un proceso improvisado y caótico. No se han definido procesos metodológicos, o se han definido pero no se siguen. El éxito que se pueda obtener depende de las habilidades, conocimientos y motivaciones del personal. No existen calendarios ni estimados de costos y las funcionalidades y calidad del producto son impredecibles, ni un ambiente estable para el desarrollo y mantenimiento del software. El proceso del software es impredecible por el continuo cambio o modificación a medida que avanza el trabajo.
- 2- **Repetible:** se establecen políticas y procedimientos de administración e implantación del proceso básico para determinar costos, calendarios y funcionalidades. La madurez metodológica de la organización permite estimar fiablemente el tamaño funcional o físico del sistema, así como recursos, esfuerzo, costes y calendario. Se han sentado las bases para repetir éxitos anteriores en proyectos con aplicaciones similares. La organización muestra problemas de calidad y carece de una adecuada estructura para mejorarla. En este nivel, las áreas clave, cuyo estado se puede conocer mediante diversas métricas, son las siguientes:
 - Gestión de requisitos.
 - Planificación del proyecto software.
 - Seguimiento y control del proyecto.
 - Gestión de la subcontratación del software.
 - Aseguramiento de la calidad del software.
 - Gestión de la configuración del software.

- 3- **Definido:** el proceso de software para las actividades administrativas y técnicas está documentado, homogeneizado e integrado en un proceso de software estándar dentro de la organización, que ayudará a obtener un desempeño más efectivo. El grupo que trabaja en el proceso enfoca y guía sus esfuerzos al mejoramiento de su desarrollo, facilita la introducción de técnicas y métodos e informa a la administración del estado del proceso. La capacidad del proceso está basada en una amplia comprensión común dentro de la organización de las actividades, roles y responsabilidades definidas en el desarrollo de software. Las áreas claves, definidas para este nivel, son las siguientes:
- Desarrollo y mejora de los procesos de la organización.
 - Definición de los procesos de la organización.
 - Programa de formación.
 - Gestión integrada del software.
 - Ingeniería de producto software.
 - Coordinación intergrupos.
 - Revisión conjunta.
- 4- **Gestionado:** se recolectan medidas detalladas del proceso de software y de la calidad del producto. Ambos son cuantitativamente entendidos y controlados. Este nivel de capacidad permite a la organización predecir las tendencias en la calidad del producto dentro de los límites establecidos y tomar las acciones necesarias en caso que sean excedidos. Se puede predecir que los productos de dicha categoría son de alta calidad. Las áreas clave definidas para este nivel son las siguientes:
- Gestión cuantitativa del proyecto.
 - Gestión de calidad del software.

5- **Optimizado:** el mejoramiento continuo del proceso es garantizado por la retroalimentación cuantitativa y desde las pruebas de técnicas y herramientas innovadoras. La organización tiene los medios para identificar los puntos débiles y conocer como fortalecerlos. Su actividad clave es el análisis de las causas de defectos y su prevención. Las áreas clave definidas para este nivel son:

- Prevención de defectos.
- Gestión de cambios tecnológicos
- Gestión de cambios en los procesos.

La estructura del CMM brinda un camino progresivo recomendado para las organizaciones dedicadas al desarrollo de software que quieren mejorar la capacidad de su proceso de software. De forma general se identifican los siguientes **usos fundamentales**:

- Equipos de asesores, que usan el modelo para identificar los puntos fuertes y débiles en la organización.
- Equipos de evaluación, que utilizan CMM para identificar el riesgo de seleccionar entre diferentes contratos de negocio y para monitorearlos.
- Personal técnico y de dirección, que usa CMM para entender las actividades necesarias que ayuden a planear e implementar el programa de mejoramiento del proceso de software de la organización.
- Grupo de mejoramiento del proceso, que lo emplean como guía para ayudarse a definir y mejorar el proceso de software en la organización.

Desde el año 1991, el modelo CMM se fue adaptando a múltiples disciplinas: Ingeniería de sistemas, Ingeniería del Software, compras, desarrollo de procesos y productos integrados, etc., derivando modelos diferentes. La principal adaptación del modelo está orientada al desarrollo software. El Modelo de Madurez de la Capacidad del Software **SW-CMM**

(*Software Capability Maturity Model*) fue definido por Paulk, Curtis, Chrisis y Weber en 1.993 como un modelo que establece los niveles por los cuales las organizaciones de software hacen evolucionar sus definiciones, implementaciones, mediciones, controles y mejoras de sus procesos de software. Además del Modelo de Madurez de la Capacidad del Software existen el Modelo de Madurez de la Capacidad en la Adquisición de Software (SA-CMM), y el Modelo de Madurez de la Capacidad de las Personas (P-CMM), etc. Las organizaciones que deseaban mejorar sus procesos en todas estas disciplinas se encontraban con que el modelo presentaba grandes diferencias de arquitectura, enfoque, contenido y aplicación. Este hecho provocaba un gran incremento del coste de la implantación de CMM en términos de formación, evaluaciones y actividades de mejora, ya que no existía una integración de todos estos modelos. El proyecto de integración de CMM o CMMI (Capability Maturity Mode of Software Integration) surgió como solución a los problemas de falta de integración, y fue puesto en marcha para desarrollar un marco de trabajo simple de mejora de procesos, para organizaciones que persiguen la mejora en todos los ámbitos y niveles de la empresa.

CMMI contiene un conjunto de productos que, además de numerosos modelos adaptables a las diferentes áreas de conocimiento, contiene métodos de evaluación según cada modelo así como material de formación. El objetivo inicial de CMM: “Obtener productos de calidad dentro de los márgenes temporales previstos con el mínimo coste” no ha cambiado en CMMI. En cambio, CMMI basa la aplicación de todos los principios de CMM a lo largo de todo el ciclo de vida de ingeniería, no únicamente al ciclo de vida del desarrollo del producto software. Además, el conjunto de productos CMMI ha sido diseñado para mantener compatibilidad y correspondencia con el modelo **SPICE**. En resumen, CMMI puede ser considerado como una extensión del CMM-SW. Las diferencias principales son:

- Se han añadido nuevas áreas de proceso.

- Se han añadido mejores y más modernas prácticas clave.
- Se ha añadido un objetivo genérico para cada área de proceso.

Si se analizan estas diferencias en función del Nivel de madurez en que se hallan, se pueden encontrar las siguientes áreas de proceso en el modelo CMMI que no se encuentran en el modelo CMM:

- **Nivel 2.** Medición y análisis. Han sido aisladas de CMM todas las prácticas relacionadas con este objetivo y han sido agrupadas dentro de esta nueva área de proceso.
- **Nivel 3.** El área Ingeniería del producto software de CMM ha sido reemplazada en CMMI por múltiples y más detalladas áreas de proceso:
 - o Desarrollo de requisitos,
 - o Soluciones técnicas,
 - o Integración del producto,
 - o Verificación y Validación.

En el área de Gestión integrada del proyecto de CMM se contemplaba la Gestión de riesgos, pero ahora ha sido considerada como un área de proceso independiente. Finalmente, a este Nivel se ha añadido una nueva área denominada Análisis de decisiones y resolución, que no se encontraba en CMM.

- **Nivel 4.** Este Nivel ha sufrido una reestructuración y las áreas de Gestión cuantitativa de procesos y Gestión de la calidad de software han sido convertidas a Gestión cuantitativa del proyecto y Rendimiento o realización del proceso organizacional, respectivamente.
- **Nivel 5.** Tampoco ha habido grandes cambios en este Nivel, simplemente una fusión de las áreas Gestión de los

cambiostecnológicos y Gestión del cambio en los procesos en una única área de proceso: Innovación organizacional y despliegue. El área de Prevención de defectos ha sido reestructurada y renombrada a Análisis causal y resolución.

CMMI v1.1 tiene cuatro disciplinas disponibles:

- Ingeniería de Software: CMMI-SW (Software Engineering)
- Ingeniería de sistemas: CMMI-SE (Systems Engineering)
- Desarrollo integrado del producto y del proceso: CMMI-IPPD (Integrated Product and Process Development)
- Proveedores externos: CMMI-SS (Supplier Sourcing)

CMMI establece dos representaciones del modelo:

- **Continua:** capacidad de cada área de proceso. En esta representación, se enfoca la capacidad de cada área de proceso para establecer una línea a partir de la cual se puede medir la mejora individual en cada área. Al igual que el modelo por etapas, el modelo continuo tiene áreas de proceso que contienen prácticas, pero éstas se organizan de manera que soportan el crecimiento y la mejora de un área de proceso individual. Hay seis niveles de capacidad, del 0 al 5. La representación continua se centra en seleccionar una cierta área de procesos que mejorar y en fijar el nivel de capacidad deseado para esa área
- **Por etapas:** madurez organizacional. En esta representación se da un mapa predefinido dividido en etapas (los niveles de madurez), para la mejora organizacional y que se basa en procesos probados, agrupados y ordenados y sus relaciones asociadas. Cada nivel de madurez tiene un conjunto de áreas de proceso que indican donde una organización debería enfocar la mejora de su proceso. Cada área de proceso se describe en términos de prácticas que contribuyen a satisfacer sus objetivos. Las prácticas describen las actividades que

más contribuyen a la implementación eficiente de un área de proceso; se aumenta el “nivel de madurez” cuando se satisfacen los objetivos de todas las áreas de proceso de un determinado nivel de madurez.

Ambas representaciones incluyen Metas (Genéricas y Específicas, definiciones de resultados a obtener por la implementación efectiva de los grupos de prácticas) y Prácticas (Genéricas y Específicas, acciones a realizar para cumplir objetivos de área de proceso).

2.3 Software Process Improvement Capability Determination y la norma ISO 15504

En 1991, la ISO aprobó la realización de un estudio sobre la necesidad de crear un estándar internacional para la evaluación de procesos software, debido en gran parte al gran número de métodos de evaluación de procesos disponibles, y al uso creciente de estas técnicas en áreas comerciales sensibles. A raíz de esta aprobación se creó el proyecto **SPICE (Software Process Improvement Capability Determination)** con unos objetivos bien definidos:

- Desarrollar un borrador de trabajo para un estándar de evaluación de procesos de software.
- Llevar a cabo los ensayos de la industria de la norma emergente.
- Promover la transferencia de tecnología de la evaluación de procesos de software a la industria del software a nivel mundial.

El resultado de este proyecto se recogió en un conjunto de normas que derivaron en lo que actualmente se conoce como familia de estándares **ISO/IEC 15504**.

El **ISO/IEC 15504** es un modelo para la mejora y evaluación de los procesos de desarrollo y mantenimiento de sistemas de información y productos de software. Su filosofía es desarrollar un conjunto de medidas de capacidad

estructuradas para todos los procesos del ciclo de vida y para todos los participantes.

SPICE inicialmente absorbe la escala de puntuación de capacidad de CMM, las actividades de proceso de ingeniería y ciclo de vida de ISO/IEC 12207, Trillium y CMM, la representación de capacidad basada en perfiles de atributos de BOOTSTRAP y la experiencia del sistema de gestión de la calidad general de ISO 9001.

El alcance de SPICE abarca la planificación, gestión, ejecución, control y mejora de la adquisición, provisión, desarrollo, operación, mantenimiento y soporte del software y de la organización responsable. Esta basado en las “buenas prácticas” de la industria. Define los requisitos para la realización de evaluaciones de procesos como punto de partida para la determinación de la capacidad y mejora de los procesos. Tiene una arquitectura basada en **dos dimensiones**: *de proceso y de capacidad de proceso*.

Hoy en día se estructura en diez **partes**, estando las siete primeras terminadas, y de la ocho a la diez en fase de desarrollo. Las partes ya terminadas son:

- **Parte 1:** Conceptos y Vocabulario (publicada en el 2004).
- **Parte 2:** Realización de una Evaluación, Requisitos y Normativa (publicada en el 2003).
- **Parte 3:** Guía para Realización de Evaluaciones (publicada en el 2004)
- **Parte 4:** Guía para el uso en la mejora de los procesos y la determinación de la capacidad (publicada en el 2004)
- **Parte 5:** Ejemplo del un Modelo de Evaluación de Procesos (publicada en 2006)
- **Parte 6:** Un ejemplo de modelo de evaluación del ciclo de vida de sistema (Publicada en 2008)



- **Parte 7:** Evaluación de la madurez de una organización (Publicada en 2008)

A continuación mostramos los niveles de capacidad y los atributos de los procesos del modelo **ISO 15504**:

- 1- **Incompleto:** El proceso no está implementado o falla en alcanzar su propósito. No es fácil identificar los productos o salidas de los procesos.
- 2- **Realizado:** El propósito del proceso se logra generalmente, aunque no sea rigurosamente planificado ni llevado a cabo. Hay productos identificables que testifican el alcance del propósito.
 - o Realización del proceso
- 3- **Gestionado:** El proceso es gestionado y los entregables resultado de procedimientos específicos, planificados y seguidos, con requisitos de calidad, tiempo y recursos.
 - o Gestión de realización
 - o Gestión de los productos del trabajo
- 4- **Establecido:** Un proceso realizado y gestionado usado un proceso definido, basado en unos principios de buenas prácticas de ingeniería del software.
 - o Definición del proceso
 - o Implantación del proceso
- 5- **Predecible:** El proceso definido es puesto consistentemente en práctica dentro de límites de control establecidos para alcanzar metas del proceso ya definidas. Entendimiento cuantitativo de la capacidad del proceso y habilidad mejorada de predecir y gestionar el rendimiento.
 - o Medida del proceso
 - o Control del proceso

6- **Optimizado:** Realización del proceso optimizada en labúsqueda de las necesidades actuales y futurasdel negocio. Objetivos cuantitativos deeficiencia y efectividad se establecen en funciónde los objetivos de la organización. La Optimización puede llevar a estudiar y adoptarideas innovadoras o productos tecnológicosnovedosos que incluyan y modifiquen elproceso definido.

- o Innovación delproceso
- o Optimización delproceso

Para que una organización pueda alcanzar un nivel de madurez debe evaluarse frente a la norma ISO/IEC 15504. Existen 3 clases de evaluaciones, clase 1, clase 2 y clase 3. Las dos últimas se corresponden con evaluaciones internas y no ofrecen una certificación oficial, a diferencia de la clase 1 que es una evaluación más exhaustiva y rigurosa que permite alcanzar una puntuación oficial. En España **AENOR** ofrece este tipo de evaluaciones y certificaciones bajo esta norma.

Por último decir que existe equivalencia y compatibilidad con **CMMI**. ISO forma parte del panel elaborador del modelo CMMI y SEI y viceversa, y se mantiene la compatibilidad y equivalencia de ésta última con 15504.

2.4 ISO 9000-3

La Organización de Estandarización Internacional (ISO), ha definido una serie de estándares que son generalmente aplicables a todos los procesos de producción.

El ISO 9000 proporciona un conjunto de estándares para la gestión de la calidad en cualquier actividad relacionada con el proceso de producción. La ISO 9000 se ha especializado en todo lo referente a la solución del software en la ISO 9000-3, puesto que esta disciplina tiene características propias diferentes como para distinguirse del proceso de producción en general.

Las ideas básicas que se nos propone para el estándar ISO 9000-3 son las siguientes:

- El control de calidad debe ser aplicado a todas las fases de la producción de software, incluido el mantenimiento y tareas posteriores a su implantación.
- Debe existir una estricta colaboración entre la organización que adquiere el software y el proveedor del mismo.
- El proveedor del software debe definir su sistema de calidad y asegurarse que toda la organización ponga en práctica este sistema.

Es importante resaltar que en la ISO 9000-3 trata el concepto de ciclo de vida, pero en ningún momento no desea imponer la utilización de un determinado ciclo como puede ser el ciclo en espiral de Boeh. Pero a parte del ciclo de vida que elijamos, el ISO 9000-3 introduce otras actividades que tienen lugar de forma independiente a las fases del ciclo y que son las actividades referentes a la configuración y distingue entre la verificación y validación.

Además el ISO 9000-3 puede ser utilizado en relaciones contractuales cuando comprador y proveedor establecen que algunos elementos de calidad deben formar parte del sistema de calidad que proporciona el proveedor y que este se compromete a seguir los principios de calidad definidos en el estándar.

La ISO 9000-3 es una guía que está formada por una serie de cláusulas que indican como aplicar esta guía. Las cláusulas son las siguientes:

NUMER O	CLAUSULA
--------------------	-----------------

- | | |
|-----|--------------------------------------|
| 4.1 | Administración de la Responsabilidad |
| 4.2 | Sistema de Calidad |



- 4.3 Auditorias Internas del Sistema de Calidad
- 4.4 Acción Correctora
- 5.1 General
- 5.2 Revisión del Contrato
- 5.3 Especificación de los requerimientos de la Organización
- 5.4 Planificación del desarrollo
- 5.5 Planificación de la Calidad
- 5.6 Diseño e Implementación
- 5.7 Testeo y Validación
- 5.8 Aceptación
- 5.9 Generación, Entrega e Instalación
- 5.10 Mantenimiento
- 6.1 Administración de la Configuración
- 6.2 Documentos de Control
- 6.3 Calidad de los Archivos
- 6.4 Medidas
- 6.5 Reglas y Convenciones
- 6.6 Herramientas y Técnicas
- 6.7 Compra
- 6.8 Productos de software incluidos
- 6.9 Formación

A continuación pasamos a comentar las cláusulas más importantes:

- **Administración de la Responsabilidad:** Esta cláusula permite organizar la estructura del sistema de calidad, abordando la

estrategia y organización como requerimientos para verificar y revisar la calidad.

- **Sistema de Calidad:** Requiere una planificación y documentación del sistema de calidad, requisito conocido como 'Plan de Garantía de Calidad del Software' o SQAP utilizado en el estándar IEEE 730.
- **Acción correctora:** No existe una receta para el proceso de acciones correctoras, pero el estándar IEEE 1044 nos puede ser útil, para clasificar los tipos de anomalías que pueden ser encontradas en un sistema semejante al que estamos tratando.
- **Revisión del contrato:** Esta cláusula, aunque aparentemente parece obvia, insiste en la necesidad de que el proveedor examine los contratos referidos al sistema de calidad.
- **Especificación de los requerimientos de la Organización:** Se establece la premisa, de la mutua colaboración entre el proveedor y la organización que adquiere el producto software.
- **Planificación del desarrollo:** Esta cláusula sitúa los requerimientos en un plan de desarrollo. Particularmente la cláusula 5.4.2.1 exige la definición de un proceso disciplinado o metodología que incluye: fases de desarrollo, entradas, salidas y procesos de verificación. El estándar IEEE 1074, Procesos del Ciclo de Vida del Desarrollo de Software, podría resultarnos particularmente útil para satisfacer estos requerimientos.
- **Planificación de la Calidad:** La metodología de medidas de Calidad descrita en el estándar IEEE 1061, puede sernos útil para establecer los objetivos de calidad.
- **Diseño e Implementación / Testeo y Validación:** Estas dos cláusulas se centran en las actividades centrales del proceso de desarrollo de software.
- **Aceptación:** Estas pruebas son más bien generales, dado que en los estándares del IEEE no hay definido un homólogo

- **Generación, Entrega e Instalación:** Los requerimientos de pruebas y medios de control existentes en el IEEE 730, pueden ser de utilidad pero no son suficientes, para abordar los contenidos de esta cláusula.
- **Mantenimiento:** Esta cláusula proporciona una extensa lista de requerimientos de calidad, para la fase de mantenimiento del ciclo de vida. El estándar IEEE 1219 proporciona unos requerimientos detallados e importantes para llevar a cabo un proceso de mantenimiento adecuado.

Las cláusulas restantes proporcionan requerimientos para las **actividades de soporte**, es decir aquellas que no son específicas de ninguna fase en concreto, del ciclo de vida.

- **Administración de la Configuración/ Documentos de Control:** Las actividades que detallan estos requerimientos, se encuentran en los llamados Planes de Gestión de la Configuración del Software, los cuales quedan descritos en el estándar IEEE 828.
- **Medidas / Reglas y Convenciones / Herramientas y Técnicas:** Estas cláusulas nos hablan del uso de procedimientos y herramientas apropiados para implementar el sistema de calidad.
- **Compra / Productos de software incluidos:** Los requerimientos que rigen las compras del proveedor de los vendedores se encuentran en estas dos cláusulas.
- **Formación:** La única mención que se realiza en los estándares del IEEE, se encuentra en el estándar 730.

2.5 Modelos Ágiles

Las metodologías ágiles son sin duda uno de los temas recientes en ingeniería de software que están acaparando gran interés. Los modelos

ágiles son aquellos modelos que son tan solo lo suficientemente buenos, lo cual implica que exhiben las siguientes características:

1. Satisfacen su propósito.
2. Son inteligibles.
3. Son suficientemente precisos.
4. Son suficientemente consistentes.
5. Son suficientemente detallados.
6. Aportan valor positivos.
7. Son lo más simple posible.

El origen de las metodologías ágiles surge en marzo de 2001. El principal impulsor, Kent Beck, es el escritor de un libro, *Extreme Programming Explained*, en el que se exponía una nueva metodología denominada Extreme Programming (Programación Extrema), fundamentada principalmente en poner más énfasis en la adaptabilidad que en la previsibilidad. Beck, junto con un grupo de críticos, analizó un replanteamiento de los modelos de mejora del desarrollo de software basados en procesos.

En la reunión se acuñó el término **Métodos Ágiles** para definir a los métodos que estaban surgiendo como alternativa a las metodologías formales (*CMMI*, *SPICE*) a las que consideraban excesivamente “pesadas” y rígidas por su carácter normativo y fuerte dependencia de planificaciones detalladas previas al desarrollo. Los integrantes de la reunión resumieron los principios sobre los que se basan los métodos alternativos en cuatro postulados, que quedaron acuñados como **Manifiesto Ágil**.

Los **cuatro postulados** del Manifiesto Ágil son:

- **Valorar más a los individuos y su interacción que a los procesos y las herramientas.** Este es posiblemente el postulado más importante del manifiesto. Por supuesto que los procesos ayudan al trabajo. Son una guía de operación. Las herramientas mejoran la



eficiencia, pero sin personas con conocimiento técnico y actitud adecuada, no producen resultados. Los procesos deben ser una ayuda y un soporte para guiar el trabajo. Deben adaptarse a la organización, a los equipos y a las personas; y no al revés. La defensa a ultranza de los procesos lleva a postular que con ellos se pueden conseguir resultados extraordinarios con personas mediocres, y lo cierto es que este principio es peligroso cuando los trabajos necesitan creatividad e innovación.

- **Valorar más el software que funciona que la documentación exhaustiva.** Poder ver anticipadamente como se comportan las funcionalidades esperadas sobre prototipos o sobre las partes ya elaboradas del sistema final ofrece una retroalimentación (feedback) muy estimulante y enriquecedora que genera ideas imposibles de concebir en un primer momento; difícilmente se podrá conseguir un documento que contenga requisitos detallados antes de comenzar el proyecto. El manifiesto no afirma que no haga falta los documentos, pero se resalta que son menos importantes que los productos que funcionan. Los documentos no pueden sustituir, ni pueden ofrecer la riqueza y generación de valor que se logra con la comunicación directa entre las personas y a través de la interacción con los prototipos.
- **Valorar más la colaboración con el cliente que la negociación contractual.** Las prácticas ágiles están especialmente indicadas para productos difíciles de definir con detalle en el principio, o que si se definieran así tendrían al final menos valor que si se van enriqueciendo con retro-información continua durante el desarrollo. También para los casos en los que los requisitos van a ser muy inestables por la velocidad del entorno de negocio. Un contrato no aporta valor al producto. Es una formalidad que establece líneas divisorias entre responsabilidades, que fija los referentes para

posibles disputas contractuales entre cliente y proveedor. En el desarrollo ágil el cliente es un miembro más del equipo, que se integra y colabora en el grupo de trabajo.

- **Valorar más la respuesta al cambio que el seguimiento de un plan.** Para un modelo de desarrollo que surge de entornos inestables, que tienen como factor inherente al cambio y la evolución rápida y continua, resulta mucho más valiosa la capacidad de respuesta que la capacidad de seguimiento y aseguramiento de planes pre-establecidos. Los principales valores de la gestión ágil son la anticipación y la adaptación.

Tras los cuatro postulados descritos, los firmantes redactaron los **12 principios** siguientes, derivados de los postulados.

1. Nuestra mayor prioridad es satisfacer al cliente mediante la entrega temprana y continua de software con valor.
2. Aceptamos que los requisitos cambien, incluso en etapas tardías del desarrollo. Los procesos Ágiles aprovechan el cambio para proporcionar ventaja competitiva al cliente.
3. Entregamos software funcional frecuentemente, entre dos semanas y dos meses, con preferencia al periodo de tiempo más corto posible.
4. Los responsables de negocio y los desarrolladores trabajamos juntos de forma cotidiana durante todo el proyecto.
5. Los proyectos se desarrollan en torno a individuos motivados. Hay que darles el entorno y el apoyo que necesitan, y confiarles la ejecución del trabajo.
6. El método más eficiente y efectivo de comunicar información al equipo de desarrollo y entre sus miembros es la conversación cara a cara.
7. El software funcionando es la medida principal de progreso.



8. Los procesos Ágiles promueven el desarrollo sostenible. Los promotores, desarrolladores y usuarios debemos ser capaces de mantener un ritmo constante de forma indefinida.
9. La atención continua a la excelencia técnica y al buen diseño mejora la Agilidad.
10. La simplicidad, o el arte de maximizar la cantidad de trabajo no realizado, es esencial.
11. Las mejores arquitecturas, requisitos y diseños emergen de equipos auto-organizados.
12. A intervalos regulares el equipo reflexiona sobre cómo ser más efectivo para a continuación ajustar y perfeccionar su comportamiento en consecuencia.

Por lo tanto, podemos decir que las metodologías ágiles serían mejores que las formales cuando los requerimientos son poco claros, se desea fomentar la mejora continua del proceso, o el cliente entiendo el proceso y está dispuesto a implicarse para que salga adelante.

BIBLIOGRAFÍA

- Ingeniería del Software. Un enfoque práctico. ROGER S. PRESSMAN. Ed. McGraw Hill.
- Ben-Menachem, M.; Marliss (1997), Software Quality, Producing Practical and Consistent Software, Thomson Computer Press.
- Spinellis, D. (2006), Code Quality, Addison Wesley.
- Ebert, Christof; Dumke, Reiner, Software Measurement: Establish - Extract - Evaluate - Execute, Kindle Edition, p. 91
- Ben-Menachem, M.; Marliss (1997), Software Quality, Producing Practical and Consistent Software, Thomson Computer Press
- <http://modelosdegestiondelacalidad.blogspot.com/>



- Apuntes y papeles de trabajo de Ingeniería de Sistemas de Información. RAMÓN ORTIGOSA.
- Temario de las pruebas selectivas para ingreso en el Cuerpo Superior de Sistemas y Tecnologías de la Información de la Administración del Estado. ASTIC.
- <http://www.iso15504.es>
- http://es.wikipedia.org/wiki/ISO/IEC_15504
- Enginyeria del Software III. Antonia Mas Pichaco. Universitat de les illes Balears.
- ["Appraisal Requirements for CMMI, Version 1.2 \(ARC, V1.2\)"](#). Carnegie Mellon University Software Engineering Institute. 2006. Retrieved 16 February 2011.
- CMMI Guidebook Acquirer Team (2007). ["Understanding and Leveraging a Supplier's CMMI Efforts: A Guidebook for Acquirers"](#) (pdf). CMU/SEI-2007-TR-004. Software Engineering Institute. Retrieved 23 August 2007.
- Norma ISO 9000-3. Francisco D'Angelo. Douglas García. Claudia Herrera. Luis Laviosa. Universidad Simón Bolívar. Dpto. de Computación y Tecnología de la Información
- ISO 9000-3 Laboratorio de Sistemas de Información. Facultad de Informática - Universidad Politécnica de Valencia
- <http://agilemanifesto.org/iso/es/>
- http://es.wikipedia.org/wiki/Manifiesto_ágil

Autor: Francisco Javier Rodríguez Martínez
Subdirector de la Escuela Superior de Ingeniería Informática.
Universidad de Vigo.

40. SEGURIDAD INFORMÁTICA: AUTENTICACIÓN, INTEGRIDAD, CONFIDENCIALIDAD, DISPONIBILIDAD, TRAZABILIDAD. ANÁLISIS Y GESTIÓN DE RIESGOS. METODOLOGÍA MAGERIT.

Tema 40. Seguridad Informática: Autenticación, Integridad, Confidencialidad, Disponibilidad, Trazabilidad. Análisis y gestión de riesgos. Metodología MAGERIT.

INDICE

1. SEGURIDAD INFORMÁTICA: AUTENTICIDAD, INTEGRIDAD, CONFIDENCIALIDAD, DISPONIBILIDAD, TRAZABILIDAD.....	2
1.1. Introducción.....	2
1.2. Plan de seguridad y plan de contingencias.....	3
1.2.1. El plan de seguridad.....	3
1.2.2. El plan de contingencias.....	4
1.2. Las dimensiones de la seguridad.....	5
1.3. Amenazas a la seguridad.....	8
1.3.1. Personas.....	8
1.3.2. Amenazas lógicas.....	8
1.3.3. Catástrofes.....	10
1.4. Seguridad Física.....	11
1.5. Seguridad Lógica.....	13
1.5.1. Ataques contra la seguridad lógica	14
1.5.2. La protección de la seguridad lógica.....	20
2. ANALISIS Y GESTIÓN DE RIESGOS.....	24
2.1. Introducción.....	24
2.2. Análisis de riesgos.....	25
2.3. Gestión de riesgos.....	27
2.1. La metodología MAGERIT.....	28
2.1.1. Elementos de la metodología.....	30
2.1.2. Estructura de la metodología:.....	31
2.1.3. Procesos de la metodología:.....	32
3. REFERENCIAS.....	34

1. SEGURIDAD INFORMATICA: AUTENTICIDAD, INTEGRIDAD, CONFIDENCIALIDAD, DISPONIBILIDAD, TRAZABILIDAD.

1.1. Introducción

Definimos un sistema informático como el conjunto formado por recursos físicos denominados hardware, recursos lógicos denominados software y recursos humanos, que interactúan entre sí con el objetivo de obtener, almacenar y procesar la información.

En este contexto, la seguridad informática será una característica de los sistemas informáticos que indicará si el sistema está libre de peligro, daño o riesgo. A menudo, la seguridad absoluta es difícil, o incluso imposible, de alcanzar y los sistemas informáticos no son una excepción.

En un sistema informático los esfuerzos se centrarán en proteger el software, el hardware y los datos. Éstos últimos suelen ser el elemento más valioso por lo que requieren de una mayor inversión en seguridad al tratarse del recurso más amenazado y el más difícil de recuperar.

Sin embargo, teniendo en cuenta que la seguridad absoluta de los sistemas de información es inalcanzable, se debe buscar siempre un compromiso entre el nivel de riesgo asumido y el coste de las medidas de seguridad de tal modo que dicho coste no supere nunca el valor de lo que se pretende proteger.

La seguridad en los sistemas de información atañe a todos los miembros de la organización. Su naturaleza dinámica hace que deba ser planificada, diseñada, ejecutada y mejorada de forma continua ya que todos los días surgen nuevas amenazas. Para protegernos contra ellas no es suficiente con implementar medidas técnicas, sino que tendremos que preparar una

política de seguridad de la organización, planes de actuación, medidas de seguridad física, formación, concienciación, etc.

1.2. Plan de seguridad y plan de contingencias

La seguridad informática no es una tarea exclusiva de los departamentos de tecnologías de la información o una cuestión meramente técnica. Debe ser una cuestión que abarque todos los ámbitos de la organización, con un gran componente técnico basado en tecnologías de la información, pero también político, de concienciación y formación de todo el personal.

1.2.1. El plan de seguridad

El Plan de Seguridad Informática establece los principios organizativos y funcionales de la actividad de seguridad informática en una organización. Recoge claramente las políticas de seguridad y las responsabilidades de cada uno de los participantes en el proceso informático, así como las medidas y procedimientos que permitan prevenir, detectar y responder a las amenazas que gravitan sobre el mismo.

Una vez que la política de seguridad es aprobada, debe ponerse a disposición de todos los miembros de la organización ya que serán ellos los responsables finales de su éxito. Las políticas deben ser revisadas y actualizadas anualmente (o si es posible cada seis meses) para reflejar los cambios en la organización.

No debería haber dos políticas de seguridad iguales puesto que cada empresa es diferente y los detalles de la política dependen de las necesidades exclusivas de cada una. Sin embargo, se puede comenzar con un conjunto general de políticas de seguridad y luego personalizarlo de acuerdo con los requerimientos específicos, limitaciones de financiación e infraestructura existente.

Un plan de seguridad informática completo es un recurso valioso que justifica la dedicación de tiempo y esfuerzo a su elaboración.

1.2.2. El plan de contingencias

Un plan de contingencias es un conjunto de procedimientos alternativos al orden normal de la organización, cuyo fin es permitir el normal funcionamiento de esta, aun cuando alguna de sus funciones se viese dañada por un fallo de seguridad.

Que una organización prepare sus planes de contingencias, no significa que reconozca la ineficacia de su plan de seguridad, sino que supone un avance a la hora de superar cualquier eventualidad que puedan acarrear pérdidas importantes.

Los planes de contingencias se deben hacer de cara a futuros acontecimientos para los que hace falta estar preparado.

La función principal de un plan de contingencias es la continuidad de las operaciones de la empresa. Dividimos su elaboración en cuatro etapas:

1. Evaluación.
2. Planificación.
3. Pruebas de viabilidad.
4. Ejecución.

Las tres primeras hacen referencia al componente preventivo y la última a la ejecución del plan una vez ocurrido el siniestro.

Se deben crear planes de contingencias para todos los riesgos de seguridad conocidos para prevenir la aparición de nuevas amenazas o vulnerabilidades desconocidas que dañen a nuestros sistemas.

Los planes de contingencias de seguridad deben especificar claramente las acciones a realizar si se produce un incidente para minimizar las consecuencias y la repercusión en los activos de la organización. Lo ideal es contar con planes de respuesta a incidentes y planes de continuación de negocio para garantizar una reacción eficaz durante y después de un ataque.

1.2. Las dimensiones de la seguridad

Las dimensiones de la seguridad, también denominadas servicios o factores de seguridad, hacen referencia a las propiedades que la información debe cumplir para considerar un sistema como seguro. Un sistema informático se encuentra en óptimas condiciones de seguridad para operar cuando es capaz de garantizar la seguridad de todos sus componentes en cinco dimensiones:

- **Confidencialidad:** es la propiedad de la información por la que se garantiza que únicamente está accesible para los usuarios y procesos.

Si la información se encuentra almacenada en un sistema propio, la confidencialidad se basa en primer lugar en garantizar la autenticidad de cualquier usuario que intente acceder a ella. Una vez autenticado, debe controlarse que el usuario está autorizado, es decir, que cuenta con los permisos para acceder a esa información en concreto.

Sin embargo, cuando la información se transmite entre un emisor y un receptor a través de un medio externo y por tanto inseguro,



la confidencialidad debe garantizarse mediante el uso de técnicas de cifrado, con el fin de evitar que un tercero que pueda interceptar el mensaje sea capaz de extraer cualquier información inteligible del mismo.

- **Integridad:** es la propiedad de la información por la que se garantiza que ésta no ha sido manipulada intencionada o accidentalmente por usuarios no autorizados.

La integridad puede protegerse mediante técnicas de validación de datos que permitan detectar cualquier alteración de los mismos como sumas de validación (*checksum*), uso de bits de paridad, chequeos de redundancia cíclica (CRC), algoritmos de resumen (SHA1, MD5, etc.) y cualquier otro algoritmo destinado a detectar cualquier cambio no autorizado en la información.

- **Disponibilidad:** es la propiedad de la información por la que se garantiza que ésta se encontrará a disposición de las personas, procesos o aplicaciones que deban acceder a ella y dispongan de autorización para ello.

La disponibilidad implica que el sistema, tanto a nivel hardware como a nivel software, debe mantenerse funcionando eficientemente y que es capaz de recuperarse rápidamente en caso de fallo. Esto se consigue diseñando los sistemas de manera apropiada en términos de capacidad y escalabilidad para poder crecer de forma ordenada en caso de ser necesario. Además de esto, existen técnicas destinadas a evitar problemas de disponibilidad como el balanceo de carga entre servidores, virtualización de servidores, redundancia de sistemas de comunicaciones, alimentación eléctrica y de almacenamiento (RAID) o los sistemas de respaldo.



- **Autenticidad:** es la propiedad de la información por la que se garantiza su genuinidad y que permite identificar a su autor o generador.

Existe una propiedad relacionada con la autenticidad conocida como imposibilidad de rechazo o 'no repudio'. Esta propiedad permite demostrar ante terceros que una información ha sido enviada o consignada por una entidad sin que esta pueda negarlo.

La autenticidad implica la necesidad de dar pruebas de identidad de los participantes en una comunicación. El modo en que un usuario puede demostrar su identidad recae en uno o más de los siguientes factores: algo que el usuario sabe (por ejemplo una clave de acceso), algo que tiene (por ejemplo una tarjeta de acceso) o algo que es parte del propio usuario (por ejemplo medidas biométricas como la huella digital). Se considera que para que una autenticación sea realmente segura debe involucrar al menos elementos de dos de los tres (si no de los tres) factores.

Por ejemplo, la arquitectura de firma electrónica con certificados emitidos por entidades confiables (Autoridades de Certificación) es un sistema de autenticación multifactor, ya que primero debemos poseer un documento que nos identifique para poder obtener un certificado avalado por un tercero y conocer un código personal para realizar las firmas.

- **Trazabilidad:** la trazabilidad en un sistema de información hace referencia a su capacidad para seguir y conservar la secuencia de todas las acciones (o al menos de aquellas que puedan afectar a la seguridad del sistema) que ocurran en el sistema para determinar su origen. Un sistema con procesos trazables facilitará la respuesta a incidencias en la seguridad. También será de gran ayuda a la hora de realizar auditorías de seguridad y diseñar

sistemas de repuesta basados en el estudio de patrones de situaciones, como los sistemas de detección de intrusos (IDS).

1.3. Amenazas a la seguridad

Los sistemas informáticos se encuentran expuestos a diversos agentes externos o internos capaces de causarles daño. Dependiendo de su origen, distinguiremos tres tipos de amenazas: personas, amenazas lógicas y catástrofes.

1.3.1. Personas

Tanto el propio personal de la organización como curiosos o intrusos suponen una amenaza para la seguridad de la información. Los primeros, aunque normalmente lo harán de forma no intencionada, pueden causar daños al sistema durante el ejercicio de su actividad diaria. Estos daños serán proporcionales al nivel de exposición de la información ya que no todos los usuarios tendrán el mismo nivel de acceso a la información. Por su parte, los intrusos suponen a menudo una amenaza mayor ya que atacan de forma consciente con la intención de hacer el mayor daño posible. Dentro de este grupo podemos incluir a ex-empleados, crackers, terroristas, intrusos remunerados etc.

1.3.2. Amenazas lógicas

En esta categoría se incluyen todo tipo de programas que de una forma u otra pueden dañar nuestro sistema, ya sea intencionadamente o por error. Podemos enumerar en esta categoría las siguientes amenazas:

- **Software incorrecto:** programas que debido a defectos en su código pueden causar daños al sistema o facilitar ataques desde el exterior.



- **Herramientas de seguridad:** pueden ser una excelente herramienta de ayuda para gestionar la seguridad y configurar nuestros sistemas correctamente, pero constituyen un arma de doble filo, ya que también son útiles para descubrir vulnerabilidades en nuestro sistema. Ejemplos de este tipo de herramientas son los *sniffers*¹ (como por ejemplo *Wireshark*) o las herramientas de escaneo de puertos (como por ejemplo *nmap*).
- **Bombas lógicas:** son partes del código de ciertos programas que permanecen inactivos hasta que se cumple cierta condición (ausencia o presencia de ciertos ficheros, fechas, etc.). Cuando esta condición se activa, se ejecuta el código malicioso que ataca al sistema.
- **Canales de comunicación ocultos:** permiten que un proceso transfiera información, violando la política de seguridad.
- **Puertas traseras:** son 'atajos' dejados por los programadores para acelerar los procesos de pruebas del software, pero que si no son corregidos antes del paso a producción pueden convertirse en peligrosos agujeros en la seguridad.
- **Virus:** son secuencias de código que se insertan en algún lugar del sistema (habitualmente en archivos ejecutables, aunque pueden residir en otros lugares) para realizar su tarea maliciosa e intentar extenderse a otras partes del mismo sistema o incluso a otros sistemas.
- **Gusanos:** programas capaces de ejecutarse y propagarse por sí mismos a través de redes.

¹ Programas que permiten registrar y analizar toda la información transmitida a través de una red.



- **Troyanos:** son instrucciones de código escondidas en programas que se alojan en el sistema y que realizan funciones ocultas, generalmente destinadas a tomar el control de un sistema (Por ejemplo, los *rootkit*).
- **Programas conejo** (también conocidos como programas bacteria): programas que no hacen nada salvo reproducirse hasta agotar los recursos del sistema y conseguir bloquearlo.
- **Técnicas Salami:** robo automatizado y sistemático de pequeñas cantidades de bienes de una gran cantidad original.

1.3.3. Catástrofes

Las catástrofes, ya sean naturales o artificiales, constituyen la amenaza menos probable pero también la más desastrosa para los sistemas de información. La defensa contra ellas se basa en recursos físicos y diseño adecuado de la sede física de nuestros sistemas.

- Incendios: El centro de proceso de datos debe contar con un sistema de extinción de incendios adecuado que permita sofocar cualquier conato sin que la propia extinción cause daños a los sistemas.
- Inundaciones: Además de buscar un emplazamiento con el mínimo riesgo de inundación, es recomendable instalar sensores que detecten posibles fugas de agua y alerten sobre ellas antes de que puedan causar daño.
- Terremotos: En las zonas con actividad sísmica es un riesgo a tener en cuenta.

- Tormentas eléctricas: La instalación eléctrica debe contar con todas las garantías proporcionando alimentación ininterrumpida y neutralizando los picos de tensión que pudiesen producirse.
- Temperaturas extremas: Los equipos informáticos, como aparatos electrónicos que son, necesitan unas condiciones de temperatura y humedad adecuadas para un funcionamiento óptimo. Estas condiciones suelen conseguirse mediante la instalación de equipos de climatización.

1.4. Seguridad Física

La seguridad física se encarga de la protección contra amenazas a las instalaciones, equipamientos, sistemas de comunicaciones y personal que forman parte de un sistema de información. Consiste en la aplicación de barreras físicas y procedimientos de control ante amenazas a los recursos del sistema.

Resulta habitual que las organizaciones se centren en la seguridad lógica descuidando a veces la seguridad física, lo que puede ser fuente de problemas ya que la seguridad física afecta a los tres tipos de recursos: hardware, software y datos, y los ataques con acceso físico exitosos pueden ser muy dañinos. Por ejemplo, un acceso no autorizado que tiene como resultado la desaparición de un equipo con datos sensibles de la organización.

Las amenazas a la seguridad física pueden clasificarse atendiendo a diversos aspectos. Establecemos aquí tres tipos:

- Amenazas ocasionadas involuntariamente por personas: se trata accidentes causados por personas de forma fortuita por accidente o negligencia en el uso del sistema. Estas personas no tienen por qué ser exclusivamente trabajadores técnicos. Incluye también a

personal de limpieza y mantenimiento, visitantes, etc. En la práctica se traduce en derrames de líquidos, desconexiones bruscas de la red, caídas y roturas de material, etc.

- Acciones hostiles deliberadas: se trata de amenazas que pueden ser realmente peligrosas en función de la capacidad e intenciones del atacante. Son acciones deliberadas y usualmente planificadas contra nuestro sistemas o las personas que trabajan en el. Incluye accesos no autorizados a las instalaciones, robo, secuestros, fraudes, sabotajes, etc.
- Desastres naturales, incendios, humedad e inundaciones: son agentes externos que de afectar a nuestros sistemas suelen causar graves daños. Aunque son infrecuentes, es necesario preverlos y tenerlos en cuenta a lo largo de todo el diseño y la vida útil de nuestro sistema.

Las medidas de seguridad física permiten limitar el alcance de las amenazas citadas mediante el uso de controles y procedimientos de seguridad. El estándar TIA-942, aprobado por la *Telecommunications Industry Association* y por ANSI², proporciona una guía de recomendaciones y normas para el diseño e instalación de infraestructuras de centros de procesamiento de datos (CPD) que contribuyen a un considerable aumento de la seguridad física del sistema de información. Establece cuatro niveles (*tiers*) de disponibilidad implementados mediante medidas de carácter arquitectónico, de telecomunicaciones, eléctricas y mecánicas.³

² Siglas en inglés de American National Standards Institute.

³ Dejamos para el tema 56, dedicado al diseño de centros de procesamiento de datos, el desarrollo de las medidas seguridad física.

1.5. Seguridad Lógica

La seguridad lógica hace referencia al conjunto de operaciones y técnicas destinadas a la protección de la información, procesos y programas contra la destrucción, la modificación, la divulgación indebida o el retraso en su gestación.

Es poco frecuente que un ataque lógico afecte al hardware, aunque existe la posibilidad de que algún ataque de este tipo pueda llegar a dañar algún componente.

En un sistema de información, los datos constituyen uno de los recursos más importantes y valiosos. La gran variedad de los ataques, el posible origen remoto de los mismos y el impacto que pueden causar nos obliga a establecer medidas de protección similares o superiores a las asumidas en la seguridad física.

La seguridad lógica plantea una serie de requerimientos íntimamente relacionados con las precitadas dimensiones de la seguridad entre los que podemos mencionar los siguientes:

- Asegurar que los operadores puedan trabajar sin necesidad de una supervisión minuciosa y que no puedan modificar los programas ni los archivos que no les correspondan.
- Asegurar que se estén utilizando los datos y los programas correctos por el procedimiento correcto.
- Restringir el acceso al software y a los datos.
- Que la información transmitida sea recibida por el destinatario al que ha sido enviada y no por otro.
- Proveer técnicas que permitan garantizar que la información no resulta alterada durante un proceso de transmisión.

- Procurar que los sistemas de comunicación entre los distintos componentes del sistema de información estén redundados.
- Mantener un registro de las operaciones llevadas a cabo en el sistema junto con el usuario que las realiza para poder realizar su seguimiento en caso de ser necesario.

1.5.1. Ataques contra la seguridad lógica

La seguridad lógica puede ser vulnerada por medio de ataques muy heterogéneos y que además se encuentran bajo continua evolución. Dada la gran diversidad de sistemas operativos, aplicaciones y protocolos, es imposible determinar su número, que sigue aumentando día a día.

Por otro lado, la transmisión de información a través de sistemas de ajenos a la organización, como Internet, resulta cada vez más frecuente y el volumen de información transmitido aumenta también de un modo notable. Estas operaciones de transmisión de información a través de un canal no controlado por la organización y compartido con terceros son especialmente vulnerables a los ataques de estos.

Podemos clasificar estos ataques atendiendo al objetivo de los mismos de la siguiente manera:

1. **Ataques Pasivos:** la información no resulta alterada sino que el atacante únicamente la captura o monitoriza para obtener los datos que están siendo transmitidos.

Los objetivos de estos ataques son la interceptación de datos y el análisis de tráfico con las siguientes finalidades:

- o Recopilación de datos sobre cuentas de usuarios y claves de acceso para utilizar más tarde en ataques activos.



- o Obtención del origen y destinatario de la comunicación, a través de la lectura de las cabeceras de los paquetes monitorizados.
 - o Monitorización del volumen de tráfico intercambiado entre las entidades objeto del ataque, obteniendo así información acerca de actividad o inactividades inusuales.
 - o Monitorización de las horas habituales de intercambio de datos entre las entidades de la comunicación, para extraer información acerca de los periodos de actividad.
2. **Ataques activos:** implican algún tipo de modificación de los datos o la creación de datos falsos. Suelen ser intencionados y realizados por personas con conocimientos y consciencia de lo que están haciendo.

Se los pueden subdividir en varias categorías atendiendo a las acciones que se realizan durante el ataque:

- o **Interceptación:** un elemento no autorizado consigue un acceso a un determinado objeto del sistema, pero este no es modificado en ningún modo. Si se trata de una comunicación, esta llegará a su destino sin constancia de la interceptación.
- o **Destrucción:** algunos autores consideran un caso especial de la modificación la destrucción, entendiéndola como una modificación que inutiliza al objeto afectado.
- o **Modificación:** Si además de lograrse una interceptación el ataque consigue modificar el objeto de datos.

- o **Interrupción:** un ataque se clasifica como interrupción si hace que un objeto del sistema se pierda, quede inutilizable o no disponible.
- o **Fabricación:** modificación destinada a suplantar al objeto real.

Como decíamos, existe un elevado número de tipos de ataques contra la seguridad lógica. Citamos a continuación algunos de ellos:⁴

- **Ingeniería Social:** consiste en manipular a las personas del entorno para obtener acceso a los sistemas o a información confidencial que facilite otros ataques técnicos.
- **Ingeniería Social Inversa:** el intruso da a conocer de alguna manera que es capaz de brindar ayuda a los usuarios, y estos le llaman ante algún imprevisto. El intruso aprovechará la oportunidad para pedir información necesaria para solucionar el problema consiguiendo información útil para realizar ataques.
- **Shoulder-surfing**⁵: consiste en espiar físicamente a los usuarios mientras introducen su nombre de usuario y clave de acceso correspondiente o cuando están accediendo a información restringida.
- **Piggybacking:** relacionado con el anterior. Hoy en día hace referencia al uso de redes wireless ajenas, pero su significado original era el de 'colarse' en un lugar detrás de otra persona.
- **Masquerading/spoofing** (Suplantación): suplantación electrónica o física de personas autorizadas para acceder al

⁴ El RFC 4949 (*Internet Security Glossary, Version 2*) proporciona un listado más extenso y descriptivo.

⁵ Expresión en inglés que se refiere a mirar por encima del hombro.

sistema u obtener información relevante sobre el mismo. Dependiendo del objeto de la implantación podríamos hablar de IP spoofing, DNS spoofing, web spoofing, etc.

- **Basureo:** paradójicamente, uno de los ataques más efectivos. Consiste en inspeccionar los deshechos en papeleras, contenedores, etc. en busca de información sensible.
- **Exploits:** aprovechamiento de errores conocidos (bugs) en determinadas versiones del software instalado en el sistema de información que pueden ser usados como puerta de entrada de ataques.
- **Escaneo de puertos:** técnicas de ataque pasivas que analizan las máquinas de un sistema para determinar cual es el estado de los puertos (abierto/cerrado). En algunos casos permite incluso conocer cual es el sistema operativo de la máquina e incluso que software y que versión del mismo se encuentra escuchando en cada puerto.
- **Wiretapping:** un tipo de ataque que intercepta y accede a información que se transmite por un canal de comunicaciones. El nombre del término (que podríamos traducir como ‘pinchar cables’) tiene como origen el pinchazo de teléfonos que se hacía de forma mecánica. Hoy en día hace referencia a la captura de datos mediante cualquier técnica con o sin cables de por medio.
- **Eavesdropping-packet sniffing:** un tipo de ataque wiretapping pasivo. Es la interceptación pasiva del tráfico de red. Esto se realiza con aplicaciones llamadas sniffers, que son programas que capturan paquetes de datos que circulan por la red. Esto puede hacerse colocando el sniffer en uno de los equipos pertenecientes

a la red o consiguiendo conectar un equipo externo a la misma. Este último caso es la forma más habitual en redes wireless.

- **Man-in-the-middle:** un tipo de ataque wiretapping activo. El atacante intercepta y modifica selectivamente los paquetes de datos capturados para simular ser uno de los participantes en una comunicación ajena.
- **Denegación de servicio:** conocido habitualmente por sus siglas en inglés DOS (Denial of Service), este tipo de ataques consiste en conseguir que el objetivo del ataque deje de realizar su función de modo temporal o definitivo. El objetivo del ataque puede ser una máquina, una red de comunicaciones, un servicio concreto, etc. Se trata de uno de los tipos de ataques más comunes y efectivos. En la práctica existen múltiples variedades de este ataque de las que podemos nombrar: Flooding, ICMP flood, Syn flood, ping of death, land, smurf, teardrop, etc.
- **Denegación de Servicio Distribuida:** un caso especial del anterior, también conocida por sus siglas en inglés DDOS (Distributed Denial of Service). En este caso el ataque de DoS no proviene de un único atacante, sino que proviene de muchos a la vez de forma coordinada. El conjunto de atacantes puede no ser realmente un conjunto de personas, ya que es habitual el uso de máquinas secuestradas (máquinas zombies) que participan en el ataque muchas veces sin que su legítimo dueño tenga conocimiento de ello.
- **Ataques de secuestro (Hijack):** se centran en el secuestro de algún elemento en una comunicación previamente establecida por la víctima o de un recurso vital de una máquina. Los objetivos del secuestro pueden ser la sesión de un usuario ya autenticado en un sistema, el propio navegador de la víctima o incluso una



página ofrecida por un servidor para modificarla y hacer que los datos insertados en ella sean enviados a una máquina bajo el control del atacante, por ejemplo.

- **Tamper:** ataque consistente en realizar modificaciones en la configuración de una máquina o sistema objetivo que degraden el nivel de seguridad de la misma.
- **Phishing:** es en realidad un tipo de ataque de tipo masquerading que ha crecido en frecuencia en los últimos años. Es un ataque que intenta adquirir información sensible del objetivo (número de cuentas bancarias, nombres de usuario y claves de acceso, etc.) mediante una solicitud fraudulenta en un correo electrónico o página web que el atacante ha construido para simular ser una entidad o persona de confianza del objetivo.
- **SQL injection:** es un tipo de ataque por inserción de código dirigido a la base de datos en lenguaje SQL. La técnica consiste en insertar secuencias concretas que son sintácticamente correctas en SQL en campos de texto de aplicaciones (usualmente web) para ejecutar consultas fraudulentas. Aunque es un ataque peligroso es fácilmente contrarrestable filtrando adecuadamente las entradas.
- **Cross-site request forgery:** abreviado habitualmente como CSRF ó XSRF y también conocido como 'ataque de un click'. Se basa en aprovechar la confianza que un sitio web tiene en el navegador web de un usuario. La víctima es engañado para usar un hipervínculo manipulado por el atacante. La manipulación consiste en la construcción de un objeto de petición (request) que realiza directamente una acción fraudulenta e involuntaria para el usuario que la ejecuta. La clave reside en que el sitio web debe confiar en el usuario (porque ya se haya autenticado previamente,

por ejemplo) y ejecutar la petición directamente, de ahí el nombre de ‘ataque en un click’.

- **Cross site scripting:** abreviado habitualmente como XSS. Se trata de cualquier ataque que permita ejecutar código de scripting (VBScript, Javascript, etc.) insertado por el atacante en el contexto un sitio web.

1.5.2. La protección de la seguridad lógica

Existen medidas de protección que pueden y deben ser utilizadas para aumentar la seguridad de nuestros sistemas de información.

Más adelante veremos que los niveles de seguridad pueden ser controlados y gestionados mediante al análisis de riesgos, por lo que en este apartado nos limitaremos a enunciar las medidas organizativas y técnicas que podemos aplicar para aumentar nuestra seguridad.

Los ataques a la seguridad lógica, suelen basarse en realidad en fallos de diseño inherentes a Internet (o sus protocolos), o a los sistemas operativos utilizados. La continua aparición de nuevas tecnologías hace que el número de tipos de ataques aumente también.

Por lo tanto, los responsables de seguridad y administradores de los sistemas deben mantenerse actualizados en cuanto a nuevos ataques y como protegerse contra ellos. Y por supuesto es de vital importancia que mantengan actualizado el sistema operativo y todo el software usado en las máquinas del sistema.

Una máquina que contenga información que no sea considerada valiosa, debe ser igualmente tenida en cuenta a la hora de definir las políticas de seguridad ya que puede resultar útil para un atacante a la hora de ser empleada en un ataque de denegación de servicio distribuido (DDoS) o ser

utilizada como intermediaria (*proxy*) para ocultar la verdadera dirección del atacante.

Se deben realizar auditorías de seguridad de forma periódica y valorar la posibilidad de implantar sistemas de gestión de la seguridad de la información (SGSI) que garanticen la calidad de nuestros sistemas y medidas de seguridad.

Uno de los ataques con mayor tasa de éxito de todos los citados es el de la ingeniería social. De nada sirve que tengamos nuestro sistema perfectamente actualizado y que contemos con las medidas de seguridad físicas y lógicas más avanzadas si mediante una llamada telefónica un atacante puede conseguir que un usuario le transmita su usuario y clave de acceso.

La defensa contra ataques de ingeniería social pasa por mantener a los usuarios del sistema informados y formados en materia de seguridad. Hay que mantenerlos alerta y generarles un espíritu de desconfianza que permita evitar ataques basados en la ingeniería social o el *phishing*.

Algunas herramientas y técnicas de protección de la seguridad que podemos aplicar a nuestros sistemas de información son:

- **Análisis de riesgos:** el análisis de riesgos debe realizarse siempre como paso inicial en el diseño de la seguridad de nuestros sistemas de información. Supone identificar los activos a proteger y el daño que sufriría la organización en caso de ser afectados por un ataque. Veremos este punto en profundidad en el próximo capítulo.
- **Identificación de amenazas:** consiste en identificar cada una de las amenazas y vulnerabilidades que pueden afectar a los recursos del sistema.



- **Políticas de seguridad:** es fundamental contar con una política de seguridad, diseñada a medida para la organización y conocida por todos los empleados y/o usuarios. En este sentido, el RFC 2196 *Site Security Handbook* es una guía para el desarrollo de políticas y procedimientos de seguridad aplicables a sistemas de información. Está destinado principalmente a sistemas que trabajan en el ámbito de Internet, pero también a aquellos sistemas que simplemente se comunican con otros. Y en forma general también puede ser utilizado en sistemas aislados. El contenido incluye políticas, conceptos de seguridad en redes y sistemas, y respuestas a los incidentes de seguridad.
- **Estrategia de seguridad:** una estrategia adecuada debe ser concebida de modo que abarque varios niveles de seguridad: seguridad física, seguridad lógica, el personal de la organización y la interacción que existe entre estos factores. El plan de seguridad es un documento fundamental en la organización que debe incluir una estrategia de previsión de ataques para minimizar los puntos vulnerables existentes en la directiva de seguridad. Debe también desarrollar planes de contingencias. Estos servirán como una estrategia reactiva de respuesta al ataque que ayude al personal de seguridad a evaluar el daño causado y a recuperar los niveles de servicio necesarios.
- **Uso de sistemas operativos seguros:** el mercado ofrece diferentes sistemas operativos que pueden ser usados en nuestros sistemas. Como es de suponer, no todos ellos ofrecen el mismo nivel de seguridad. Es conveniente usar sistemas operativos con niveles de seguridad acordes a las necesidades de nuestra estrategia de seguridad. Existe una catalogación de los niveles de seguridad que ofrece un sistema operativo determinada por el estándar unificado *Common Criteria for*



Information Technology Security Evaluation (simplificado habitualmente por *Common Criteria*).

- **Equipos de respuesta a incidencias:** es aconsejable formar un equipo de respuestas a incidencias que dé apoyo al responsable de seguridad y que actúe siguiendo los planes de contingencia en caso de ser necesario.
- **Copias de respaldo** (*backups*): el backup de datos permite tener disponible una copia íntegra de los datos en caso de pérdida o corrupción de los mismos tras un ataque o un accidente. Es conveniente diseñar cuidadosamente la política y el procedimiento de creación, transporte y almacenamiento de las copias de respaldo de los datos y también de los programas usados en la organización.
- **Cortafuegos** (*firewalls*): son sistemas, hardware o software, destinados a filtrar el tráfico que circula por los sistemas de comunicaciones. Es habitual utilizarlos para controlar el tráfico que entra y sale de nuestra organización para evitar así algunos tipos de ataques basados en manipulación de paquetes. Además, permiten también controlar las aplicaciones y protocolos que son utilizados por los empleados.
- **Sistemas de Detección de Intrusos:** conocidos por sus siglas en inglés IDS. Un IDS es capaz de recoger y usar información de los eventos ocurridos en el sistema para detectar patrones de ataques y alertar al administrador de posibles ataques. Algunos tipos de IDS son incluso capaces de llevar acabo acciones reactivas destinadas a abortar los ataques detectados.
- **Programas antivirus:** son programas destinados a la detección y eliminación de virus informáticos. Es conveniente contar con

antivirus en todos los equipos del sistema de información. Para que los antivirus sean efectivos es vital que se encuentren actualizados.

- **Herramientas de seguridad:** como ya se ha comentado, pueden ser de gran utilidad para gestionar la seguridad y configurar nuestros sistemas correctamente aumentando así la protección de nuestro sistema.
- **Encriptación de la información:** dado que por muchas medidas de seguridad que tomemos seguiremos corriendo el riesgo de sufrir accesos no autorizados a nuestra información, es una buena práctica usar la encriptación para aumentar la protección de la información sensible. La encriptación debe aplicarse tanto a la información que se transmite a través de sistemas de comunicación como a aquella de especial importancia aunque ésta no salga de nuestro sistema.

2. ANALISIS Y GESTIÓN DE RIESGOS

2.1. Introducción

En toda organización existen una serie de activos sensibles desde el punto de vista de la seguridad. Estos activos están sujetos a riesgos que, en caso de materializarse, los dañarán causando un perjuicio a la organización. Una de las tareas en la gestión de la seguridad pasa por analizar y gestionar esos riesgos para mantenerlos bajo control o para estar preparados para reaccionar en caso de que dañen o destruyan nuestros activos.

El análisis de riesgos consiste en identificar las amenazas a nuestros activos y estimar la magnitud de las mismas. Debe realizarse para todos aquellos activos de importancia estratégica en la continuidad del negocio,

aquellos de carácter único o aquellos necesarios para cumplir con la legislación vigente.

La gestión de los riesgos se define como la selección e implantación de medidas de seguridad para conocer, prevenir, reducir o controlar los riesgos identificados. La gestión de los riesgos debe tener como objetivo mantener el nivel de riesgo por debajo de un umbral determinado por la organización.

El proceso de análisis y gestión de riesgos puede completarse mediante auditorías internas y externas que garanticen la revisión objetiva de las decisiones tomadas. Incluso es posible llegar a obtener certificaciones de nuestro sistema de gestión de la seguridad de la información (SGSI) cómo la ISO/IEC 27001.

Por último, hay que tener en cuenta que una organización y sus activos son elementos dinámicos que cambian con el tiempo y que por tanto los riesgos que les afectan también lo hacen. En la práctica esto tiene como consecuencia la necesidad de la revisión periódica de los análisis de riesgos y de las medidas de gestión de riesgos implementadas.

2.2. Análisis de riesgos

El proceso del análisis de riesgos incluye las siguientes tareas:

- **Identificar y valorar los activos:** todos aquellos activos de la organización deben ser identificados y valorados económicamente desde el prisma del sistema de la información. Además deben identificarse las relaciones de dependencia que existen entre ellos.
- **Identificar vulnerabilidades:** todas aquellas debilidades o posibles agujeros de seguridad que pudieran ser aprovechados para realizar ataques contra los activos.

- **Identificar amenazas:** serán todas aquellas situaciones que podrían generar una situación de peligro o daño para los activos.
- **Clasificar los riesgos:** debe obtenerse una clasificación de todos los riesgos que afectan a la seguridad de la organización, ordenados según el nivel de riesgo que soporte. El nivel de riesgo será una medida combinada del valor del activo afectado, la valoración del impacto y la probabilidad de que este ocurra.
- **Evaluar el impacto:** estimaremos también qué probabilidad existe de que una de las amenazas se materialice sobre un activo y qué coste tendría eso para la organización si el activo quedase dañado o inutilizado.
- **Determinar el grado de aseguramiento:** por último, debe determinarse el nivel de riesgo que la organización está dispuesta a asumir. Servirá como medida en la fase de gestión de riesgos para determinar qué controles debemos aplicar en cada caso para obtener un riesgo aceptable y conforme con el grado de aseguramiento que la organización necesita.

El análisis de riesgos tiene un carácter altamente subjetivo, ya que cualquier valoración es siempre en base a las necesidades y objetivos de la organización sobre la que se realiza el análisis.

Aun así, existen técnicas destinadas a realizar las evaluaciones de modo cualitativo (sesiones de *brainstorming*, entrevistas y cuestionarios estructurados, técnicas Delphi, gráficos DAFO, etc.) e incluso cuantitativo (método Montecarlo, análisis algorítmico cuantitativo, etc.).

2.3. Gestión de riesgos

Como ya hemos apuntado, la fase de gestión de riesgos implica diseñar y aplicar las acciones o políticas necesarias para que los riesgos identificados se mantengan por debajo del nivel de riesgo que la organización puede aceptar.

Básicamente existen cuatro acciones que podemos realizar para reducir el riesgo en la organización:

- **Aceptar:** a priori es la menos costosa, ya que simplemente se conocen los riesgos y la probabilidad de que ocurran, pero se aceptan sin realizar ninguna acción de protección.

Evidentemente esta opción es válida solo para riesgos sobre activos realmente poco importantes o con probabilidades de materialización ínfimas. Algunos riesgos de seguridad, especialmente las amenazas relacionadas con desastres naturales, son de tal envergadura que sencillamente no es posible intervenir con medidas preventivas ni reactivas de una forma eficaz.

Por lo tanto, el equipo de seguridad puede decidir simplemente aceptar el problema de seguridad. Aún así, y a pesar de aceptar el riesgo, deberían desarrollarse planes de contingencias para el caso en que un desastre llegara a suceder.

- **Anular:** en algunos casos puede ser beneficioso para la organización la anulación total de los riesgos de un activo simplemente prescindiendo de dicho activo.

Esto puede implicar, por ejemplo, la eliminación de algún servicio no esencial, el dejar de usar algún software o cortar el tráfico de ciertos protocolos de red en nuestro sistema.

- **Transferir:** a veces es posible ceder la responsabilidad sobre el activo a un tercero. Esta opción pasa por contratar seguros sobre nuestros activos o utilizar directamente los activos de otra entidad proveedora.

La transferencia de un riesgo de seguridad no significa que un riesgo se haya eliminado. En general, una estrategia de transferencia generará nuevos riesgos de seguridad relacionados con los proveedores o aseguradoras que requerirán administración preventiva. Sin embargo, la transferencia del riesgo reducirá la amenaza a un nivel más aceptable.

- **Mitigar:** consiste en implementar medidas de seguridad efectivas que nos permitan reducir los riesgos identificados. La mitigación supone tomar acciones preventivas para evitar que un riesgo se materialice o para reducir sus consecuencias a un nivel aceptable.

El objetivo es la prevención y la minimización de las amenazas hasta niveles aceptables por la organización. Por ejemplo, el uso de una directiva de contraseña segura reducirá la probabilidad de que un usuario externo averigüe una contraseña para tener acceso a un sistema de nóminas.

Los controles de seguridad a aplicar y las medidas que permitan determinar su eficacia, deben ser seleccionados, diseñados y, una vez implantados, revisados periódicamente con el fin de descubrir necesidades de nuevos controles o la adaptación de los mismos.

2.1. La metodología **MAGERIT**

MAGERIT es una metodología para el análisis y gestión de riesgos de los sistemas de información elaborada originalmente por el Consejo Superior de Administración Electrónica del Gobierno de España (aunque

actualmente depende del Ministerio de Política Territorial y Administración Pública y es administrada por la Dirección General para el Impulso de la Administración Electrónica).

Su objetivo final es la minimización de los riesgos de la implantación y uso de las tecnologías de la información en las Administraciones Públicas. Actualmente se encuentra en su versión 2.

La utilización de la metodología MAGERIT en sí no requiere de ningún tipo de autorización previa y la documentación que la describe es de dominio público e incluso el Centro Criptológico Nacional (CCN) ofrece de forma gratuita una aplicación (llamada PILAR⁶) que constituye un Entorno de Análisis de Riesgos (EAR) para el análisis y gestión de riesgos de un Sistema de Información usando la metodología MAGERIT. Este aperturismo se debe a la convicción de que la generalización del uso de las tecnologías de la información y de las comunicaciones es potencialmente beneficiosa para los ciudadanos, las empresas y la propia Administración Pública, pero que también da lugar a ciertos riesgos que deben minimizarse con medidas de seguridad que generen confianza en su utilización.

En definitiva, MAGERIT persigue los siguientes objetivos:

- Concienciar a los responsables de los sistemas de información de la existencia de riesgos y de la necesidad de atajarlos a tiempo.
- Ofrecer un método sistemático para analizar tales riesgos.
- Ayudar a descubrir y planificar las medidas oportunas para mantener los riesgos bajo control.
- Preparar a la Organización para procesos de evaluación, auditoría, certificación o acreditación, según corresponda en cada caso.

⁶ Puede encontrarse en la página del CCN (<https://www.ccn-cert.cni.es/>) dentro del apartado herramientas.

2.1.1. Elementos de la metodología

A continuación, y aunque alguno de ellos ya ha sido mencionado en el contexto de los riesgos de seguridad, definimos brevemente los elementos considerados significativos por MAGERIT para el estudio de la Seguridad en Sistemas de Información.

- **Activos:** recursos del sistema de información o relacionados con éste, necesarios para que la organización funcione correctamente y alcance los objetivos propuestos por la dirección.
- **Amenazas:** eventos que pueden desencadenar un incidente en la organización, produciendo daños materiales o pérdidas inmateriales en sus activos.
- **Vulnerabilidad de un activo:** potencialidad o posibilidad de ocurrencia de la materialización de una amenaza sobre dicho activo.
- **Impacto en un activo:** consecuencia sobre éste de la materialización de una amenaza.
- **Riesgo:** posibilidad de que se produzca un impacto determinado en un activo, en un dominio o en toda la organización
- **Servicio de salvaguarda:** acción que reduce el riesgo.
- **Mecanismo de salvaguarda:** procedimiento, dispositivo, físico o lógico, que reduce el riesgo.

Los activos están expuestos a amenazas que, cuando se materializan, degradan el activo, produciendo un impacto. Si estimamos la frecuencia con que se materializan las amenazas, podemos deducir el riesgo al que está expuesto el sistema. Degradación y frecuencia califican la vulnerabilidad del sistema. El administrador del sistema de información

dispone de salvaguardas, que o bien reducen la frecuencia de ocurrencia, o bien reducen o limitan el impacto.

2.1.2. Estructura de la metodología:

El desarrollo de la metodología MAGERIT versión 2 se estructura en tres guías:

- **Método:** describe los procesos, actividades y tareas para realizar un proyecto de análisis y gestión de riesgos, y proporciona una serie de consejos y casos prácticos de ejemplo. Incluye además un anexo en el que se establecen correspondencias con la versión 1 de MAGERIT.
- **Catálogo de Elementos:** ofrece una serie de pautas en cuanto a tipos de activos, dimensiones de valoración de los activos, criterios de valoración de los activos, amenazas típicas sobre los sistemas de información y salvaguardas a considerar para proteger sistemas de información.
- **Guías de Técnicas:** se trata de una guía de consulta que proporciona algunas técnicas que se emplean habitualmente para llevar a cabo proyectos de análisis y gestión de riesgos: técnicas específicas para el análisis de riesgos, análisis mediante tablas, análisis algorítmico, árboles de ataque, técnicas generales, análisis coste-beneficio, diagramas de flujo de datos, diagramas de procesos, técnicas gráficas, planificación de proyectos, sesiones de trabajo (entrevistas, reuniones y presentaciones) y valoración Delphi.

2.1.3. Procesos de la metodología:

La guía del Método Magerit Versión 2 especifica que un proyecto de análisis y gestión de riesgos consta de tres procesos, que a su vez se dividirán en actividades y tareas que se detallan en la guía del Método:

- Proceso P1: Planificación:
 - Se establecen las consideraciones necesarias para arrancar el proyecto de análisis y gestión de riesgos.
 - Se investiga la oportunidad de realizarlo.
 - Se definen los objetivos que ha de cumplir y el dominio (ámbito) que abarcará.
 - Se planifican los medios materiales y humanos para su realización.
 - Se procede al lanzamiento del proyecto.
 - Se generan los siguientes documentos: Tipología de Activos, Dimensiones de Seguridad Relevantes, Criterios de Evaluación.
 -
- Proceso P2: Análisis de riesgos:
 - Se identifican los activos a tratar, las relaciones entre ellos y la valoración que merecen.
 - Se identifican las amenazas significativas sobre aquellos activos y se valoran en términos de frecuencia de ocurrencia y degradación que causan sobre el valor del activo afectado.



- Se identifican las salvaguardas existentes y se valora la eficacia de su implantación.
- Se estima el impacto y el riesgo al que están expuestos los activos del sistema.
- Se interpreta el significado del impacto y el riesgo.
- Se generan los siguientes documentos: Modelo de Valor, Mapa de Riesgos, Evaluación de Salvaguardas, Estado de Riesgo, Informe de Insuficiencias.
-
- Proceso P3: Gestión de riesgos:
- Se elige una estrategia para mitigar impacto y riesgo.
- Se determinan las salvaguardas oportunas para el objetivo anterior.
- Se determina la calidad necesaria para dichas salvaguardas.
- Se diseña un plan de seguridad (plan de acción o plan director) para llevar el impacto y el riesgo a niveles aceptables.
- Se lleva a cabo el plan de seguridad.
- Como producto de esta fase se genera el Plan de Seguridad.

3. REFERENCIAS⁷

- Telecommunications Industry Association (TIA)

<http://www.tiaonline.org/>

- RFC 4949 Internet Security Glossary, Version 2

<http://tools.ietf.org/html/rfc4949>

- RFC 2196 Site Security Handbook

<http://tools.ietf.org/html/rfc2196>

- *Common Criteria* for Information Technology Security Evaluation

<http://www.commoncriteriaportal.org/>

- Documentación de la metodología MAGERIT versión 2.

http://www.mpt.gob.es/publicaciones/centro_de_publicaciones_de_la_sgt/Monografias0

Autor: Juan Otero Pombo

Ingeniero en Informática en el Concello de Ourense

Colegiado del CPEIG

⁷ Los enlaces fueron comprobados en noviembre de 2011.

41. SISTEMAS DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN: NORMAS DE LA SERIE ISO 27.000.

Tema 41. Sistemas de gestión de la seguridad de la información: normas de la serie ISO 27000

INDICE

<u>1. SISTEMAS DE GESTION DE LA SEGURIDAD DE LA INFORMACION</u>	<u>1</u>
<u>1.1. Introducción.....</u>	<u>2</u>
<u>1.2. Características principales de un SGSI.....</u>	<u>3</u>
<u>1.3. Implementación de un SGSI.....</u>	<u>6</u>
<u>1.3.1 Planificar (Plan).....</u>	<u>7</u>
<u>1.3.2 Hacer (Do):.....</u>	<u>11</u>
<u>1.3.3 Verificar (Check):.....</u>	<u>12</u>
<u>1.3.4 Actuar (Act):.....</u>	<u>13</u>
<u>1.4. La responsabilidad de dirección en un SGSI.....</u>	<u>14</u>
<u>1.5. Beneficios de un SGSI.....</u>	<u>15</u>
<u>2. NORMAS DE LA SERIE ISO/IEC 27000.....</u>	<u>16</u>
<u>2.1. Las organizaciones ISO e IEC.....</u>	<u>16</u>
<u>2.2. La serie ISO/IEC 27000.....</u>	<u>17</u>
<u>2.3. Contenido de la norma.....</u>	<u>19</u>
<u>2.3.1 ISO/IEC 27001.....</u>	<u>20</u>
<u>2.3.2 ISO/IEC 27002.....</u>	<u>21</u>
<u>2.3.3 ISO/IEC 27003.....</u>	<u>23</u>
<u>2.3.4 ISO/IEC 27006.....</u>	<u>25</u>
<u>2.4. El proceso de implantación.....</u>	<u>26</u>
<u>2.5. El proceso de certificación.....</u>	<u>29</u>
<u>3. REFERENCIAS.....</u>	<u>33</u>

1. SISTEMAS DE GESTION DE LA SEGURIDAD DE LA INFORMACION

1.1. Introducción

La información se ha convertido en uno de los principales activos de las empresas y las organizaciones constituyendo una ventaja competitiva. Es por esto que la seguridad de la información se antoja vital en el seno de cualquier organización, especialmente si esta se encuentra en formato electrónico.

La complejidad creciente de los sistemas de información y la relevancia de estos dentro de las organizaciones hace que la gestión de la seguridad se convierta en un factor a controlar con interés.

El establecimiento de un Sistema de Gestión de la Seguridad de la Información (SGSI)¹ permite manejar la gestión de la seguridad de un modo ordenado y orientado a la mejora continua estableciendo un conjunto de políticas de administración de la información.

En síntesis, un SGSI se encargará del diseño, implantación y mantenimiento de un conjunto de procesos orientados a gestionar eficientemente la accesibilidad de la información, buscando asegurar la confidencialidad, integridad y disponibilidad de los activos de información minimizando a la vez los riesgos de seguridad.

A menudo se confunde la seguridad informática con la seguridad de la información. Esta confusión se debe a que con la digitalización de la información la preocupación por la seguridad de la misma ha ido creciendo. Podemos decir que el término seguridad de la información engloba también la seguridad informática ya que esta se centra en los elementos propios de la infraestructura de las tecnologías de la información y de las comunicaciones que nuestra organización necesita (componentes hardware, redes, software, etc.). Sin embargo, la

¹ En inglés, Information Security Management System (ISMS).

información de la organización puede encontrarse en diversos formatos como archivos de texto, imágenes, contratos, documentos en papel, etc.

Por lo tanto, aunque habitualmente se relacionan los SGSI con sistemas digitales, su alcance incluye también la información que se encuentra en soportes no digitales.

La amenaza de accesos no autorizados a la información almacenada en equipos conectados a una red es constante. Esto, unido al continuo y vertiginoso desarrollo de las tecnologías de la información, que ha hecho posible que millones de ordenadores separados por miles de kilómetros puedan estar interconectados como si estuviesen en una misma habitación, nos conduce a una conclusión inmediata: la seguridad absoluta no existe.

El objetivo de cualquier sistema de seguridad será la reducción de los riesgos contra los activos de la empresa hasta un nivel (o umbral) aceptable. Un SGSI constituye una valiosa herramienta para controlar y mejorar los sistemas de seguridad mediante un proceso sistemático, documentado y conocido por toda la organización.

1.2. Características principales de un SGSI

Un **Sistema de Gestión de la Seguridad de la Información**, denominado habitualmente por sus siglas **SGSI**, es una herramienta que implementa un conjunto de políticas de administración de la información que permiten conocer, gestionar y minimizar los posibles riesgos que atenten contra la seguridad de la misma.

El concepto de SGSI constituye el término central sobre el que se define la norma **ISO 27001**.

La información es uno de los principales activos de las organizaciones. La defensa de este activo es una tarea esencial para asegurar la continuidad y el desarrollo del negocio, así como también es una exigencia legal (protección de la propiedad intelectual, protección de datos personales, servicios para la sociedad de la información), y además traslada confianza a los clientes y usuarios.

Cuanto mayor es el valor de la información, mayores son los riesgos asociados a su pérdida, sustracción, deterioro, manipulación indebida o malintencionada.

Los Sistemas de Gestión de Seguridad de la Información (SGSI) son el medio más eficaz de minimizar los riesgos, al asegurar que se identifican y valoran los activos y sus riesgos, considerando el impacto para la organización, y se adoptan los controles y procedimientos más eficaces y coherentes con la estrategia de negocio.

Una gestión eficaz de la seguridad de la información permite garantizar:

- su confidencialidad, asegurando que sólo quienes estén autorizados puedan acceder a la información,
- su integridad, asegurando que la información y sus métodos de proceso son exactos y completos, y
- su disponibilidad, asegurando que los usuarios autorizados tienen acceso a la información y a sus activos asociados cuando lo requieran.

En muchas organizaciones la mayor parte de la información reside en equipos informáticos, redes de datos y soportes de almacenamiento, encuadrados todos dentro de lo que se conoce como sistemas de información. Estos sistemas están sujetos a riesgos e inseguridades tanto desde dentro de la propia organización como desde fuera. A los riesgos

físicos (acceso de personas no autorizadas a la información, catástrofes naturales, incendios, etc.) hay que sumarle los riesgos lógicos (accesos remotos no autorizados, virus, ataques de denegación de servicio, etc.).

La adecuada gestión de la seguridad permite disminuir de forma significativa el impacto de los riesgos sin necesidad de realizar grandes inversiones en software y sin contar con una gran estructura de personal. Para ello se hace necesario:

- Conocer y afrontar de manera ordenada los riesgos a los que está sometida la información.
- Contar con la participación activa de toda la organización, especialmente con el respaldo y la implicación de la dirección.
- Establecer políticas, procedimientos y controles de seguridad adecuados.
- Planificar e implantar controles de seguridad basados en una evaluación de riesgos y en una medición de la eficacia de los mismos.
- Realizar un proceso de evaluación y mejora continua.

Un SGSI ayuda a una organización a establecer las políticas, procedimientos y controles en relación a los objetivos de negocio de la organización, con objeto de mantener siempre el riesgo por debajo del nivel asumible por la propia organización. Además, proporciona una cobertura completa de la gestión de la seguridad, desde el nivel estratégico más alto, donde la dirección definirá y aprobará las políticas de seguridad, hasta el nivel más bajo, donde, entre otras acciones, se implementarán los controles técnicos y se gestionarán las incidencias del sistema.

Otra de las ventajas de la implantación de un SGSI es la asistencia a la organización en el tratamiento de aspectos clave como el cumplimiento de la legalidad, la adaptación dinámica y continuada a las condiciones variables del entorno, la protección adecuada de los objetivos de negocio para asegurar el máximo beneficio o el aprovechamiento de nuevas oportunidades de negocio.

En definitiva, mediante el uso de un SGSI, la organización conoce los riesgos a los que está sometida su información y los gestiona mediante un plan definido, documentado y conocido por todos, que se revisa y mejora constantemente.

1.3. Implementación de un SGSI

Cuando una organización afronta la implantación de un SGSI debe tener presente se trata de una decisión de carácter estratégico y que, como tal, afecta a toda la organización.

La tarea de la implantación no recaerá única y exclusivamente en el área de tecnologías de la información, sino que debe involucrar a toda la organización y estar apoyada y dirigida por la dirección. De hecho, la primera fase de la implantación debería consistir en alcanzar la aprobación y el apoyo de la dirección para todo el proceso.

El alcance y diseño del SGSI dependerá de los objetivos de la empresa, sus características (actividad, tamaño, dispersión geográfica, etc.), recursos económicos, etc. De hecho, es posible que en algunos casos el SGSI no se implante en todas las áreas de la organización de un solo paso, sino que se haga solamente en aquellas en las que la información que utiliza tenga especial relevancia y completar el resto en una implantación por fases.

Es frecuente la redefinición de políticas de seguridad de la información, por lo el establecimiento de un SGSI debe hacerse siguiendo un método de implantación orientado a la mejora continua. Esto pasa por una metodología cíclica que incluya de manera fundamental un mecanismo de retroalimentación en cuanto a errores e incidencias detectadas.

El método comúnmente aceptado es el PDCA² (Planificar-Hacer-Verificar-Actuar). Se trata de un modelo en cuatro fases en el que una vez realizada la última y analizados los resultados, continua de nuevo en la primera fase del modelo.

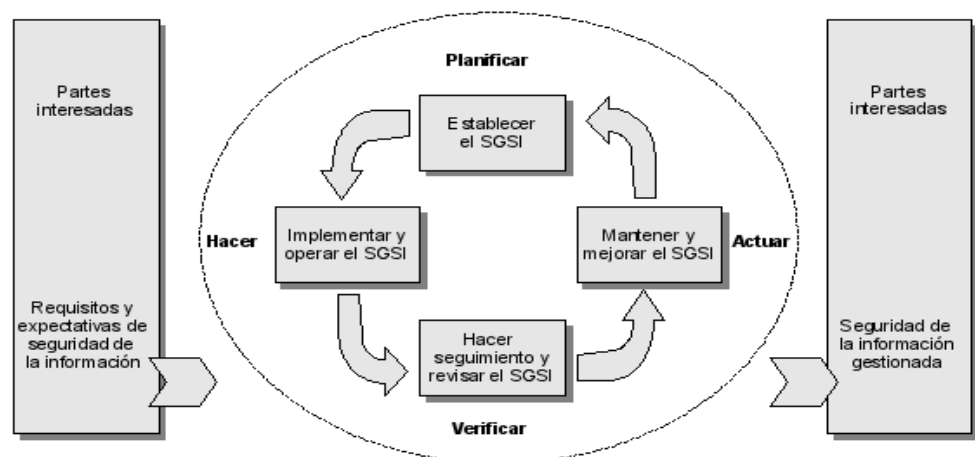


Imagen 1: Esquema del modelo PDCA (fuente: Instituto Uruguayo de Normas Técnicas)

1.3.1 Planificar (Plan)

En la primera fase del modelo PDCA aplicado a SGSIs se realiza un estudio de la situación de la organización desde el punto de vista de la seguridad, para determinar el alcance de las medidas que se van a implantar en función de las necesidades detectadas.

² Siglas en inglés de Plan-Do-Check-Act, también conocido como “Ciclo de Deming” en referencia al estadístico Edwards Deming, que promocionó su uso en el ámbito del aseguramiento de la calidad.

Es importante realizar un análisis de riesgos que valore los activos de información y las vulnerabilidades a las que están expuestos ya que no toda la información de la que disponemos tiene el mismo valor o está sometida a los mismos riesgos. El objetivo es gestionar dichos riesgos estableciendo los controles adecuados que nos permitan minimizarlos.

Durante esta fase se realizan las siguientes acciones:

- o Estimación de los recursos económicos y de personal que van a ser necesarios para la correcta implantación y mantenimiento del SGSI.
- o Determinar el alcance del SGSI en base a la información y a los procesos de la organización que serán incluidos en el SGSI. Deben quedar definidas las actividades de la organización, las ubicaciones físicas que van a verse involucradas, la tecnología de la organización y también las áreas que quedarán excluidas en la implantación del sistema.
- o Determinar la metodología de evaluación de riesgos apropiada para el SGSI y las características de nuestra organización, además de establecer los criterios de aceptación del riesgo y especificar los niveles de riesgo aceptables.
- o Revisar los aspectos organizativos de la entidad y la asignación de nuevas responsabilidades. Deben existir al menos tres roles fundamentales:
 - 1. El Responsable de Seguridad debe ser una única persona cuya misión es la de coordinar todas las actuaciones en materia de seguridad que se desarrollen en la organización.



2. El Comité de Gestión se hará cargo las acciones de la implantación del sistema colaborando muy estrechamente con el responsable de seguridad de la entidad. Este comité estará formado por personal de los diferentes departamentos involucrados en la implantación del sistema y tendrá potestad para asumir decisiones de seguridad.

3. El Comité de Dirección será el responsable de tomar y asumir decisiones de alto nivel necesarias para apoyar los objetivos del SGSI y estará formado por miembros de la dirección con poder ejecutivo.

o Establecer la **Política de Seguridad**. Se trata de uno de los documentos más importantes en un SGSI y debe estar aprobado por el comité de dirección. Su principal objetivo es recoger las directrices que debe seguir la seguridad de la información de acuerdo a las necesidades de la organización y a la legislación vigente. Además, debe establecer las pautas de actuación en el caso de incidentes y definir las responsabilidades.

La política de seguridad se plasmará en un documento que debe estar accesible para todos los miembros de la organización e incluir, al menos, los siguientes apartados:

1. Declaración de apoyo por parte de la Dirección a los objetivos y principios de la seguridad de la información.
2. Breve explicación de las políticas.
3. Definición de la seguridad de la información y sus objetivos globales, el alcance de la seguridad y su importancia como mecanismo de control que permite compartir la información.



4. Definición de responsabilidades generales y específicas, en las que se incluirán los roles pero nunca personas concretas dentro de la organización.
 5. Referencias a documentación que pueda sustentar la política.
- o Identificar y determinar las distintas opciones de gestión del riesgo y seleccionar aquellas que se van a aplicar. Básicamente, existen tres opciones para el tratamiento del riesgo:
1. Asumir el riesgo sin tomar ninguna medida. Esto es posible siempre y cuando no entre en conflicto con la política de seguridad establecida por la organización.
 2. Transferir el riesgo mediante la contratación de servicios externos o seguros. Evidentemente, esto no siempre es posible.
 3. Reducir el riesgo hasta los niveles aceptables mediante la implantación de controles de seguridad.
- o Desarrollo de la formación necesaria para que el personal realice sus actividades correctamente dentro de la normativa que aplique el SGSI.
- o Concienciación y divulgación en torno al personal de la organización para que todos conozcan las acciones que se están llevando a cabo y cuales son sus consecuencias y beneficios en el marco de la seguridad.

- o Construir la Declaración de Aplicabilidad³, que determina qué controles son los que serán aplicados en el sistema, cuales ya se encuentran implementados y cuales no serán de aplicación y por qué.

Como se puede apreciar, la carga de trabajo en esta primera fase del modelo PDCA para la gestión de la seguridad es muy fuerte. Esto es algo lógico y habitual en cualquier sistema de gestión, donde la parte de planificación es un aspecto fundamental.

1.3.2 **Hacer (Do):**

Los controles técnicos de seguridad elegidos en la fase anterior son implantados en esta segunda fase del modelo PDCA desarrollando la documentación necesaria. Esta fase también requiere un tiempo de concienciación y formación para dar a conocer qué se está haciendo y por qué, al personal de la empresa.

En esta fase del modelo, se llevarán a cabo las siguientes tareas:

- o Definir e implantar un plan de tratamiento de riesgos que identifique las acciones, recursos, responsabilidades y prioridades en la gestión de los riesgos de seguridad de la información. La finalidad de este plan será alcanzar los objetivos de control identificados, incluyendo la asignación de recursos, responsabilidades y prioridades.
- o Definir un sistema de métricas que permita obtener resultados reproducibles y comparables para medir la eficacia de los controles o grupos de controles.

³ Conocida como SOA (Statement Of Applicability).



- o Gestionar los recursos necesarios asignados al SGSI para el mantenimiento de la seguridad de la información.
- o Implantar procedimientos y controles que permitan una rápida detección y respuesta a los incidentes de seguridad.
- o Desarrollar programas de formación y concienciación en relación a la seguridad de la información a todo el personal.
- o Gestionar las operaciones del SGSI.

1.3.3 Verificar (Check):

La tercera fase de nuestro Modelo PDCA es la fase de verificación o seguimiento. En ella se evalúa la eficacia y el éxito de los controles implantados. Por ello, es muy importante contar con registros e indicadores que provengan de estos controles.

Las tareas a realizar en esta fase son las siguientes:

- o Comprobar de modo continuo que el SGSI cumple la política y objetivos establecidos.
- o Medir la efectividad de los controles para verificar que se cumple con los requisitos de seguridad.
- o Ejecutar procedimientos de monitorización y revisión para detectar incidentes y determinar si las acciones llevadas a cabo para solucionarlos fueron efectivas.
- o Revisar regularmente en intervalos planificados las evaluaciones de riesgo, los riesgos residuales y sus niveles aceptables teniendo en cuenta los posibles cambios que hayan podido producirse en la organización; revisar la tecnología usada, los objetivos y procesos de negocio, las amenazas identificadas, la



- efectividad de los controles implementados y el entorno exterior; controlar los requerimientos legales, las obligaciones contractuales, etc.
- o Realizar periódicamente auditorías internas del SGSI en intervalos planificados.
 - o Revisión periódica del SGSI por parte de la dirección para garantizar que el alcance definido sigue siendo el adecuado y que las mejoras en el proceso del SGSI son evidentes.
 - o Actualizar los planes de seguridad en función de las conclusiones y nuevos hallazgos encontrados durante las actividades de monitorización y revisión.
 - o Registrar acciones y eventos que puedan haber impactado sobre la efectividad o el rendimiento del SGSI.

1.3.4 **Actuar (Act):**

En la última fase del modelo PDCA se llevarán a cabo las labores de mantenimiento del sistema. Si durante la fase anterior de seguimiento se ha detectado algún punto débil, este es el momento de mejorarlo o corregirlo, por eso a esta fase se la conoce a veces como fase de mejora

Las tareas a realizar en esta fase son las siguientes:

- o Realizar las acciones preventivas y correctivas adecuadas.
- o Implantar en el SGSI las mejoras identificadas en la fase anterior.
- o Asegurarse que las mejoras introducidas alcanzan los objetivos previstos.

- o Comunicar las acciones y mejoras a todas las partes interesadas con el nivel de detalle adecuado y acordar, si es pertinente, la forma de proceder.

Al finalizar las cuatro fases, se entra en un proceso iterativo de mejora continua partiendo de los resultados de la última se comienza nuevamente la primera consiguiendo así una retroalimentación del sistema con las soluciones a las deficiencias encontradas

1.4. La responsabilidad de dirección en un SGSI

La implantación de un SGSI requiere que la dirección sea consciente de la importancia que tendrá dentro de la organización. Si cae en el error de pensar que se trata de una mera cuestión técnica que debe ser solucionada en solitario por el área de tecnologías de la información, la implantación del SGSI estará sin duda condenada al fracaso.

El apoyo de la alta dirección de la organización debe materializarse en su involucración en el proceso asignando y proporcionando los recursos necesarios y preocupándose de formar y concienciar a toda la organización.

La tres responsabilidades principales de la dirección serán:

- o La asignación de recursos tanto económicos como de personal al desarrollo del SGSI así como para su mantenimiento y adaptación si fueran necesarios.
- o Revisión del SGSI para comprobar que sigue siendo adecuado y eficiente para la organización. Esta revisión debe ser llevada a cabo al menos una vez al año.

- o Concienciación y formación de todos los miembros de la organización en la medida que corresponda en función de la posición que ocupen.

1.5. Beneficios de un SGSI

La seguridad de la información es un aspecto que debe recibir una especial consideración en toda organización. Los SGSI constituyen una solución, casi siempre de bajo coste, que ayuda a controlar los riesgos. Pero además, la mejora de la seguridad trae consigo otros beneficios que se describen a continuación.

- **Cumplimiento Legal:** La implantación de un SGSI sirve para revisar y adaptar nuestra organización a aspectos relacionados con la legislación del país que posiblemente no se habían tenido en cuenta anteriormente.
- **Ahorro Económico:** Un SGSI permite mejorar el uso de los recursos, lo que repercute en un ahorro de costes. Poder tomar decisiones basadas en datos cuantitativos y no solo cualitativos, permite gestionar mejor el gasto en TI. De esta manera las inversiones en tecnología se ajustan a las prioridades que se han impuesto a través del Análisis de Riesgos, evitando los gastos innecesarios, inesperados, y sobredimensionados.
- **Reducción de riesgos:** es el fin último del SGSI. Partiendo del Análisis de Riesgos hasta la implementación de los controles, el conjunto de acciones adoptadas reducirá los riesgos de muchos aspectos de la organización hasta un nivel asumible.
- **Calidad de la seguridad:** la implementación de un SGSI transforma la seguridad en una actividad de gestión. Este concepto es importante ya que deja de lado un conjunto de actividades técnicas

más o menos organizadas, para transformarse en un ciclo de vida metódico y controlado, en el que al participar toda la organización, se crea conciencia y compromiso de seguridad en todos los niveles de la empresa.

- **Competitividad en el mercado:** contar con un SGSI es sin duda una ventaja competitiva ya que contribuye a mejorar la gestión de la organización y a dar a los clientes confianza suficiente al ceder su información a la organización. Además, la norma ISO/IEC 27001 permite certificar la conformidad de un SGSI. Esta norma es tan importante como otras relacionadas con la calidad en diferentes áreas, por ejemplo la ISO 9001. Poco a poco las grandes empresas, los clientes y las administraciones comenzarán a exigir esta certificación para abrir y compartir sus sistemas. Contar con una certificación de estas características se convierte entonces en un importante factor diferenciador con la competencia, por las ventajas derivadas de la mejora de imagen y ventaja competitiva en el mercado.

2. NORMAS DE LA SERIE ISO/IEC 27000

2.1. Las organizaciones ISO e IEC

La **Organización Internacional para la Estandarización** ISO⁴ es una federación de alcance mundial integrada en la actualidad por instituciones nacionales de estandarización de 162 países, uno por cada país. Tiene su sede central en Génova (Suiza), desde donde se coordinan sus actividades. Se trata de una organización no gubernamental, que intenta desarrollar estándares en diferentes campos que cubran las necesidades tanto de empresas privadas como de la propia sociedad en general.

⁴ Siglas en inglés de *International Organization for Standardization*.

La **Comisión Electrotécnica Internacional** IEC⁵, es también una organización no gubernamental sin ánimo de lucro. Destaca por ser una de las organizaciones más importantes y activas del mundo en el desarrollo de estándares internacionales para todo tipo de tecnologías relacionadas con la electricidad y la electrónica.

Algunos de los estándares mayormente aceptados en el mundo de las tecnologías de la información han surgido del trabajo coordinado de estas dos organizaciones. Hablamos de normas como la ISO/IEC 8613 (Arquitectura Open Document) o ISO/IEC 9945 (Portable Operating System Interface - POSIX) entre muchas otras, que se han convertido en estándares relacionados con conceptos de tecnologías de la información profundamente implantados y aceptados.

Existe, sin embargo, un conjunto de normas que destacan por su relación con el concepto de la calidad en diferentes campos de las tecnologías de la información. Se trata de ISO/IEC 15504 (SPICE), sobre la calidad en los procesos de construcción del software, la serie ISO/IEC 20000, centrada en la gestión de servicios de tecnologías de la información, y de la serie ISO/IEC 27000 para la gestión de la seguridad de sistemas de información.

2.2. La serie ISO/IEC 27000

La serie de normas ISO/IEC 27000⁶ proporciona recomendaciones de buenas prácticas sobre gestión, riesgos y controles en el ámbito de la seguridad de la información, conformando lo que se conoce como Sistemas de Gestión de la Seguridad de la Información.

⁵ Siglas en inglés de *International Electrotechnical Commission*.

⁶ Conocida a veces simplemente como ISO 27000 o ISO27K

El conjunto de normas es aplicable a cualquier organización sin importar su tamaño, y sigue un patrón de implantación basado en el modelo PDCA (Plan-Do-Check-Act), descrito anteriormente.

El diseño de la serie es similar a otras normas de aseguramiento de la calidad para sistemas de gestión (especialmente a la serie ISO 9000). Los rangos reservados de numeración por ISO para normas de esta serie van de 27000 a 27019 y de 27030 a 27044.

Las siguientes normas de la serie ya han sido publicadas y están siendo usadas en la práctica:

- ISO/IEC 27000: SGSI - Presentación y vocabulario.
- ISO/IEC 27001: SGSI - Requisitos.
- ISO/IEC 27002: Código de buenas prácticas para la gestión de la seguridad de la información.
- ISO/IEC 27003: Guía de implantación de SGSI.
- ISO/IEC 27004: Gestión de la seguridad de la información - Métricas.
- ISO/IEC 27005: Gestión de riesgos de la seguridad de la información.
- ISO/IEC 27006: Requisitos para organismos de auditoría y certificación de SGSI.
- ISO/IEC 27011: Guía sectorial de gestión de la seguridad de la información para organizaciones de telecomunicaciones.
- ISO/IEC 27031: Guía de gestión de la información y las tecnologías de las comunicaciones para la continuidad del negocio.

- ISO/IEC 27033: Introducción y conceptos de la seguridad en la red. Parte I.
- ISO 27799: Guía sectorial para la aplicación de la norma ISO/IEC 27002 en entornos relacionados con la salud.

Los textos traducidos al castellano de algunas de las normas de esta serie pueden obtenerse (previo pago) de la página web de AENOR (<http://www.aenor.es>).

La serie podría completarse en un futuro próximo con las siguientes normas:

- ISO/IEC 27007: Guía para la auditoría de SGSI centrada en las actividades de gestión.
- ISO/IEC 27008: Guía para la auditoría de SGSI centrada en los controles de seguridad de la información.
- ISO/IEC 27013: Guía para la implementación integrada de ISO/IEC 20000-1 e ISO/IEC 27001.
- ISO/IEC 27036: Guía para la seguridad de servicios externalizados (*outsourcing*).

2.3. Contenido de la norma

El número de normas incluidas en la serie es bastante elevado, por lo que nos centraremos únicamente en la descripción del contenido de algunas de ellas: 27001, 27002, 27003 y 27006.

2.3.1 ISO/IEC 27001

Esta norma sustituyó a la antigua BS7799-2⁷ con fecha de publicación 15 de Octubre de 2005, centrándose en la definición de un modelo para la creación, implementación, operación, supervisión, revisión, mantenimiento y mejora de un SGSI. Es la única norma en la que una organización se puede certificar dentro del esquema.

Dentro de esta norma podremos encontrar los siguientes apartados:

- o **Introducción:** generalidades e introducción al método PDCA.
- o **Objeto y campo de aplicación:** se especifica el objetivo, la aplicación y el tratamiento de exclusiones.
- o **Normas para consulta:** otras normas que pueden servir de referencia en el proceso.
- o **Términos y definiciones:** breve descripción de los términos más usados en la norma.
- o **Sistema de gestión de la seguridad de la información:** cómo crear, implementar, operar, supervisar, revisar, mantener y mejorar el SGSI; requisitos de documentación y control de la misma.
- o **Responsabilidad de la dirección:** en cuanto a compromiso con el SGSI, gestión y provisión de recursos y concienciación, formación y capacitación del personal.
- o **Auditorías internas del SGSI:** cómo realizar las auditorías internas de control y cumplimiento.
- o **Revisión del SGSI por la dirección:** cómo gestionar el proceso periódico de revisión del SGSI por parte de la dirección.
- o **Mejora del SGSI:** mejora continua, acciones correctivas y acciones preventivas.

⁷ De la British Standards Institution (BSI), la organización británica equivalente a AENOR en España.

- o **Anexo A: Objetivos de control y controles.**
- o **Anexo B: Relación con los Principios de la Organización para la Cooperación y el Desarrollo Económico (OCDE).**
- o **Anexo C: Correspondencia con otras normas.**
- o **Bibliografía:** normas y publicaciones de referencia.

2.3.2 ISO/IEC 27002

La norma ISO 17799, que constituía un código de buenas prácticas para la seguridad de la información, se convirtió en la ISO/IEC 27002 desde el 1 de Julio de 2007. Se trata más de un código de buenas prácticas que de una norma como tal. No establece obligatoriedad en sus especificaciones y cabe recordar que no es una norma certificable. En lugar de eso, presenta 39 objetivos de control y desglosa los 139 controles presentados en el Anexo A de la ISO/IEC 27001, dando a veces varias opciones de implementación, que podrían ser, en teoría, implantados tomando como guía las especificaciones de la ISO/IEC 27001.

El contenido de la norma tiene su origen en un documento del gobierno del Reino Unido que se convirtió en 1995 en la norma BS7799 y posteriormente, en el año 2000, en la norma ISO 17799:2000, con una versión posterior 17799:2005. Finalmente, en 2007 se publica la norma ISO/IEC 27002 sustituyendo a la citada 17799:2005.

Los planes de ISO para estos estándares pasan por centrarse en otros códigos de buenas prácticas sectoriales, como por ejemplo en el entorno de la salud (ya publicada en forma de ISO/IEC 27799).

Dentro de esta norma podremos encontrar los siguientes apartados:



- o **Introducción:** conceptos generales de seguridad de la información y SGSI.
- o **Campo de aplicación:** se especifica el objetivo de la norma.
- o **Términos y definiciones:** breve descripción de los términos más usados en la norma.
- o **Estructura del estándar:** descripción de la estructura de la norma.
- o **Evaluación y tratamiento del riesgo:** indicaciones sobre cómo evaluar y tratar los riesgos de seguridad de la información.
- o **Política de seguridad:** documento de política de seguridad y su gestión.
- o **Aspectos organizativos de la seguridad de la información:** organización interna; terceros.
- o **Gestión de activos:** responsabilidad sobre los activos; clasificación de la información.
- o **Seguridad ligada a los recursos humanos:** antes del empleo; durante el empleo; cese del empleo o cambio de puesto de trabajo.
- o **Seguridad física y ambiental:** áreas seguras; seguridad de los equipos.
- o **Gestión de comunicaciones y operaciones:** responsabilidades y procedimientos de operación; gestión de la provisión de servicios por terceros; planificación y aceptación del sistema; protección contra código malicioso y descargable; copias de seguridad; gestión de la seguridad de las redes; manipulación de los soportes; intercambio de información; servicios de comercio electrónico; supervisión.

- o **Control de acceso:** requisitos de negocio para el control de acceso; gestión de acceso de usuario; responsabilidades de usuario; control de acceso a la red; control de acceso al sistema operativo; control de acceso a las aplicaciones y a la información; ordenadores portátiles y teletrabajo.
- o **Adquisición, desarrollo y mantenimiento de los sistemas de información:** requisitos de seguridad de los sistemas de información; tratamiento correcto de las aplicaciones; controles criptográficos; seguridad de los archivos de sistema; seguridad en los procesos de desarrollo y soporte; gestión de la vulnerabilidad técnica.
- o **Gestión de incidentes de seguridad de la información:** notificación de eventos y puntos débiles de la seguridad de la información; gestión de incidentes de seguridad de la información y mejoras.
- o **Gestión de la continuidad del negocio:** aspectos de la seguridad de la información en la gestión de la continuidad del negocio.
- o **Cumplimiento:** cumplimiento de los requisitos legales; cumplimiento de las políticas y normas de seguridad y cumplimiento técnico; consideraciones sobre las auditorías de los sistemas de información.
- o **Bibliografía:** normas y publicaciones de referencia.

2.3.3 ISO/IEC 27003

La norma ISO/IEC 27003, cuya última versión publicada data de Febrero de 2010, constituye la "Guía oficial de implementación de un SGSI" en cualquier organización. Su contenido se centra en los aspectos críticos necesarios para el exitoso diseño e implementación de un SGSI de acuerdo con la norma ISO/IEC 27001:2005. Describe el proceso de delimitación de

un SGSI, y el diseño y puesta en marcha de diferentes planes de implementación. Igualmente incluye el proceso para obtener la aprobación de la dirección para implementar un SGSI, define un alcance inicial del SGSI, y proporciona una guía de cómo hacer desde la planificación inicial hasta la implementación final de un proyecto de SGSI.

Dentro de esta norma podremos encontrar los siguientes apartados:

- o **Alcance:** descripción del contenido de la norma, que en la práctica abarca la totalidad del proceso de implantación de un SGSI paso por paso.
- o **Referencias Normativas:** otras normas y documentos de referencia.
- o **Términos y Definiciones:** breve descripción de los términos más usados en la norma.
- o **Estructura de esta Norma Internacional:** descripción de la estructura de la propia norma.
- o **Obteniendo la aprobación de la alta dirección para iniciar un SGSI**
- o **Definir el alcance del SGSI, límites y políticas**
- o **Evaluación de los requerimientos de seguridad de la información**
- o **Evaluación de Riesgos y Plan de tratamiento de riesgos**
- o **Diseño del SGSI**
- o **Anexo A: lista de chequeo para la implementación de un SGSI.**
- o **Anexo B: roles y responsabilidades en seguridad de la información.**
- o **Anexo C: información sobre auditorías internas.**

- o **Anexo D: estructura de las políticas de seguridad.**
- o **Anexo E: monitorización y seguimiento del SGSI.**

2.3.4 ISO/IEC 27006

Conocida formalmente como "Information technology - Security techniques. Requirements for bodies providing audit and certification of information security management systems", está compuesta por diez capítulos y cuatro anexos. Se constituye como una guía para la acreditación de organizaciones que deseen convertirse en certificadores de las normas de la serie ISO/IEC 27000 relativas a sistemas de gestión de la seguridad de la información. Se basa en la norma general de certificación ISO 17021⁸, a la que añade requisitos específicos referentes a SGSI.

Dentro de esta norma podremos encontrar los siguientes apartados:

- o **Preámbulo:** presentación de las organizaciones ISO e IEC y sus actividades.
- o **Introducción:** antecedentes de ISO 27006 y guía de uso para la norma.
- o **Campo de aplicación:** a quién aplica este estándar.
- o **Referencias normativas:** otras normas que sirven de referencia.
- o **Términos y definiciones:** breve descripción de los términos más usados en la norma.
- o **Principios:** principios que rigen esta norma.
- o **Requisitos generales:** aspectos generales que deben cumplir las entidades de certificación de SGSIs.

⁸ Norma ISO que define requisitos para organismos que realizan la auditoría y la certificación de sistemas de gestión.



- o **Requisitos estructurales:** estructura organizativa que deben tener las entidades de certificación de SGSIs.
- o **Requisitos en cuanto a recursos:** competencias requeridas para el personal de dirección, administración y auditoría de la entidad de certificación, así como para auditores externos, expertos técnicos externos y subcontratas.
- o **Requisitos de información:** información pública, documentos de certificación, relación de clientes certificados, referencias a la certificación y marcas, confidencialidad e intercambio de información entre la entidad de certificación y sus clientes.
- o **Requisitos del proceso:** requisitos generales del proceso de certificación, auditoría inicial y certificación, auditorías de seguimiento, recertificación, auditorías especiales, suspensión, retirada o modificación de alcance de la certificación, apelaciones, reclamaciones y registros de solicitantes y clientes.
- o **Requisitos del sistema de gestión de entidades de certificación:** requisitos del sistema de gestión de acuerdo con ISO 9001 y requisitos del sistema de gestión general.
- o **Anexo A - Análisis de la complejidad de la organización de un cliente y aspectos específicos del sector.**
- o **Anexo B - Áreas de ejemplo de competencia del auditor.**
- o **Anexo C - Tiempos de auditoría.**
- o **Anexo D - Guía para la revisión de controles implantados del Anexo A de ISO 27001:2005.**

2.4. El proceso de implantación

La implantación de un SGSI según la norma ISO/IEC 27001 se realiza siguiendo el ya citado modelo PDCA. La duración del proceso de implantación depende de las características propias de la organización, como pueden ser su tamaño, el tipo de actividades que realice y también

del estado de madurez en el que se encuentren sus procesos de gestión y control de la información. En todo caso, es fundamental realizar un análisis inicial y una planificación del proceso completo de implantación para obtener un resultado exitoso.

La implantación del SGSI puede ser en algunos casos complicada y costosa, y no es extraño que se produzcan desviaciones sobre la planificación inicial. Esto ocurre sobre todo cuando no existe una buena planificación inicial.

Hay que tener presente, una vez más, que la implantación no es una tarea que incumba exclusivamente a las áreas de TI de la organización, sino que todas las áreas de negocio deben verse involucradas en el proceso. Es habitual que la organización designe uno o varios auditores internos que dirigirán el proceso de implantación. Estos auditores internos suelen pertenecer al departamento de TI. Junto a ellos, representantes de las principales áreas de negocio conformarán el equipo interno de implantación.

Además de contar con auditores internos, es bueno contar con la ayuda de alguna empresa externa especializada en la implantación de este tipo de sistemas. Esta empresa proporcionará auditores externos que trabajarán en colaboración con el equipo interno. A nivel de España, el Instituto Nacional de Tecnologías de la Comunicación (INTECO) dispone de un catálogo de empresas que ofrecen este tipo de servicios.

Es importante recordar que la organización debe contar con una estructura organizativa así como de recursos necesarios, entre otras cosas, para llevar a cabo la implantación del SGSI. La implantación y el mantenimiento del SGSI consumirán recursos que deben estar disponibles en el tiempo y que la organización debe proveer adecuadamente. No en vano la base de

cualquier Sistema de Gestión de Seguridad de la Información es la continua evaluación y mejora siguiendo el modelo PDCA.

La documentación y su ciclo de vida tienen una importancia capital dentro de un SGSI. La implantación y mantenimiento de nuestro SGSI debe estar documentada y además existe un ciclo de vida de la documentación que debe ser seguido para garantizar que toda ella se encuentre actualizada y disponible para los usuarios que la requieran. ISO/IEC 27000 recoge cuatro tipos distintos de documentación:

- **Políticas:** sientan las bases de la seguridad. Indican las líneas generales para conseguir los objetivos de la organización sin entrar en detalles técnicos. Toda la organización debe conocer estas Políticas.
- **Procedimientos:** desarrollan los objetivos marcados por las Políticas. En ellos aparecen detalles más técnicos y se concreta cómo conseguir los objetivos expuestos en las Políticas. Los Procedimientos deben ser conocidos por aquellas personas que lo requieran para el desarrollo de sus funciones.
- **Instrucciones:** constituyen el desarrollo de los Procedimientos. En ellos se describen los comandos técnicos que se deben realizar para la ejecución de los Procedimientos.
- **Registros:** evidencian la efectiva implantación del sistema y el cumplimiento de los requisitos. Entre estos Registros se incluyen indicadores y métricas de seguridad que permitan evaluar la consecuencia de los objetivos de seguridad establecidos.

Para los documentos generados se debe establecer, documentar, implantar y mantener un procedimiento que definan las acciones de gestión necesarias orientadas a:



- Aprobar documentos apropiados antes de su emisión.
- Revisar y actualizar documentos cuando sea necesario y renovar su validez.
- Garantizar que los cambios y el estado actual de revisión de los documentos están identificados.
- Garantizar que las versiones relevantes de documentos vigentes están disponibles en los lugares de empleo.
- Garantizar que los documentos se mantienen legibles y fácilmente identificables.
- Garantizar que los documentos permanecen disponibles para aquellas personas que los necesiten y que son transmitidos, almacenados y finalmente destruidos de acuerdo con los procedimientos aplicables según su clasificación.
- Garantizar que los documentos procedentes del exterior están identificados.
- Garantizar que la distribución de documentos está controlada.
- Prevenir la utilización de documentos obsoletos.
- Aplicar la identificación apropiada a documentos que son retenidos con algún propósito.

2.5. El proceso de certificación

Una vez que nuestro SGSI esté totalmente implantado podríamos optar a certificarlo con la norma ISO/IEC 27001. Esto es, que una entidad de certificación audite nuestro sistema y obtengamos un documento que asegure que el SGSI de nuestra organización es acorde con la norma. Hay que tener presente que esta certificación no prueba que los controles y medidas de seguridad implantadas sean las correctas, sino que la seguridad de la información se gestiona en la forma que indica la norma. Hay una más que sutil diferencia.

En el momento de seleccionar una entidad certificadora, debemos asegurarnos de que cuenta con auditores cualificados para verificar la correcta implantación del sistema según la norma ISO/IEC 27001. Además, deberemos comprobar que posee la adecuada acreditación que la reconoce como una entidad competente para la realización de esa actividad. La entidad de certificación debe estar acreditada para la norma en la que se desea realizar la certificación, asegurando así que cumple con los requisitos para realizar correctamente su trabajo.

La entidad de acreditación española es la Empresa Nacional de Certificación (ENAC), aunque existen numerosas entidades de acreditación en todo el mundo. Las empresas certificadoras podrían estar acreditadas por una entidad que no fuese la española. En este caso sería necesario que la entidad de acreditación validase las actividades también en el territorio español, indicándolo específicamente en sus credenciales.

Una vez seleccionada la entidad de certificación y habiendo presentado evidencias de que nuestro SGSI se encuentra implantado y funcionando podremos comenzar realmente el proceso de certificación. Al igual que en el proceso de implantación, hay que tener en cuenta que la organización debe contar con recursos económicos y de personal que deben estar destinados a la realización del proceso de certificación, puesto que los auditores necesitarán ayuda y colaboración del personal de la organización para realizar sus tareas.

El proceso de certificación puede dividirse en tres fases principales:

- o **Gestión de la solicitud de certificación:** la empresa debe solicitar una oferta a la entidad de certificación en la que se especificarán una serie de datos sobre la organización y la implantación del SGSI, tales como el alcance, el número de empleados y los centros de trabajo dentro del alcance, etc. Con

- ello la empresa podrá presentarnos una oferta que incluya tiempo y coste. Incluirá en todo caso el número de días de duración de la auditoría así como el número de auditores que la llevarán a cabo.
- o **Auditoría Documental:** a continuación tiene lugar la auditoría documental, que es la primera fase de la auditoría. En ella se revisa la documentación generada durante la implantación del sistema. Incluirá, al menos, la política de seguridad, el alcance de la certificación, el análisis de riesgos, la selección de los controles de acuerdo con la declaración de aplicabilidad (SOA) y la revisión de la documentación controles seleccionados por la entidad de certificación.
 - o **Auditoría In-Situ:** La segunda fase de la auditoría es la auditoría in-situ. En esta fase el equipo de auditores de la entidad de certificación se desplazará a las instalaciones de la organización. Durante el tiempo planificado trabajarán en colaboración de miembros de la empresa para realizar la revisión del SGSI en funcionamiento. Durante esta fase los auditores verifican de nuevo la documentación revisada en la fase anterior, confirman que la organización cumple con sus políticas y procedimientos, comprueban que el sistema desarrollado está conforme con las especificaciones de la norma y verifican que está logrando los objetivos que la organización se ha marcado.

Como resultado de cada una de las fases de la auditoría externa, la entidad certificadora emite un informe que puede contener los siguientes resultados:

- o Todo correcto. No existe ninguna *no conformidad* y se acepta la certificación del sistema.
- o Observaciones sobre el sistema que no tienen excesiva relevancia pero que deben ser tenidas en cuenta en la siguiente fase de la



- auditoría, bien para ser revisadas in-situ o bien para ser mejoradas en el siguiente ciclo de mejora.
- o No conformidades menores. Estas son incidencias encontradas en la implantación y que son subsanables mediante la presentación de un Plan de Acciones Correctivas en el que se identifica la incidencia y la manera de solucionarlas.
 - o No conformidades mayores que deben ser subsanadas por la empresa. Sin su resolución y, en la mayor parte de los casos, la realización de una auditoría extraordinaria por parte de la entidad de certificación, no se obtendría el certificado ya que se trata de incumplimientos graves de la norma. En caso de darse tras la auditoría documental es necesario su resolución antes de llevar a cabo la auditoría in-situ.

Una vez conseguida la certificación del sistema, éste tiene una validez de tres años, aunque está sujeto a revisiones anuales. Durante el primer año se realiza la auditoría inicial. Posteriormente cada tres años se realiza una auditoría de renovación. En los dos años posteriores tanto a la auditoría inicial como a las de renovación se realizarán auditorías de seguimiento.

3. REFERENCIAS

- Instituto Nacional de Tecnologías de la Comunicación - Centro de Respuestas a Incidentes de Seguridad. (<http://cert.inteco.es>)
- Asociación Española de Normalización y Certificación. (www.aenor.es)
- El portal de ISO 27001 en Español. (www.iso27000.es)
- The ISO 27000 Directory. (www.27000.org)
- International Organization for Standardization (ISO). (www.iso.org)
- International Electrotechnical Commission (IEC). (www.iec.ch)
- Instituto Uruguayo de Normas Técnicas. (<http://www.unit.org.uy/iso27000/>)

(Todos los enlaces fueron verificados en Junio de 2011)

Autor: Juan Otero Pombo
Ingeniero en Informática en el Concello de Ourense
Colegiado del CPEIG



42. VIRUS Y OTRO SOFTWARE MALIGNO. TIPOS. MEDIOS PREVENTIVOS Y REACTIVOS. SISTEMAS ANTIVIRUS Y DE PROTECCIÓN.

TEMA 42: VIRUS Y OTRO SOFTWARE MALIGNO. TIPOS. MEDIOS PREVENTIVOS Y REACTIVOS. SISTEMAS ANTIVIRUS Y DE PROTECCION.

INDICE

<u>1.1. INTRODUCCIÓN.....</u>	<u>3</u>
<u>1.2. MALWARE.....</u>	<u>4</u>
<u>1.3. VIRUS.....</u>	<u>7</u>
<u>1.3.1. Funcionamiento de los virus.....</u>	<u>7</u>
<u>1.3.2. Caracterización de los virus.....</u>	<u>9</u>
<u>1.3.3. Ciclo de vida de los virus.....</u>	<u>10</u>
<u>1.3.4. Tipos de virus.....</u>	<u>13</u>
<u>1.4. TROYANOS.....</u>	<u>17</u>
<u>1.4.1. Tipos de troyanos.....</u>	<u>18</u>
<u>1.4.2. Modos de infección.....</u>	<u>20</u>
<u>1.5. GUSANOS.....</u>	<u>21</u>
<u>1.5.1. Tipos de gusanos.....</u>	<u>22</u>
<u>2. MEDIOS PREVENTIVOS Y REACTIVOS.....</u>	<u>24</u>
<u>3. SISTEMAS ANTIVIRUS Y DE PROTECCIÓN.....</u>	<u>25</u>
<u>3.1. ANTIVIRUS.....</u>	<u>25</u>
<u>3.2. OTRAS MEDIDAS DE PROTECCIÓN.....</u>	<u>29</u>
<u>3.2.1. Cortafuegos (firewalls).....</u>	<u>29</u>
<u>3.2.2. NIDS (Sistemas de detección de intrusos de red).....</u>	<u>29</u>

<u>3.2.3. HIDS (Sistemas de detección de intrusos de host).....</u>	<u>29</u>
<u>3.2.4. Sandboxes.....</u>	<u>30</u>
<u>3.2.5. Honeypot.....</u>	<u>30</u>
<u>4. REFERENCIAS.....</u>	<u>31</u>

VIRUS Y OTRO SOFTWARE MALIGNO. TIPOS.

1.1. Introducción

Los sistemas informáticos se encuentran permanentemente expuestos a la amenaza de los virus informáticos cuyo nombre proviene de la analogía de su comportamiento con los virus biológicos.

Desde que en la década de 1970 apareciesen los primeros virus, han existido siempre amenazas de este tipo que, en algunos casos, han llegado a convertirse en verdaderas infectando millones de ordenadores y generando importantes pérdidas económicas. Ejemplos de estas grandes epidemias fueron las generadas por el Gusano de Morris, Melissa o ILoveYou.

En realidad los virus son un subtipo del software maligno en general, que suele denominarse como *malware*. Los troyanos y gusanos son también tipos de *malware*, que junto a los virus, constituyen los tres tipos principales de software maligno que atacan a los sistemas informáticos, existiendo muchas otras variantes o subtipos de estos: *adware*, *spyware*, *scareware*, etc.

En la actualidad, el tipo de malware más extendido son los troyanos, destinados a instalarse en sistemas de usuarios para robar información confidencial: nombres de usuarios, números de tarjetas de crédito, etc. y enviarlas a los atacantes. Los atacantes se sirven de la red Internet para recibir y usar la información a miles de kilómetros, en otros países donde las leyes no recogen delitos de este tipo se encuentran a salvo. Esto les permite obtener beneficios económicos, ya que la creación de programas maliciosos es un lucrativo negocio.

1.2. Malware

El malware¹ es un tipo de software que tiene como objetivo infiltrarse o dañar una computadora sin el consentimiento de su propietario. El término malware es muy utilizado por profesionales de la informática para referirse a una variedad de software hostil, intrusivo o molesto.

Colateralmente, el malware suele perseguir un lucro de modo directo o indirecto por parte del atacante. El nivel de daño que recibe el usuario puede ir desde pequeñas alarmas inofensivas a efectos desastrosos como la pérdida masiva de datos. Internet resulta ser un medio muy apropiado para distribuir el malware de forma que se maximice el número de usuarios afectados.

Podemos establecer una primera clasificación de malware en tres tipos principales perfectamente diferenciados: virus, gusanos y troyanos. A partir de ahí existen multitud de elementos peligrosos que podrían ser catalogados en uno u otro tipo (o en varios a la vez). Así, es común oír hablar de:

- *Adware*: es un software que despliega publicidad de distintos productos o servicios. Estas aplicaciones incluyen código adicional que muestra la publicidad en ventanas emergentes, o a través de una barra que aparece en la pantalla simulando ofrecer distintos servicios útiles para el usuario. Generalmente, agregan ícono gráficos en las barras de herramientas de los navegadores de Internet o en los clientes de correo, la cuales tienen palabras claves predefinidas para que el usuario llegue a sitios con publicidad, sea lo que sea que esté buscando.
- *Spyware*: o software espía es una aplicación que recopila información sobre una persona u organización sin su conocimiento ni

¹ De las palabras inglesas *malicious software*



consentimiento. El objetivo más común es distribuirlo a empresas publicitarias u otras organizaciones interesadas. Normalmente, este software envía información a sus servidores, en función a los hábitos de navegación del usuario. También, recogen datos acerca de las webs que se navegan y la información que se solicita en esos sitios, así como direcciones IP y URLs que se visitan. Esta información es explotada para propósitos de mercadotecnia, y muchas veces es el origen de otra plaga como el SPAM, ya que pueden encarar publicidad personalizada hacia el usuario afectado. Con esta información, además es posible crear perfiles estadísticos de los hábitos de los internautas. Ambos tipos de software generalmente suelen "disfrazarse" de aplicaciones útiles y que cumplen una función al usuario, además de auto ofrecer su descarga en muchos sitios reconocidos.

Cabe destacar que el atacante no tiene por qué ser un delincuente. Por ejemplo el FBI desarrolló su propia aplicación *spyware*, llamada MagicLantern, usada en investigaciones criminales para obtener información de los sospechosos.

- **Crimeware:** Tipo de programa de computadora diseñado específicamente para cometer crímenes del tipo financiero o similares, intentando pasar desapercibido por la víctima. Por extensión, también hace referencia a aplicaciones web con iguales objetivos.

Un crimeware puede robar datos confidenciales, contraseñas, información bancaria, etc. y también puede servir para robar la identidad o espiar a una persona o empresa.

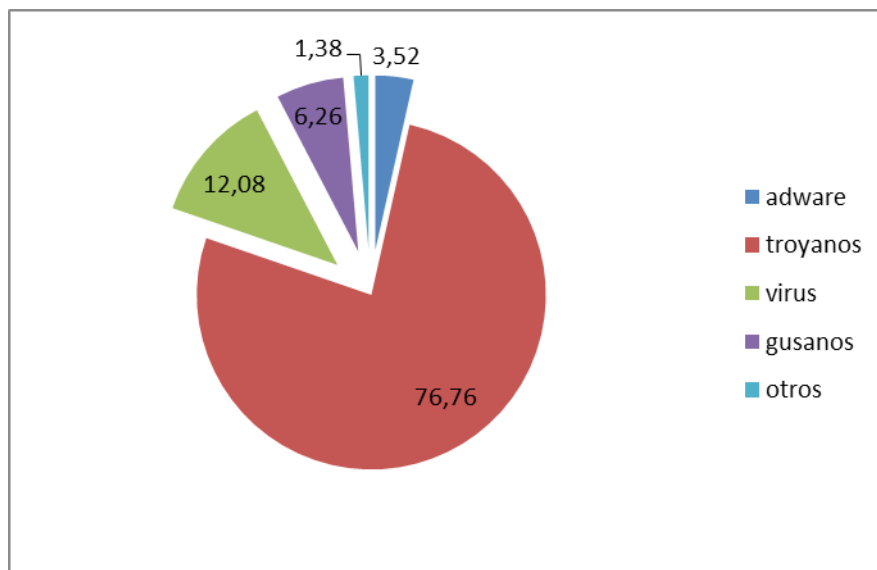
- **Scareware:** término acuñado recientemente, es lo que se conoce como "software de seguridad falso". Normalmente este software

toma ventaja de la intención de los usuarios en mantener sus equipos protegidos, y específicamente utiliza técnicas de ingeniería social que se basan principalmente en crear "paranoia" en los mismos, ofreciéndoles una solución definitiva a sus problemas de seguridad. Una vez instalada, este tipo de programas se dedica a robar información como lo haría cualquier troyano bancario o de usurpación de identidad en el equipo de la víctima.

- Un nuevo tipo de *malware* comienza a aparecer con fuerza asociado al crecimiento de las redes sociales. Se trata de aplicaciones maliciosas que se mueven dentro del contexto de redes sociales destinadas a robar datos personales, suplantar identidades, etc. Un ejemplo es el gusano Koobface, que ataca a varias redes sociales muy conocidas, incluyendo Facebook, Twitter, y Myspace.

El siguiente gráfico muestra la distribución de tipos de *malware* detectados en fechas recientes²:

² La mayoría de grandes empresas dedicadas al desarrollo de antivirus ofrecen frecuentemente informes sobre los tipos de malware detectados, los virus más activos, alertas especiales, etc.



**Estadísticas de *Malware* por tipos del tercer trimestre de 2011
(fuente: Panda Security)**

1.3. Virus

Los virus informáticos son porciones de código malicioso que se pueden introducir en los ordenadores y sistemas informáticos de formas muy diversas, produciendo efectos molestos, nocivos e incluso destructivos e irreparables. Además, el efecto inicial que lo caracteriza es una infección del equipo, seguida de una propagación del virus a medida que los archivos donde reside el virus son ejecutados. Es decir, el código del virus se ejecuta solamente cuando se ejecuta el programa o se abre el archivo infectado. Esto es lo que diferencia a los virus de los gusanos (que veremos más adelante): si no se accede al programa o archivo entonces el virus no se ejecutará y por lo tanto no se propagará.

1.3.1. Funcionamiento de los virus

La propia denominación de virus informáticos proviene de la analogía del funcionamiento de estos con los virus biológicos. Un virus biológico no

puede sobrevivir de forma independiente. En realidad no es más que una cadena de ADN protegida por una cobertura externa que se reproduce insertándose en una célula huésped y usando el mecanismo reproductor de esa célula para reproducirse él mismo.

Un virus informático tampoco es independiente ni tiene la capacidad de sobrevivir y reproducirse de modo aislado. Se trata de una secuencia de código maligno que para poder propagarse necesita infectar a un huésped, que en este caso será un programa informático o un documento.

Muchos virus se esconden dentro de archivos de programas aparentemente limpios. Estos virus se conocen como virus de archivo cuyo código se ejecuta cargándose en memoria principal de la máquina junto con el programa que lo contiene. Desde allí, el código del virus puede buscar otros programas en el sistema que puedan ser infectados. Si encuentra uno, el virus inserta su código en ese programa, que una vez infectado también puede ser usado para infectar a más programas iniciando así una cadena infecciosa similar a una epidemia de un virus biológico.

La mayoría de los virus no solo se replican a sí mismos, sino que también realizan otras operaciones que habitualmente son dañinas para sus huéspedes. Así, por ejemplo, un virus puede eliminar ciertos archivos vitales de un sistema, sobrescribir el sector de arranque de un disco duro dejando el disco inhabilitado, mostrar mensajes en la pantalla, emitir ruidos y una gran cantidad de otras acciones de mayor o menor poder destructivo.

En general, los virus están diseñados para ejecutar su código dañino en el momento de ser ejecutados. Sin embargo, hay algunos otros que no atacan en ese momento, sino que están diseñados para esperar a una fecha concreta o a un evento particular. Estos virus permanecen en estado latente en el sistema hasta que actúan.

1.3.2. Caracterización de los virus

Existen muchos tipos de virus, pero podemos indicar algunas características comunes a todos ellos:

- **Latencia:** los virus tienen capacidad para permanecer inactivos, en un estado latente, hasta que un evento los active. Este evento puede ser la ejecución de un programa, la lectura del sector de arranque, etc. Una vez activado, el virus puede realizar las tareas para las que estaba programado y replicarse.
- **Tipo de residencia:** los virus más avanzados son capaces de camuflarse para evitar ser detectados y erradicados. Los virus más básicos necesitan permanecer continuamente en la memoria principal, mientras que estos otros virus, más avanzados, son capaces de residir en otros lugares como la memoria secundaria. Pueden llegar incluso a modificar la tabla de asignación de archivos para camuflar su presencia.
- **Forma de infección:** se trata de una característica común de todos los virus. El medio por el que un virus infecta varía enormemente de unos a otros: ejecución de programas, de macros, conexiones mediante determinados protocolos, el simple arranque de una máquina, etc..
- **Composición:** cualquier virus informático cuenta con tres partes destinadas a cumplir con sus objetivos:
 - o **Sistema de reproducción:** encargado de infectar otros sistemas o archivos mediante el aprovechamiento (ilícito) de los recursos de la máquina huésped.



- o **Sistema de ataque:** en caso de existir se trata de una serie de rutinas destinadas a dañar el sistema huésped de un modo u otro. El daño puede ir desde pequeños inconvenientes como mensajes molestos, hasta ataques desastrosos como la pérdida masiva de datos.
- o **Sistema de defensa:** destinado a ocultar la presencia del virus mientras sea posible y a dificultar su eliminación.

1.3.3. Ciclo de vida de los virus

Existen una serie de fases por las que un virus pasa a lo largo de su vida:

- **Creación:** el virus es creado por programadores que escriben su código.
- **Contagio:** El contagio inicial o los contagios posteriores se realizan cuando el programa contaminado está en la memoria para su ejecución. Las vías por las que puede producirse la infección de su sistema son disquetes, memorias flash, redes de ordenadores y cualquier otro medio de transmisión de información. Estos disquetes contaminantes suelen contener programas de fácil y libre circulación y carecen de toda garantía. Es el caso de los programas de dominio público, las copias ilegales de los programas comerciales, juegos, etc.
- **El virus activo:** Cuando se dice que un virus se activa significa que el virus toma el control del sistema, y a la vez que deja funcionar normalmente a los programas que se ejecutan, realiza actividades no deseadas que pueden causar daños a los datos o a los programas.



Lo primero que suele hacer el virus es cargarse en la memoria del ordenador y modificar determinadas variables del sistema que le permiten "hacerse un hueco" e impedir que otro programa lo utilice. A esta acción se le llama "hacerse residente". Así el virus queda a la espera de que se den ciertas condiciones, que varían de unos virus a otros, para replicarse o atacar.

La replicación, que es el mecanismo más característico y para muchos expertos definitorio de la condición de virus, consiste básicamente en la producción por el propio virus de una copia de sí mismo, que se situará en un archivo. El contagio de otros programas suele ser la actividad que más veces realiza el virus, ya que cuanto más deprisa y más discretamente se copie, más posibilidades tendrá de dañar a un mayor número de ordenadores antes de ser descubierto.

- **El ataque:** Mientras que se van copiando en otros programas, los virus comprueban si determinada condición se ha cumplido para atacar, por ejemplo que sea cinco de enero en el caso del conocido virus Barrotes. Es importante tener en cuenta que los virus son diseñados con la intención de no ser descubiertos por el usuario y generalmente, sin programas antivirus, no es descubierto hasta que la tercera fase del ciclo de funcionamiento del virus se produce el daño con la consiguiente pérdida de información.
- **Descubrimiento:** esta fase comienza cuando el virus es detectado, identificado y documentado por primera vez.
- **Asimilación:** las compañías fabricantes de antivirus modifican sus soluciones para conseguir detectar y eliminar las infecciones causadas por el virus.

- **Erradicación:** el uso exhaustivo de antivirus limita las infecciones del virus eliminando su amenaza.

Un virus puede ser catalogado en base a su índice de peligrosidad, que variará dependiendo de la fase de su ciclo de vida en la que se encuentre. El índice de peligrosidad es una medida del impacto que produce su código malicioso y la capacidad de propagación a otros sistemas. Existen varios niveles de peligrosidad que van desde aquellos virus que causan daños leves y están poco extendidos, hasta aquellos otros que causan daños catastróficos y están muy extendidos.

El nivel de daño indica el perjuicio que un virus causa al infectar un sistema informático. Un virus puede ser catalogado como dañino (mensajes o ruidos molestos, apertura de ventanas involuntariamente, etc.) o muy dañino (destrucción o modificación de archivos, formateo de discos duros, envío de información a terceros, generación de gran tráfico en servidores, degradación del rendimiento de los sistemas, apertura de agujeros de seguridad, etc.).

El grado de propagación indica lo extendido que se encuentra el virus. Evidentemente, cuanto más extendido esté un virus, mayores son las probabilidades de estar afectado por él. La propagación de un virus se determina mediante el 'ratio de infección', que mide el porcentaje de ordenadores infectados en relación al total de equipos explorados. El grado de propagación de un virus podría variar entonces desde 'poco extendido' hasta 'epidemia'.

1.3.4. Tipos de virus

En función de qué es exactamente lo que un virus puede infectar, es usual clasificarlos en:

- Virus de sector de arranque maestro³: fueron el primer tipo de virus. Se esconde en el código ejecutable del sector de arranque de discos de memoria secundaria o de discos de arranque externos (diskettes, CD-ROMs, etc.). Hasta hace no mucho tiempo atrás, iniciar el ordenador desde un disco de arranque era algo bastante usual, lo que significaba que los virus se distribuían rápidamente.
- Virus de archivo: se caracterizan por unirse a archivos en los que residen y que pueden usar para propagarse entre sistemas. Suelen infectar archivos ejecutables, pero también existen virus capaces de unirse a archivos de código fuente, librerías o módulos de objetos e incluso archivos de datos. El virus *Jerusalem* (también conocido como *Viernes 13*), uno de los más conocidos, pertenece a esta categoría.
- Macrovirus o virus de macro: los virus de macro hacen uso de la capacidad que ciertas aplicaciones, como Word y Excel, tienen para ejecutar internamente ciertos códigos programados llamados macros. El virus se adjunta a dichas macros y se transmite de un documento a otro a través de ellas. El virus causante de una de las mayores epidemias de la historia, *Melissa*, corresponde a este tipo.
- Virus mixtos, bimodales o multiparte: se trata de una combinación de virus de archivo, de macro y de sector de arranque. Realizan infecciones usando varias técnicas para instalarse en cualquiera de las localizaciones posibles. Se consideran muy peligrosos por la gran capacidad de infección que tienen.

³ Conocido habitualmente por su nombre en inglés Master Boot Record (MBR).



- Virus de BIOS: se alojan en la BIOS del ordenador y cada vez que esta se arranca, infectan a los archivos del sistema. El virus *Chernobyl* realizaba una infección de este tipo.

Dentro de los anteriores, siguiendo un criterio más amplio, otros tipos de virus identificables serían:

- Virus de compañía: estos virus no modifican los archivos infectados, sino que crean una copia del archivo original y modifican esta copia. Cuando el archivo original se ejecuta, el virus hace que se pase el control al archivo infectado. Una variante de la infección consiste en renombrar el archivo original, y sustituirlo por otro con el nombre original que contiene directamente el virus.
- Retrovirus: se trata de virus especialmente diseñados para evitar ser detectados e infectar a los programas antivirus.
- Virus de sobreescritura: el código del virus se escribe encima de un fichero ejecutable destruyéndolo. Si el tamaño del virus es menor que el del ejecutable infectado, el resultado final no aumenta de tamaño, dificultando la detección del virus.
- Virus parásitos: los archivos huésped son modificados solo en parte, de modo que no son destruidos y pueden incluso simular que siguen funcionando. En estos casos el virus se aloja en lugares de archivo, normalmente al comienzo o final, donde permite que el archivo huésped siga parcialmente activo.
- Virus mutantes: cuando infectan a un huésped, modifican su propio código para evitar que su 'huella' sea detectada por programas antivirus.



- Virus sin punto de entrada: conocidos como virus EPO (Entry Point Obscuring). Se destacan porque la instrucción que hace pasar el control al virus se inserta en un lugar indeterminado del archivo huésped. Esto hace que el virus no se manifieste hasta que se realiza una acción concreta dentro del ejecutable infectado. Esto les permite permanecer en un estado latente durante mucho tiempo.
- Virus de enlace: se caracterizan porque la infección consiste en la inserción de un enlace a algún otro lugar (por ejemplo el último cluster de un disco duro o un cluster marcado como erróneo) en donde realmente se aloja el código del virus.
- Virus OBJ, LIB y código fuente: en lugar de infectar directamente un ejecutable, infectan librerías o módulos usados por otros ejecutables. Evidentemente, su capacidad para actuar y reproducirse solo aparecerá cuando la librería sea utilizada por otro programa.
- Virus de script: se trata de virus que actúan sobre lenguajes de script habitualmente asociados a páginas web. Actúan incluyéndose en páginas web o modificando los scripts que esas páginas contienen.
- Virus en estado salvaje: son aquellos que se encuentran en circulación en estos momentos y que están en condiciones de infectar.
- Virus de zoológico: son virus que no se encuentran en libertad o que han perdido su capacidad para infectar. Por ejemplo el conocido como 'virus de la pelotita'.
- Generadores de virus: son virus que al mutar generan nuevos virus.
- Virus que crean dependencia: cuando uno de estos virus infecta una máquina, se instala en lugares vitales, de modo que no es posible

eliminarlos sin hacer que la máquina pierda esos elementos vitales y deje de funcionar.

- Bombas de tiempo: se ocultan en los sistemas hasta que llega una fecha concreta o pasa un determinado periodo de tiempo. En ese momento pasan a un estado activo y realizan sus acciones de infección y replicación.

En cuanto al modo en que el virus produce la infección del sistema, podemos enumerar los siguientes:

- Añadidura o empalme: es uno de los modos más básicos y clásicos. El código del virus se añade al final de un archivo huésped (habitualmente un ejecutable) y se modifica la estructura de arranque del mismo, haciendo que el virus se ejecute en primer lugar antes de pasar el control al fichero original. El resultado es un aumento del tamaño inicial del archivo, permitiendo así una fácil detección.
- Inserción: es un modo más avanzado de infección en el que el virus se instala en zonas de código no utilizada o en segmentos de datos para que el tamaño del archivo no varíe.
- Reordenación: se introduce el código del virus en sectores del disco duro que quedan marcados como defectuosos y se distribuyen enlaces a dichos sectores en el código de otros programas ejecutables que quedan así infectados. La ventaja de este método es que al encontrarse el código del virus fuera del archivo, este código puede ser de gran tamaño y por tanto poseer mucha funcionalidad. En cambio, este tipo de virus es muy fácil de eliminar, simplemente sobrescribiendo los sectores defectuosos.

- Polimorfismo: es probablemente el método más avanzado. Se basa en infectar un archivo ejecutable, pero realizando una compactación del código del archivo huésped o del código del propio virus para evitar así un aumento del tamaño que lo delate. En el momento de actuar, el virus descomprime en memoria el código necesario para ejecutarse.
- Sustitución: este método, muy poco sutil, consiste en sustituir directamente el código del programa huésped al completo por el código del virus. De este modo el programa original simplemente desaparece y lo único que se ejecuta es el virus.

1.4. Troyanos

Hace miles de años, ante la imposibilidad de traspasar las murallas de la ciudad de Troya, los griegos construían un gran caballo de madera en el interior del cual se ocultaban una selección de sus mejores soldados. Colocaron el caballo delante de la ciudad y los troyanos, prendados de su majestuosidad de lo que aparentaba un regalo de los dioses completamente inofensivo introdujeron el caballo en la ciudad.

El tipo de malware denominado troyano debe su nombre a que para su propagación utiliza la misma estrategia que idearon los griegos para entrar en Troya. El concepto básico de un troyano consiste en introducir código malicioso dentro de un sistema que resulte atractivo para la víctima y además parezca seguro, de modo que el conjunto parece inofensivo. Este disfraz podría ser desde un juego descargado de Internet hasta un mensaje de correo electrónico de apariencia inofensiva.

Los Troyanos son códigos maliciosos que intentan mostrarse como algo útil o apetecible para que una víctima lo ejecute. Se caracterizan porque su objetivo es introducirse en el sistema y pasar desapercibidos. Mientras se encuentran en el sistema pueden dedicarse a enviar información (en ese caso suelen conocerse como *spyware*) o a preparar el sistema para un ataque posterior mediante la instalación de *rootkits*⁴ o la creación de puertas traseras (*backdoors*). Además, a diferencia de los virus, no tienen la capacidad para replicarse e infectar otros sistemas por sí solos.

Actualmente los troyanos son ampliamente utilizados con el objetivo de obtener datos de una víctima que lo tiene instalado en su sistema sin su conocimiento. Esto pueden hacerlo de muy diversas maneras, que van desde capturar las pulsaciones de teclado (los llamados *keyloggers*) hasta el acceso y manipulación de las carpetas de documentos de un usuario.

1.4.1. Tipos de troyanos

Los troyanos pueden tener características muy diversas por lo que resulta difícil catalogarlos. Sin embargo, atendiendo a su objetivo, podemos establecer la siguiente clasificación:

- **Troyanos de control remoto:** su objetivo es proporcionar al atacante el control de la máquina donde reside el troyano. Habitualmente el troyano intentará abrir conexiones de red clandestinas, desde las que podría escuchar las órdenes del atacante. Ejemplos de este tipo de troyanos son *Back_orifice* o *Netbus*
- **Troyanos que envían datos:** su objetivo es enviar al atacante datos confidenciales tomados de la máquina atacada y de la

⁴ Conjunto de herramientas destinadas a permitir que un atacante acceda a los privilegios de administrador del sistema de forma remota.



información que cualquier usuario almacene en ella. Comúnmente persiguen la obtención de usuarios y claves de acceso, número de tarjetas de crédito, cuentas bancarias, etc. El envío de datos puede hacerse de diferentes formas: mediante el envío de un correo electrónico a través de un servidor de correo público, directamente a la página web del atacante mediante un formulario, etc. Un ejemplo de este tipo es el *badtrans.b*, que es capaz de recoger las pulsaciones del teclado y enviarlas vía correo electrónico.

- **Troyanos destructivos:** se comportan en cierto modo como un virus, ya que su objetivo es causar daños mediante la destrucción de información. Pueden llevar a cabo esta tarea inmediatamente tras la infección o actuar como una bomba lógica que se activará cuando se produzca un determinado evento.
- **Troyanos de ataque de denegación de servicio:** el objetivo de estos troyanos es convertir a las víctimas en participantes involuntarios en ataques de denegación de servicio distribuidos (DDoS). La máquina infectada se denomina comúnmente *botnet* o máquina *zombie*. El atacante puede utilizar todas las máquinas infectadas para hacer un ataque coordinado contra otro servidor o incluso contra una cuenta de correo electrónico (cada máquina infectada podría enviar mensajes con remitentes capturados). Un ejemplo de este tipo es el *WinTrinoo*, una herramienta de DDoS muy extendida por su sencillez de uso.
- **Troyanos Proxy:** se trata de troyanos que permiten convertir la máquina infectada en un Proxy a disposición del atacante. Este podrá utilizarlo como punto intermedio para otros ataques, dificultando así que el ataque pueda ser rastreado hasta la máquina original. Es

común encadenar varios saltos entre máquinas Proxy involuntarias para conseguir evitar el rastreo del ataque.

- **Troyanos FTP:** se caracterizan por infectar el sistema a través del puerto del protocolo FTP (el 21) y permitir al atacante usar dicho protocolo libremente contra la máquina infectada. FTP permite la transmisión bidireccional de archivos entre equipos remotos. Es decir, el atacante tendrá capacidad para copiar y borrar archivos a su antojo en la máquina infectada.
- **Deshabilitadores de software de seguridad:** se trata de troyanos avanzados que incluyen herramientas para evitar o incluso eliminar software de protección como antivirus o *firewalls*. Suelen acompañar a virus y gusanos e instalarse cuando se produce la infección. Como en el caso del gusano *Goner*, que incluía un troyano de este tipo.

Como decíamos, existen troyanos de difícil catalogación. La realidad es que constantemente aparecen nuevos troyanos con funciones y objetivos cada vez más extravagantes. Como por ejemplo el *SMSlock.A*, que literalmente secuestra el equipo infectado impidiendo su uso y pide un rescate económico por su recuperación.⁵

1.4.2. Modos de infección

Las dos formas más frecuentes por las que un troyano puede acceder e instalarse en un equipo huésped son las siguientes:

- **Mediante adjuntos en correos electrónicos o mensajería instantánea:** el simple hecho de abrir un archivo adjunto a un correo

⁵ Este tipo de *malware* dedicado a secuestrar recursos y pedir rescate por ellos es denominado también *ransomware*.

electrónico o enviado a través de una herramienta de mensajería instantánea (como *Win32/Sdbot*, que se instalaba a través de *MSN Messenger*) puede permitir a un troyano instalarse en nuestro sistema. Incluso algunos gestores de correo, que no se encuentren configurados apropiadamente, pueden permitir que los adjuntos se ejecuten sin que el usuario lo solicite.

- **Mediante la instalación voluntaria de software:** suele tratarse de software de dudosa procedencia, *shareware*, *freeware*, versiones de prueba, etc. Al descargar de la red este software e instalarlo, el troyano se instalará en un segundo plano sin que la víctima pueda percibir nada. Contra esto, cabe destacar el uso cada vez más habitual de certificados digitales que permiten identificar tanto el servidor al que nos conectamos como el propio software que podemos descargar firmado. De este modo nos aseguraríamos que lo estamos descargando realmente de donde pretendemos y que no ha sido modificado durante la comunicación.

En todo caso, la infección por troyanos suele tener un indispensable componente de ingeniería social. Los ataques suelen usar engaños para conseguir que la víctima abra los adjuntos o llegue incluso a ejecutar su contenido. Pueden simular ser correos de amigos, peticiones solidarias, etc. También suelen aparentar ser programas útiles que se distribuyen gratuitamente para conseguir que la víctima lo descargue e instale. Incluso no es extraño encontrar troyanos detrás de programas antivirus gratuitos.

1.5. Gusanos

Un gusano es un programa que una vez ejecutado se replica sin necesidad de la intervención humana y es capaz de enviar copias de sí mismo a través de redes de comunicaciones, sin la necesidad de que un usuario

envíe un correo electrónico infectado ni establezca ninguna comunicación explícita. Se propagará de anfitrión en anfitrión haciendo un uso indebido de servicios desprotegidos: correo electrónico, herramientas de mensajería instantánea, etc. Aunque la propagación en sí no tiene por qué ser dañina, sucede lo mismo que con los virus: es habitual que los gusanos incluyan código malicioso destinado a dañar los sistemas infectados. De hecho, algunas de las infecciones más dañinas y conocidas han sido provocadas por gusanos: *ILoveYou*, *Kournikova*. Algunos gusanos no incluyen código malicioso, pero su ataque consiste en el reenvío de sí mismos hasta conseguir agotar los recursos de la máquina atacada.

Sin embargo, al contrario que los virus, los gusanos son programas completos. No solo en el sentido de que son capaces de enviarse copias de sí mismos a través de Internet, sino porque no necesitan de ningún programa huésped para hacerlo. No necesitan corromper otros programas e insertar su código allí. Su funcionamiento se basa en errores en sistemas operativos, aplicaciones o protocolos que son aprovechadas por los gusanos para ejecutarse.

1.5.1. Tipos de gusanos

Podemos clasificar los gusanos atendiendo al medio que utilizan para su propagación:

- **Gusanos de redes de área local:** se propagan a través de los recursos compartidos de una red local llegando a bloquearla o degradando las medidas de seguridad de la misma. Un ejemplo es el gusano *Lovgate*, que puede realizar la infección de la red local y también enviarse por correo electrónico a otras máquinas.



- **Gusanos de redes P2P⁶:** usan este tipo de redes y su gran popularidad para incluir en ellas archivos que al ser descargados traen consigo el gusano. El gusano *Redisto.b* utiliza este tipo de mecanismos.
- **Gusanos de correo electrónico:** es probablemente el método más habitual de propagación, y se realiza utilizando ciertos programas clientes de correo. El gusano accede a las direcciones de correo de la agenda de un usuario y se reenvía usando la propia cuenta del usuario. Algunos virus más avanzados pueden contar incluso con su propio servido SMTP con el que enviar sus copias. *Sircam* o *Nimda* son ejemplos de gusanos de correo electrónico.
- **Gusanos de mensajería instantánea** (IRC, MSN Messenger): otra fuente habitual de entrada para gusanos son las aplicaciones de mensajería instantánea, que además permiten el envío de archivos adjuntos.
- **Gusanos que se propagan directamente por Internet:** los gusanos más avanzados no dependen de ninguna aplicación en particular para propagarse. Su estrategia de infección puede basarse en encontrar puertos abiertos en las máquinas objetivo y conseguir introducirse en la máquina sin que los usuarios se percaten de ello. Otros gusanos infectan los servidores de información, haciendo que la simple petición de una página web haga que el gusano pueda pasar al cliente, como es también el caso de gusano *Nimda* en otro de sus modos de contagio.

⁶ Peer to Peer

2. MEDIOS PREVENTIVOS Y REACTIVOS

Los medios preventivos contra el *malware* en general, se basa en medidas de índole técnico combinadas con una política de seguridad que promueva buenas prácticas por parte de los administradores y del personal de la organización. Entre todas estas medidas destinadas a la prevención de infecciones y la reacción en caso de que llegase a producirse, podríamos citar:

- Utilización de programas antivirus perfectamente configurados y actualizados. Es la herramienta principal en la lucha contra infecciones. Permiten detectar y en muchos casos eliminar los virus. En el siguiente apartado hablaremos más en profundidad sobre ellos.
- Los sistemas operativos son elementos fundamentales en los sistemas informáticos. Muchos de los métodos de infección se basan en debilidades o vulnerabilidades de los sistemas operativos. Por tanto, deben mantenerse siempre actualizados, especialmente con las actualizaciones específicas de seguridad.
- También todo el resto del software instalado debe mantenerse actualizado. Los administradores deben prestar atención a las noticias sobre nuevas vulnerabilidades de dicho software y proteger el sistema ante ataques que pudieran aprovecharse de las mismas.
- Controlar el software ya instalado en las máquinas y de todo aquel que se vaya a instalar, que una vez más debería ser solamente el necesario para las tareas de la organización. Por supuesto, no debe permitirse la instalación de cualquier software que no sea original. El software pirata es uno de los principales puntos de propagación del *malware*.

- Los servicios activos en el sistema se mantendrán en el mínimo número necesario. Solo aquellos realmente necesarios para los objetivos de la organización deberían permanecer activos. Este hecho debería ser controlado periódicamente para evitar la apertura de conexiones ilegales.
- Mantener copias de seguridad de los datos, de los programas y de los sistemas operativos.
- Gestionar adecuadamente las cuotas de uso de disco y memoria de cada usuario. Esto evitará que si un usuario provoca una infección, no se consuman todos los recursos de la máquina afectada, solo los asignados a dicho usuario.
- Tanto los administradores como los usuarios deben asumir buenas prácticas de prevención: No abrir nunca archivos adjuntos de dudosa procedencia, desactivar las opciones de visualización de imágenes y vista previa de gestores de correo, no aceptar descargas ni instalaciones de software no iniciadas voluntariamente, comprobar los certificados de procedencia del software, etc.

3. SISTEMAS ANTIVIRUS Y DE PROTECCIÓN

3.1. Antivirus

Los antivirus constituyen la piedra angular sobre la que se basa la mayor parte de la defensa contra virus, troyanos, gusanos y *malware* en general. Su objetivo es el de detectar, bloquear, eliminar y prevenir infecciones provocadas por virus informáticos. La mayoría de las soluciones existentes hoy en día, son capaces también de detectar otros tipos de *malware*: troyanos, gusanos, *spyware*, *rootkits*, etc.

Cuando un antivirus detecta una infección, podrá actuar en dos modos distintos. Si tiene capacidad para ello, podría eliminar la infección sin dañar los recursos afectados. Si no es así, propondrá la puesta en cuarentena de los recursos afectados (habitualmente archivos), que quedarán aislados del resto del sistema y se impedirá que sean ejecutados. Esto último no elimina la infección, pero la bloquea impidiendo que el virus ejecute su código malicioso y evita que el virus pueda propagarse.

Los antivirus pueden detectar las infecciones siguiendo una de estas dos estrategias:

- **Detección de patrones:** cada virus tiene un patrón de identificación, que suele ser una secuencia de código que le identifica. Los antivirus poseen una base de datos de patrones de virus y las comparan con los archivos del sistema para ver si existe alguna infección. Sin embargo, los virus actuales tienen firmas muy pequeñas. Esto dificulta la tarea de los antivirus y pueden provocar falsos positivos, es decir, detecciones que aparentan ser virus y no lo son.

Los antivirus basados en patrones obtienen muy buenos resultados. Detectan un gran número de virus, pero para ello necesitan que sus bases de datos de patrones estén actualizadas. Todo aquel virus que no figure en la base de datos será simplemente indetectable. Además para funcionar de una forma eficiente, requieren el uso de algoritmos de búsqueda optimizados, ya que la estrategia de detección se basa en escanear el contenido de todos los recursos sospechosos.

- **Heurísticas:** usan técnicas de inteligencia artificial para lograr reconocer secuencias de acciones o comportamientos asociados a virus. Se trata de reconocer acciones que usualmente los virus realizan (borrado de ficheros, conexiones a Internet, modificar

archivos ejecutables, etc.) o que no realizan (abrir ventanas, emitir mensajes visibles, etc.).

Las técnicas heurísticas tienen una ventaja fundamental: permiten detectar virus nuevos sin necesidad de actualizaciones. Pero, por otro lado, pueden generar muchos falsos positivos sobre programas que en realidad no son virus.

Existe un variado abanico de soluciones antivirus, disponibles en versiones propietarias y también en versiones ofrecidas gratuitamente o como software libre. Entre los primeros podemos encontrar soluciones muy conocidas desarrolladas por grandes empresas: Norton, Symantec, PandaSoftware, McAfee, Kaspersky, etc. Entre los segundos podemos citar AVG, Avast!, ClamWin, etc.

A la hora de seleccionar el antivirus más apropiado para nuestros sistemas, deberíamos tener en cuenta las siguientes características:

- Frecuencia de actualización: cuanto más actualizado esté nuestro antivirus, más preparados estaremos para luchar contra las infecciones
- Protección en tiempo real: es conveniente que el agente antivirus resida en la memoria principal y realice un escaneado continuo en busca de posibles infecciones. Por supuesto, esto tiene un coste en recursos para la máquina que debe ser tenido en cuenta antes de optar por una solución de este tipo.
- Capacidad de centralización: algunos antivirus permiten ser instalados en varias máquinas, pero ser controlados y gestionados desde una única máquina. Esto facilita la tarea de los administradores.

- Programación de tareas: es muy interesante que los escaneos, que pueden consumir bastante tiempo y recursos de máquina, puedan ser programados para que se ejecuten en horas de poca actividad (durante la noche, por ejemplo).
- Protección del correo: hoy en día, uno de los puntos de entrada más comunes para los virus es a través de los correos electrónicos y sus archivos adjuntos. Es conveniente que nuestro antivirus sea capaz de analizar automáticamente esos archivos adjuntos.
- Generación de informes: es muy útil para los responsables de la seguridad que el antivirus sea capaz de generar informes con sus resultados y las acciones que ha llevado a cabo.

Una vez que seleccionemos un antivirus, es conveniente tener claro cómo y dónde utilizarlo. La norma base es ‘un equipo, un antivirus’. Es decir, todos los equipos del sistema deberían tener su propio antivirus instalado. Sin embargo, en algunos equipos concretos, el antivirus puede ofrecer una protección más eficiente al resto de equipos. Por ejemplo, en equipos que actúan como Proxy de conexión con redes externas. Un antivirus bien configurado y escaneando en tiempo real se protegerá a sí mismo de virus, pero también evitará que gran parte del *malware* pase a los equipos de la red interna y por tanto a los usuarios finales.

En el entorno de los antivirus, el European Institute for Computer Antivirus Research (EICAR) ha desarrollado una prueba para validar la operatividad de los antivirus. Su objetivo es comprobar que un antivirus realmente funciona sin poner en peligro una máquina con virus reales. La prueba **EICAR**, que así se conoce, consiste en un inofensivo archivo de texto que debe ser guardado con extensión de archivo ejecutable. Una vez hecho, todo antivirus debería detectarlo como un virus a eliminar.

3.2. Otras medidas de protección

Para proteger nuestros sistemas contra infecciones sería conveniente disponer de algunos otros elementos:

3.2.1. Cortafuegos (*firewalls*)

Los gusanos se propagan por la red conectándose a servicios con agujeros de seguridad, alojados en diferentes sistemas a lo largo de la red. Además de asegurarse que estos servicios vulnerables no se estén ejecutando, el siguiente paso que debe seguir el administrador, es verificar que el *firewall* no permita conexiones a estos servicios. Muchos *firewalls* modernos son capaces de filtrar en el tráfico de la red aquellos paquetes en los que se detecten ciertas firmas asociadas a virus o gusanos.

3.2.2. NIDS (Sistemas de detección de intrusos de red)

Los sistemas de detección de intrusiones de red son similares a los antivirus pero aplicados al tráfico de la red. Buscan en el tráfico de red firmas o patrones de comportamiento relacionados con virus o gusanos. Son capaces de alertar al usuario atacado o de detener el tráfico de red que intenta distribuir el *malware*.

3.2.3. HIDS (Sistemas de detección de intrusos de *host*)

Los sistemas de detección de intrusión de *host*, como por ejemplo las herramientas de software libre Tripwire y Aide, son capaces de detectar cambios realizados sobre archivos alojados en un servidor. Se basan en la hipótesis de que un archivo ejecutable, una vez compilado, no necesita ser modificado. Entonces, mediante el control de sus características, tales

como tamaño, fecha de creación y control de integridad, pueden detectar inmediatamente si ha ocurrido algo irregular que apunte a una infección.

3.2.4. Sandboxes

El concepto de *sandbox* se basa en que una aplicación o programa tiene su propio entorno para ejecutarse y no puede afectar al resto del sistema. Esto quiere decir que los recursos y los privilegios que la aplicación tiene mientras es ejecutada, son limitados. La ventaja de los *sandboxes* es que restringen el daño que un *malware* puede ocasionar al sistema infectado simplemente restringiendo los accesos de los que el *malware* dispone.

Otra opción en auge es la virtualización, que consiste en crear una máquina virtual completa mediante productos como VMWare. Esto aísla a la máquina virtual del sistema anfitrión ‘real’ limitando el acceso al mismo según lo haya configurado el administrador.

3.2.5. Honeypot

Se denomina *honeypot* a un sistema especialmente preparado para ser o parecer vulnerable, de modo que sea fácil de infectar por *malware*. Por supuesto, este sistema no contiene información ni programas valiosos (y muchas veces se trata de un sistema virtualizado). Sin embargo, este sistema está estrictamente monitorizado, de modo que el administrador puede obtener información sobre las amenazas que se ciernen sobre el sistema real con antelación. Esto permite al administrador gestionar las medidas de seguridad del sistema real para protegerse contra nuevos virus o ataques.

4. REFERENCIAS

- RFC 4949 Internet Security Glossary, Version 2

<http://tools.ietf.org/html/rfc4949>

- Observatorio de seguridad del Instituto Nacional de Tecnologías de la Comunicación

<http://www.inteco.es/Seguridad/Observatorio/>

- Web y enciclopedia del *malware* de PandaSoftware

<http://www.pandasecurity.com>

- Virus list, noticias y datos sobre *malware* de Kaspersky Labs.

<http://www.viruslist.com/sp/>

- Curso de Extensión Universitaria "Ferramentas de seguridade en GNU/Linux" (terceira edición) - Escola Superior de Enxeñaría Informática da Universidade de Vigo - (<http://ccia.ei.uvigo.es/curso2010/index.html>)

Autor: Juan Otero Pombo

Ingeniero en Informática en el Concello de Ourense

Colegiado del CPEIG

43. CERTIFICADOS DIGITALES. TARJETAS CRIPTOGRÁFICAS. FIRMA DIGITAL. TÉCNICAS DE CIFRADO. INFRAESTRUCTURA DE CLAVE PÚBLICA (PKI).

Tema 43: Certificados digitales. Tarjetas criptográficas. Firma digital. Técnicas de cifrado. Infraestructura de clave pública (PKI).

INDICE

1. TECNICAS DE CIFRADO.....	2
1.1. CRIPTOGRAFÍA Y CRIPTOANÁLISIS.....	2
1.2. TÉCNICAS CRIPTOGRÁFICAS CLÁSICAS.....	3
1.3. TÉCNICAS CRIPTOGRÁFICAS MODERNAS.....	3
1.4. CRIPTOGRAFÍA DE CLAVE PRIVADA O SIMÉTRICA.....	5
1.4.1. Sustitución monoalfabeto.....	5
1.4.2. Sustitución polialfabeto.....	6
1.4.3. Cifrado en bloque.....	7
1.4.4. Cifrado en flujo.....	13
1.4.5. Cifrado en base a funciones resumen.....	15
1.5. CRIPTOGRAFÍA DE CLAVE PÚBLICA O ASIMÉTRICA.....	16
1.5.1. Ejemplos de algoritmos de clave pública: Diffie-Hellman.....	18
1.5.2. Ejemplos de algoritmos de clave pública: RSA.....	18
2. FIRMA DIGITAL.....	18
3. INFRAESTRUCTURA DE CLAVE PÚBLICA (PKI).....	20
3.1. CERTIFICADOS DIGITALES.....	22
3.1.1. Autoridad de Certificación.....	24
3.1.2. Autoridad de Registro	27
3.1.3. Autoridad de Validación.....	28
3.1.4. Autoridad de Sellado de Tiempos.....	28
3.1.5. Directorio de Certificados.....	29
3.2. HARDWARE CRIPTOGRÁFICO	30
3.3. TARJETAS Y CHIP CRIPTOGRÁFICOS.....	30
3.4. 3.3. MARCO LEGAL Y ESTÁNDARES.....	31
4. REFERENCIAS.....	34

1. TECNICAS DE CIFRADO

La palabra **criptografía** es una palabra de origen griego (krypto -oculto- y graphos -escribir-) y se define como el arte de escribir con clave secreta o de un modo enigmático.

1.1. Criptografía y criptoanálisis

La historia de la criptografía se remonta a miles de años atrás y tiene una larga tradición en las escrituras religiosas que podrían ofender a la cultura dominante o a las autoridades políticas. La finalidad de esta técnica ha sido siempre enviar mensajes confidenciales con la garantía de que sólo el destinatario de los mismos pudiera acceder a la información contenida en el mensaje.

El método consiste en la aplicación de una transformación al mensaje conocida como **cifrado**, con el objetivo de que las personas que desconozcan la transformación realizada sean incapaces de acceder a la información contenida en el mensaje.

El estudio de técnicas destinadas a encontrar el sentido de una información cifrada, sin tener acceso a la información secreta requerida, es el **criptoanálisis**. La finalidad del criptoanálisis es, por tanto, descubrir la clave de cifrado. La vulnerabilidad de los algoritmos de cifrado dependerá de la dificultad de la tarea de descubrimiento de la clave. Una ataque por fuerza bruta consiste en buscar la clave de cifrado probando uno a uno todos los posibles valores de la.

La **criptología** es la disciplina que abarca la criptografía y el criptoanálisis.

Otro concepto relacionado es la **esteganografía**. Al igual que la criptografía lo que busca es ocultar un mensaje ante un posible atacante, pero la diferencia estriba en cómo ocultan la información ambas técnicas:

mientras que la criptografía pretende que la información no sea descifrada, la esteganografía lo que pretende es que la información pase desapercibida (por ejemplo un código secreto tatuado en el cuero cabelludo y oculto por el pelo)

Las técnicas criptográficas se pueden clasificar siguiendo varios criterios. Siguiendo un **criterio temporal** se pueden clasificar en clásicas o extemporáneas y modernas o contemporáneas.

1.2. Técnicas criptográficas clásicas

Las técnicas criptográficas clásicas, realizan el cifrado en base a la sustitución y transposición de los caracteres del mensaje. El secreto está en el algoritmo aplicado al mensaje, por lo que tienen el inconveniente de que si un atacante lo descubre, será capaz de interpretar todos los mensajes cifrados que capture. Como ejemplos podemos citar:

- **Sustitución monoalfabeto:** consiste en la sustitución de símbolos uno a uno. Como ejemplo se puede citar el algoritmo de César.
- **Sustitución polialfabeto:** consiste en la sustitución de un símbolo por uno de un conjunto. Como ejemplo se puede citar el cifrado de Vigenère.
- **Transposición:** consiste en cambiar el orden de los símbolos.
- **Combinación de sustitución y transposición** (máquinas rotoras).

1.3. Técnicas criptográficas modernas

Las técnicas criptográficas modernas, a diferencia de las clásicas, utilizan claves de cifrado para cifrar la información. Una premisa fundamental de la criptografía moderna es que la seguridad del método debe depender únicamente de la clave de cifrado, debiendo ser los algoritmos conocidos.

Esta premisa hace que estas técnicas resulten mucho más seguras y efectivas ya que resulta más sencillo mantener el secreto de la clave y además cambiar la clave de cifrado siempre será menos costoso que idear un nuevo algoritmo resultando frecuente que la clave de cifrado se genere de forma automática.

Podemos clasificar los algoritmos de cifrado atendiendo a las claves que utilizan o al modo en que procesan la información.

Si nos fijamos en el tipo de claves que utilizan tenemos dos tipos de algoritmos:

- Algoritmos de **cifrado simétrico o de clave privada**: Utilizan la misma clave para el cifrado y el descifrado por lo que debe ser secreta y compartida por el emisor y el receptor. Ejemplos de algoritmos de este tipo son DES, 3DES, AES, IDEA, RC5, etc.
- Sistemas de cifrado **asimétrico o de clave pública**: Utilizan un par de claves generadas por el emisor. Una de las claves es pública, es decir, conocida por todo el mundo y la otra es privada o secreta de forma que lo que se cifra con una clave es descifrado por la otra y viceversa. Ejemplos de algoritmos de este tipo son RSA, DSA, Diffie-Hellman, ElGamal, etc.

Si nos fijamos en el modo en que procesan tenemos 3 tipos de algoritmos:

- Técnicas criptográficas de cifrado en **modo flujo** (*stream cipher*): estos algoritmos de cifrado se basan en la combinación de un texto en claro con un texto de cifrado obtenido a partir de una clave. La característica fundamental es que se va cifrando un flujo de datos bit a bit. Ejemplos: RC4, SEAL.
- Técnicas criptográficas de cifrado en **modo bloque** (*block cipher*): se caracterizan porque el algoritmo de cifrado o descifrado se aplica separadamente a bloques de longitud l , y para cada uno de ellos el

resultado es un bloque de la misma longitud: Ejemplos: DES, 3DES, AES.

- Técnicas criptográficas basadas en funciones resumen (**hash functions**): la característica principal de estos algoritmos es que permiten obtener una cadena de bits de longitud fija a partir de un mensaje de longitud arbitraria: Ejemplos: MD5, familia SHA.

1.4. Criptografía de clave privada o simétrica

La criptografía de clave simétrica, se caracteriza porque la clave de descifrado ***k***, es idéntica a la clave de cifrado o se puede obtener a partir de esta, residiendo de este modo la fortaleza del algoritmo en el secreto de la misma.

Si ***M*** es el mensaje en claro que se quiere proteger, al cifrarlo con un algoritmo en base a una clave privada **$E_k(M)$** se obtiene otro mensaje llamado texto cifrado ***C***. Para que este cifrado sea útil, existe otra función **$D_k(C)$** que a partir del texto cifrado por el emisor permite obtener de nuevo el mensaje en claro ***M***.

$$C = E_k(M)$$

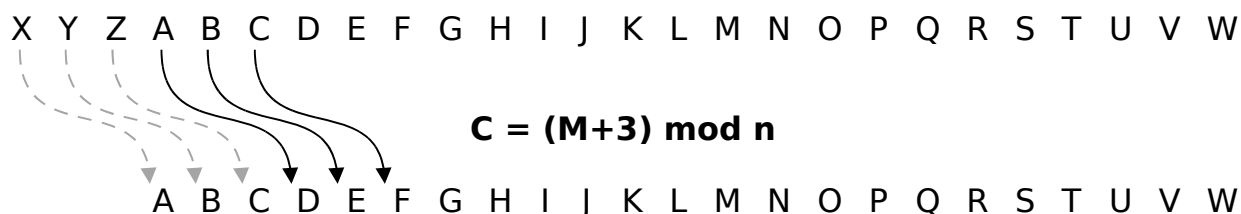
$$M = D_k(C) = D_k(E_k(M))$$

La seguridad del sistema recae pues en mantener en secreto la clave ***k***. El principal inconveniente de la criptografía simétrica, es el **intercambio de claves**. Este problema se soluciona con ayuda de la criptografía asimétrica.

1.4.1. Sustitución monoalfabeto

Un ejemplo de algoritmo de cifrado por sustitución monoalfabeto es el cifrado César. Es un tipo de cifrado por sustitución en el que cada letra en el texto original es reemplazada por otra letra que se encuentra un número

fijo de posiciones más adelante en el alfabeto. Por ejemplo, con un desplazamiento de 3, la A sería sustituida por la D (situada 3 lugares a la derecha de la A), la B sería reemplazada por la E, etc. Este método debe su nombre a Julio César, que lo usaba para comunicarse con sus generales.



Ejemplo:

Mensaje en	H O L A C E S A R
claro:	
Mensaje	K R O D G H V D U
cifrado:	

El descifrado de un mensaje consistiría en sustituir cada letra del texto por la que hay tres posiciones delante en el alfabeto.

La principal condición que debe cumplir la clave es que ha de ser una permutación del alfabeto, es decir, no puede haber letras repetidas ni faltar ninguna. Si no, la transformación no sería invertible en general.

1.4.2. Sustitución polialfabeto

El inconveniente de los algoritmos de sustitución monoalfabeto, es que el texto cifrado mantiene la misma distribución de frecuencia de caracteres que tiene el texto claro original, lo que hace que sean criptoanalizables por métodos estadísticos sencillos. Una posible mejora de los cifrados por sustitución es intentar métodos que destruyan esa correspondencia de frecuencias entre el mensaje en claro y el criptograma. Por ejemplo, utilizando varios alfabetos a la vez para el cifrado. En los cifrados

polialfabéticos la sustitución aplicada a cada carácter varía en función de la posición que ocupe este dentro del texto claro. En realidad corresponde a una aplicación cíclica de n cifrados de sustitución monoalfabeto. Un ejemplo típico de cifrado polialfabético es el Cifrado **de Vigenère**.

1.4.3. Cifrado en bloque

Un algoritmo de cifrado en bloque toma como entrada un bloque de longitud fija y una clave y genera un nuevo bloque cifrado de la misma longitud que el bloque de entrada.

La técnica consiste en dividir el texto a cifrar (con longitud L) en bloques de tamaño b y a continuación cifrar cada uno de los bloques. Si L no es múltiplo de b , se agregan bits adicionales para conseguir que todos los bloques estén completos. Para descifrar el mensaje se procede de manera análoga.

Muchos de los algoritmos de cifrado en bloque se basan en la combinación de dos operaciones básicas: sustitución y transposición.

- La **sustitución** consiste en traducir cada bloque de bits que llegan como entrada a otro de salida siguiendo una permutación determinada. El cifrado César sería un ejemplo simple de sustitución en el que cada grupo de bits correspondería a una letra.
- La **transposición** consiste en reordenar la información del texto en claro según un patrón determinado. Un ejemplo podría ser la formación de grupos de cinco letras, incluidos los espacios en blanco, y rescribir cada grupo (1, 2, 3, 4, 5) en el orden (3, 1, 5, 2, 4). Por ejemplo:

Texto en claro: "HOLA MUNDO"

Texto cifrado: "LH OANMOUD"

La transposición no dificulta extraordinariamente el criptoanálisis, pero puede combinarse con otras operaciones para añadir complejidad a los algoritmos de cifrado.

El **producto de cifras**, o combinación en cascada de distintas transformaciones criptográficas es una técnica muy efectiva para implementar algoritmos bastante seguros de forma sencilla. Por ejemplo, muchos algoritmos de cifrado en bloque se basan en una serie de iteraciones de productos sustitución-transposición.

Dos propiedades deseables en un algoritmo criptográfico son la **confusión y la difusión**. La confusión consiste en esconder la relación entre la clave y las propiedades estadísticas del texto cifrado. La difusión propaga la redundancia del texto en claro a lo largo del texto cifrado para que no sea fácilmente reconocible.

La confusión consigue que, cambiando un solo bit de la clave, cambien muchos bits del texto cifrado, y la difusión implica que el cambio de un solo bit del texto en claro afecte también a muchos bits del texto cifrado.

Modos de operación del cifrado en bloque

Un aspecto que hay que tener en cuenta cuando se utiliza el cifrado es que, aunque se puede conseguir que un atacante no descubra directamente los datos transmitidos, en ocasiones es posible que se pueda deducir información indirectamente. Por ejemplo, en un protocolo que utilice mensajes con una cabecera fija, la aparición de los mismos datos cifrados varias veces en una transmisión puede indicar dónde empiezan los mensajes. Para intentar contrarrestar esto, el cifrado bloque opera en varios modos:

- El modo **ECB** (Electronic Codebook): consiste en dividir el texto en bloques y cifrar cada uno de ellos de forma separada. El

inconveniente de este método es que bloques idénticos de mensaje sin cifrar producirán idénticos textos cifrados.

- En el modo **CBC** (Cipher Block Chaining), antes de ser cifrado, a cada bloque de texto se le aplica una operación **XOR** bit a bit, con el previo bloque ya cifrado. De este modo, cada bloque es dependiente de todos los bloques de texto previos hasta ese punto. Además, para hacer cada mensaje único se puede usar un [vector de inicialización](#). CBC es el modo usado más a menudo. Su principal contrapartida es que es secuencial y no puede funcionar en paralelo.
- En el modo **CFB** (Cipher Feedback), el algoritmo de cifrado no se aplica directamente al texto en claro sino a un vector auxiliar (inicialmente igual al IV). Del resultado del cifrado se toman n bits que se suman a n bits del texto en claro para obtener n bits de texto cifrado. Estos bits cifrados se utilizan también para actualizar el vector auxiliar. El número n de bits generados en cada iteración puede ser menor o igual que la longitud de bloque b . Tomando como ejemplo $n=8$, tenemos un cifrado que genera un byte cada vez sin que sea necesario esperar a tener un bloque entero para poderlo descifrar.
- El modo **OFB** (Output Feedback) opera como el CFB pero en lugar de actualizar el vector auxiliar con el texto cifrado, se actualiza con el resultado obtenido del algoritmo de cifrado. La propiedad que distingue este modo de los demás consiste en que un error en la recuperación de un bit cifrado afecta solamente al descifrado de este bit.

Ejemplos de algoritmos de cifrado en bloque: DES

DES¹ es uno de los algoritmos de cifrado más usados en el mundo. Fue publicado en 1977 en el documento **FIPS**² PUB 46 del Instituto Nacional de Estándares y Tecnología (NIST).

El algoritmo fue controvertido al principio, con algunos elementos de diseño clasificados, una [longitud de clave](#) relativamente corta, y las continuas sospechas sobre la existencia de alguna [puerta trasera](#) para la NSA³. Posteriormente DES fue sometido a un intenso análisis académico y motivó el concepto moderno del [cifrado por bloques](#) y su [criptoanálisis](#).

Hoy en día, DES se considera inseguro para muchas aplicaciones. Esto se debe principalmente a que el tamaño de clave de 56 bits es corto. A finales de 2001 el algoritmo ha sido sustituido por el nuevo [AES](#)⁴.

DES es el prototipo de algoritmo de [cifrado por bloques](#): toma un texto en claro de una longitud fija de bits y lo transforma mediante una serie de operaciones básicas en otro texto cifrado de la misma longitud, dividiendo para ello el mensaje, en bloques de 64 bits. El algoritmo DES utiliza una [clave criptográfica](#) para modificar la transformación, de modo que el descifrado sólo puede ser realizado por aquellos que conozcan la clave concreta utilizada en el cifrado. La longitud de la clave es de 64 bits, aunque en realidad, sólo 56 de ellos son empleados por el algoritmo. Los ocho bits restantes se utilizan únicamente para comprobar la [paridad](#), y después son descartados.

La parte central del algoritmo consiste en dividir el mensaje de entrada en grupos de bits, hacer una sustitución distinta sobre cada grupo y, a continuación una transposición de todos los bits. Esta transformación se repite dieciséis veces: en cada iteración, la entrada es una transposición

¹ Siglas en inglés de Data Encryption Standard.

² Siglas en inglés de *Federal Information Processing Standard*.

³ Siglas en inglés de *National Security Agency*.

⁴ Siglas en inglés de *Advanced Encryption Standard*.

distinta de los bits de la clave sumada bit a bit (XOR) con la salida de la iteración anterior. Este entrecruzamiento se conoce como [esquema Feistel](#).

La estructura de *Feistel* asegura que el cifrado y el descifrado sean procesos muy similares. La única diferencia es que las subclaves se aplican en orden inverso cuando desciframos. Esto simplifica enormemente la implementación, en especial sobre hardware, al no haber necesidad de algoritmos distintos para el cifrado y el descifrado.

Ejemplos de algoritmos de cifrado en bloque: 3DES

Aunque a lo largo de los años el algoritmo DES se ha mostrado muy resistente al criptoanálisis, su principal problema es actualmente la vulnerabilidad a los ataques de fuerza bruta, a causa de la longitud de la clave, de sólo 56 bits. En los años 70 era muy costoso realizar una búsqueda entre las 2^{56} combinaciones posibles, pero la tecnología actual permite romper el algoritmo en un tiempo cada vez más corto. Por este motivo, en 1999 el NIST cambió el algoritmo DES por el “Triple DES” como estándar oficial, mientras no estuviera disponible el nuevo estándar AES. El Triple DES, como su nombre indica, consiste en aplicar el DES tres veces consecutivas. Esto se puede realizar con tres claves (k_1 , k_2 , k_3), o bien con sólo dos (k_1 , k_2 , y otra vez k_1). La longitud total de la clave con la segunda opción es de 112 bits (dos claves de 56 bits). La primera opción proporciona más seguridad, pero a costa de utilizar una clave total de 168 bits (3 claves de 56 bits), que puede ser un poco más difícil de gestionar e intercambiar. Para conseguir que el sistema sea adaptable al estándar antiguo, en el Triple DES se aplica una secuencia cifrado-descifrado-cifrado (E-D-E) en lugar de tres cifrados:

$$\mathbf{C} = \mathbf{E}(k_3, \mathbf{D}(k_2, \mathbf{E}(k_1, \mathbf{M})))$$

$$\text{o bien: } \mathbf{C} = \mathbf{E}(k_1, \mathbf{D}(k_2, \mathbf{E}(k_1, \mathbf{M})))$$

De este modo, para cifrar un mensaje M , primero se cifra con k_1 , luego se descifra con k_2 y finalmente se vuelve a cifrar con k_3 (o k_1). Nótese que en el caso de usar 2 claves si hacemos que $k_1=k_2$ tenemos un sistema equivalente al DES simple.

Ejemplos de algoritmos de cifrado en bloque: AES

La longitud de la clave del algoritmo DES se ha ido convirtiendo en un problema a medida que iban aumentando las capacidades de procesamiento y el algoritmo se hacía cada vez más vulnerable a un ataque por fuerza bruta.

En 1977, a la vista de que el Triple DES no es excesivamente eficiente cuando se implementa en software, el NIST convocó a la comunidad criptográfica a presentar propuestas para un nuevo estándar que sustituyera al DES. De los quince algoritmos candidatos que se aceptaron, se escogieron cinco como finalistas (MARS, RC6, RIJNDAEL, SERPENT y TWOFISH), y en octubre de 2000 se dio a conocer el ganador: el algoritmo Rijndael, propuesto por los criptógrafos belgas Joan Daemen y Vincent Rijmen. En noviembre de 2001 se publicó el documento FIPS 197 donde AES se asumía oficialmente.

El Rijndael puede trabajar en bloques de 128, 192 o 256 bits, y la longitud de la clave también puede ser de 128, 192 o 256 bits. Dependiendo de esta última longitud, el número de iteraciones del algoritmo es 10, 12 ó 14, respectivamente. Cada iteración incluye una sustitución fija byte a byte, una transposición, una transformación consistente en desplazamientos de bits y XORs, y una suma binaria (XOR) con bits obtenidos a partir de la clave.

1.4.4. Cifrado en flujo

Para algunas aplicaciones, tales como el cifrado de conversaciones telefónicas, el cifrado en bloques es inapropiada porque los flujos de datos se producen en tiempo real en pequeños fragmentos. Las muestras de datos pueden ser tan pequeñas como 8 bits o incluso de 1 bit, y sería un desperdicio rellenar el resto de los 64 bits antes de cifrar y transmitirlos.

El funcionamiento de un cifrado en flujo consiste en la combinación de un texto claro **M** con un texto de cifrado **S** que se obtiene a partir la clave simétrica **k** obteniendo un texto cifrado **C**. Para descifrar, sólo se requiere realizar la operación inversa con el texto cifrado **C** y el mismo texto de cifrado **S**.

La operación de combinación que se utiliza normalmente es la suma y como operación inversa la resta. Si el texto está formado por caracteres, el algoritmo sería como un cifrado César en que la clave va cambiando de un carácter a otro. La clave que corresponde viene dada por el texto de cifrado **S** (llamado *keystream* en inglés).

Considerando el texto formado por bits, la suma y la resta son equivalentes. Cuando se aplican bit a bit, ambas son idénticas a la operación lógica “o exclusiva”, denotada con el operador XOR (eXclusive OR). Así pues:

$$\mathbf{C} = \mathbf{M} \text{ XOR } \mathbf{S(k)}$$

$$\mathbf{M} = \mathbf{C} \text{ XOR } \mathbf{S(k)}$$

En los esquemas de cifrado en flujo, el texto claro **M** tiene una longitud variable y el texto de cifrado **S** ha de ser como mínimo igual de largo. No es necesario disponer del mensaje entero antes de empezar a cifrarlo o descifrarlo, ya que se puede implementar el algoritmo para que trabaje con un “flujo de datos” que se va generando a partir de la clave (el texto cifrado). De ahí procede el nombre de este tipo de algoritmos.

Existen varias formas de obtener el texto cifrado **S** en función de la clave **k**:

- Si se escoge una secuencia **k** más corta que el mensaje **M**, una posibilidad sería repetirla cíclicamente tantas veces como sea necesario para ir sumándola al texto en claro. El inconveniente de este método es que se puede romper fácilmente, sobre todo cuanto más corta sea la clave.
- En el otro extremo, se podría tomar directamente **S(k) = k**. Esto quiere decir que la propia clave debe ser tan larga como el mensaje que hay que cifrar. Este es el principio del conocido **cifrado de Vernam**. Si **k** es una secuencia totalmente aleatoria que no se repite cíclicamente, estamos ante un ejemplo de cifrado incondicionalmente seguro. Este método de cifrado se llama en inglés *one-time-pad* (“cuaderno de un solo uso”). Un ejemplo de uso del cifrado de Vernam ocurre a veces entre los portaaviones y los aviones. En este caso, se aprovecha que en un instante dado (antes del despegue) tanto el avión como el portaaviones están en el mismo sitio, con lo cual, intercambiarse un disco duro de 20GB con una secuencia pseudoaleatoria no es ningún problema. Posteriormente cuando el avión despegue puede establecerse una comunicación segura con el portaaviones utilizando un cifrado de Vernam con la clave aleatoria que ambos comparten.
- Lo que en la práctica se utiliza son funciones que generan **secuencias pseudoaleatorias** a partir de una **semilla** (un número que actúa como parámetro del generador), y lo que se intercambia como clave secreta **k** es solamente esta semilla. En cada paso el algoritmo se encontrará en un determinado estado, que vendrá dado por sus variables internas. Dado que las variables serán finitas, habrá un número máximo de posibles estados distintos. Esto significa que al cabo de un cierto período, los datos generados se volverán a repetir. Para que el algoritmo sea seguro, interesa que el período de

repetición sea cuanto más largo mejor (con relación al mensaje que hay que cifrar), con el fin de dificultar el criptoanálisis.

Las características de este tipo de cifrado lo hacen apropiado para entornos en los que se necesita un rendimiento alto y los recursos (capacidad de cálculo, consumo de energía) sean limitados. Por ello se suelen utilizar en comunicaciones móviles: redes sin hilos, telefonía móvil, etc.

Un ejemplo clásico de cifrado en flujo es **RC4** (Ron's Code 4). Fue diseñado por Ronald Rivest en 1987 y publicado en Internet por un remitente anónimo en 1994. Es conocido por ser el algoritmo de cifrado empleado en el sistema de seguridad **WEP** (*Wired Equivalent Privacy*) reconocido en el estándar **IEEE 802.11**. [RC4](#) utiliza claves de 64 bits (40 bits más 24 bits del vector de iniciación IV) o de 128 bits (104 bits más 24 bits del IV).

1.4.5. Cifrado en base a funciones resumen

A veces los algoritmos de cifrado no sólo se usan para cifrar datos, sino que son utilizados para garantizar la autenticidad de los mismos. Como ejemplo de algoritmo de estas características se puede citar las llamadas **funciones hash**, también conocidas como **funciones de resumen** de mensaje⁵.

En general, podemos decir que una función resumen nos permite obtener una cadena de bits de longitud fija, relativamente corta, a partir de un mensaje de longitud arbitraria:

$$\mathbf{H} = h(\mathbf{M})$$

Para mensajes **M** iguales, la función **h** debe dar resúmenes **H** iguales. Pero si dos mensajes dan el mismo resumen **H** no deben ser necesariamente iguales. Esto es así porque sólo existe un conjunto limitado de posibles valores **H**, ya que su longitud es fija.

⁵ *Message Digest*, en inglés.

Para que una función ***h*** se pueda aplicar en sistemas de autenticación, debe cumplir una serie de condiciones que le permitan ser considerada una **función resumen segura**. Entre ellas destacan la **unidireccionalidad y la resistencia a colisiones**.

Para dificultar los ataques contra las funciones de resumen, por un lado los algoritmos tienen que definir una relación compleja entre los bits de entrada y cada bit de salida. Por otro lado, los ataques por fuerza bruta se contrarrestan alargando lo suficiente la longitud del resumen.

Hasta hace poco, el algoritmo de resumen más usado era el **MD5** (*Message Digest 5*). Pero como el resumen que obtiene es de sólo 128 bits, y aparte se han encontrado otras formas de generar colisiones parciales en el algoritmo, actualmente se recomienda utilizar algoritmos más seguros, como el **SHA-1**⁶. El algoritmo **SHA-1**, publicado el 1995 en un estándar del NIST (como revisión de un algoritmo anterior llamado simplemente SHA), obtiene resúmenes de 160 bits. El año 2002 el NIST publicó variantes de este algoritmo que generan resúmenes de 256, 384 y 512 bits.

1.5. Criptografía de clave pública o asimétrica

Los **sistemas de cifrado de clave pública** o **sistemas de cifrado asimétricos** se inventaron con el fin de evitar por completo el problema del intercambio de claves de los sistemas de cifrado simétricos.

En un algoritmo criptográfico de clave pública se utilizan claves distintas para el cifrado y el descifrado. Una de ellas, la **clave pública**, se puede obtener fácilmente a partir de la otra, la **clave privada**, pero por el contrario es prácticamente imposible. Los algoritmos de clave pública típicos permiten cifrar con la clave pública (k_{pub}) y descifrar con la clave privada (k_{pr}):

⁶ Siglas en inglés de *Secure Hash Algorithm-1*

$$C = e(k_{pub}, M)$$

$$M = d(k_{pr}, C)$$

Pero también puede haber algoritmos que permitan cifrar con la clave privada y descifrar con la pública:

$$C = e(k_{pr}, M)$$

$$M = d(k_{pub}, C)$$

En la práctica, los algoritmos utilizados permiten cifrar y descifrar fácilmente, pero todos ellos **son considerablemente más lentos que los equivalentes con criptografía simétrica**. Por eso, la criptografía de clave pública se suele utilizar solo en los problemas que la criptografía simétrica no puede resolver: el intercambio de claves y la autenticación con no repudio (firmas digitales).

Los mecanismos de **intercambio de claves** permiten que dos partes se pongan de acuerdo en las claves simétricas que utilizarán para comunicarse, sin que un tercero que esté escuchando el diálogo pueda deducir cuáles son estas claves.

La **autenticación** basada en clave pública se puede utilizar si el algoritmo permite utilizar las claves a la inversa: la clave privada para cifrar y la clave pública para descifrar. Si A envía un mensaje cifrado con su clave privada, todo el mundo podrá descifrarlo con la clave pública de A, y al mismo tiempo todo el mundo sabrá que el mensaje sólo lo puede haber generado quien conozca la clave privada asociada (que debería ser A). Ésta es la base de las **firmas digitales**.

1.5.1. Ejemplos de algoritmos de clave pública: Diffie-Hellman

Es un mecanismo que permite que dos partes se pongan de acuerdo de forma segura sobre una clave secreta utilizando un canal inseguro. El algoritmo se basa en la dificultad de calcular logaritmos discretos y se usa generalmente como medio para acordar claves simétricas que serán empleadas para el cifrado de una sesión.

1.5.2. Ejemplos de algoritmos de clave pública: RSA

Es el algoritmo más utilizado en la historia de la criptografía de clave pública. Su nombre procede de las iniciales de quienes lo diseñaron en 1977: Ronald Rivest, Adi Shamir y Leonard Adleman. La clave pública está formada por un número n , calculado como producto de dos factores primos muy grandes ($n = p * q$) y un exponente e . La clave privada es otro exponente d calculado a partir de p , q y e , de tal forma que el cifrado y el descifrado se puede realizar de la siguiente forma:

$$\text{Cifrado: } \mathbf{C = M^e \text{ mod } n}$$

$$\text{Descifrado: } \mathbf{M = C^d \text{ mod } n}$$

Como se puede ver, la clave pública y la privada son intercambiables: si se usa cualquiera de ellas para cifrar, se deberá utilizar la otra para descifrar. La fortaleza del algoritmo RSA se basa, por un lado, en la dificultad de obtener M a partir de C sin conocer d (problema del logaritmo discreto), y por otro lado, en la dificultad de obtener p y q (y, por tanto, d) a partir de n (problema de la factorización de números grandes, que es otro de los problemas considerados difíciles).

2. FIRMA DIGITAL

Una firma digital es, básicamente, un mensaje cifrado con la clave privada del firmante. Pero, por cuestiones de eficiencia, lo que se cifra no es

directamente el mensaje a firmar, sino solamente su resumen calculado con una función *resumen* segura.

La firma digital está basada en algoritmos criptográficos asimétricos, en los que son necesarias un par de claves para el intercambio de la información: una clave pública y una clave privada. La clave privada está bajo custodia del emisor y solamente es conocida por él. La clave pública es distribuida entre todos los posibles destinatarios de los mensajes o documentos firmados. El proceso para realizar una firma digital se resume a continuación:

- El emisor obtiene un resumen del mensaje a través de una función resumen (*Hash*). La propiedad más importante de ese resumen o *hash* es que dos documentos diferentes siempre deben producir resúmenes diferentes.
- El resumen obtenido se cifra con la clave privada del firmante y se obtiene la firma digital del documento.
- El receptor del mensaje firmado utiliza la clave pública para descifrar la firma, obtiene el resumen del documento recibido y comprueba que es igual que el resumen que le ha llegado cifrado en la firma digital. De esta forma se garantiza que el contenido del mensaje no ha sido manipulado.

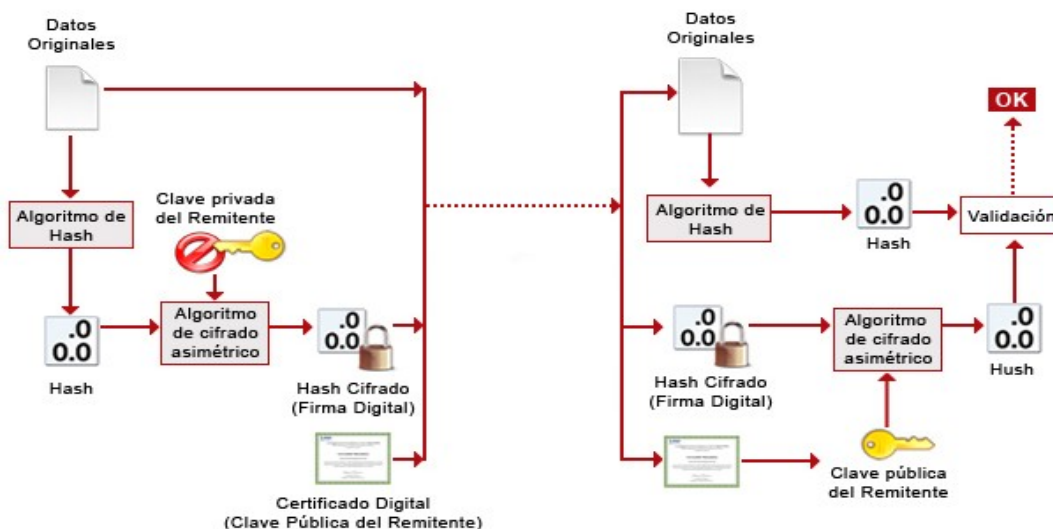


Figura 1: Proceso de creación de una firma digital (fuente: INTECO)

La firma digital, por si misma, no aporta confidencialidad al mensaje pero es habitual que los mensajes firmados electrónicamente se suelen enviar cifrados con la misma clave privada utilizada para mayor seguridad. La firma digital aporta:

- Identificación del firmante: la firma identifica al firmante de forma única igual que su firma manuscrita.
- Integridad del contenido firmado: es posible verificar que los documentos firmados no hayan sido alterados por terceras partes.
- No repudio del firmante: un documento firmado electrónicamente no puede repudiarse por parte de su firmante.

3. INFRAESTRUCTURA DE CLAVE PÚBLICA (PKI)

Como se ha visto hasta ahora, la criptografía de clave pública permite resolver el problema del intercambio de claves, utilizando las claves

públicas de los participantes. Pero se plantea otro problema: si alguien afirma ser A y su clave pública es k_{pub} ,

¿cómo podemos saber que realmente k_{pub} es la clave pública de A?

Porque es perfectamente posible que un atacante Z genere su par de claves (k'_{pr} , k'_{pub}) y afirme “yo soy A, y mi clave pública es k'_{pub} ”.

Una posible solución a este problema es que exista una entidad de confianza que nos asegure que, efectivamente, las claves públicas pertenecen a sus supuestos propietarios. Esta entidad puede firmar un documento que afirme “la clave pública de A es k_{pub} ”, y publicarlo para que todos los usuarios lo sepan. Este tipo de documento se llama **certificado de clave pública** o **certificado digital**, y es la base de lo que se conoce como **infraestructura de clave pública o PKI**.

Una **PKI** está formada entre otros por los siguientes elementos:

- **Certificados digitales:** Son documentos firmados electrónicamente por las autoridades de certificación que certifican que una clave pública pertenece a un determinado usuario.
- **Autoridades de certificación (AC):** Son entidades de confianza que se encargan de emitir y revocar los certificados digitales.
- **Autoridades de registro (RA):** Son entidades que registran las peticiones que hagan los usuarios para obtener un certificado, comprueban la veracidad y corrección de los datos que aportan los usuarios en dichas peticiones y las envían a una AC para que sean procesadas.
- **Autoridades de validación (VA):** suministran información sobre la vigencia de los certificados electrónicos que, a su vez, hayan sido registrados por una RA y certificados por la AC.

- **Autoridades de sellado de tiempos (TSA):** proporcionan certeza sobre la preexistencia de determinados documentos electrónicos en un momento dado, cuya indicación temporal junto con el hash del documento se firma por la Autoridad de sellado de tiempo.
- **Directorios de certificados:** proporcionan almacenamiento y distribución de certificados y listas de revocación (CRLs).
- **Hardware criptográfico (HSM):** dispositivos criptográficos basados en hardware que generan, almacenan y protegen claves criptográficas y suelen aportar aceleración hardware para operaciones criptográficas
- **Tarjetas criptográficas (TI):** son tarjetas que incluyen un chip con un microprocesador con módulos hardware específicos para realizar operaciones criptográficas.

3.1. Certificados Digitales

Un certificado digital es un documento emitido y firmado electrónicamente por una autoridad certificadora en el que certifica la asociación entre una clave pública y un participante.

El certificado garantiza que la clave pública pertenece al participante identificado y que el participante posee la correspondiente clave privada.

Los certificados digitales sólo son útiles si existe una *Autoridad de Certificación (CA)*, de confianza para las dos partes, que los valide

Los certificados digitales proporcionan un **mecanismo criptográfico** para implementar la **autenticación**. También proporcionan un mecanismo seguro y escalable para **distribuir claves públicas** en comunidades con gran número de participantes.

El formato de los certificados X.509 es una recomendación del ITU⁷ que se publicó por primera vez en 1988. La revisión actual del estándar fue publicada en 1996 y se conoce con el nombre de X.509 v3. Los elementos que componen un certificado X.509 v3 son:

- **Versión.** Es el número de versión del certificado codificado. Los valores aceptables son 1, 2 y 3.
- **Número de serie del certificado.** Es un entero asignado por la autoridad certificadora. Cada certificado emitido por una CA debe tener un número de serie único.
- **Identificador del algoritmo de firmado.** Especifica el algoritmo empleado para firmar el certificado (ej: *sha1withRSAEncryption*).
- **Nombre del emisor.** identifica la CA que ha firmado y emitido el certificado.
- **Periodo de validez.** Es el periodo de tiempo durante el cual el certificado es válido y la CA está obligada a mantener información sobre el estado del mismo.
- **Nombre del sujeto.** Identifica al sujeto cuya clave pública está certificada en el campo siguiente. El nombre debe ser único para cada entidad certificada por una CA dada, aunque puede emitir más de un certificado con el mismo nombre si es para la misma entidad.
- **Información de clave pública del sujeto.** Almacena la clave pública, sus parámetros y el identificador del algoritmo con el que se emplea la clave.
- **Identificador único del emisor.** Este es un campo opcional que permite reutilizar nombres de emisor.
- **Identificador único del sujeto.** Este es un campo opcional que permite reutilizar nombres de sujeto.
- **Extensiones:** Las extensiones del X.509 v3 proporcionan una manera de asociar información adicional a sujetos, claves públicas, etc.

⁷Siglas en inglés de *International Telecommunication Union*.

- **Firma de la AC:** En este campo se almacena la firma digital del certificado por parte de la AC.

Los certificados digitales se diferencian **según la finalidad** para la que son solicitados. Así podemos tener certificados para **personas físicas**, certificados de **servidor**, certificados para la **firma de código**, certificados de **entidad**, etc.

3.1.1. Autoridad de Certificación

Una Autoridad de Certificación, es una entidad de confianza, encargada de emitir y revocar los certificados digitales que garantizan de forma unívoca y segura la identidad asociada a una clave pública.

La Autoridad de Certificación, por sí misma o por mediación de una [Autoridad de Registro](#), verifica la identidad del solicitante de un certificado antes de su expedición o, en caso de certificados expedidos con la condición de revocados, elimina la revocación de los certificados al comprobar dicha identidad.

Los certificados son documentos que recogen ciertos datos de su titular y su [clave pública](#) y están [firmados electrónicamente](#) por la Autoridad de Certificación utilizando su clave privada.

La Autoridad de Certificación es un tipo particular de [Prestador de Servicios de Certificación](#) que legitima ante los terceros que confían en sus certificados la relación entre la identidad de un usuario y su clave pública. La confianza de los usuarios en la CA es importante para el funcionamiento del servicio y justifica la filosofía de su empleo, pero no existe un procedimiento normalizado para demostrar que una CA merece dicha confianza.

La autoridad de certificación se encarga de renovar los certificados, proporcionar servicios de backup y archivo de claves de cifrado. También

crea la infraestructura de seguridad para la confianza de los participantes, establece políticas de operación segura y genera información de auditoría.

El mecanismo habitual **de solicitud de un certificado** de servidor web a una CA consiste en que la entidad solicitante, utilizando ciertas funciones del [software](#) de [servidor web](#), completa ciertos datos identificativos (entre los que se incluye el localizador [URL](#) del servidor) y genera una pareja de claves pública/privada. Con esa información el [software](#) de servidor compone un [fichero](#) que contiene una petición CSR⁸ en formato *PKCS#10* que contiene la clave pública y que se hace llegar a la CA elegida. Esta, tras verificar por sí o mediante los servicios de una [Autoridad de Registro](#) la información de identificación aportada y la realización del pago, envía el certificado firmado al solicitante, que lo instala en el [servidor web](#) con la misma herramienta con la que generó la petición CSR.

Las CA disponen de sus propios [certificados públicos](#), cuyas claves privadas asociadas son empleadas por las CA para firmar los certificados que emiten. Un certificado de CA estará firmado por otra CA de rango superior estableciéndose así una jerarquía de certificación.

Existen **certificados de CA raíz** que están auto-firmados por la propia CA que los emite y que constituyen el elemento inicial de la jerarquía de certificación.

Una **jerarquía de certificación** consiste en una estructura jerárquica de CAs en la que se parte de una CA auto-firmada, y en cada nivel, existe una o más CAs que pueden firmar certificados de entidad final ([servidor web](#), persona, [aplicación](#) de [software](#)) o bien certificados de otras CA subordinadas plenamente identificadas y cuya [Política de Certificación](#) sea compatible con las CAs de rango superior.

Una de las formas por las que se **establece la confianza en una CA** por parte de un usuario, consiste en la "instalación" en el ordenador del usuario

⁸ *Certificate Signing Request*

(tercero que confía), del certificado autofirmado de la CA raíz de la jerarquía en la que se desea confiar.

Cuando el modelo de CA incluye una **jerarquía**, es preciso **establecer explícitamente la confianza en los certificados de todas las cadenas de certificación** en las que se confíe. Para ello, se puede localizar sus certificados mediante distintos medios de publicación en internet, pero también es posible que un certificado contenga toda la cadena de certificación necesaria para ser instalado con confianza.

Un **certificado revocado** es un certificado que no es válido aunque se emplee dentro de su período de vigencia. Un certificado revocado tiene la condición de suspendido si su vigencia puede restablecerse en determinadas condiciones.

Es necesario establecer un mecanismo que permita revocar un certificado antes de que este caduque para los casos de sustracción, errores, cambios de derechos, ruptura de la CA, etc.

Para comprobar si un certificado está revocado generalmente se utilizan las **CRL (Certificate Revocation List)**. De este modo, cuando se quiere verificar la firma de un documento, el usuario no sólo ha de verificar el certificado y su validez, sino que también ha de comprobar que el certificado no ha sido revocado consultando para ello la versión más reciente de la CRL .

Con las CRL se opera siguiendo dos modelos:

- **Modelo pull:** el cliente que tiene que hacer la verificación obtiene la CRL de la CA cuando lo necesita.
- **Modelo push:** una vez que la CA actualiza la CRL, la información es enviada a los clientes que necesitan verificar certificados.

Otro método alternativo de comprobación es el *protocolo de estado de certificado en línea* **OCSP**⁹. Este método permite a los clientes desprenderse de la gestión del estado de los certificados y obtener una confirmación online del estado. Para ello la CA debe poner a disposición de todos los usuarios potenciales un servicio seguro online de alta disponibilidad. Este protocolo está definido por el IETF en el RFC 2560.

Los mensajes *OCSP* se codifican en [ASN.1](#) y habitualmente se transmiten sobre el protocolo [HTTP](#). La naturaleza de las peticiones y respuestas de *OCSP* hace que a los servidores *OCSP* se les conozca como "**OCSP responders**". Las CAs delegan la responsabilidad de proporcionar información de revocaciones en los *responders* creando así una arquitectura distribuida. Los **clientes envían una petición de estado** a un *responder* y suspende su aceptación hasta recibir la respuesta. Este modo de funcionamiento evita el uso de *CRLs*, reduciendo así el ancho de banda consumido, el uso de CPU y se evitan los problemas asociados a la gestión de información sensible que contienen las *CRLs*.

3.1.2. Autoridad de Registro

La Autoridad de Registro **gestiona el registro de usuarios y sus peticiones de certificación/revocación**, así como los certificados respuesta a dichas peticiones. Indica a la CA si debe emitir un certificado. La Autoridad de Registro es la que autoriza la asociación entre una clave pública y el titular de un certificado. Durante el ciclo de vida de un certificado, la Autoridad de Registro, es la que se encarga de las siguientes operaciones:

- Revocación.
- Expiración.

⁹ Siglas en inglés de *Online Certificate Status Protocol*.

- Renovación (extensión del período de validez del certificado, respetando el plan de claves).
- Reemisión del par de claves del usuario.
- Actualización de datos del certificado.

3.1.3. Autoridad de Validación

La Autoridad de Validación **suministra información de forma online acerca del estado de un certificado**. La Autoridad de Validación suele proporcionar dos servicios de validación: el tradicional, permitiendo la descarga de **CRLs** para que el usuario las interprete él mismo, o a través del protocolo **OCSP** (*Online Certification Status Protocol*).

Los usuarios y las aplicaciones que deseen obtener el estado de un certificado, sólo tienen que realizar una petición *OCSP* contra la Autoridad de Validación para obtener dicho estado. La CA actualiza la información de la Autoridad de Validación cada vez que se modifica el estado de un certificado, con lo que, usando *OCSP*, se dispone de información en tiempo real.

3.1.4. Autoridad de Sellado de Tiempos

La Autoridad de Sellado de Tiempos (*TSA*) permite **firmar documentos con sellos de tiempo**, de manera que permite obtener una prueba de que un determinado dato existía en una fecha concreta. El sello de tiempo es uno de los servicios más importantes de la firma electrónica. Con el sello de tiempo se puede demostrar que una serie de datos han existido y no han sido alterados desde un instante específico en el tiempo. Este protocolo se describe en el RFC 3161 y está en el registro de estándares de Internet. Una autoridad de sellado de tiempo actúa como tercera parte de confianza testificando la existencia de dichos datos electrónicos en una fecha y hora

concretas. Los pasos que se siguen para generar un sello de tiempo son los siguientes:

- Un usuario quiere obtener un sello de tiempo para un documento electrónico que él posee.
- Un resumen digital (técnicamente un *hash*) se genera para el documento en el ordenador del usuario.
- Este resumen forma la solicitud que se envía a la autoridad de sellado de tiempo (*TSA*).
- La *TSA* genera un sello de tiempo con esta huella, la fecha y hora obtenida de una fuente fiable y la firma electrónica de la *TSA*.
- El sello de tiempo se envía de vuelta al usuario.
- La *TSA* mantiene un registro de los sellos emitidos para su futura verificación.

Las aplicaciones del sellado de tiempo son innumerables, ya que los certificados digitales se emiten con un período de validez determinado y es fundamental por ejemplo, poder verificar que una firma de un documento realizada hace *X* años atrás efectivamente se hizo con un certificado que no estaba revocado en ese instante. Ejemplos de uso: factura electrónica, voto electrónico, protección de la propiedad intelectual, etc.

3.1.5. Directorio de Certificados

Los directorios proporcionan almacenamiento y distribución de certificados y listas de revocación (*CRLs*). Cuando una Autoridad de Certificación emite un certificado o *CRL*, lo envía al Directorio y además, guarda el certificado o *CRL* en su base de datos local. Generalmente se utiliza *LDAP* (*Light-weight Directory Access Protocol*) para acceder a los directorios. El usuario puede obtener certificados de otros usuarios y comprobar el estado de los mismos.

3.2. Hardware Criptográfico

Los **Módulos de Seguridad Hardware (HSM)** son dispositivos especializados en realizar labores criptográficas. Proporcionan almacenamiento seguro de claves y/o realización de funciones criptográficas básicas como cifrado, firma, generación de claves, etc. Para ello usan interfaces estándar como *PKCS#11* y *CryptoAPI*. Este tipo de dispositivos aumentan significativamente la seguridad en comparación con los certificados basados en disco por lo siguiente:

- La clave privada y las firmas digitales se generan dentro del HSM.
- La clave privada se almacena cifrada dentro del HSM.

Si se compara el hardware criptográfico con las tecnologías de cifrado basado en software se puede decir que el hardware criptográfico es mucho más rápido a la hora de realizar el proceso. Dependiendo del tipo de hardware *HSM*, los ratios de trabajo oscilan de las 600 a 4000 operaciones de firma RSA/segundo. Además proporcionan seguridad física al no poder modificar los algoritmos de cifrado y limitando el acceso al almacenamiento seguro de claves. Esto permite que estas soluciones puedan ser certificadas por un tercero en jerarquías de certificación.

3.3. Tarjetas y chip criptográficos

Una tarjeta inteligente (**smart card**), o tarjeta con [circuito integrado \(TCI\)](#), es cualquier tarjeta de tipo bolsillo con circuitos integrados que permiten la ejecución de cierta lógica programada. Aunque existe un diverso rango de aplicaciones, hay varias categorías de *TCI*: **Las tarjetas de memoria** contienen sólo componentes de memoria no volátil y posiblemente alguna lógica de seguridad. **Las tarjetas microprocesadoras** contienen memoria y tienen capacidad de procesamiento limitada. Las **tarjetas con chip criptográfico** son tarjetas microprocesadas avanzadas en las que

hay módulos hardware para la ejecución de algoritmos usados en cifrado y firmas digitales.

Una **tarjeta inteligente con un chip criptográfico** se puede definir como una llave muy segura, no duplicable e inviolable, que contiene las claves y certificados necesarios para la firma electrónica grabados en la tarjeta y que además está protegida por un PIN secreto y/o biometría. El **chip criptográfico** contiene un microprocesador que realiza las operaciones criptográficas con la clave privada, con la característica adicional de que no es posible el acceso a la clave desde el exterior. Las características principales son las siguientes:

- Doble seguridad: posesión de la tarjeta y PIN de acceso (o mecanismos biométricos).
- Puede ser multipropósito: Tarjeta de identificación gráfica, tarjeta de control de acceso/horario mediante banda magnética o chip de radiofrecuencia, tarjeta monedero, tarjeta generadora de contraseñas de un solo uso (*OTP*).
- Se precisa de un middleware (*CSP*) específico para utilizar la tarjeta, así como de un lector (*USB*, integrado en teclado o *PCMCIA*)
- El número de certificados que se pueden cargar depende del perfil de certificado, de la capacidad del chip y del espacio que se reserve para los certificados.

3.4. 3.3. Marco legal y estándares

Legislación Española

- **Ley 59/2003**, de 19 de diciembre, de firma electrónica (BOE nº 304, 20/12/2003)

Directiva Europea

- **Directiva 1999/93/CE del parlamento europeo** y del consejo de 13 de diciembre de 1999 por la que se establece un marco comunitario para la firma electrónica

Estándares europeos

- ETSI TS 102 042: Policy requirements for certification authorities issuing public key certificates
- ETSI TS 102 023: Policy requirements for time-stamping authorities
- ETSI TS 101 862: Qualified Certificate profile
- ETSI TS 101 456: Policy requirements for certification authorities issuing qualified certificates
- CWA 14167-2 Security Req. for Trustworthy Systems Managing Certificates for Electronic Signatures
- CWA 14172 EESSI Conformity Assessment Guidance (Guía para aplicar los estándares de firma electrónica de acuerdo con la iniciativa de estandarización europea)

Internet Engineering Task Force (IETF) - Request For Comment

- RFC 3280: Certificate and Certificate Revocation List (CRL) Profile
- RFC 3739: Qualified Certificates Profile
- RFC 3647: Certificate Policy and Certification Practices Framework (Obsoletes RFC2527)

PKCS (Public Key Cryptography Standards): Familia de estándares para los sistemas de criptografía de clave pública definidos por los Laboratorios RSA:

- PKCS#1,#2,#4: RSA Cryptography Standard
- PKCS#3: Diffie-Hellman Key Agreement Standard
- PKCS#5: Password-Based Encryption Standard
- PKCS#6: Extended-Certificate Syntax Standard
- PKCS#7: Cryptographic Message Syntax Standard
- PKCS#8: Private Key Information Syntax Standard
- PKCS#9: Selected Attribute Types

- PKCS#10: Certification Request Standard
- PKCS#11: Cryptographic Token Interface
- PKCS#12: Personal Information Exchange Syntax Standard
- PKCS#13: Elliptic Curve Cryptography Standard

4. REFERENCIAS

- Universidad de Vigo. Asignatura Seguridad en sistemas de información.
(<http://ccia.ei.uvigo.es/docencia/SSI/>)
- Centro Criptológico Nacional. (<https://www.ccn.es/>)
- Instituto Nacional de Tecnologías de la Comunicación - DNI Electrónico.
(<http://cert.inteco.es>)
- Universidad Politécnica de Madrid - Departamento de Matemática Aplicada de la Facultad de Informática.
(<http://www.dma.fi.upm.es/java/matematicadiscreta/aritmeticamodular/>)
- Universidad Pontificia Comillas (Madrid) - Asignatura de Seguridad Informática. (<http://www.iit.upcomillas.es/seguridad>)

(Todos los enlaces fueron verificados en noviembre de 2011)

Autor: Juan Otero Pombo

Ingeniero en Informática en el Concello de Ourense

Colegiado del CPEIG

**44. SEGURIDAD EN ENTORNOS
DE RED PRIVADOS.
MECANISMOS DE PROTECCIÓN
DE LA CONFIDENCIALIDAD.
SERVICIOS DE DIRECTORIO.
GESTIÓN DE IDENTIDADES.
SINGLE SIGN-ON. TIPOS DE
CONECTIVIDAD. ACCESO
REMOTO. VPN.**



Tema 44. Seguridad en entornos de red privados. Mecanismos de protección de la confidencialidad. Servicios de directorio. Gestión de identidades. Single sign-on. Tipos de conectividad. Acceso remoto. VPN.

INDICE

<u>1 SEGURIDAD EN ENTORNOS DE RED PRIVADOS. MECANISMOS DE PROTECCIÓN DE LA CONFIDENCIALIDAD.....</u>	<u>2</u>
<u>2 SERVICIOS DE DIRECTORIO.....</u>	<u>5</u>
<u>2.1 LDAP.....</u>	<u>7</u>
2.1.1 El modelo de información.....	9
2.1.2 El modelo de nombrado.....	10
2.1.3 El modelo funcional.....	11
2.1.4 El modelo de seguridad.....	11
<u>3 GESTION DE IDENTIDADES Y SINGLE SIGN-ON.....</u>	<u>12</u>
3.1 Gestión federada de identidades.....	15
<u>4 TIPOS DE CONECTIVIDAD. ACCESO REMOTO. VPN.....</u>	<u>18</u>
4.1 Virtual Private Networks (VPN).....	21
4.2 SSL/TLS.....	25
4.3 Secure Shell: SSH.....	26
<u>REFERENCIAS.....</u>	<u>29</u>

1 SEGURIDAD EN ENTORNOS DE RED PRIVADOS. MECANISMOS DE PROTECCIÓN DE LA CONFIDENCIALIDAD

La seguridad es una característica de cualquier sistema, informático o no, que lo protege de todo peligro, daño o riesgo al que pudiera estar expuesto. En el caso de las redes de ordenadores, esta característica es muy difícil de conseguir (incluso podríamos decir que es imposible) por lo que cuando hablamos de seguridad en entornos de red hacemos referencia a la fiabilidad como una medida de la probabilidad de que el sistema se comporte tal y como se espera de él. Nos referimos, por tanto, a todas las medidas hardware y software, personal, documentación, y procesos dentro de la infraestructura de red, que en conjunto protegen la integridad y privacidad de las aplicaciones, datos y flujos de información. El diseño e implementación de una infraestructura de seguridad es una tarea crítica ya que: evoluciona rápidamente, crece en complejidad y tiene especial incidencia en la consecución de los objetivos de la organización.

Hay una serie de aspectos fundamentales que debemos garantizar a la hora de mantener un sistema seguro:

- **Confidencialidad:** Consiste en proteger la información contra la lectura no autorizada explícitamente. Incluye no sólo la protección de la información en su totalidad, sino también las piezas individuales que pueden ser utilizadas para inferir otros elementos de información confidencial.

En un entorno de red, se dispone de dos mecanismos básicos de protección de la confidencialidad:

- o **Control de acceso:** garantiza la confidencialidad de la información almacenada en un sistema informático al impedir el acceso a la misma por parte de usuarios no autorizados.



- o Técnicas de cifrado: permiten mantener la privacidad de la comunicación entre 2 entidades alterando el mensaje original de modo que sea incomprensible a toda persona distinta del destinatario.
- **Integridad:** Es necesario proteger la información contra la modificación sin el permiso del dueño. La información a ser protegida incluye no sólo la que está almacenada directamente en los sistemas de cómputo sino que también se deben considerar elementos menos obvios como respaldos, documentación, registros de contabilidad del sistema, tránsito en una red, etc. Esto comprende cualquier tipo de modificaciones:
 - o Causadas por errores de hardware y/o software.
 - o Causadas de forma intencional.
 - o Causadas de forma accidental

Cuando se trabaja con una red, se debe comprobar que los datos no fueron modificados durante su transferencia

- **Disponibilidad:** Una buena medida para proteger la información es impedir el acceso a la misma, pero resulta evidente que en ese caso la información dejaría de ser útil. Por tanto, se deben proteger los servicios de cómputo de manera que no se degraden o dejen de estar disponibles a los usuarios de forma no autorizada. La disponibilidad también se entiende como la capacidad de un sistema para recuperarse rápidamente en caso de algún problema.
- **Autenticación:** consiste en la confirmación de la identidad de un usuario; es decir, la garantía para cada una de las partes de que su interlocutor es realmente quien dice ser. Un control de acceso permite garantizar el acceso a recursos únicamente a las personas autorizadas.

- **No repudio:** constituye la garantía de que ninguna de las partes involucradas pueda negar en el futuro una operación realizada.

Para tener una visión global, es de utilidad ver en que capa del modelo de referencia OSI se abordarían cada uno de los aspectos descritos en el apartado anterior. Esto se puede ver en la Tabla 1. Los servicios de la seguridad en la red se expanden sobre las siete capas. Cada tecnología puede trabajar en una o varias capas: Por ejemplo, SSL es una tecnología que trabaja normalmente en la capa de aplicación.

APLICACIÓN	Servicios seguridad Confidencialidad Autenticación Integridad Autorización No repudio	Seguridad lógica	Seguridad proporcionada por fabricante o proveedor
PRESENTACIÓN			Servicio de seguridad proporcionado en la red backbone de transporte
SESION			
TRANSPORTE			
RED			
ENLACE			
FISICO		Seguridad física	

Tabla 1 Seguridad en la red y Modelo de referencia OSI

Una vez identificados los cinco servicios básicos de la seguridad en la red, se pueden examinar las tecnologías que se han definido y desarrollado para implementar esos servicios para necesidades específicas de seguridad y bajo diferentes entornos operativos. Una forma de clasificar estas tecnologías es en base a la manera en que implementan los servicios de seguridad:

- **Tecnologías básicas:** se definen como tecnologías básicas las que sólo implementan un único servicio de seguridad específico. Ejemplos de estas tecnologías son el cifrado, el uso de circuitos permanentes

virtuales (PVCs) en Frame Relay para hacer VPNs de capa 2, o las listas de control de acceso de los routers (ACLs).

- **Tecnologías avanzadas:** este tipo de tecnologías también son diseñadas para implementar un único servicio de seguridad, pero son relativamente más complejas y con frecuencia necesitan del uso de varias tecnologías básicas para conseguir sus objetivos. Un ejemplo es la firma digital para conseguir no repudio en origen.
- **Tecnologías integradas:** este tipo de tecnologías son definidas utilizando otras tecnologías básicas, pero son diseñadas para dar soporte a más de un servicio de seguridad. Ejemplos de estas tecnologías son SSL e IPSEC.
- **Arquitecturas de seguridad:** son tecnologías de arquitectura de seguridad en red, que se definen en base a las tecnologías básicas, avanzadas e integradas. Proporcionan guías para implementar sistemas de seguridad dentro de la arquitectura definida. El mejor ejemplo para esta categoría es el uso de una infraestructura de clave pública (PKI).

2 SERVICIOS DE DIRECTORIO

Un servicio de directorio es una herramienta que almacena y organiza de una manera clara y efectiva la información relativa a los usuarios, aplicaciones, archivos, impresoras y otros recursos accesibles dentro de una red con el objetivo de mejorar la funcionalidad, la facilidad de uso y poder hacer una gestión eficiente de los recursos de la organización.

Un directorio es un listado de información de objetos que están dispuestos en un orden concreto y que aporta información detallada acerca de cada objeto concreto. Ejemplos comunes son la guía de teléfonos de una ciudad o un catálogo de una biblioteca.

Los directorios suelen ser descritos a menudo como una base de datos, pero realmente es una base de datos especializada que tiene unas características propias que los distinguen de las bases de datos relacionales de carácter general:

- Una característica especial es que se accede con mucha frecuencia mediante operaciones de lectura, búsquedas y navegación, mientras que las operaciones de escritura son mucho menos frecuentes.
- Debido a la característica anterior, estos sistemas están diseñados para soportar gran número de solicitudes de lectura y el acceso mediante operaciones de escritura puede estar limitado a ciertos administradores.
- Otra diferencia con las BBDD de propósito general es que la mayoría de implementaciones de los servicios de directorio no son compatibles entre sí.
- Las consultas a las BBDD de propósito general se hacen en base a una herramienta estandarizada de consulta llamada SQL mientras que los directorios suelen utilizar un protocolo de acceso simplificado y optimizado.

Existen numerosas implementaciones de los servicios de directorio de diferentes compañías. Algunos ejemplos son:

- **NIS:** *Network Information Service* es una implementación de Sun Microsystems para redes en el entorno UNIX.
- **Active Directory:** es el servicio de directorio de Microsoft.
- **ApacheDS:** *Apache Directory Studio* es el servidor de directorio de Apache.

- **eDirectory:** es un servicio de directorio desarrollado por Novell que soportado por múltiples plataformas incluyendo Windows, NetWare, Linux.
- **OpenLDAP:** derivado de la implementación original de referencia LDAP de la Universidad de Michigan, pero significativamente evolucionado. Es compatible con prácticamente todas las plataformas actuales: UNIX, Linux, Windows, etc.

Los servicios de directorio formaron parte de una iniciativa del OSI (*Open Systems Interconnection*) para poner de acuerdo a los miembros de la industria en establecer unos estándares de red comunes y así garantizar la interoperabilidad. En la década de los 80 la UIT y la ISO crearon el conjunto de estándares X.500 sobre el modelo de referencia OSI para servicios de directorio. X.500 Consta de los siguientes protocolos: protocolo de acceso al directorio (DAP), protocolo de sistema de directorio, protocolo de ocultación de información y protocolo de gestión de enlaces de directorio.

2.1 LDAP

X.500 es un conjunto de protocolos producido por la *Unión Internacional de Telecomunicaciones*¹ en la década de 1980 que organiza las entradas en el directorio de manera jerárquica, y con una alta capacidad de almacenamiento de datos, proporcionando grandes facilidades de búsqueda y una arquitectura fácilmente escalable. X.500 especifica que la comunicación entre el cliente y el servidor debe emplear el *Directory Access Protocol* (DAP), pero DAP es un protocolo a nivel de aplicación, por lo que tanto el cliente como el servidor debían implementar completamente la pila de protocolos OSI.

¹ ITU por sus siglas en inglés.

LDAP (*Lightweight Directory Access Protocol*) surge como una alternativa a DAP. Se trata de una serie de estándares del *Internet Engineering Task Force*² definidos en varios RFC. La versión más reciente es la v3 y está publicada como el RFC 4510. Las claves del éxito de LDAP en comparación con DAP de X.500 son:

- LDAP utiliza TCP/IP en lugar de los protocolos OSI. TCP/IP requiere menos recursos y está más disponible.
- LDAP representa la información mediante cadenas de caracteres en lugar de complicadas estructuras ASN.1.
- El modelo funcional de LDAP es más simple y ha eliminado opciones raramente utilizadas en X.500, por lo que es más fácil de comprender e implementar.

LDAP define el contenido de los mensajes intercambiados entre un cliente y un servidor LDAP. Los mensajes especifican las operaciones requeridas por el cliente, las respuestas del servidor y los datos transportados en el mensaje. Un ejemplo de interacción general entre un cliente y un servidor LDAP tiene la siguiente forma:

- El cliente establece una sesión con el servidor LDAP. Se conoce como *binding*. El cliente especifica el nombre de host y el puerto dónde escucha el servidor.
- El cliente puede proporcionar un nombre de usuario y contraseña para autenticarse contra el servidor o establecer una sesión anónima con los derechos de acceso por defecto.
- El cliente realiza operaciones sobre los datos del directorio. LDAP ofrece capacidades de lectura y actualización. También posee capacidades de búsqueda de datos en el directorio a través de criterios especificados por el usuario. Las búsquedas son operaciones

² IETF por sus siglas en inglés.

frecuentes en el directorio y se llevan a cabo con ayuda de los filtros de búsquedas.

- Cuando el cliente termina de hacer peticiones, cierra la sesión con el servidor. Esto también se conoce como *unbinding*.

Además de definir el protocolo de acceso al directorio, el estándar LDAP define cuatro modelos que permiten entender mejor el servicio de directorio.

2.1.1 El modelo de información

El modelo de información describe la estructura de la información almacenada en un directorio LDAP. La unidad básica de información almacenada en el directorio es la entrada (entry). Generalmente una entrada representa un objeto del mundo real (una persona, un servidor, etc.), pero el modelo no exige este aspecto.

Una entrada se compone de un conjunto de atributos, cada uno de ellos tiene un tipo y uno o varios valores. El tipo define la clase de información que va a almacenar y los valores son la información en si. Además los atributos tienen un identificador de objeto (OID) y una sintaxis que indica que valores puede contener y como se hacen las comparaciones.

- Ejemplo de atributos: cn: Manuel Rodríguez, ou: VENTAS.

Los esquemas (schemas) definen el tipo de objetos que se van a almacenar en el directorio, también contiene los atributos que tienen estos objetos y si son opcionales u obligatorios.

Dado que cada servidor puede definirse su propio esquema, para permitir la interoperabilidad entre distintos servidores de directorio, se espera que un esquema común sea estandarizado (RFC 2252 y RFC 2256).

2.1.2 El modelo de nombrado

El modelo de nombrado de LDAP define como se organizan y se referencian los datos, es decir, define los tipos de estructuras que se pueden definir utilizando las entradas. Una vez organizadas las entradas formando una determinada estructura, el modelo de nombrado nos indica como referenciar estas entradas.

Las entradas en el directorio describen objetos (una impresora, un usuario, etc.), tienen asociado un identificador llamado *Distinguished Name* (DN) que los identifica unívocamente y se organizan en una estructura de árbol conocida como *Directory Information Tree* (DIT).

A su vez un DN consiste en una secuencia de trozos de información más pequeños conocidos como *Relative Distinguished Name* (RDN). En la estructura de árbol el RDN se correspondería con una rama y el DN se obtendría al seguir todo el árbol desde la raíz a una hoja.

Generalmente el DN se representa mediante una secuencia de RDNs separados por comas. Ejemplo:

- “cn=Pedro Pérez, ou=VENTAS, o=empresa, c=es”.

De este modo, no puede haber ninguna entrada suelta, solo la entrada raíz puede no tener entrada padre. En el caso de añadir una entrada en un punto inexistente en el directorio, el servidor devolverá un mensaje de error y no realizará la operación.

Esta flexibilidad permite que el directorio almacene la información de la forma más conveniente, se puede crear un grupo que contenga todas las personas de la organización y otro que contenga todos los grupos o se puede elegir una estructura que refleje la estructura jerárquica de la organización.

2.1.3 El modelo funcional

El modelo funcional describe que operaciones se pueden llevar a cabo sobre la información almacenada en el directorio LDAP. Estas operaciones se pueden agrupar en tres categorías principales:

- **Autenticación:** *bind, unbind* son operaciones utilizadas para conectar y desconectar con el servidor LDAP, establecer derechos de acceso y proteger la información. Se puede securizar una sesión a varios niveles, eligiendo entre una sesión anónima, una sesión autenticada y una sesión autenticada utilizando mecanismos SASL (*Simple Authentication and Security Layer*).
- **Consultas:** es la operación más utilizada. Se pueden hacer búsquedas y comparar información por diversos criterios especificados por el usuario. Las búsquedas se pueden acotar estableciendo un punto de partida en el DIT (*baseDN*), la profundidad a buscar a partir desde el punto de partida (*scope*), los atributos que nos interesan, etc. El elemento clave en las consultas es la definición de filtros de búsqueda (*search Filter*). Los filtros de búsqueda tienen una sintaxis propia que se debe seguir: Ejemplo de filtro: `(|(sn=León)(sn=Castilla))` obtendría las entradas en las que el apellido sea Castilla o León.
- **Actualización:** permite las operaciones de añadir, modificar y borrar las entradas (*add, delete, modify*).

2.1.4 El modelo de seguridad

El modelo de seguridad describe como la información del directorio puede ser protegida contra accesos no autorizados. El modelo de seguridad se

centra en la operación de *bind*. Hay varias formas de inicio de sesión por parte de un usuario:

- Puede iniciar una sesión de forma anónima con los permisos por defecto.
- Puede iniciar una sesión con un nombre de usuario y contraseña en claro.
- En LDAPv2 solo se permiten sesiones anónimas y autenticación mediante texto en claro, debido a esto algunos fabricantes incorporaron mecanismos de seguridad adicionales, como Kerberos..
- La operación bind de LDAPv3 tiene soporte para Simple Authentication Security Layer (SASL), además se han definido operaciones extendidas, una de ellas relacionada con la seguridad es la Extension for Transport Layer Security (TLS) for LDAPv3.

3 GESTION DE IDENTIDADES Y SINGLE SIGN-ON

Un sistema de gestión de identidades integra políticas y procesos organizacionales destinados a simplificar y controlar el acceso a los sistemas de información y a las instalaciones de una organización por parte de empleados y otras entidades autorizadas. La gestión de identidades persigue la definición de una identidad para cada usuario (persona o proceso), que llevará asociados una serie de atributos.

El concepto central de un sistema de gestión de la identidad es el uso de lo que se conoce como *single sign-on* (SSO). El SSO habilita a un usuario para acceder a todos los recursos de la red después de una única autenticación.

Los principales aspectos que debe cubrir un sistema de gestión de la identidad son los siguientes:

- **Autenticación:** confirmación de que la identidad se corresponde con el nombre de usuario que se proporciona.
- **Autorización:** capacidad de proporcionar permisos para servicios y recursos específicos basándose en la autenticación.
- **Trazabilidad:** proceso que se encarga de registrar accesos y autorizaciones.
- **Aprovisionamiento:** inscripción de usuarios en el sistema
- **Automatización de flujos de trabajo:** movimiento de datos en procesos de negocio.
- **Administración delegada:** el uso de control de accesos basado en roles para proporcionar acceso a recursos.
- **Sincronización de contraseñas:** creación de un proceso para acceder por medio de SSO. *Single sing-on* habilita a un usuario para acceder a todos los recursos del sistema después de una autenticación sencilla.
- **Servicio de reseteo de contraseñas:** capacidad que permite a un usuario cambiar su contraseña.
- **Federación:** proceso por el cual la autenticación y permisos son pasados de un sistema a otro, generalmente a través de diferentes organizaciones, reduciendo así el número de autenticaciones necesarias para el usuario.

En la Figura 1, se pueden ver los elementos que conforman una arquitectura genérica de gestión de la identidad:



- **Principales:** un *principal* es un contenedor de identidad. Típicamente es un usuario que intenta acceder a los servicios y recursos de la red. Dispositivos de usuario, procesos agente y sistemas servidor pueden ser también *principals*. Los *principals* se autentican contra un proveedor de identidad.
- **Proveedor de identidad:** asocia información de autenticación con un *principal*, así como atributos y uno o más identificadores.
- **Servicio de atributos:** las identidades digitales incorporan más atributos que un identificador e información de autenticación. El servicio de atributos gestiona la creación y mantenimiento de estos atributos. Por ejemplo: un usuario que necesita proporcionar una dirección cada vez que entra en una Web de compras. El servicio de gestión de identidad permite proporcionar esta información una sola vez, y será aportada a los consumidores de datos de acuerdo con las políticas de privacidad y autorización establecidas.
- **Consumidores de datos:** son entidades que obtienen y emplean datos gestionados y proporcionados por los proveedores de atributos, y generalmente son utilizados para llevar a cabo decisiones de autorización y auditoria. Por ejemplo un servidor de base de datos es un consumidor de datos que necesita las credenciales del cliente para saber que niveles de acceso debe proporcionarle.

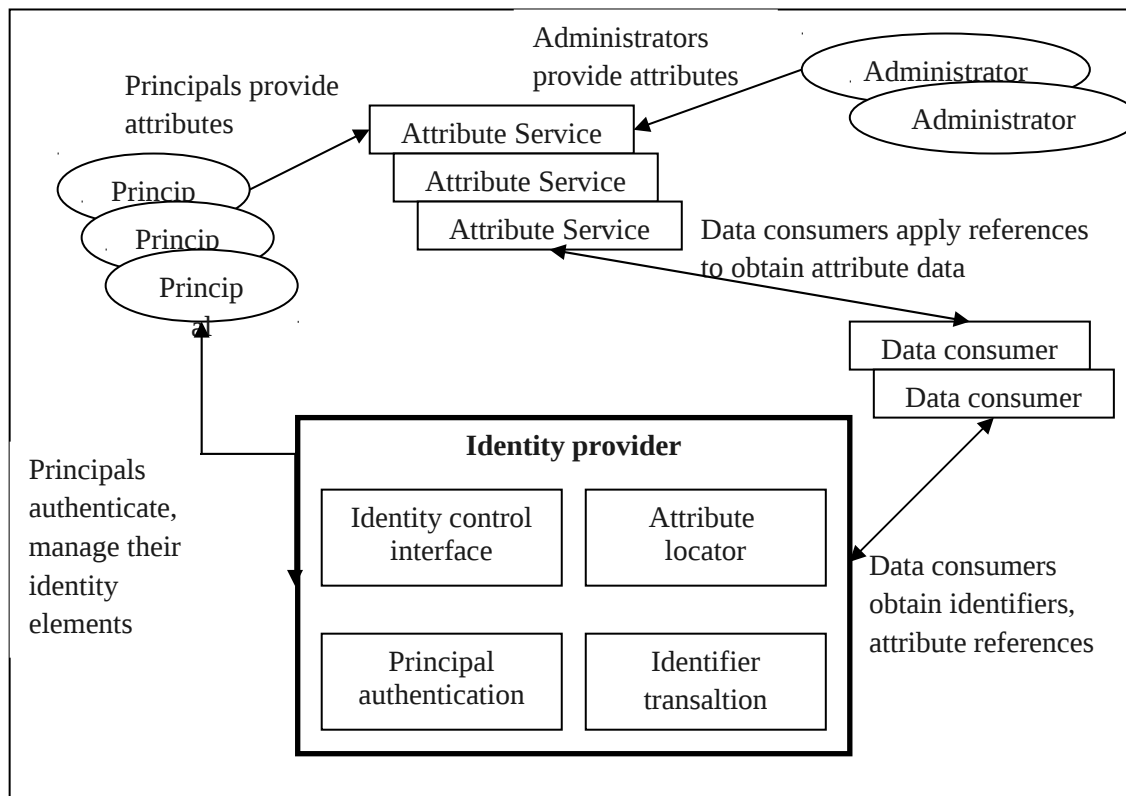


Figura 1: Arquitectura genérica de gestión de la identidad

3.1 Gestión federada de identidades

La federación de identidades es en esencia, la extensión de la gestión de la identidad a múltiples dominios de seguridad. Dichos dominios incluyen unidades internas de negocio, socios de negocio externos y otras aplicaciones y servicios de terceros. El objetivo es proporcionar el intercambio de identidades digitales para que un usuario pueda ser autenticado una sola vez y después pueda acceder a recursos a través de múltiples dominios. Debido a que estos dominios son relativamente autónomos o independientes, no es posible un control centralizado. Sin embargo, las organizaciones colaboradoras deben formar una federación, basada en estándares y niveles de confianza mutua para compartir de forma segura las identidades digitales.

La gestión federada de identidades se refiere a los acuerdos, normas y tecnologías que permiten la portabilidad de las identidades, atributos de identidad, y derechos, a través de múltiples organizaciones y aplicaciones y con la participación de muchos usuarios. Cuando varias organizaciones implementan un esquema de interoperabilidad de identidad federada, un empleado en una organización puede usar un único inicio de sesión, para acceder a servicios a través de la federación mediante relaciones de confianza asociadas a la identidad.

Más allá del SSO, la gestión de identidad federada ofrece otras capacidades: una de ellas es que proporciona un medio estandarizado de representar atributos. Normalmente, las identidades digitales incorporan más atributos que un simple identificador e información de autenticación. Ejemplos de atributos son los números de cuenta, roles en la organización, ubicación física, y propietarios de archivos. Un usuario puede tener múltiples identificadores; por ejemplo, cada identificador puede estar asociado a un único rol, con sus propios permisos de acceso.

La Figura 2 ilustra las entidades y flujos de datos en una arquitectura genérica de gestión federada de la identidad:

1. El navegador del usuario final u otras aplicaciones inician un diálogo con un proveedor de identidad (IdP) en el mismo dominio. El usuario final también proporciona valores de atributos asociados con su identidad.
2. Algunos atributos asociados con la identidad, como por ejemplo roles permitidos, pueden ser proporcionados por un administrador en el mismo dominio.
3. Un proveedor de servicios (SP) en un dominio remoto al que el usuario desea acceder, obtiene el identificador de la identidad, información de autenticación, y atributos asociados desde el proveedor de identidad en el dominio de origen.

4. El proveedor de servicio (SP), abre una sesión con el usuario remoto y refuerza las restricciones de control de acceso basándose en la identidad y atributos del usuario.

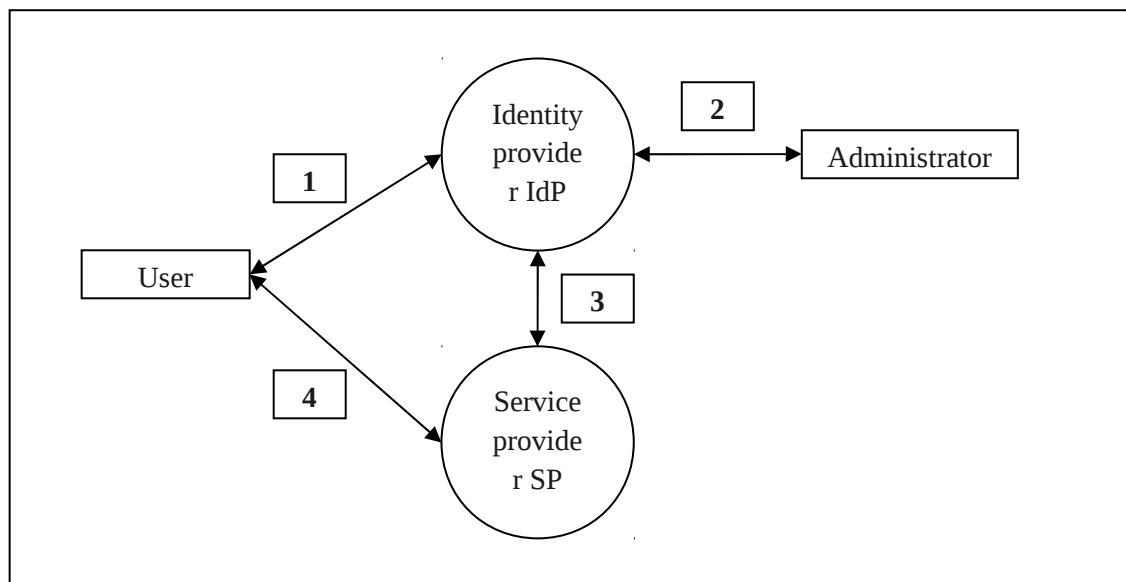


Figura 2: Modo de operación de una federación de identidades

Existe un amplio número de soluciones en el campo de la gestión federada de identidades. Hay estándares abiertos desarrollados por grandes consorcios, soluciones propietarias desarrolladas por compañías privadas y proyectos *opensource* de menor escala. Algunos ejemplos son:

- **SAML:** *Security Assertion Markup Language* es un estándar basado en XML desarrollado por OASIS (*Organisation for the Advancement of Structured Information Standards*). La versión actual es la 2.0 y fue reconocida como estándar en 2005. (<http://www.oasis-open.org/>)
- **OpenID:** es un estándar abierto desarrollado por la *OpenId Foundation*. (<http://openid.net/foundation/>)
- **Shibboleth:** Es un proyecto del consorcio *Internet2*, que proporciona una arquitectura y una implementación *opensource* de un sistema de gestión de la identidad federado basado en SAML. La versión más



reciente de su proveedor de identidad es la 2.3.0 y data de 2011.
(<http://shibboleth.internet2.edu/>)

- **WS-Federation:** Es un Framework desarrollado por varios fabricantes entre los que destacan IBM y Microsoft. Su especificación mas reciente es la 1.1 y data de 2006.
(<http://www.ibm.com/developerworks/library/specification/ws-fed/>)
- **Liberty Identity Federation Framework (ID-FF):** Es un Framework de gestión federada de la identidad, desarrollado por un consorcio formado por más de 150 empresas y organizaciones y conocida con el nombre de Liberty Alliance.

4 TIPOS DE CONECTIVIDAD. ACCESO REMOTO. VPN.

El acceso remoto es la capacidad de un usuario de obtener acceso a un servidor o a una red desde una localización remota. Personal en delegaciones de la organización, teletrabajadores o personal que está viajando pueden necesitar acceder a la red corporativa. Hay varias formas de conectar el equipo o red remota con la red corporativa:

- Los usuarios que trabajan desde casa consiguen acceso a Internet a través de un proveedor de servicios de Internet (ISP). Una forma de conectarse es por medio de conexiones desde un portátil o equipo de sobremesa con ayuda de líneas DSL y cable módem con ayuda de VPNs.
- Otra alternativa basada en el uso de VPN es la que pueden utilizar los usuarios que están viajando y no disponen de una conexión cableada. Para ello se pueden valer de conexiones inalámbricas (Wifi, Wimax) proporcionadas por dispositivos móviles preparados

para gestionar este tipo de conexiones. También pueden acceder con ayuda de conexiones de datos de telefonía móvil.

- El uso de un enlace privado, entre una red remota y la red corporativa es una opción útil para por ejemplo conectar la sede de una organización con sus delegaciones. Los enlaces privados suelen ser más caros, pero ofrecen mayor fiabilidad y ratios de transferencia más elevados. Ejemplos de tecnologías que proporcionan enlaces privados son ATM, Frame Relay, Clear Channel, RDSI, Fibra óptica.
- La utilización de radio enlaces de larga distancia o conexiones vía satélite es otra forma de comunicar una red remota con la red de la organización.

Para acceder remotamente de una forma segura a la red de la organización, son necesarias algunas capacidades básicas relacionadas con la seguridad en los sistemas de acceso remoto:

- **Control de acceso a la red:** la primera línea de defensa, en la seguridad de acceso remoto, es el control de acceso para prevenir que accedan los intrusos no deseados. Para ello se define una política de seguridad que describe como se puede acceder de forma segura a la red. Ejemplos de esto son los portales cautivos, el uso del protocolo 802.1X, etc.
- **Autenticación de usuarios y autorización:** es la segunda línea de defensa y asegura que la autenticidad de un usuario mediante el uso de protocolos de autenticación.
- **Protección de la conexión e integridad del tráfico:** una vez que se establece una sesión, es necesario asegurar la confidencialidad e integridad del tráfico intercambiado entre las partes.

No hay estándares formales definidos específicamente para explicar como debe ser una arquitectura de acceso remoto, porque cada organización tiene sus características y requisitos de acceso remoto. Sin embargo, hay componentes funcionales que se convierten en estándares de facto en un despliegue típico de acceso remoto. Los componentes clave que deberían ser tenidos en cuenta en una arquitectura de acceso remoto típica son los siguientes:

- **Firewall:** es un conjunto de tecnologías hardware y software instaladas estratégicamente entre las redes privadas de la compañía y una o más redes no seguras (incluida Internet).
- **Zona desmilitarizada (DMZ):** es un elemento común en la mayoría de despliegues de cortafuegos. Es utilizada para proporcionar una zona diferenciada entre los equipos de la red privada que no tienen acceso desde el exterior y los servidores que si tienen conexión exterior. En esta red hay servidores bastión que actúan como intermediarios entre los accesos remotos y la organización. Ejemplos de este tipo de servidores son los proxies y los servidores de autenticación.
- **Servidor de acceso remoto (RAS):** es un servidor que actúa de puerta de enlace entre el cliente remoto y la red, en arquitecturas de conexión mediante enlaces conmutados analógicos y/o digitales (p.ej: RDSI). Una vez que un usuario remoto establece la conexión por medio de una llamada, la línea telefónica es transparente para el usuario, y puede acceder a los recursos de la red interna.
- **Servidor Proxy:** es un servidor, que actúa como intermediario entre un usuario remoto y las aplicaciones y servicios internos de la organización a los que desea acceder. De esta manera la empresa puede garantizar la seguridad de las aplicaciones internas, el control administrativo y tener capacidades de caché (por ejemplo en accesos

vía Web). La autenticación del usuario puede ser hecha por el propio Servidor Proxy o por un servidor de autenticación.

- **Servidor de autenticación:** es el encargado de verificar la identidad de los usuarios que intentan acceder a la red privada de la organización.

4.1 Virtual Private Networks (VPN)

Las redes privadas virtuales (VPN), proporcionan una forma segura de conectarse desde una ubicación remota con una red de área local privada (LAN) a través de Internet o cualquier otra red pública no segura. Una VPN es una conexión que tiene la apariencia y muchas de las ventajas de un enlace dedicado pero trabajando sobre una red pública. Para esto se utiliza una técnica llamada *tunneling* que permite enrutar los paquetes de datos por la red pública en un túnel privado que simula una conexión punto a punto. Las VPN son utilizadas frecuentemente por los trabajadores remotos o empleados en las delegaciones de la organización, para compartir datos y recursos de la red privada. Una red privada virtual puede proporcionar los siguientes beneficios para la organización:

1. **Seguridad mejorada:** al reducir el número de conexiones con el mundo exterior se reduce considerablemente la posibilidad de un ataque. Además también se reduce la posibilidad de interceptación del tráfico.
2. **Rendimiento predecible:** en VPNs con canales dedicados se puede garantizar el ancho de banda entre los sitios y el rendimiento de la red se hace más predecible.
3. **Independencia en la elección de las tecnologías de transporte para las redes de usuarios:** las posibilidades están limitadas por la elección de un proveedor o fabricante. Así la organización puede usar

Ethernet, Frame Relay, IP y otras tecnologías de red para conectar sus sitios.

- 4. Espacio de direcciones IP independiente:** en las redes privadas es posible utilizar cualquier direccionamiento. Por ejemplo, casi todos los servicios de VPN permiten el uso de direcciones IP privadas tales como 10.0.0.1 o 192.168.0.3, que no pueden ser enrutadas a través de las redes públicas.

Estas características serán de utilidad para algunos usuarios, pero de importancia relativa para otros. Las vulnerabilidades y bajo rendimiento de las redes públicas pueden hacer que la “seguridad mejorada” y “rendimiento predecible” sean las características más deseables de una VPN. Recientemente, la “independencia de elección de tecnología” y el “espacio de direcciones independiente” parece que se han vuelto menos importantes: el primero debido a la dominación de las tecnologías Ethernet en capa 2 e IP en capa 3. La segunda debido a que con la implantación de IPv6 se espera acabar con el déficit de direcciones. De todas formas, tener un espacio de direcciones independiente mejora la seguridad, utilizando rangos de direcciones para separar sitios dentro de la organización y restringir accesos.

A la hora de crear una VPN para proporcionar acceso remoto, hay que escoger la tecnología que mejor se adapte al escenario en cuestión. Esta elección de tecnología implica técnicas de *tunneling*, autenticación, control de acceso y seguridad de datos. Generalmente se definen tres arquitecturas principales de VPN:

- **Intranet VPN (LAN-to-LAN VPN):** en este escenario las redes remotas de la organización son conectadas entre sí utilizando la red pública, convirtiéndose de esta manera en una única red LAN corporativa global.

- **VPN de acceso remoto:** en este tipo de VPNs se ubicarían los usuarios que desde un host remoto crean un túnel para conectarse a la red privada de la organización. El dispositivo remoto puede ser un equipo personal con un software cliente para crear VPN, y usar una conexión conmutada o una conexión de banda ancha permanente.
- **Extranet VPN:** este tipo de arquitecturas permiten que ciertos recursos de la red privada de la organización sean accedidos por redes de otras compañías, tales como clientes o proveedores. En este escenario es fundamental el control de acceso.

Hay una amplia variedad de tecnologías que se pueden utilizar para la implementación de VPNs. Los criterios que deben cumplir estas tecnologías son:

- **Seguridad:** las conexiones deben ser brindadas cumpliendo con los requisitos de autenticación, autorización, privacidad, integridad y contabilidad.
- **Eficiencia:** los tiempos de respuesta deben ser adecuados y comparables con las redes consideradas “no seguras.”
- **Facilidad de administración:** los usuarios y administradores de este tipo de redes, pueden hacer su trabajo de una manera rápida y efectiva.
- **Cumplimiento de estándares e interoperabilidad:** hay muchas tecnologías que son estándares y que participan en la creación de VPNs: IPSec, MD5, SOCKSv5, IKE, ISAKMP, Diffie-Hellman, X.509, RADIUS, etc.

Para clasificar las tecnologías que se pueden utilizar en la implementación de una arquitectura de VPN, se puede tomar como referencia el modelo OSI y ubicarlas en función del nivel en el que son implementadas. La Figura 3

muestra los principales protocolos utilizados para el establecimiento de conexiones VPN y su ubicación en el modelo de referencia OSI.

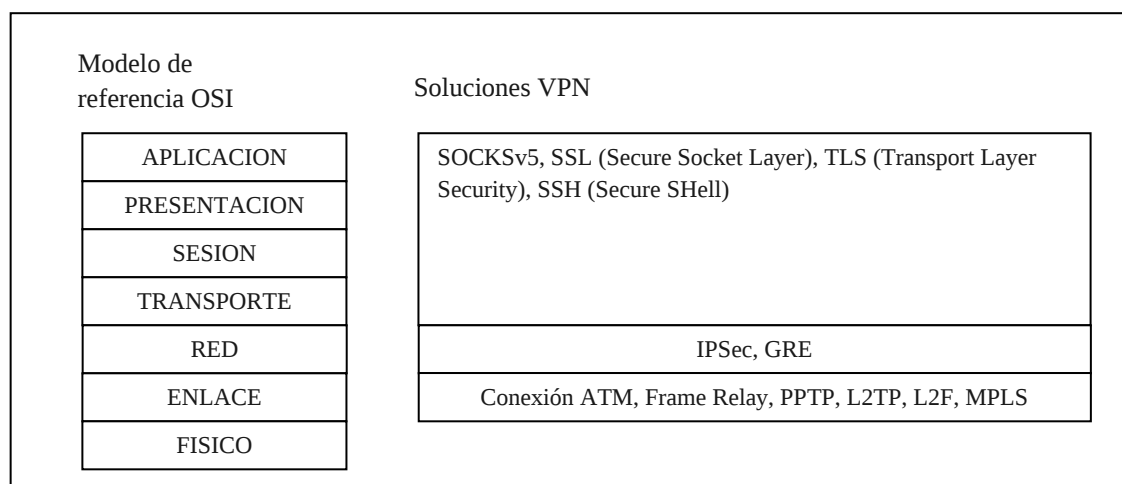


Figura 3: Ubicación de las soluciones VPN en el modelo de referencia OSI

A la hora de implementar una arquitectura de red basada en VPN hay dos posibles opciones. Hacer una implementación por hardware o por software.

Las implementaciones por Hardware realizan el proceso de encriptación y desencriptación del tráfico a nivel físico entre los extremos de la línea de comunicación. Los dispositivos utilizados normalmente son routers con capacidades de VPN incorporadas. Como ventajas de esta solución se puede decir que la instalación y configuración son relativamente sencillas, no se necesita personal especializado y su mantenimiento es mínimo. Por el contrario presentan el inconveniente de que el sistema de encriptación viene impuesto por el fabricante y se depende del mismo para las actualizaciones.

Por otro lado las implementaciones basadas Software se están imponiendo cada día más. La explicación radica en que, la necesidad de los usuarios pequeños y medianos de implantar sistemas de seguridad en el acceso a sus máquinas va en aumento. Las implementaciones software son mucho

más baratas que comprar hardware preparado para VPNs y existe un gran número de VPNs desarrolladas por software. Como inconvenientes de esta aproximación se puede decir que es necesaria una máquina para dar soporte a la solución, el sistema de claves y certificados reside en máquinas potencialmente inseguras y en los casos que se utilice software de libre distribución puede ser que tenga puertas traseras u otras deficiencias de seguridad.

4.2 SSL/TLS

SSL/TLS son los acrónimos de *Secure Sockets Layer/Transport Layer Security*. El protocolo SSL es desarrollado en 1995 por Netscape. Se basa en una arquitectura cliente/servidor y fue diseñado originalmente para permitir el intercambio de información seguro entre un servidor Web y un navegador. Hoy en día el IETF mantiene el desarrollo de TLS como un protocolo estándar de Internet. La versión más reciente TLS 1.2 está definida en el RFC 5246 y fue publicada en 2008.

SSL es un protocolo que proporciona autenticación y confidencialidad entre los extremos de la comunicación mediante el uso de criptografía. Cuando se establece una comunicación por SSL, habitualmente sólo el servidor es autenticado, aunque es posible la identificación mutua mediante el despliegue de una infraestructura de claves públicas (PKI). SSL implica una serie de fases básicas:

- Negociar entre las partes el algoritmo que se empleará en la comunicación.
- Intercambio de claves públicas y autenticación basada en claves públicas.
- Encriptación del tráfico por medio del uso de cifrado simétrico.

Durante la primera fase, se negocian los algoritmos criptográficos que se van a usar entre el cliente y el servidor:

- Protocolos de clave pública: RSA, DSA, Diffie-Hellman, etc.
- Protocolos de cifrado simétrico: DES, 3DES, IDEA, AES, RC2, etc.
- Funciones resumen: MD5 o familia SHA.

SSL/TLS proporcionan un abanico amplio de medidas de seguridad:

- Se numeran todos los registros usando el número de secuencia en el MAC (*Message Authentication Code*).
- Se usa un resumen de mensaje mejorado con una clave (sólo se puede comprobar el MAC con dicha clave).
- Proporcionan protección contra varios ataques conocidos (por ejemplo: *man-in-the-middle-attack*).
- Al finalizar la conexión se envía en el mensaje un hash de todos los datos intercambiados y vistos por ambas partes.

SSL se ejecuta en una capa entre los protocolos de aplicación como HTTP, SMTP, NNTP y sobre la capa de transporte TCP del protocolo TCP/IP. Aunque puede proporcionar seguridad a cualquier protocolo que utilice conexiones de confianza (tal como TCP), se usa en la mayoría de los casos junto a HTTP para formar HTTPS. Otra aplicación en la que se puede utilizar SSL es en el *tunneling* de una red completa y poder crear así una VPN, como se hace por ejemplo con *OpenVPN*.

4.3 Secure Shell: SSH

Secure Shell o SSH es un protocolo de red que permite el intercambio de datos entre dos dispositivos conectados a la red utilizando un canal seguro.

Las dos principales versiones del protocolo son conocidas como SSH1 y SSH2. Se usa principalmente en entornos UNIX y Linux para acceder a consolas remotas. Fue creado en el año 1995 por el investigador de la Universidad de Helsinki Tatu Ylönen y su principal objetivo era proporcionar una alternativa segura para Telnet y otros intérpretes de comandos remotos. En el año 2006 se convierte en un estándar del IETF descrito en el RFC 4253. La definición de su arquitectura incluye tres protocolos apilados en las capas de transporte y aplicación:

- *SSH Connection Protocol*: en este protocolo se define el concepto de canales, peticiones de canal y peticiones globales que los servicios SSH proporcionan.
- *SSH User Authentication Protocol*: en este protocolo se maneja la autenticación de clientes y se proporcionan varios métodos de autenticación. Algunos de los métodos utilizados son: el uso de contraseñas ordinarias, autenticación de clave pública basada en DSA, RSA y certificados X.509, Kerberos, etc.
- *SSH Transport Layer Protocol*: este protocolo maneja el intercambio inicial de claves, así como la autenticación del servidor, el establecimiento del tipo de cifrado, compresión y verificación de integridad.

El uso de SSH se extendió y puede ser utilizado por un amplio número de aplicaciones sobre múltiples plataformas incluidas UNIX, Windows, MAC OS y Linux:

- Transferencia segura de ficheros utilizando las aplicaciones SCP y SFTP.
- Sistemas de ficheros en red: SSHFS. Es una alternativa a NFS, en la que el cliente no necesita que el servidor exporte un directorio por NFS, le basta tener acceso por SSH.



- *Port forwarding*: Permite una comunicación segura sobre red una insegura, muy similar a una VPN, pero trabajando con un único puerto.
- *OpenSSH* desde la versión 4.3 permite hacer verdaderas VPN (todos los puertos), tanto en nivel de enlace como nivel de red.

En el mercado existen diversas implementaciones:

- *ssh* original con licencia freeware.
- *OpenSSH*, desarrollada originalmente para OpenBSD, portada a muchos otros SO, es la versión más empleada.
- *Dropbear*, es una versión reducida, habitual en sistemas empuotrados como OpenWRT.
- En Microsoft Windows se puede utilizar el servidor *CopSSH* y el cliente *Putty*.

REFERENCIAS

- **FUNG, K. T.** (2005). Network security Technologies. Second Edition. AUERBACH PUBLICATIONS.
- **STALLINGS, W.** (2011). Network Security Essentials. Applications and Standards. Fourth Edition. Prentice Hall.
- Curso de Extensión Universitaria "Ferramentas de seguridade en GNU/Linux" (terceira edición) - Escola Superior de Enxeñaría Informática da Universidade de Vigo - (<http://ccia.ei.uvigo.es/curso2010/index.html>)
- Apuntes de la asignatura Diseño y Administración de Sistemas y Redes – Ingeniería Informática – Universidad Rey Juan Carlos. (http://gsyc.escet.urjc.es/~mortuno/index_dasr.html).

(Todos los enlaces fueron verificados en Junio de 2011)

Autor: Juan Otero Pombo
Ingeniero en Informática en el Concello de Ourense
Colegiado del CPEIG

**45. SEGURIDAD EN REDES WAN
E INTERNET: CRIPTOGRAFÍA Y
AUTENTICACIÓN.
ARQUITECTURA DE
SEGURIDAD EN REDES.
SISTEMAS DE AUTENTICACIÓN
PARA SEGURIDAD EN REDES.
ELEMENTOS DE SEGURIDAD
PARA INTERNET.
TELECOMUNICACIONES.**

Tema 45. Seguridad en redes WAN e Internet: criptografía y autenticación. Arquitectura de seguridad en redes. Sistemas de autenticación para seguridad en redes. Elementos de seguridad para Internet.

INDICE

1 ARQUITECTURA DE SEGURIDAD EN REDES.....	3
1.1 Arquitectura de seguridad en el modelo OSI.....	4
1.2 Mecanismos de seguridad.....	5
1.3 Servicios de Seguridad.....	7
1.4 Ataques contra la seguridad.....	9
2 SEGURIDAD EN REDES WAN E INTERNET: CRIPTOGRAFIA Y AUTENTICACION.....	12
2.1 Mecanismos criptográficos de autenticación.....	13
2.1.1 Checksum criptográfico.....	13
2.1.2 Técnicas de cifrado.....	14
2.1.3 Funciones resumen.....	15
3 SISTEMAS DE AUTENTICACION PARA SEGURIDAD EN REDES.....	17
3.1 Distribución de claves utilizando criptografía simétrica.....	18
3.2 Distribución de claves utilizando criptografía asimétrica.....	19
3.3 Protocolos y métodos de autenticación en red.....	20
3.4 Protocolos de seguridad en Internet.....	21
3.4.1 Kerberos.....	21
3.4.2 PGP.....	23
4 ELEMENTOS DE SEGURIDAD PARA INTERNET	25
4.1 Cortafuegos.....	25
4.1.1 Características de un cortafuegos.....	26
4.1.2 Tipos de cortafuegos.....	26
4.1.3 Localizaciones del Cortafuegos y configuraciones.....	27
4.2 Sistemas de detección de intrusiones.....	28

REFERENCIAS.....	30
------------------	----

1 ARQUITECTURA DE SEGURIDAD EN REDES

La irrupción de los sistemas informáticos en las organizaciones provocado un cambio importante en el modo de garantizar la **seguridad de la información**. Antes del uso extendido de los sistemas informáticos, la documentación sensible se encontraba en soporte papel por lo que la seguridad de la información para la organización, era provista en un sentido físico y administrativo. Un claro ejemplo de esto eran, los armarios con cerradura de combinación utilizados para almacenar los documentos con información sensible y los procesos de selección utilizados para incorporar nuevo personal.

La implantación de los sistemas informáticos trajo consigo la necesidad de herramientas automatizadas para la protección de archivos y otra información almacenada en los sistemas. En la actualidad, la información se encuentra almacenada en sistemas compartidos y distribuidos que ofrecen la posibilidad de acceder a ella a través de una red privada de ordenadores o a través de Internet. Las **medidas de seguridad en la red** son el conjunto de medidas adoptadas para proteger los datos durante la transmisión a través de redes no seguras. Sin embargo, debido a que la práctica totalidad de empresas, gobiernos y organizaciones académicas tienen interconectados sus sistemas informáticos con una colección de redes que a su vez están interconectadas entre sí, dando lugar a lo que conocemos como Internet, es más frecuente el uso del término **seguridad en Internet**. La seguridad en internet abarca la prevención, detección y corrección de violaciones de la seguridad que puedan afectar a la transmisión de información.

El *Computer Security Handbook* del NIST [NIST95] define el término **computer security** como la protección conferida a un sistema informático con el fin de alcanzar los objetivos de preservar la integridad, disponibilidad

y confidencialidad de los recursos de información del sistema (incluyendo hardware, software, firmware, información/datos y telecomunicaciones). Esta definición abarca los objetivos centrales de la seguridad de los sistemas de información: confidencialidad, integridad, disponibilidad, autenticación y trazabilidad.

1.1 Arquitectura de seguridad en el modelo OSI

Si la seguridad en entornos de procesamiento de datos cerrados es compleja, el uso de redes de área local y extensa aumenta esa complejidad de forma considerable. Es por esto que el administrador responsable de la seguridad de una organización necesita alguna metodología que le permita definir los requisitos de seguridad e identificar los mecanismos que le permitirán cumplirlos. Esta metodología deberá facilitar la cobertura efectiva de las necesidades de seguridad de la organización así como la evaluación y posterior elección de los distintos productos y políticas.

UIT-T¹ Recomendación X.800, *Security Architecture for OSI*, describe los servicios de seguridad básicos que pueden ser aplicados cuando es necesario proteger la comunicación entre sistemas. Aunque se trata de un modelo genérico definido en los años 90, sus conceptos y definiciones aún siguen vigentes en el día a día de los administradores de la seguridad. La arquitectura de seguridad del modelo OSI es útil para los administradores, ya que establece un protocolo para organizar la tarea de proporcionar seguridad. Además, como esta arquitectura fue desarrollada como un estándar internacional, los fabricantes de computadoras y sistemas de comunicación, han añadido características de seguridad a sus productos y servicios que se relacionan con esta definición estructurada de mecanismos y servicios. El modelo OSI de arquitectura de la seguridad se centra en los siguientes conceptos: **mecanismos de seguridad, servicios de**

¹ UIT-T son las siglas de la Unión Internacional de las Telecomunicaciones, Sector de Estandarización de las Telecomunicaciones que es una agencia patrocinada por las Naciones Unidas, que desarrolla estándares, llamadas Recomendaciones, relacionadas con las Telecomunicaciones.

seguridad y ataques contra la seguridad. Se pueden definir de manera resumida:

- **Mecanismos de seguridad:** serán los procesos que permiten detectar, prevenir, o recuperarse frente a un ataque contra la seguridad.
- **Servicios de seguridad:** un servicio de comunicación o procesado que incrementa la seguridad de los sistemas de información y las transferencias de datos realizadas por una organización. Los servicios intentan prevenir los ataques contra la seguridad haciendo uso de uno o varios mecanismos de seguridad.
- **Ataques contra la seguridad:** cualquier acción que atenta contra la seguridad de la información de la organización.

1.2 Mecanismos de seguridad

Los mecanismos de seguridad en X.800 se dividen en los que se aplican a una capa de protocolo específico y los que no son específicos de una capa de protocolo o servicio de seguridad (conocidos también como mecanismos de seguridad persistentes).

Mecanismos específicos de seguridad: pueden ser incorporados en una de las capas del protocolo con el fin de proporcionar alguno de los servicios de seguridad OSI:

- **Autenticación:** corrobora que una entidad, ya sea origen o destino de la información, es la deseada, por ejemplo, A envía un número aleatorio cifrado con la clave pública de B, B lo descifra con su clave privada y se lo reenvía a A, demostrando así que es quien pretende ser. Por supuesto, hay que ser cuidadoso a la hora de diseñar estos protocolos, ya que existen ataques para desbaratarlos.

- **Control de accesos:** esfuerzo para que sólo aquellos usuarios autorizados accedan a los recursos del sistema o a la red, como por ejemplo mediante las contraseñas de acceso.
- **Firma digital:** consiste en adjuntar una serie de datos a un mensaje o realizar una transformación criptográfica que permita al receptor comprobar el origen de un mensaje y verificar su integridad.
- **Cifrado:** consiste en la transformación de la información, por medio del uso de algoritmos matemáticos, a un formato que no es inteligible. La transformación y recuperación de la información depende de un algoritmo de cifrado y/o del uso claves de cifrado.
- **Notarización:** el uso de un tercero de confianza para asegurar ciertas propiedades en un intercambio de datos.
- **Integridad:** conjunto de mecanismos para asegurar la corrección y completitud de una unidad de datos o un flujo de datos.
- **Tráfico de relleno:** consiste en enviar tráfico espurio junto con los datos válidos para que el atacante no sepa si se está enviando información, ni qué cantidad de datos útiles se está transmitiendo.
- **Control de enrutado:** permite la selección, para ciertos datos, de rutas físicas seguras y la variación de las mismas, especialmente cuando se sospecha de una violación de la seguridad.

Dentro de los **mecanismos de seguridad persistentes** tenemos:

- **Registro de auditoría de seguridad:** datos recogidos y potencialmente usables para realizar una auditoría de seguridad.
- **Etiquetas de seguridad:** los atributos o propiedades de seguridad asociadas a un recurso o unidad de datos.

- **Funcionalidad de confianza:** lo que se debe percibir como correcto con respecto a algún criterio (por ejemplo: según lo establecido por una política de seguridad).
- **Detección de eventos:** detección de eventos relevantes de seguridad.
- **Recuperación de la seguridad:** se ocupa de las peticiones de los mecanismos, tales como manejo de eventos y gestión de funciones, y lleva a cabo tareas de recuperación.

1.3 Servicios de Seguridad

X.800 define un Servicio de Seguridad como un servicio que es provisto por una capa del protocolo de comunicación y que garantiza la adecuada seguridad de los sistemas o transferencias de datos. Tal vez, una definición más clara se encuentra en la RFC 4949, que presenta la siguiente definición: Un servicio de información o comunicación que es proporcionado por un sistema para una clase específica de protección de recursos informáticos. X.800 divide estos servicios en cinco categorías:

- **Confidencialidad:** requiere que la información sea accesible únicamente por las entidades autorizadas. La confidencialidad de datos se aplica a todos los datos intercambiados por las entidades autorizadas o tal vez a sólo porciones o segmentos seleccionados de los datos, por ejemplo mediante cifrado. La confidencialidad de flujo de tráfico protege la identidad del origen y destino(s) del mensaje, por ejemplo enviando los datos confidenciales a muchos destinos además del verdadero, así como el volumen y el momento de tráfico intercambiado, por ejemplo produciendo una cantidad de tráfico constante al añadir tráfico espurio al significativo, de forma que sean indistinguibles para un intruso. La desventaja de estos métodos es que incrementan drásticamente el volumen de tráfico intercambiado,

repercutiendo negativamente en la disponibilidad del ancho de banda bajo demanda.

- **Servicio de autenticación:** requiere una identificación correcta del origen del mensaje, asegurando que la entidad no es falsa. Se distinguen dos tipos: de entidad, que asegura la identidad de las entidades participantes en la comunicación, mediante biométrica (huellas dactilares, identificación de iris, etc.), tarjetas de banda magnética, contraseñas, o procedimientos similares; y de origen de información, que asegura que una unidad de información proviene de cierta entidad, siendo la firma digital el mecanismo más extendido.
- **Control de accesos:** en el contexto de seguridad informática, el control de acceso es la capacidad de controlar y limitar el acceso a través de la red a los sistemas y aplicaciones. Para lograr esto, cada entidad que intenta conseguir acceso debe ser autenticada, por lo que los derechos de acceso se pueden adaptar a cada usuario.
- **Integridad:** de la misma manera que la confidencialidad, la integridad se puede aplicar a un flujo de mensajes, a un único mensaje, o a un conjunto de campos seleccionados de un mensaje. De nuevo, el enfoque más sencillo y útil es la protección total del flujo de comunicación. Un servicio de **integridad orientado a conexión** trabaja con flujos de mensajes y garantiza que los mensajes son recibidos tal y como son enviados, sin ser duplicados, modificados, reordenados o repetidos.
- **No repudio:** el no repudio evita que el emisor o receptor de un mensaje puedan negar la transmisión. Así, cuando se envía el mensaje, el receptor puede probar que el supuesto emisor ha hecho el envío. Del mismo modo, cuando un mensaje es recibido, el emisor puede probar el hecho de que el mensaje, efectivamente ha sido recibido.

Ambos X.800 y RFC 4949 definen la **disponibilidad** como la propiedad de un sistema o recurso de ser usado y disponible bajo un sistema de autorización de entidad, de acuerdo con las especificaciones de rendimiento para el sistema. Es decir, el sistema está disponible si proporciona sus servicios de acuerdo con el diseño del sistema cada vez que los usuarios lo solicitan. Una gran variedad de ataques pueden producir la pérdida o reducción de la disponibilidad. Algunos de esos ataques pueden ser evitados con medidas automáticas, tales como la autenticación y el cifrado, mientras que otros requieren algún tipo de acción física para prevenir o recuperarse de una pérdida de disponibilidad en los elementos de un sistema distribuido.

La *Tabla 1* indica la relación entre los servicios de seguridad y los mecanismos de seguridad.

1.4 Ataques contra la seguridad

Una forma útil de clasificar los ataques contra la seguridad, utilizada tanto en X.800 como en la RFC 4949, es por medio de los términos *ataque activo* y *ataque pasivo*.

Un ataque pasivo intenta conocer o hacer uso de la información del sistema pero sin afectar a sus recursos. Los ataques pasivos son muy difíciles de detectar, ya que no provocan ninguna alteración de los datos. Sin embargo, es posible evitar su éxito mediante el cifrado de la información y otros mecanismos que se verán más adelante.

Un ataque activo intenta cambiar los recursos del sistema o alterar su modo de funcionamiento. Los esfuerzos contra los ataques pasivos se centran en la prevención más que en la detección, mientras que por el contrario, frente a los ataques activos lo más importante es recuperarse lo antes posible de cualquier interrupción o retraso causado.

Servicio \ Mecanismo	Cifrado	Firma Digital	Control Accesos	Integridad	Autenticación	Tráfico Relleno	Control Enrutado	Notarización
Autenticación entidad	X	X			X			
Autenticación origen datos	X	X						
Control de accesos			X					
Confidencialidad	X						X	
Confidencialidad flujo tráfico	X					X	X	
Integridad	X	X		X				
No repudio		X		X				X
Disponibilidad				X	X			

Tabla 1. Relación entre servicios de seguridad y mecanismos de seguridad.

2 SEGURIDAD EN REDES WAN E INTERNET: CRIPTOGRAFIA Y AUTENTICACION

La **autenticación** es el mecanismo que permite confirmar la identidad de una entidad (ya sea usuario, hardware, software, etc.). Con este mecanismo, se puede controlar el acceso a los sistemas de información y a su vez, prevenir la usurpación de identidades y evitar que la información de la organización se vea comprometida.

Los mecanismos de autenticación para los seres humanos se clasifican, generalmente, en cuatro casos:

- **Algo que el usuario es:** se suelen utilizar identificadores biométricos como la huella digital, el patrón retiniano, la secuencia de ADN, el patrón de la voz, el reconocimiento de la firma, las señales bio-eléctricas únicas producidas por el cuerpo vivo, etc.
- **Algo que el usuario tiene:** una tarjeta de identificación, el teléfono móvil, una llave, etc.
- **Algo que el usuario sabe:** una contraseña, una frase o un número de identificación personal.
- **Algo que el usuario hace:** reconocimiento de voz, firma, etc.

Es posible combinar distintos mecanismos como el caso de los tokens criptográficos que además de tenerlos en nuestro poder (algo que el usuario tiene) es necesario conocer la clave (algo que el usuario sabe). Incluso hay tokens criptográficos que además incorporan un lector de huella digital.

La **autenticación criptográfica** es un mecanismo mediante el cual, una entidad que quiere autenticarse, realiza una serie de operaciones criptográficas sobre un mensaje con el fin de que su identidad pueda ser

verificada. Este tipo de autenticación es muy adecuada para sistemas distribuidos en los que la autenticación se realiza a distancia.

2.1 Mecanismos criptográficos de autenticación

Cuando se realiza la transmisión de un mensaje entre un emisor y un receptor los aspectos más importantes a verificar para garantizar una comunicación segura son la no alteración del mensaje y la autenticidad del emisor. También suele ser relevante la oportunidad de los datos (no han sido retrasados ni reemplazados artificialmente) y verificar la secuencia relativa a otros mensajes que fluyen entre los dos extremos de una comunicación.

La **autenticación de mensajes** proporciona seguridad contra ataques activos tales como la falsificación de datos y transacciones. Existen los siguientes mecanismos de autenticación de mensajes: **checksum criptográfico, cifrado de mensajes y funciones resumen o hash**.

2.1.1 Checksum criptográfico

Con esta técnica los mensajes se transmiten sin cifrar por lo que no se garantiza la confidencialidad del mismo. En su lugar se genera una *etiqueta de autenticación* que se incorpora al mensaje para su transmisión.

Este mecanismo implica la utilización de una clave secreta con la que se genera un pequeño bloque de datos de longitud fija, conocido como *código de autenticación de mensaje* (MAC), que se incorpora al mensaje.

Cuando *el emisor* desea enviar un mensaje, calcula el código MAC en base al mensaje y a la clave compartida. El mensaje y el código son transmitidos al *receptor* que realiza la misma operación sobre el mensaje recibido, utilizando la misma clave, y verifica que el código obtenido coincide con el

recibido. Si se asume que solo *emisor* y *receptor* conocen la clave se puede decir que:

- El receptor puede asegurar que el mensaje que ha recibido no ha sido alterado.
- El mensaje ha sido enviado por el supuesto emisor.
- Si el mensaje contiene un número de secuencia, entonces el receptor puede estar seguro de que la secuencia es la correcta.

2.1.2 Técnicas de cifrado

Hay dos técnicas básicas para cifrar información: el **cifrado simétrico** (también denominado cifrado de clave secreta) y **cifrado asimétrico** (también denominado cifrado de clave pública).

El cifrado simétrico es la técnica más antigua y conocida. El emisor y receptor conocen la clave secreta de cifrado que se aplica al mensaje de un modo determinado. Esta técnica garantiza que solamente el emisor y receptor del mensaje deberían ser capaces de cifrarlo y descifrarlo. El mayor inconveniente del cifrado asimétrico es la distribución y custodia de claves.

El cifrado asimétrico se basa en un par de claves cuya relación entre ambas consiste en que lo que se cifra con una se descifra con la otra y viceversa. Una de las claves se hace pública y la otra sólo la conoce el propietario de la misma. De este modo si se desea garantizar que sólo el destinatario de un mensaje pueda descifrarlo basta con cifrarlo con su clave pública. Si además el emisor del mensaje lo cifra utilizando su propia clave privada el receptor podrá comprobar que el emisor es quién dice ser descifrando el mensaje con la clave pública de aquél. El cifrado asimétrico resuelve los problemas del cifrado simétrico, pero a cambio requiere más capacidad de procesamiento.

Para asegurar que el mensaje no ha sido alterado ni ha sido retrasado deliberadamente durante su tránsito por la red se suelen combinar las técnicas de cifrado con el uso de códigos de detección de errores y marcas de tiempo.

2.1.3 Funciones resumen

El uso de **funciones *hash* tampoco conlleva un cifrado del mensaje enviado** y admite mensajes de longitud variable.

La función *hash* acepta un mensaje de longitud variable M como entrada y produce como salida una cadena de tamaño fijo $H(M)$, normalmente conocida como resumen del mensaje. El resumen se envía junto al mensaje de tal forma que puede ser utilizado por parte del receptor para realizar la autenticación. Además de la autenticación, el resumen proporciona un mecanismo de comprobación de la integridad de los datos. Si en el tránsito del mensaje por la red, se altera algún bit, el resumen calculado por parte del destinatario será diferente del que viene desde el origen, por lo que el mensaje será erróneo.

A la hora de enviar el mensaje y resumen de una forma autenticada, las funciones *hash* se pueden utilizar de tres maneras diferentes:

- **Utilización de criptografía simétrica para cifrar el resumen:** se cifra el resumen en origen con ayuda de un algoritmo basado en criptografía simétrica. Si solamente el emisor y receptor conocen la clave se puede garantizar que el resumen es auténtico.
- **Utilización de criptografía de clave pública para cifrar el resumen:** proporciona una **firma digital** del mensaje y **autenticación**; además no se requiere la distribución de claves a los participantes en la comunicación.

- **Autenticación de mensajes sin utilizar cifrado:** las dos partes comunicantes comparten un secreto común. El emisor, antes de enviar el mensaje, calcula el resumen del mensaje concatenado con el secreto. A continuación procede al envío del mensaje y resumen. En destino se repite la operación: se concatena el secreto con el mensaje y se calcula el resumen. Si coincide con el resumen que llegó desde el origen se concluye que el mensaje es auténtico. Ya que el secreto no se envía, no es posible que un atacante modifique el mensaje interceptado. La seguridad de este sistema reside en que no sea revelado el secreto compartido.

Las **funciones hash** son importantes además de para autenticación de mensajes para la realización de **firmas digitales**. El propósito de una función *hash* es producir una “huella” del mensaje. Para que una **función hash (H) se considere segura** debe verificar las siguientes propiedades:

1. **H** debe poder ser aplicada a mensajes de cualquier tamaño.
2. **H** produce una salida de longitud fija.
3. **H(x)** es relativamente fácil de calcular para un **x** dado, haciendo práctica la implementación en hardware y software.
4. Para un código dado **m**, es imposible computacionalmente encontrar un **x** tal que **H(x)=m**.
5. Para un bloque dado **x**, es imposible computacionalmente encontrar un **y** \neq **x** con **H(y)= H(x)**.
6. Es imposible computacionalmente encontrar una pareja **(x, y)** tal que **H(x)=H(y)**.

Las tres primeras propiedades son requisitos para la aplicación práctica de una función resumen a la autenticación de mensajes. La cuarta propiedad garantiza la unidireccionalidad del resumen: es fácil generar el resumen, pero imposible obtener el mensaje a partir del resumen. La quinta y sexta

propiedad tienen que ver con la protección contra las “colisiones”, garantizando que no es computacionalmente posible encontrar dos mensajes diferentes con el mismo resumen. Los ejemplos más conocidos de funciones resumen son **MD5** y la familia **SHA**.

3 SISTEMAS DE AUTENTICACION PARA SEGURIDAD EN REDES

Todos los sistemas de autenticación en redes utilizan criptografía para garantizar la seguridad, lo que hace necesario la realización de una serie de tareas:

- **Generación de claves:** existen diversos algoritmos de generación de claves, aunque lo más común es utilizar una fuente de números pseudo-aleatorios.
- **Registro:** las claves generadas deben quedar ligadas de forma unívoca a una identidad.
- **Distribución:** antes de iniciar la comunicación es necesario que las partes implicadas conozcan tanto las claves como los algoritmos de cifrado a utilizar. El mecanismo de distribución de claves variará en función de la técnica de cifrado utilizada.
- **Protección:** es imprescindible garantizar la custodia de las claves ya que la revelación de las mismas comprometería el sistema de autenticación.
- **Mecanismos de revocación:** cuando existen evidencias de que una clave ha sido revelada deben existir mecanismos para retirarla.

3.1 Distribución de claves utilizando criptografía simétrica

La criptografía simétrica se basa en una clave secreta compartida por el emisor y el receptor que debe ser custodiada por ambos y protegida contra el acceso por parte de terceros no autorizados. Además, como prevención ante la posible vulneración del secreto es recomendable cambiar la clave cada cierto tiempo. De este modo, la distribución de las claves resulta crítica para el sistema de cifrado simétrico. Por lo tanto, uno de los elementos que aseguran la fortaleza de un sistema de cifrado simétrico es la técnica de distribución de claves.

Para la distribución de claves entre dos entidades, que denominaremos A y B, se pueden utilizar distintas estrategias:

1. **A** puede generar la clave y enviarla físicamente a **B**.
2. Un tercero de confianza **C** genera la clave y la envía físicamente a **A** y **B**.
3. En los casos en los que **A** y **B** dispongan ya de una clave secreta común, cualquiera de ellos puede generar una nueva clave y enviarla a la otra parte cifrando el envío con la clave previamente establecida.
4. Si existe un tercero de confianza **C** con el que tanto **A** como **B** disponen de un canal de comunicación cifrado, **C** podría generar la nueva clave y enviarla a **A** y **B** de forma.

Las opciones 1 y 2 se conocen como entrega manual de la clave. Estas técnicas tienen un coste asumible en cifrados de enlace donde toda la comunicación se cifra entre los dos mismos elementos de comunicación. Por ejemplo: se podría intercambiar manualmente una clave secreta de un tamaño considerable para crear una VPN sitio a sitio entre dos delegaciones de una organización. Sin embargo, se complica para cifrados extremo a extremo en redes, donde cada origen puede establecer

comunicaciones con destinos variados. Por ejemplo cuando un cliente remoto tiene que acceder a múltiples servicios en diversas organizaciones, le resulta inviable pedir un envío físico de una clave por cada acceso.

La opción 3 es viable tanto para cifrados de enlace como para cifrados extremo a extremo. Tiene el inconveniente de que si un atacante tiene éxito y obtiene la clave, entonces todas las claves subsiguientes estarán comprometidas.

La opción 4 es la más adecuada para proporcionar claves en cifrados extremo a extremo. En esta opción, se utilizan dos tipos de claves:

- **Claves de sesión:** cuando dos sistemas (hosts, terminales, etc.) se quieren comunicar, establecen una conexión lógica (por ejemplo un circuito virtual). Mientras perdure esa conexión lógica, llamada sesión, todos los datos de usuario son cifrados con una clave de sesión de un solo uso. Al final de la sesión esta clave es destruida.
- **Claves maestras:** una clave maestra es una clave utilizada entre entidades para el propósito de distribución de claves de sesión.

Un elemento necesario para la opción 4 es el **centro de distribución de claves (KDC)**. El KDC determina que sistemas tienen permitido comunicarse entre sí. Cuando se concede permiso a dos sistemas para comunicarse entre sí, el KDC proporciona una clave de sesión de un solo uso.

3.2 Distribución de claves utilizando criptografía asimétrica

A pesar de que en la criptografía asimétrica la clave pública es conocida por toda la comunidad, la distribución de claves presenta también una problemática que debe ser abordada.

Partiendo de la utilización de un algoritmo ampliamente aceptado como RSA, cualquier participante puede generar su par de claves y enviar su clave pública a la comunidad. El problema de esta aproximación es que resulta imposible comprobar que alguien que envía su clave pública asegurando ser **A** realmente lo sea. De este modo, si un impostor **B** hace pública una clave diciendo que es **A** podría leer todos los mensajes que fuesen dirigidos al auténtico **A**, mientras no se descubriese el fraude. La solución a este problema viene de la mano de los **certificados digitales**. Un certificado digital es un conjunto de información acerca de una entidad, con su clave pública y todo ello **firmado por una tercera entidad de confianza**.

3.3 Protocolos y métodos de autenticación en red

La verificación de la identidad de un sujeto de forma remota presenta una dificultad añadida, especialmente cuando los datos intercambiados durante el mismo se transmiten a través de una red no segura, ya que cualquier impostor podría hacerse pasar por alguien que no es consiguiendo así acceder a recursos a los que, de otro modo, no le estaría permitido. Las técnicas criptográficas constituyen una herramienta de gran utilidad para superar esta dificultad.

El modo de operación que utilizan los protocolos de autenticación en red se resume de la siguiente manera: Dos entidades *A* y *B* (conocidas como principales) quieren establecer una conexión segura y tener acceso a datos y servicios. Para ello, uno de los principales comienza a intercambiar información con el otro principal o con un Centro de Distribución de Claves confiable (KDC). Después de una serie de retos se consigue una clave de sesión única para preservar la confidencialidad de los datos intercambiados. Una premisa fundamental es establecer una clave de sesión nueva para cada conexión, y así reducir la cantidad de información

comprometida en caso de que un atacante tenga éxito. Hay una amplia variedad de protocolos de autenticación en red:

- **TACACS, RADIUS:** métodos basados en servidores con registro de todos los usuarios.
- **Kerberos:** método basado en centro de distribución de claves.
- **X.500, LDAP:** métodos basados en servicios de directorio.
- **Certificados:** métodos basados en certificados digitales.
- **NIS, NIS+:** métodos basados en *Network Information Service*.
- **EAP-TLS, EAP-TTLS, EAP-MD5, etc:** métodos basados en el framework de autenticación EAP.

3.4 Protocolos de seguridad en Internet

3.4.1 Kerberos

Kerberos es un servicio de distribución de claves y autenticación de usuarios desarrollado por el MIT (*Massachusetts Institute of Technology*). El problema que aborda Kerberos es el siguiente: en un entorno distribuido en el cual los usuarios intentan acceder desde sus estaciones de trabajo a servicios y servidores en la red, se debe disponer de medios para restringir el acceso a los usuarios autorizados además de tener la capacidad de autenticarlos. En esta situación, no se puede confiar en que las estaciones de trabajo autenticuen correctamente a sus usuarios para acceder a los servicios de la red. En particular, existen tres amenazas que se deben gestionar:

- Un usuario puede conseguir acceso a una estación de trabajo particular y hacerse pasar por otro para realizar operaciones desde esa estación.

- Un usuario puede cambiar la dirección de red de una estación de trabajo, por lo que las peticiones enviadas, parecen venir de una estación desconocida.
- Un usuario puede realizar escuchas en la red y utilizar un ataque de repetición para conseguir acceso a un servidor o interrumpir operaciones.

En todos los casos, un usuario no autorizado puede conseguir acceso a servicios y datos para los que no está autorizado. En vez de construir elaborados protocolos en cada servidor, Kerberos proporciona un servidor centralizado de autenticación basado en criptografía de clave simétrica. Para un usuario, la clave es un *hash* de su contraseña, guardada normalmente en el KDC (**Key Distribution Center**). Para un servicio, la clave es una secuencia generada aleatoriamente, que actúa como una contraseña y se almacena también en el KDC.

Para que el esquema de autenticación funcione clientes y servidores tienen que confiar en una tercera parte (el servidor Kerberos) que solicita las claves necesarias bajo demanda. La comunicación en Kerberos está basada en el uso de **Tickets**. Los *Tickets* son un tipo de datos cifrado que se almacenan del lado del cliente.

El KDC es la parte principal de una red Kerberos. Consta de los siguiente elementos:

- Un servidor de autenticación, que responde a las peticiones de autenticación lanzadas por los clientes. Aquí es donde el cliente consigue un TGT (**Ticket Granting Ticket**) que sirve después de la autenticación para acceder a los servicios.
- Un servidor de concesión de accesos (**Ticket Granting Server**), que se encarga gestionar el acceso de los clientes a los servicios. En esta etapa, el cliente recibe un TGS (**Ticket Granting Service**) que le permite autenticarse ante un servicio que está disponible en la red.

- Una base de datos que guarda todas las claves secretas (de clientes y servicios), así como información relacionada con las cuentas Kerberos: fecha de creación, políticas, etc.

KerberosV5 Tickets Negotiation mechanism

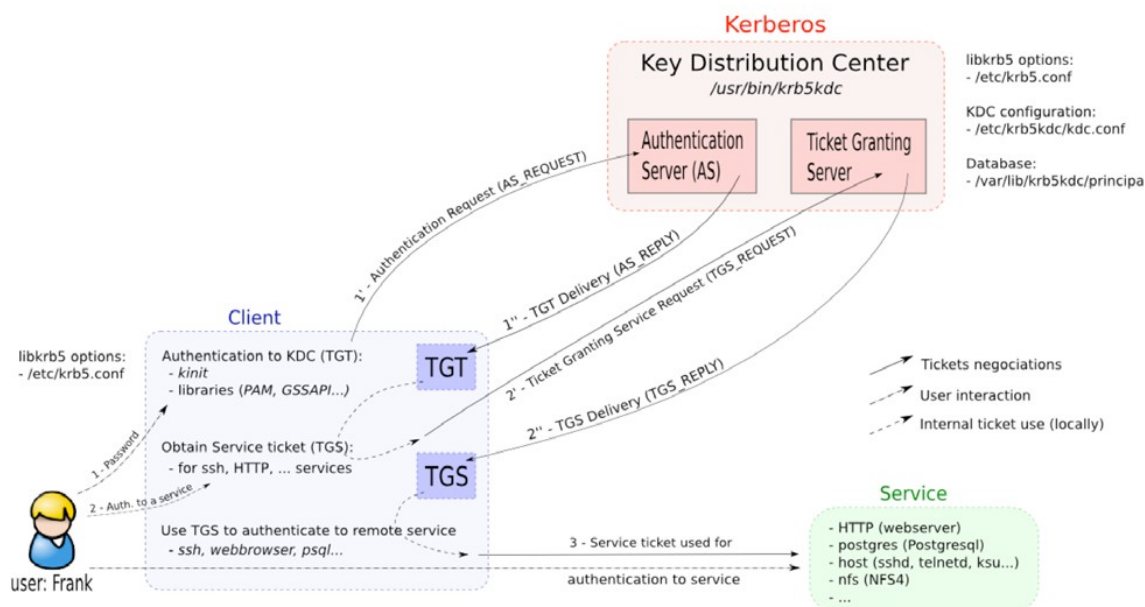


Figura 1: Mecanismo de negociación de Tickets KerberosV5 (fuente MIT Kerberos consortium)

3.4.2 PGP

El correo electrónico es un servicio que requiere servicios para permitir la autenticación de los usuarios y garantizar la confidencialidad de los mensajes que intercambian. PGP (*Pretty Good Privacy*) es un protocolo que proporciona confidencialidad de los mensajes que son enviados y almacenados. Además proporciona un mecanismo de autenticación que se basa en la firma de los correos enviados.

PGP es un sistema híbrido, combinando características del cifrado simétrico y del cifrado asimétrico. Cuando un usuario A, quiere enviar un mensaje cifrado a B utilizando PGP, se llevan a cabo los siguientes pasos:

- Se crea una clave de sesión aleatoria de que es utilizada para cifrar el mensaje.
- La clave de sesión se cifra con la clave pública de B y se añade al mensaje. El mensaje es enviado a B.
- B descifra el mensaje con su clave privada. De esta manera lo que obtiene es la clave de sesión en claro y el mensaje cifrado. Para obtener el mensaje en claro debe usar la clave de sesión y aplicar el algoritmo de descifrado basado en criptografía simétrica.

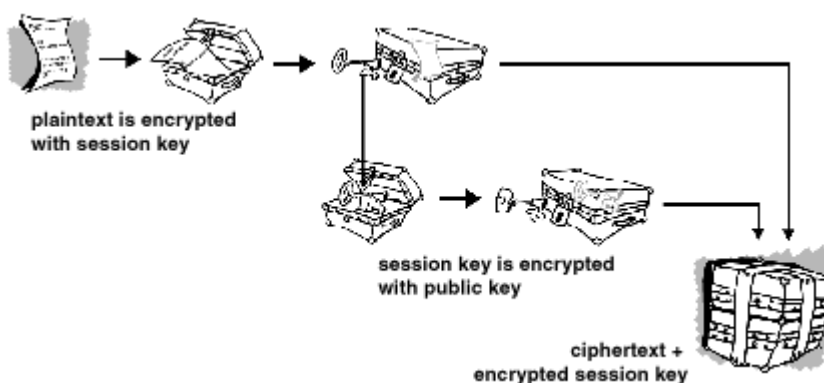


Figura 2: Cifrado con PGP (Fuente: International PGP Home Page)

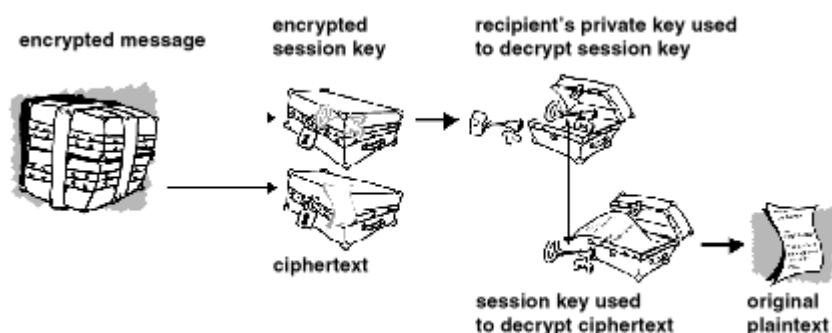


Figura 3: Descifrado con PGP (Fuente: International PGP Home Page)

Para proporcionar autenticación, PGP hace uso de firmas digitales. Para ello los integrantes de una conversación deben intercambiar sus claves

públicas. La certificación en este sistema se basa en la idea de que la confianza es un concepto social: cada persona confía en sus amigos. Así se pueden establecer cadenas de confianza si la clave de un tercero desconocido, viene firmada con la clave pública de un amigo en el que se confía. Esta forma de proceder, tiene el inconveniente de que no siempre se puede verificar la identidad de un tercero a no ser que se tenga un amigo en común.

4 ELEMENTOS DE SEGURIDAD PARA INTERNET

Se debe tener muy presente que al conectar un equipo informático a Internet se está asumiendo un riesgo ya que ese equipo pasa a estar conectado a millones de equipos distribuidos por todo el mundo. En este escenario se deben utilizar elementos de seguridad física y lógica que impidan accesos no autorizados y, en caso de que se produzcan, faciliten su detección.

4.1 Cortafuegos

El mayor nivel de seguridad que se podría adoptar en un sistema informático consistiría en desenchufarlo de la red. Sin embargo, esta no suele ser una opción aceptable ya que, a día de hoy, la mayor parte de las empresas necesitan intercambiar información, ya sea a través de una red local o a través de internet.

Aunque se pueden tener todos los servidores y estaciones de trabajo protegidas con fuertes medidas de seguridad, no suele ser suficiente con la seguridad basada en host. Una medida complementaria, que es

ampliamente aceptada, consiste en complementar la seguridad del host con un **servicio de cortafuegos**². Un cortafuegos es un elemento que se sitúa entre la red interna y los intrusos potenciales externos constituyendo una barrera de protección. Normalmente se establece entre la red local e Internet, haciendo así de muro de protección exterior de la red local. El *cortafuegos* puede ser un software en un equipo o puede ser un conjunto formado por varios sistemas específicos destinados a controlar el acceso a la red interna de la organización.

4.1.1 Características de un cortafuegos

Un servicio de cortafuegos presenta una serie de características entre las que se pueden destacar las siguientes:

- Define un punto único de control, que permite alejar a los usuarios no autorizados de la red protegida, y proporciona protección contra ataques de *spoofing* y enrutado. Esto simplifica la gestión, porque las características de seguridad están centralizadas en un único sistema o conjunto de sistemas.
- Proporciona una localización para monitorizar eventos relacionados con la seguridad. En un sistema *cortafuegos* se pueden implementar auditorías de seguridad y alarmas.
- Proporciona una plataforma para otras funciones de Internet que no están relacionadas con la seguridad: traducción de direcciones, funciones de gestión para auditoría y registros de log para medir el uso de Internet.
- Puede ser utilizado para implementar redes privadas virtuales (VPN).

4.1.2 Tipos de cortafuegos

Atendiendo a la función desempeñada por el sistema cortafuegos podemos establecer la siguiente clasificación:

² Es muy común el uso del término en inglés *Firewall*.

- **Cortafuegos de filtrado de paquetes:** aplica un conjunto de reglas para cada paquete IP de entrada y salida y a continuación reenvía o descarta el paquete. Las reglas de filtrado están basadas en la información contenida en cada paquete: IP origen, IP destino, protocolo, interfaz, etc.
- **Cortafuegos de inspección de estados:** Además de hacer el filtrado en base a paquetes guarda información de las sesiones y conexiones abiertas. Esto permite políticas de seguridad más avanzadas y evitar muchos ataques.
- **Proxy de aplicaciones:** Actúa como intermediario en el tráfico de la capa de aplicación permitiendo acceder a ciertas características de las aplicaciones y reenviando la información.

4.1.3 Localizaciones del Cortafuegos y configuraciones

Atendiendo a la localización del cortafuegos se pueden obtener distintas configuraciones:

- **Redes DMZ:** se utilizan para aislar una o varias subredes (conocidas como “zonas desmilitarizadas”) los principales servicios de la organización que tienen que ser accedidos desde el exterior (Web, correo, DNS). A este segmento se le aplican unas reglas de filtrado para garantizar una conectividad controlada desde el exterior. Al resto de la red interna se le cierra el acceso desde el exterior.
- **Redes privada virtuales (VPN):** es una solución que ofrece grandes ventajas a los gestores de red. Consiste en dar acceso mediante una conexión segura a un equipo o segmento de una red privada a través de una red considerada insegura como puede ser Internet.
- **Cortafuegoss Distribuidos:** consiste en agrupar bajo un mismo mecanismo de control centralizado la gestión de dispositivos

cortafuegos y la gestión de *cortafuegos* basados en host. Con estas herramientas, el administrador puede establecer políticas de seguridad y aplicarlas a equipos *cortafuegos*, servidores y estaciones de trabajo tanto locales como remotas. Además proporcionan capacidades de monitorización y alertas de seguridad.

4.2 Sistemas de detección de intrusiones

Un *cortafuegos* es mecanismo de seguridad, que permite cerrar todos aquellos puertos de servicios que no se estén utilizando y así reducir la posibilidad de ataques por parte de intrusos. Pero aunque se permita solamente el acceso a los servicios básicos y teóricamente seguros, estos a veces tienen vulnerabilidades que pueden ser aprovechadas por un atacante con fines maliciosos para saltarse esta medida de protección. Haciendo un símil con la protección de una casa, el *cortafuegos* se correspondería con la puerta de entrada, pero es necesario un sistema de alarma que se encargue de avisar en caso de que un intruso logre entrar. El elemento correspondiente al sistema de alarma en el mundo de la seguridad informática es el IDS (*Intrusion Detection System*). Se puede definir un IDS como un sistema que se encarga de vigilar la red, absorbiendo todo el tráfico e inspeccionándolo en busca de patrones de ataque. Las características principales de los IDS son las siguientes:

- Añade un alto nivel de integridad al resto de la red, ya que, en cierta forma, sabemos que el resto de sistemas están bien porque el IDS no avisa de lo contrario.
- Puede monitorizar la actividad de un atacante. Dependiendo de la infraestructura de IDS, se podrá monitorizar esta actividad en un único segmento o en varios.
- Alerta ante patrones de ataque comunes conocidos.

- Automatiza la búsqueda de nuevos patrones de ataque, ya que proporcionan herramientas estadísticas de búsqueda y monitorización de tráfico anómalo.
- Puede detectar ataques en tiempo real.
- Puede detectar errores de configuración en los equipos.

Los sistemas IDS constan de un equipo con una consola central de administración y una o varias “sondas” que se encargan de capturar el tráfico que se debe analizar. Dependiendo de la arquitectura de red de la organización se pueden seguir diversos criterios para ubicar las sondas: en la DMZ, detrás del cortafuegos, en los accesos de usuario, entre la Extranet e Internet, etc.

Una variante de los sistemas de detección de intrusiones son los IPS (*Intrusion Prevention System*). La diferencia con respecto a los IDS estriba en que los IPS además de detectar un ataque y generar la correspondiente alerta son capaces de actuar e intentar neutralizar el ataque. Un ejemplo claro sería cuando el IPS detecta actividad maliciosa por parte de un usuario conectado a un servidor a través de una conexión remota. Una de las acciones drásticas que podría tomar el IPS es cortar la conexión.

Los sistemas IPS/IDS se pueden instalar como un software en un servidor (ej. Snort) o puede ser un equipo hardware con su software completo e independiente proporcionado por un fabricante de dispositivos de seguridad.

REFERENCIAS

- **STALLINGS, W.** (2011). *Network Security Essentials. Applications and Standards. Fourth Edition.* Prentice Hall.
- MIT Kerberos Consortium Publications.
(<http://www.kerberos.org/software/whitepapers.html>)
- The International PGP Home Page – PGP Documentation
(<http://www.pgpi.org/doc/>)

(Todos los enlaces fueron verificados en noviembre de 2011)

Autor: Juan Otero Pombo
Ingeniero en Informática en el Concello de Ourense
Colegiado del CPEIG



**46. MODELO OSI. REDES LAN,
MAN Y WAN. ESTRUCTURA DE
REDES: TRONCAL,
DISTRIBUCIÓN ACCESO.
REDES PÚBLICAS DE
TRANSMISIÓN DE DATOS.
PROTOCOLOS DE RED.**

Tema 46. Modelo OSI. Redes LAN, MAN y WAN. Estructura de redes: troncal, distribución acceso. Redes públicas de transmisión de datos. Protocolos de red.

ÍNDICE

46.1 Modelo OSI

46.1.1 Introducción

46.1.2 Conceptos generales

46.1.3 Transmisión entre entidades del mismo nivel (pares)

46.1.4 Conexiones

46.1.4.1 Establecimiento de conexiones

46.1.4.2 Liberación de conexiones

46.1.4.3 Multiplexación y división

46.1.4.4 Transmisión de datos

46.1.5 Capas del modelo OSI

46.1.5.1 Capa física (NIVEL 1)

46.1.5.2 Capa de enlace de datos (NIVEL 2)

46.1.5.3 Capa de red (NIVEL 3)

46.1.5.4 Capa de transporte (NIVEL 4)

46.1.5.5 Capa de sesión (NIVEL 5)

46.1.5.6 Capa de presentación (NIVEL 6)

46.1.5.7 Capa de aplicación (NIVEL 7)

46.1.6 Críticas al modelo OSI

46.2 Redes LAN, MAN y WAN

46.2.1 PAN

46.2.2 LAN

46.2.3 MAN

46.2.4 WAN

46.3 Estructura de redes: troncal, distribución y acceso

46.3.1 Troncal

46.3.2 Distribución

46.3.3 Acceso

46.4 Redes públicas de transmisión de datos

46.4.1 Conceptos generales

46.5 Protocolos de red

46.5.1 Redes de conmutación de circuitos

46.5.2 Redes de conmutación de paquetes

46.6 Bibliografía

46.1 MODELO OSI

46.1.1 INTRODUCCIÓN

Inicialmente, los computadores eran elementos aislados que almacenaban en sus propios ficheros y necesitaban la conexión de sus propios periféricos. La independencia era tal que, si se necesitaba imprimir un documento alojado en una máquina que no disponía de impresora, era necesario copiar el fichero en un disquete y llevarlo hasta un equipo con una impresora, conectarla e imprimirlo en este. Para evitar esto, la solución era instalar una impresora en el computador inicial, con la consiguiente duplicación de recursos y dispositivos.

Con instalaciones informáticas así, la configuración y gestión de todos los ordenadores y periféricos a ellos conectados suponía un coste y una tarea muy grandes, llegando a ser poco práctica cuando el número de computadores fue creciendo en las distintas empresas.

Por esta razón, apareció la necesidad de conectar los diferentes ordenadores entre sí e implantar métodos de comunicación y transferencia de datos entre ellos. Nace el concepto de “redes de ordenadores” y “trabajo en red”.

A mediados de los 70 diversos fabricantes desarrollan sus propios sistemas de redes locales. Sin embargo, la comunicación entre ordenadores pertenecientes a redes distintas de distintos fabricantes era imposible, debido a que los sistemas de comunicación de cada red eran propietarios. Es decir, estaban desarrollados con hardware y software propios y usaban protocolos y arquitecturas diferentes a los de otros fabricantes.

Las empresas se dieron cuenta de la necesidad de abandonar los sistemas propietarios y definir una arquitectura de red con un modelo común que permitiera conectar varias redes sin problemas.

En 1977, la Organización Internacional de Normas (ISO, International Standard Organization), integrada por industrias representativas del sector, creó un subcomité para el desarrollo de estándares de comunicación de datos que permitiera la interoperabilidad entre productos de diferentes fabricantes. Tras varias investigaciones acerca de los modelos de red, elaboraron el modelo de referencia OSI (Open Systems Interconnection), en 1984.

46.1.2 CONCEPTOS GENERALES

El modelo de referencia para la Interconexión de Sistemas Abiertos se caracteriza por:

- Se ocupa de la conexión de sistemas abiertos, es decir, sistemas que permiten la comunicación con otros sistemas.
- Consta de siete capas. Por capa se entiende una (o varias) entidad(es) que realiza por sí misma una función específica. Las entidades del mismo nivel se denominan entidades pares.
- Representa el primer paso a la estandarización internacional de los protocolos que se usan en las diversas capas.
- No es una arquitectura de red en sí, ya que no especifica los servicios y protocolos exactos que se tienen que usar en cada capa, si no que solo define lo que debe hacer cada capa.

En el modelo OSI existen tres conceptos fundamentales:

- Servicio: Capacidad de comportamiento de una capa. Cada capa presta algunos servicios a las entidades que se encuentran sobre ella, que acceden a los mismos a través de los puntos de acceso al servicio (SAP), intercambiando primitivas de servicio.
- Interfaz: Indica a los procesos de la capa superior cómo acceder a ella, especificando cuáles son los parámetros y qué resultados

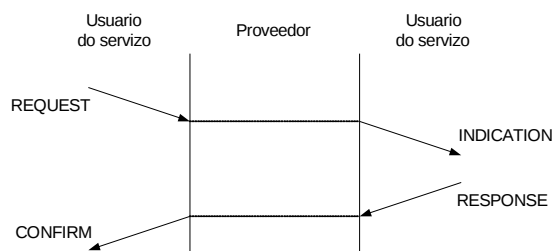
esperar. La interfaz entre dos capas en una máquina no tiene porque ser igual a la correspondiente en otra máquina.

- Protocolo: Conjunto de reglas que determinan el comportamiento de comunicación horizontal entre entidades pares. Se pueden cambiar los protocolos de una capa sin afectar a las demás.

46.1.3 TRANSMISIÓN ENTRE ENTIDADES DEL MISMO NIVEL (PARES)

Las entidades pares residentes en el nivel N+1 se comunican entre sí a través del nivel N, mediante el uso de primitivas de servicio. Sin embargo, existe una comunicación lógica horizontal entre entidades pares. Las reglas que regulan esta comunicación vienen reflejadas en el protocolo de pares. Por lo tanto, en la especificación de cada capa existen dos documentos:

- Especificación del servicio, que informa sobre las primitivas existentes. En la descripción de las primitivas se indica cuántos parámetros puede o debe haber y qué información contienen, pero no se especifica cómo ni con qué formato tienen que ser “pasados”. Esto es un asunto local y definir esto equivale a definir la Interfaz. Existen cuatro tipos de primitivas.
 - o De petición (REQUEST). Empleada para invocar un servicio y pasarle los parámetros necesarios para su ejecución.
 - o De indicación (INDICATION). Usada para indicar que un procedimiento fue invocado por el usuario par del servicio en la conexión y pasar los parámetros asociados o para indicar al usuario del servicio el inicio de una acción por parte del proveedor.
 - o De respuesta (RESPONSE). Empleada por el usuario del servicio para reconocer o completar algún procedimiento previamente iniciado por una indicación del proveedor.
 - o De confirmación (CONFIRM). Usada por el proveedor del servicio para reconocer o completar algún procedimiento previamente iniciado por una petición del usuario.



TEXTO: USUARIO DEL SERVICIO

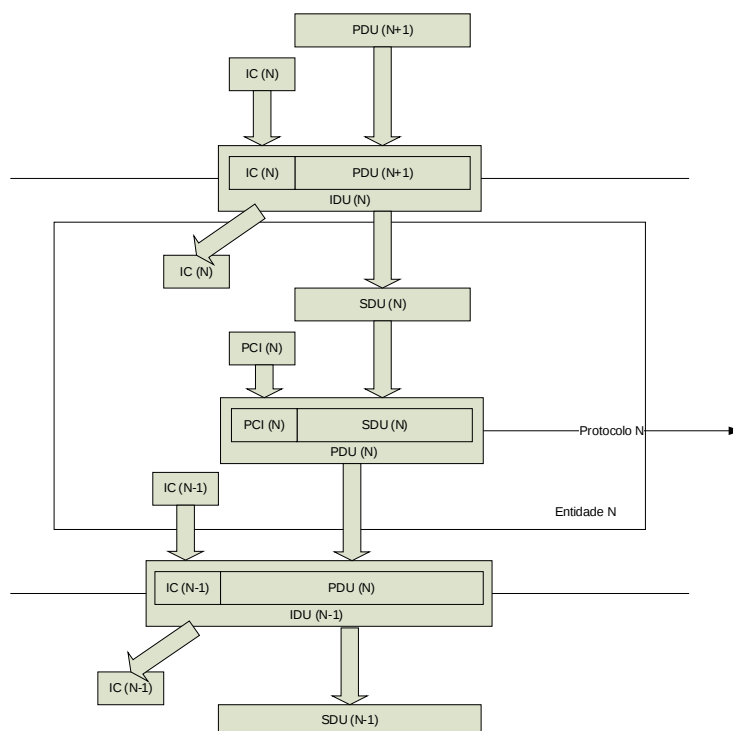
- Especificación del protocolo, que describe las PDUs (Protocol Data Units) y las reglas que determinan su intercambio entre unidades pares. Existen dos clases de PDUs:
 - o De datos, que contiene los datos del usuario final (en el caso de la capa de aplicación) o la PDU del nivel inmediatamente superior.
 - o De control, que sirve para gobernar el comportamiento completo del protocolo en sus funciones de establecimiento y ruptura de la conexión, control de flujo, control de errores, etc. No contienen información alguna procedente del nivel N+1.

En la siguiente figura se ilustra la nomenclatura utilizada por ISO en la pila que envía la información.

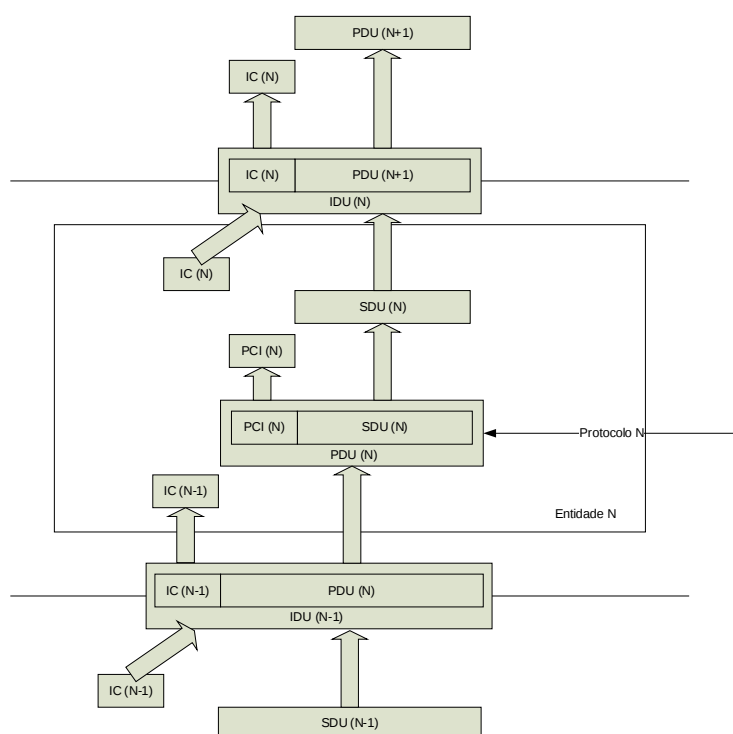
- PDU (N) -> Unidad de Datos del Protocolo del nivel N. Contiene información de control del protocolo y, posiblemente, datos de usuario. Debe estar puntual y perfectamente definida (sintáctica y semánticamente).
- ICI (N) -> Información de Control de la Interfaz del nivel N. Es transferida entre una entidad N+1 y una entidad N para coordinar el funcionamiento local conjunto. Su sintaxis y semántica son un asunto local cuando actúa como información complementaria en la transferencia de una PDU.
- IDU (N) -> Unidad de Datos de la Interfaz del nivel N. Es transferida a través del punto de acceso al servicio N. Contiene la ICI más la

totalidad (o parte) de la información de la PDU (N+1). La estructura de las informaciones de la IDU es un asunto local.

- SDU (N) -> Unidad de Datos del Servicio del nivel N. Representa la información entregada por el nivel inmediatamente superior.
- PCI (N) -> Información de Control del Protocolo del nivel N. Información generada por la entidad N para coordinar el funcionamiento conjunto con otra u otras entidades del nivel N con las que está intercambiando información “horizontal”.
- UD (N) -> Datos del Usuario. Datos transferidos entre entidades del nivel N en nombre de las entidades del nivel N+1.



En la pila que recibe la información, la relación existente entre las unidades de datos residentes en las entidades del nivel N-1, N y N+1 es similar a la representada mas arriba, solo que en lugar de añadir elementos lo que se producen son reducciones y las flechas son ascendentes, como muestra la figura siguiente.



Cuando las unidades de datos de los niveles limítrofes no tienen tamaños compatibles, se recurre a alguna de las siguientes funciones:

- Segmentación de la SDU. Cuando la SDU es demasiado grande, se reparte en más de una PDU. La función simétrica en el extremo receptor es el reensamblado, que consiste en la identificación de varias PDUs con una sola SDU. La PCI incluye, en este caso, información adicional para posibilitar el reensamblado.
- Empaquetado de la SDU. Cuando el tamaño de la SDU es más pequeño que el de la PDU, puede ser conveniente o necesario agrupar varias SDUs en una sola PDU. El empaquetado es el caso contrario a la segmentación de la SDU. La función inversa del empaquetado es el desempaquetado, que consiste en descomponer una PDU en varias SDUs. El caso de segmentación se da con más frecuencia que el de empaquetado.
- Segmentación de la PDU. Si la PDU es muy grande, puede ser necesario repartirla en más de una IDU del nivel inferior. Por eso, en la definición de IDU se dice que cuentan la ICI más la totalidad (o

parte) de la PDU. También en este caso deben existir informaciones adicionales que posibiliten el reensamblado en el extremo receptor.

- Concatenación de PDU. Si el tamaño de la SDU del nivel inferior, y como resultado, de la IDU del nivel inferior, es mayor que el de la PDU, puede ser conveniente agrupar varias PDUs sobre una sola SDU. La función inversa a esta, que se realiza en el extremo receptor, es la separación. La concatenación-separación es el caso contrario de la segmentación-reensamblado de la PDU, siendo este último el más frecuente.

46.1.4 CONEXIONES

El modelo de referencia OSI está orientado a conexión. Esto significa que, en todos los niveles, es necesario que se establezca previamente una conexión para que pueda existir intercambio de datos. Sin embargo, existen protocolos que no requieren esta condición, son los no orientados a conexión (connectionless).

En las comunicaciones orientadas a conexión se pierde tiempo y recursos en establecer y liberar la conexión entre dos nodos, pero se garantiza que el nodo remoto está escuchando. Por el contrario, en las comunicaciones no orientadas a conexión se ahorra tiempo y recursos, pero a costa de no saber si el otro extremo está escuchando.

A nivel N-1 se establece una asociación, una conexión N-1, para que dos entidades del nivel N puedan comunicarse. La conexión N-1 es un servicio ofrecido por el nivel N-1, a través del cual circulan unidades de información del nivel N.

El Punto de Acceso al Servicio (SAP) del nivel N identifica la dirección del nivel N a la que se conectan las entidades del nivel N+1. La relación entre direcciones de dos niveles consecutivos puede ser 1 a 1 (1 dirección del nivel N por cada dirección del N +1), N a 1 (Varias direcciones del nivel N por cada dirección del N +1) (no confundir con la multiplexación, que se explica más adelante) o 1 a N (1 dirección del nivel N para varias direcciones del N +1).

46.1.4.1 ESTABLECIMIENTO DE CONEXIONES

Para que dos entidades N establezcan una conexión, es necesario:

- Disponer de una conexión N-1 por debajo. Es necesario establecer previamente la conexión N-1 antes de intentar establecer la conexión N, descendiendo hasta que se encuentre una disponible a nivel físico (el nivel mas bajo). Sin embargo, en los niveles altos, se aprovecha la circunstancia de establecimiento de la conexión N para establecer, al mismo tiempo, la conexión N+1.
- Estar ambas entidades conformes con el establecimiento.

Una vez establecida la conexión, es cómo si la entidad dispusiera de un “tubo” a través del cual pudiera enviar datos a su entidad de comunicación correspondiente.

46.1.4.2 LIBERACIÓN DE CONEXIONES

La liberación de una conexión N es iniciada, normalmente, por una de las entidades N+1 que la está usando. Sin embargo, esta ruptura puede ser también iniciada por una de las entidades N que le dan soporte.

Al contrario de lo que ocurre en el establecimiento, la liberación de una conexión N-1 no implica la liberación de la conexión N. Esto es así para permitir que, si la conexión N-1 rompe por dificultades de la comunicación, pueda intentarse reestablecerla o sustituirla por otra.

La liberación de una conexión puede ser:

- Abrupta. Se libera de inmediato y los datos pendientes de envío se pierden.
- Suave o diferida. Antes de romper la conexión, se espera a no tener datos pendientes.

46.1.4.3 MULTIPLEXACIÓN Y DIVISIÓN

La multiplexación es la función que permite utilizar una sola conexión N-1 para soportar varias conexiones del nivel N. Todos los “tubos” de conexión N viajan por dentro del “tubo” de conexión N-1. Varias comunicaciones entre entidades pares de nivel N se realizan apoyadas en una sola conexión del nivel N-1. Es decir, las distintas

entidades utilizan un solo punto de acceso al servicio N-1. La función inversa realizada en el receptor se denomina demultiplexación. No debe confundirse el concepto de multiplexación con el de concatenación, ya explicado.

La división es la función que permite la utilización de más de una conexión N-1 por una sola conexión de nivel N. Con ello, el flujo de datos que soporta puede ser mayor. El flujo de datos del “tubo” correspondiente a la conexión N se reparte entre todos los “tubos” de conexiones N-1. En el extremo receptor, la función inversa se denomina recombinación y debe ser capaz de recuperar el orden en el que las PDUs fueron generadas por el extremo emisor. No debe confundirse el concepto de división con el de segmentación, ya explicado.

46.1.4.4 TRANSMISIÓN DE DATOS

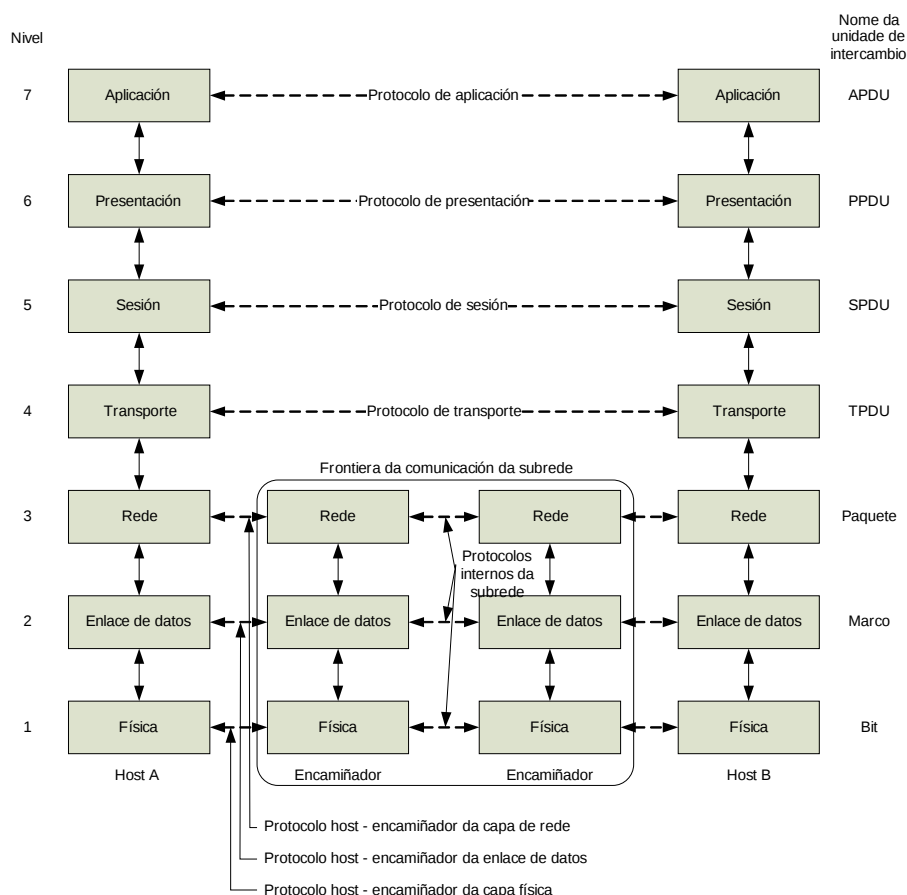
Una capa de una máquina no puede transferir los datos de forma directa a su capa par en otra máquina, sino que necesita de los servicios de todas las capas que se encuentran por debajo de ella en la jerarquía de capas, pasándose la información hacia abajo hasta llegar al nivel físico, donde se transmiten a la máquina receptora.

Cada capa utiliza el encapsulamiento para colocar la PDU de la capa superior en su campo de datos y agregar cualquier encabezado e información final que la capa necesite para realizar su función. De esta forma, a medida que los datos se desplazan hacia abajo a través de las capas del modelo OSI, el tamaño del mensaje va creciendo. A nivel 3, la PDU se llama paquete e incluye las direcciones lógicas origen y destino. A nivel 2, la trama incluye las direcciones físicas. Y, finalmente, la capa física codifica los datos de la trama de enlace de datos en un patrón de unos y ceros para su transmisión a través del medio.

En la máquina receptora se realiza el proceso inverso, retirando los distintos encabezados, uno por uno, conforme el mensaje se propaga hacia arriba por la capas.

46.1.5 CAPAS DEL MODELO OSI

Como se dijo en el punto anterior, el modelo de referencia OSI se dividió en siete niveles o capas, para poder simplificar la implementación de la arquitectura necesaria.



TEXTO: Nombre de la unidad de intercambio. Frontera de comunicación de la subred. Encaminador.

Los principios que se aplicaron para llegar a estas siete capas son los siguientes:

- Se debe crear una nueva capa siempre que se precise un grado diferente de abstracción.
- A cada capa se le asigna una función bien definida o un conjunto de funciones relacionadas entre sí, tratando de resolver en cada capa un problema distinto.

- La funcionalidad de cada capa se debe elegir habida cuenta la posibilidad de definir protocolos normalizados a nivel internacional.
- La frontera de las capas será tal que se minimice el flujo de información a través de la interfaz existente entre ambas.
- El número de capas debe ser lo suficientemente grande para no reunir en un mismo nivel funcionalidades distintas y suficientemente pequeño para que la arquitectura resultante sea manejable.

46.1.5.1 CAPA FÍSICA (NIVEL 1)

La capa física está relacionada con la transmisión de bits por un canal de comunicación, de forma que sólo reconoce bits individuales, sin estructura alguna. Es decir, la PDU del nivel físico se corresponde con un bit o, dicho de otro modo, cada bit se considera una unidad de datos.

Las consideraciones de diseño tienen que ver con las interfaces mecánica, eléctrica y de procedimiento, así como con el medio de transmisión que está bajo la capa física, asegurando que cuando un lado envíe un bit con el valor “1”, se reciba en el otro extremo el valor “1”, no como el valor “0”.

La capa física proporciona sus servicios a la capa de enlace de datos. Sus principales funciones son:

- Definición de características materiales (componentes y conectores mecánicos) y eléctricas (niveles de tensión, tipo de señal) que se van a utilizar en la transmisión de los datos por el medio físico.
- Definición de las características funcionales de la interfaz en cuanto al establecimiento, mantenimiento y liberación del enlace físico.
- Definición de reglas de procedimiento, es decir, la secuencia de eventos para transmitir.
- Transmisión de flujos de bits a través del medio.
- Manejo de voltajes y pulsos eléctricos para representar 1's ó 0's.
- Especificación de cables, polos en un enchufe, componentes de la interfaz con el medio, etc.
- Especificación del medio físico de transmisión (coaxial, fibra óptica, par trenzado, etc.)

- Garantizar la conexión física, pero no la fiabilidad de la misma. Es decir, no se realiza ningún control de errores en este nivel. Eso corresponde al nivel superior.

46.1.5.2 CAPA DE ENLACE DE DATOS (NIVEL 2)

Puesto que la capa física solo acepta y transmite una corriente de bits sin preocuparse por su significado o estructura, corresponde al nivel de enlace tomar el medio de transmisión en bruto y transformarlo en una línea que parezca estar libre de errores a los ojos de la capa de red.

La capa de enlace de datos puede ofrecer a la capa de red varias clases de servicio con diferentes calidades.

Algunas de las funciones más importantes de la capa de enlace son:

- Establecimiento de los medios necesarios para la comunicación fiable y eficiente entre dos máquinas de la red.
- Estructuración de los datos en un formato predefinido, denominado trama, que suele ser de unos cientos de bytes, añadiendo una secuencia especial de bits al principio y al final de la misma.
- Sincronización en el envío de tramas.
- Detección y control de errores provenientes del medio físico mediante el uso de bits de paridad, CRC (Códigos de Redundancia Cíclica) y envío de acuses de recibo por parte del receptor que debe procesar el emisor.
- Utilización de números de secuencia en las tramas para evitar pérdidas y duplicidades.
- Utilización de la técnica de “piggybacking”, consistente en el envío de acuses de recibo dentro de tramas de datos.
- Resolución de los problemas provocados por las tramas dañadas, perdidas o duplicadas.
- Control de la congestión de la red.
- Mecanismos de regulación de tráfico o control de flujo, para evitar que un transmisor veloz sature de datos a un receptor lento.
- Control del acceso al canal compartido en las redes de difusión.

46.1.5.3 CAPA DE RED (NIVEL 3)

La capa de red es una capa compleja que ofrece sus servicios a la capa de transporte. Responsable de la conmutación y encaminado de la información, sus funciones se pueden resumir de la siguiente forma:

- Conocimiento de la topología de la red, es decir, de la forma en que están interconectados los nodos, con objeto de determinar la mejor ruta para la comunicación entre máquinas que puedan estar situadas en redes geográficamente distintas.
- División de los mensajes de la capa de transporte en unidades más complejas, llamadas paquetes (NPDUs), y asignación de direcciones lógicas a los mismos.
- Ensamblado de paquetes en el host destino.
- Establecimiento, mantenimiento y liberación de las conexiones de red entre sistemas.
- Determinación del camino de los paquetes desde la fuente hasta el destino a través de dispositivos intermedios (routers):
 - o Las rutas pueden basarse en tablas estáticas.
 - o Las rutas se pueden determinar al inicio de cada conversación.
 - o Las rutas pueden ser dinámicas, determinándose con cada paquete en función de la carga de la red.
- Envío de paquetes de nodo a nodo usando un circuito virtual (orientado a conexión) o datagramas (no orientado a conexión).
- Control de la congestión.
- Control de flujo.
- Control de errores.
- Reencaminamiento de paquetes en caso de caída de un enlace.
- Con frecuencia, funciones de contabilidad, para determinar cuántos paquetes, caracteres o bits envía cada cliente y producir información de facturación.

Esta capa sólo es necesaria en las redes de conmutación o redes interconectadas. En redes punto a punto o de difusión existe un canal directo entre los dos equipos, por lo que el nivel 2 proporciona directamente conexión fiable entre los dos equipos.

46.1.5.4 CAPA DE TRANSPORTE (NIVEL 4)

Se trata de una verdadera capa extremo a extremo, desde el origen hasta el destino. La comunicación en los niveles inferiores es entre máquinas adyacentes.

La capa de transporte proporciona sus servicios a la capa de sesión, efectuando la transferencia de datos de manera transparente entre dos entidades de sesión.

El nivel 4 tiene la interfaz más sencilla de todo el modelo OSI, siendo la que tiene menos primitivas. No tiene primitivas de confirmación, pues se considerara a todos los efectos que es un nivel fiable.

Su función mas importante es la aceptación de datos de la capa de sesión, división en unidades más pequeñas, si es preciso, denominadas segmentos, y envío de esta información a la capa de red, asegurando que todas las partes lleguen correctamente al otro extremo de forma eficiente, donde son reensambladas.

Otras funcionalidades son:

- Establecimiento, mantenimiento y terminación adecuados de los circuitos virtuales (conexiones que se establecen dentro de una red). Cuando se inicia la conexión se determina una ruta desde la fuente hasta el destino, ruta que es usada para todo el tráfico de datos posterior.
- Determinación, en el momento del establecimiento de la sesión, del tipo de clase de servicio de transporte que se proporcionará a la capa de sesión:
 - o Canal punto a punto libre de errores, que entrega los mensajes o bytes en el orden en que se envían.
 - o Mensajes aislados sin garantía respecto a la orden de entrega.

- o Difusión de mensajes a múltiples destinos.
- Control de flujo, que desempeña un papel clave en esta capa. El control de flujo entre nodos es distinto del control de flujo entre encaminadores, que tiene lugar en la capa de red. Los datos pueden ser normales o urgentes. Estos últimos saltan los mecanismos de control de flujo.
- Detección y recuperación de errores de transporte.
- Control de la congestión.
- Numeración de los segmentos para prevenir pérdidas y doble procesamiento de transmisiones.
- Garantía de recepción de todos los datos y en el orden adecuado, sin pérdidas ni duplicados.
- Asignación de una dirección única de transporte a cada usuario.
- Aislamiento de las capas superiores de los cambios inevitables de la tecnología del hardware.
- Contabilidad a través de la red.

Lo normal es que la capa de nivel 4 cree una conexión de red distinta para cada conexión de transporte que requiere la capa de sesión. Sin embargo, es posible crear múltiples conexiones de red, dividiendo los datos entre ellas para aumentar el volumen, si se requiere un volumen de transmisión alto. De igual forma, si resulta costoso mantener una conexión de red, el nivel 4 puede multiplexar varias conexiones de transporte en la misma conexión de red para reducir el coste. En la cabecera que añade este nivel se envía la información que identifica a qué conexión pertenece cada mensaje. En cualquier caso, la capa de transporte debe hacer esto de forma transparente a la capa de sesión.

46.1.5.5 CAPA DE SESIÓN (NIVEL 5)

Esta capa proporciona sus servicios a la capa de presentación, facilitando el medio necesario para que las entidades de presentación de dos máquinas diferentes organicen y sincronicen su diálogo y procedan al intercambio de datos, mediante el establecimiento de sesiones.

Por tanto, la función principal de la capa de sesión es el establecimiento, administración y finalización ordenada de sesiones entre dos máquinas. Una sesión permite el transporte común de datos, como efectuar un login en un sistema remoto o transferir un fichero entre dos nodos, pero también proporciona servicios mejorados, útiles en algunas aplicaciones, como los que se detallan a continuación.

- Manejo del control del diálogo (quién habla, cuándo, cuánto tiempo, half duplex o full duplex). Las sesiones pueden permitir que el tráfico vaya en una única dirección, comunicaciones bidireccionales alternadas (half duplex), o en ambas direcciones al mismo tiempo, comunicaciones bidireccionales simultáneas (full duplex). En las comunicaciones half duplex, la capa de sesión ayuda a llevar el control de los turnos, mediante el manejo de fichas, también llamadas testigos o tokens. Solo el lado que posea la ficha puede efectuar la operación.
- Sincronización del diálogo, mediante la inserción de puntos de verificación en la corriente de datos (APDU), de modo que si se produce una interrupción solo es necesario repetir la transferencia de los datos después del último punto de verificación. La decisión de dónde colocar los puntos de sincronización es competencia directa del nivel de aplicación. Los puntos de sincronización pueden ser de dos tipos.
 - o Mayor. Necesita confirmación del otro extremo para seguir con la transferencia del siguiente bloque.
 - o Menor. Se intercalan entre dos puntos de sincronización mayores. No necesitan confirmación. Al confirmarse un punto de sincronización mayor se dan por confirmados los puntos menores intermedios.

El bloque entre el primero y el último punto de sincronización mayor se llama actividad. Cuando se establece una conexión de sesión, automáticamente se abre una actividad para poder trabajar. Solo un

tipo de datos concreto puede enviarse además de una actividad, los datos de capacidades (CD), que son datos de control. Las actividades se dividen en unidades de diálogo, que es el contenido entre dos puntos de sincronización mayor consecutivos.

En esta capa la referencia a los dispositivos es por el nombre y no por la dirección. Además, es aquí donde se definen las API's (Application Program Interface).

El protocolo de nivel de sesión es orientado a la aplicación, ya que sus funcionalidades se adaptan a las necesidades de la aplicación.

Las unidades de datos del nivel de sesión, SPDUs, que regulan el diálogo, fluyen horizontalmente a través del nivel 5, pero son puestas en circulación por iniciativa de los correspondientes procesos de aplicación que residen en el nivel 7. Es decir, la capa de sesión no es un nivel autónomo que tenga capacidad para tomar decisiones sobre quien habla y quien escucha. Estas decisiones están reservadas a las entidades de la capa de aplicación. El nivel 5 sólo proporciona los mecanismos para que las entidades de aplicación puedan regular el diálogo entre sí.

En el párrafo anterior se habla como si la capa de aplicación residiera directamente encima de la de sesión. Esto no es así. Como se indica en la enumeración de capa, la capa de sesión ofrece sus servicios a la capa de presentación. Lo que ocurre es que el protocolo de nivel 6 no es un protocolo "normal". De hecho, la mayor parte de las primitivas que comunican la capa de presentación con el nivel 7 son traslación exacta de las correspondientes primitivas entre el nivel 6 y la capa de sesión.

46.1.5.6 CAPA DE PRESENTACIÓN (NIVEL 6)

A diferencia de las capas inferiores, las explicadas hasta ahora, que se ocupan solo del movimiento fiable de bits de parte a parte, la capa de presentación se encarga de la sintaxis y la semántica de la información que se transmite. Además, aísla de dichas capas inferiores el formato de los datos de las aplicaciones específicas.

Las estructuras de datos a intercambiar se tienen que definir de forma abstracta, mediante la codificación de estos datos de una manera estándar

acordada, haciendo posible así la comunicación entre computadoras con representaciones locales diferentes. La capa de presentación maneja estas estructuras de datos abstractas y las convierte de la representación de la computadora a la representación estándar de la red y viceversa.

Además de esta funcionalidad, la capa de presentación ofrece a la capa de aplicación los servicios de:

- Garantía de que la información que envía la capa de aplicación de un sistema pueda ser entendida y utilizada por la capa de aplicación de otro sistema.
- Acuerdo y negociación de la sintaxis de transferencia en la fase de establecimiento de la conexión. La sintaxis escogida puede ser cambiada durante el tiempo que dure la conexión.
- Definición del código a utilizar para representar una cadena de caracteres (ASCII, EBCDIC, etc.)
- Interpretación de los formatos de números...
- Compresión de los datos, si es necesario.
- Aplicación de procesos criptográficos, si así se requiere. Es el nivel clave para el sistema de seguridad del modelo OSI.
- Formateo de la información para su visualización o impresión.

46.1.5.7 CAPA DE APLICACIÓN (NIVEL 7)

Es la capa del modelo OSI más próxima al usuario. Difiere de las demás capas en que no proporciona servicios a ninguna otra capa OSI, sino a las aplicaciones que se encuentran fuera del modelo. Todas las capas anteriores sirven de mera infraestructura de telecomunicaciones, es decir, mantienen en buen estado el camino para que fluyan los datos. Es la capa de aplicación la que hace posible que una red se pueda usar, a pesar de estar abstraída de todas las restantes funciones necesarias para el establecimiento de la comunicación.

Las aplicaciones más importantes que hacen uso de esta capa, para que los procesos de las aplicaciones accedan al entorno OSI son, entre otras:

- Correo electrónico. Primera aplicación que se normalizó en OSI.

- Terminal virtual de red abstracta, que diferentes editores y programas puedan manejar.
- Transferencia de archivos.
- Carga remota de trabajos.
- Servicios de directorio.
- Login remoto (rlogin, telnet).
- Acceso a bases de datos.
- Sistemas operativos de red.
- Aplicaciones Cliente/Servidor...

Por supuesto, en el nivel 7 también hay cabida para aplicaciones “particulares” diseñadas por y para un núcleo reducido de usuarios, pero carecen de demasiado interés.

Las PDUs de la capa de aplicación, APDUs, son de formato muy flexible y variable. Entre dos APDUs pueden encontrarse diferencias sustanciales en cuanto a su tamaño, número de campos presentes, etc., que dependen de las necesidades de cada momento.

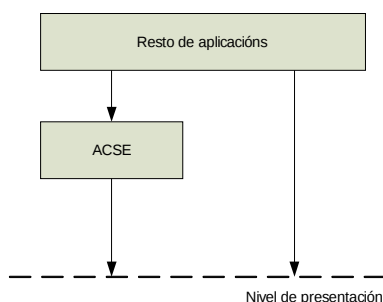
A cada una de las partes de una aplicación que se encarga de una tarea específica se le denomina Elemento de Servicio de Aplicación (ASE). El conjunto de todos los Ases que forman una aplicación concreta y la relación entre ellos forman el contexto de aplicación.

Hay ASEs válidos para varias aplicaciones:

- ACSE (Association Control Service Element). Establecimiento, manejo y liberación ordenada o abrupta de conexiones. Lo utilizan todas las aplicaciones.
- RTSE (Reliable Transfer Service Element). Garantiza la fiabilidad en la transferencia de datos, solucionando los problemas que se habían producido del nivel 4 hacia arriba. El responsable de manejar todas las funciones de nivel 5. Lo utilizan algunas aplicaciones, no todas.
- ROSE (Remote Operation Service Element). Facilita el trabajo de petición de operaciones remotas y devolución de los resultados.

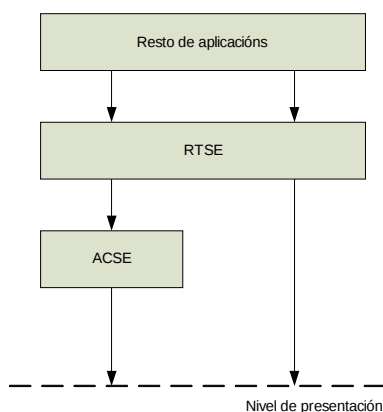
Las aplicaciones se componen de una mezcla de elementos específicos y comunes. Las siguientes figuras ilustran las relaciones entre ASEs comunes.

- Para aplicaciones que no manejan RTSE ni ROSE. Tienen que gestionar por sí mismas los puntos de sincronización, los token, etc.

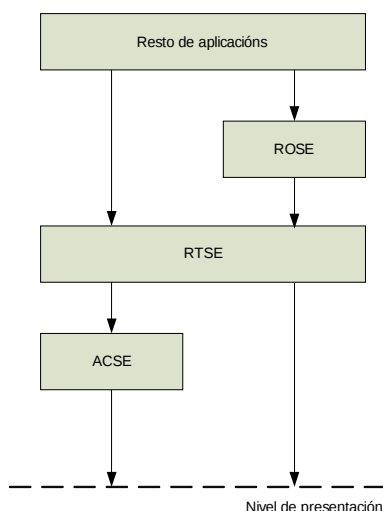


TEXTO: Resto de aplicaciones

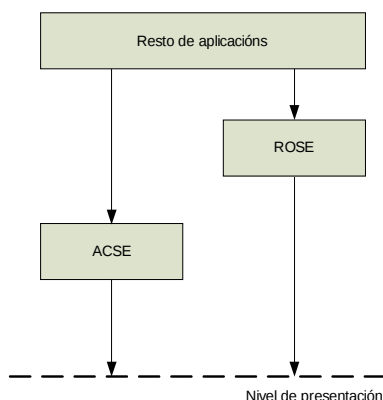
- RTSE es lo que se encarga de las RTSE actividades, los puntos de sincronización, etc. En este caso, la aplicación no maneja directamente el nivel 5, sino que lo hace a través de RTSE.



- Para las aplicaciones que hacen uso de los tres ASEs comunes.



- En este caso, ROSE trabaja directamente sobre el nivel 5.



46.1.6 CRÍTICAS AL MODELO OSI

La verdadera razón de que el modelo OSI tenga siete capas es que, en el momento de diseño, IBM tenía un protocolo patentado de siete capas, llamado SNA (System Network Architecture, Arquitectura de Red de Sistemas) y, en esa época, IBM dominaba la industria de la computación. Por otro lado, el proceso de estandarización fue demasiado largo. Cuando aún se trabajaba en la definición de OSI, ya existían implementaciones completas y gratuitas de TCP/IP y aplicaciones como e-mail, telnet, ftp, etc. Algunos de los problemas o fallos que se detectaron en el modelo de referencia OSI son:

- Aunque el modelo OSI, junto con sus definiciones y protocolos de servicios, es muy completo; hay que reconocer que los estándares son difíciles de implementar e ineficientes en su operación. Las implementaciones iniciales fueron enormes, inmanejables y lentas.

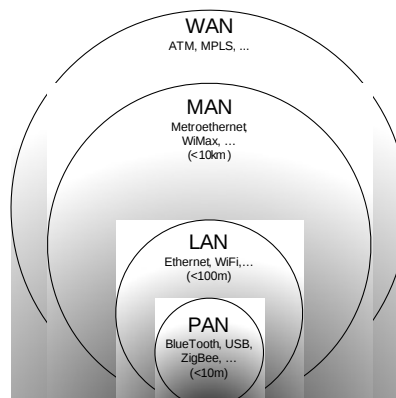
- OSI se desarrolló antes de que se hubiesen inventado los protocolos. Así que los diseñadores no supieron bien qué funcionalidad poner en cada capa.
- La capa de sesión tiene poco uso en la mayor parte de las aplicaciones.
- La capa de presentación está prácticamente vacía.
- Por el contrario, las capas de red y de enlace de datos están muy llenas, hasta tal punto que llegaron a dividirse en múltiples subcapas, cada una con funciones distintas.
- Algunas funciones, como el direccionamiento, el control de flujo y el control de errores, reaparecen una y otra vez en cada capa.
- Omisión de la administración de la red en el modelo.
- Aunque en el presente documento se situó en la capa de presentación la función de cifrado y seguridad de los datos, inicialmente se dejó fuera del modelo por falta de acuerdo sobre en qué capa colocarlo.
- En la capa de red se ofrece servicio orientado a conexión y no orientado a conexión. Sin embargo, en la capa de transporte, donde el servicio es visible a los usuarios, solo se ofrece comunicación orientada a conexión.
- El modelo está dominado por una mentalidad de comunicaciones. Las computadoras son diferentes de los teléfonos. Muchas de las decisiones tomadas son inapropiadas para la forma de trabajar de las computadoras y el software. El modelo de un sistema controlado por interrupciones no se ajusta conceptualmente a las ideas modernas de la programación estructurada.

46.2 REDES LAN, MAN Y WAN

Una de las formas clásicas de clasificar las redes es por su extensión física (o alcance) de la que se obtienen los siguientes tipos:

- Personal Area Network (PAN): red que conecta elementos próximos a una persona.

- Local Area Network (LAN): elementos en una área geográfica limitada, como son una casa, un etc.
- Metropolitan Area Network (MAN algunas veces referida como Medium Area Network conecta elementos al ancho de una o espacios de similar tamaño.
- Wide Area Network (WAN): son redes de gran extensión cubriendo ciudades, una provincia o incluso varios países.

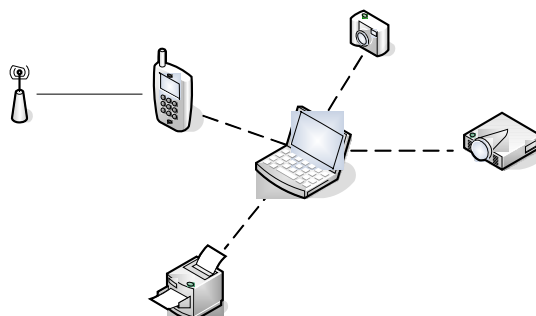


conecta
edificio,
)
ciudad

46.2.1 PAN

Una PAN es una red usada para la comunicación de ordenadores y diferentes dispositivos informáticos próximos a una persona. Algunos ejemplos de estos dispositivos usados en una PAN son PCs, impresoras, teléfonos, PDAs o consolas de videojuegos.

La necesidad de estas redes es doble, por un lado conectar dispositivos de uso personal próximos como el teléfono móvil con un manos libres o con dispositivos de recogida de datos médicos. Y por el otro permitir la movilidad de las personas aprovechando el uso y conectividad de estos dispositivos, siguiendo el ejemplo anterior, el móvil puede cambiar de conectarse a un manos libres en el coche a conectarse a otro en casa. Una PAN puede incluir dispositivos conectados por cable y dispositivos sin hilos alcanzando un máximo de 10 metros de distancia.

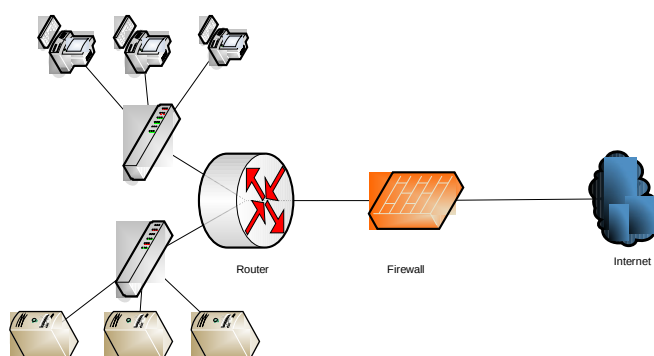


Las típicas tecnologías en las que se basan las PAN son USB y FireWire para las cableadas y BlueTooth y ZigBee para las sin hilos.

46.2.2 LAN

Una LAN conecta ordenadores y otros dispositivos en un espacio limitado como puede ser una casa, un edificio, una oficina o un conjunto de edificios próximos entre sí.

Típicamente la distancia que abarca una LAN no supera los 100 metros.



El ejemplo más común de LAN se da en el ámbito doméstico y de las pequeñas empresas donde varios equipos están conectados a un concentrador (switch), posiblemente varios servidores están conectados a otro y esos concentradores están conectados a un encaminador (router) para la conexión a Internet.

Las tecnologías dominantes usadas en las LAN son Ethernet (hoy en día gigabit ethernet) y WiFi (habitualmente 802.11g) aunque existen muchas otras tecnologías que se empiezan (o continúan) a utilizar, como pueden ser las basadas en PLC, como por ejemplo HomePlug.

46.2.3 MAN

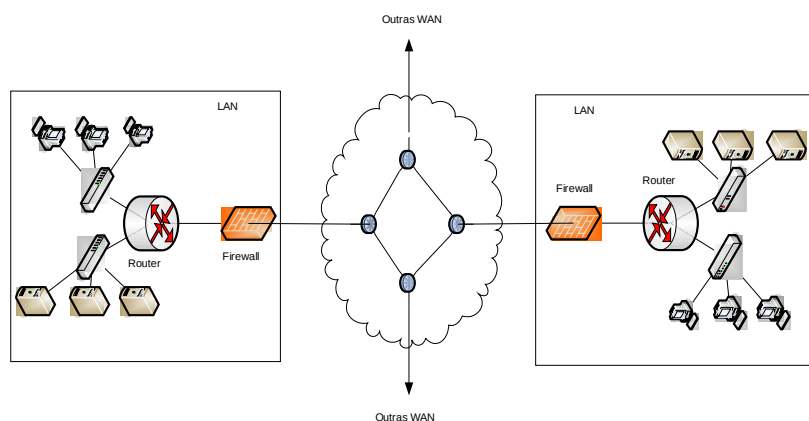
Una MAN es una red optimizada para un área geográfica mayor que una LAN, que va desde varios bloques de edificios hasta una ciudad. Una MAN puede ser propiedad de una organización pero normalmente es usada por muchos individuos y organizaciones distintas. Su utilidad típica es proporcionar conectividad entre varias LAN.

La distancia típica que cubre una MAN es de 10 km.

Tradicionalmente estas redes están basadas en tecnologías como MetroEthernet, en redes cableadas, o Wimax, en redes sin hilos.

46.2.4 WAN

Las WAN son redes de ordenadores que cubren grandes áreas y suelen enlazar varias ciudades, provincias o países.



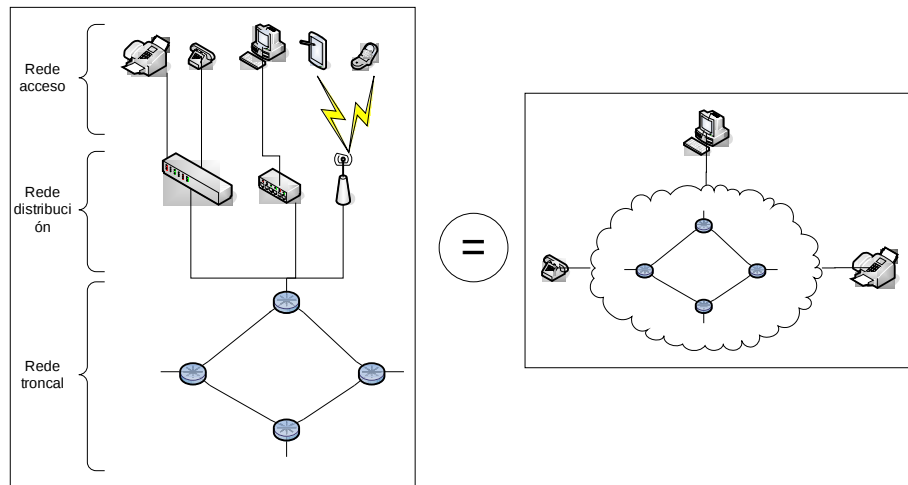
De forma análoga a las MAN la función típica de las WAN es conectar varias redes de menor extensión como varias MAN o varias LAN además de conectarse con otras redes WAN.

En contraste con los otros tipos de redes, las WAN no están limitadas a un tamaño máximo.

ATM o MPLS son algunas de las tecnologías usadas para desplegar redes WAN.

46.3 ESTRUCTURA DE REDES: TRONCAL, DISTRIBUCIÓN Y ACCESO

Las redes (ya sea la red de un operador o de una compañía) se estructuran de forma jerárquica. Esta estructura les aporta modularidad, permite aumentar los elementos de un nivel para expandir las redes sin afectar al resto de la misma (escalabilidad) y facilita la identificación y resolución de problemas.



TEXTO: Red

Normalmente esta jerarquía se divide en 3 niveles (aunque, dependiendo de la red concreta, puede haber más, por ejemplo en las redes de cable):

- Troncal (en inglés *backbone* o *core*): es la espina dorsal de la red conectando los distintos elementos del nivel de distribución.
- Distribución: conecta varios elementos del nivel inferior con el nivel superior y suele estar limitada a una de las zonas físicas (como por ejemplo una ciudad) en las que la red está presente.
- Acceso: los elementos del nivel de acceso permiten conectar los equipos finales.

46.3.1 TRONCAL

La red troncal es el nivel jerárquico más alto dentro de la división en niveles y está formada por una parte de la infraestructura de la red de ordenadores que conecta varias partes de la misma (subredes).

Normalmente la capacidad de transferencia de datos de la red troncal es mayor que la de las subredes que conecta y posee caminos redundantes (los operadores suelen usar varios anillos y en las redes corporativas suele haber varias conexiones).

De tratarse de una red corporativa el acceso a Internet acostumbra a encontrarse en la red troncal.

Un ejemplo de este tipo puede ser la red que conecta las distintas ciudades donde da servicio un proveedor de Internet.

46.3.2 DISTRIBUCIÓN

En el nivel de distribución se agregan los datos provenientes de los elementos del nivel de acceso para ser enviados al nivel superior.

Los elementos de este nivel también suelen estar redundados pero en menor medida que en el nivel superior.

De tratarse de una red corporativa es en este nivel donde se establecen las VLANs para cada departamento / división y donde se limitan los dominios de broadcast.

Siguiendo el ejemplo de antes estas podrían ser la red que conecta los distintos nodos dentro de una ciudad.

46.3.3 ACCESO

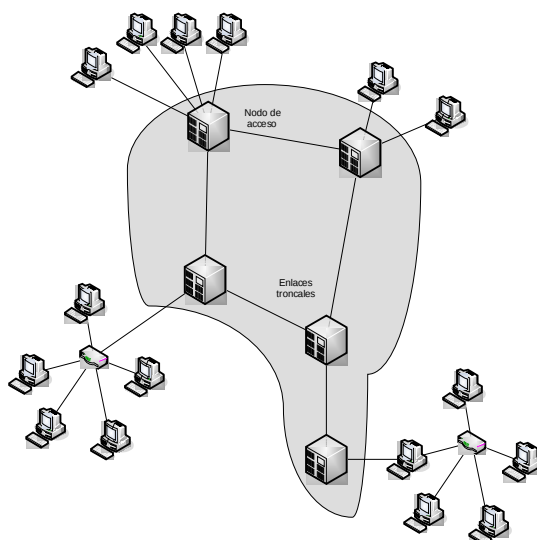
El nivel de acceso es el nivel de la red donde se conectan los equipos finales (ordenadores, teléfonos,...).

En el ejemplo anterior esta sería la red que conecta los distintos usuarios a un nodo.

46.4 REDES PÚBLICAS DE TRANSMISIÓN DE DATOS

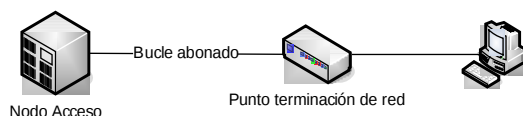
Desde el momento en que nació la necesidad de conectar dos localizaciones pasando por el dominio público, nació la necesidad de las redes públicas. Una red pública es aquella a la que cualquier entidad puede conectarse (normalmente bajo pago de una cuota) para comunicarse con otra entidad conectada a la misma red pero en distinta localización geográfica.

Esta disponibilidad de conectar cualesquiera dos entidades lleva a que haya varias entidades (individuos, compañías, gobiernos,...) conectadas a esta red, como oposición a una red personal donde sólo hay una entidad aprovechando los recursos de la red. Esto da como resultado que en muchas ocasiones las entidades quieran usar la red pública como una red personal (ya sea por simplicidad en la configuración, seguridad u otras razones) dando lugar a las Redes Personales Virtuales (VPN por sus siglas en inglés).



46.4.1 CONCEPTOS GENERALES

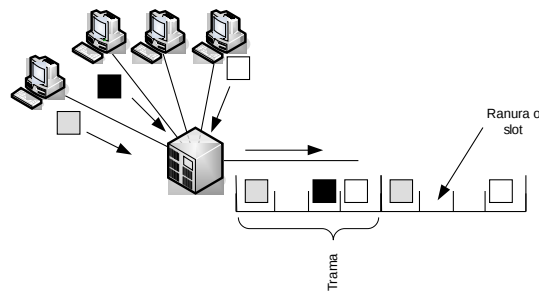
El bucle de abonado (bucle local o lazo local) es el cableado que se extiende desde los nodos de acceso (centrales de teléfonos,...) hasta el domicilio o local del usuario.



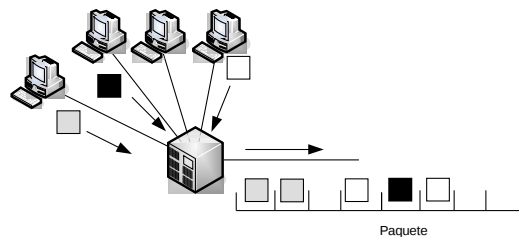
La conmutación es la conexión que realizan los diferentes nodos para lograr un camino apropiado para conectar dos usuarios de una red de telecomunicaciones. La conmutación permite la descongestión entre los usuarios de la red reduciendo el tráfico y aumentando el ancho de banda (comparándola con los sistemas basados en bus, por ejemplo).

La multiplexación es la combinación de dos o más canales de información en un sólo medio de transmisión usando un dispositivo llamado multiplexor. El proceso se conoce como demultiplexación. Existen muchas estrategias de multiplexación, según el protocolo de comunicación empleado se pueden combinar para alcanzar el uso más eficiente; las más utilizadas son:

- La multiplexación por división de tiempo el TDM (Time division multiplexing). Dentro de esta estrategia podemos encontrar:
 - a. Multiplexación estática o síncrona.



b. Multiplexación estadística o asíncrona.



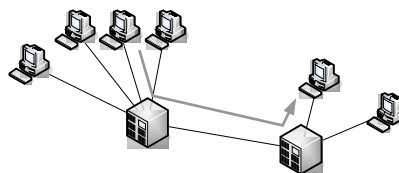
- La multiplexación por división de frecuencia el FDM (Frequency-division multiplexing) y su equivalente para medios ópticos, por división de longitud de onda o WDM (de Wavelength).
- La multiplexación por división en código o CDM (Code division multiplexing).

46.5 PROTOCOLOS DE RED

46.5.1 REDES DE CONMUTACIÓN DE CIRCUITOS

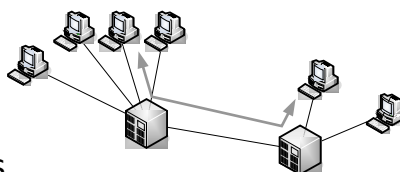
La conmutación de circuitos es un tipo de conexión que realizan los diferentes nodos de una red para lograr un camino apropiado para conectar dos usuarios. En este tipo de conmutación se establece un canal de comunicaciones dedicado entre las dos estaciones. Se reservan recursos de transmisión y de conmutación de la red para su uso exclusivo en el circuito durante la conexión.

En este tipo de redes la comunicación tiene tres fases:

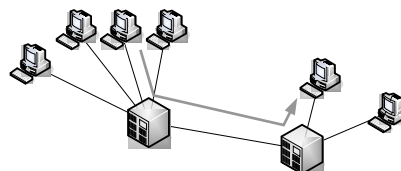


1. Establecimiento del circuito

2. Transmisión de los datos



3. Liberación del circuito



Este tipo de redes usa TDM, lo que permite disponer de un retardo fijo y predecible. Desde el punto de vista del usuario el enlace es punto a punto. Un ejemplo de este tipo de red es la Red Telefónica Conmutada (RTC).

46.5.2 REDES DE CONMUTACIÓN DE PAQUETES

La conmutación de paquetes es el sistema más usado para el envío de datos en una red de ordenadores. Un paquete es un grupo de información que consta de dos partes: los datos propiamente dichos, y una información de control, que especifica la ruta a seguir a lo largo de la red hasta el destino del paquete. Existe un límite superior para el tamaño de los paquetes; en caso de superarlo es necesario dividir el paquete en otros más pequeños. También puede existir un límite inferior para el tamaño del paquete dependiendo de la tecnología de transmisión usada.

Existen dos técnicas para la transmisión de paquetes en las redes de conmutación de paquetes:

- La basada en circuitos virtuales: Muy similar a la conmutación de circuitos, la diferencia radica en que con los circuitos virtuales la ruta no es dedicada, si no que un único enlace entre dos nodos se puede compartir dinámicamente en el tiempo por varios paquetes (TDM asíncrono). Requiere las mismas 3 fases que la conmutación de circuitos (Establecimiento del circuito, transmisión de datos y liberación del circuito).
- La basada en datagramas: No debemos establecer el circuito de forma previa a la transferencia de información. Cada paquete debe llevar la dirección de destino y se trata de forma individualizada, sin

establecer ningún vínculo con los demás paquetes que llevan datos de A a B, sean o no de la misma aplicación.

Los usuarios comparten los medios de transmisión por TDM estadístico.

Los retardos son ahora variables, dependientes de la carga instantánea en la red.

Cuando se establece el circuito virtual o cada vez que se transmite un datagrama conmutador debe seleccionar por qué enlace encamina los datos usando un algoritmo de encaminamiento. Esta decisión tiene que ser tomada por cada nodo de la red implicado. Esta decisión debe tomarse minimizando el coste (tiempo, recursos,...) y, con este fin, cada nodo construye una tabla (usando el mencionado algoritmo), llamada tabla de encaminamiento que indica por qué enlace debe transmitir los datos para llegar el destino.

En el caso de los circuitos virtuales (además de la tabla de encaminamiento que se usará para seleccionar la ruta del circuito virtual), el nodo debe construir una tabla con los circuitos virtuales, donde se asigna el identificador de un circuito virtual de un enlace (entrada) a otro enlace (salida).

Un ejemplo de red que usa circuitos virtuales es X.25 y uno de conmutación de paquetes es IP.

46.6 BIBLIOGRAFÍA

- Andrew S. Tanenbaum. Redes de computadoras. PRENTICE HALL, 1997
- ISO 7498:1984 - Information processing systems - Open Systems Interconnection

Autor: Matías Villanueva Sampayo

Director de Informática Asociación Provincial de Pensionistas y Jubilados de A Coruña

Colegiado del CPEIG

47. TECNOLOGÍAS DE ACCESO: REDES TELEFÓNICAS (RDSI, XDSL), REDES DE TELEFONÍA MÓVIL, CABLE, PLC, REDES RADIO (LMDS, WIMAX), SATÉLITE, LÍNEAS PUNTO A PUNTO, METROETHERNET.

Tema 47. Tecnologías de acceso: redes telefónicas (RDSI, xDSL), redes de telefonía móvil, cable, PLC, redes radio (LMDS, Wimax), satélite, líneas punto a punto, MetroEthernet.

47.1 Redes telefónicas (RDSI, xDSL)

47.1.1 RDSI

47.1.1.1 Ventajas de RDSI

47.1.1.2 RDSI de banda estrecha

47.1.1.3 RDSI de banda ancha

47.1.1.3.1 Servicios RDSI-BA

47.1.2 XDSL

47.1.2.1 ADSL

47.1.2.1.1 Arquitectura ADSL

47.1.2.1.2 Nivel físico

47.1.2.2 HDSL

47.1.2.3 SDSL

47.1.2.4 VDSL

47.2 Redes de telefonía móvil

47.2.1 GSM

47.2.1.1 Arquitectura de la red GSM

47.2.2 GPRS, HSCSD

47.2.2.1 GPRS

47.2.2.1.1 Arquitectura de GPRS

47.2.2.1.2 EDGE o E-GPRS

47.2.2.2 HSCSD

47.2.3 Sistemas de tercera generación: UMTS

47.2.3.1 HSPA

47.3 Cable

47.4 PLC

47.5 Redes radio (LMDS, Wimax)

47.5.1 LMDS

47.5.2 WIMAX

47.6 Satélite

47.7 Líneas punto a punto

47.7.1 X.25

47.7.2 FrameRelay

47.7.3 MetroEthernet

47.8 MetroEthernet

47.8.1 MAN basada en Ethernet

47.8.2 MAN basada en SDH

47.8.3 MAN basada en MPLS

47.9 Bibliografía

47.1 REDES TELEFÓNICAS (RDSI, XDSL)

Originalmente la única red pública disponible era la Red Telefónica Conmutada (RTC) que estaba compuesta por elementos analógicos siendo su principal objetivo el transporte de la voz que se transmitía por líneas modulada como una forma de onda analógica.

Para poder transmitir datos sobre esta red se necesitaba convertir la señal digital en una señal analógica en el origen y volver a convertirla en digital en el destino. Dado que las líneas de voz se pensaron solo para transmitir voz usaban conmutación de circuitos. Además, debido a que no fueron diseñadas para garantizar la transmisión sin pérdida, eran los protocolos de transmisión de datos los que debían garantizar la corrección de errores, reconexión, etc.

Posteriormente, para solucionar el problema de la pérdida de calidad del sonido en las llamadas a larga distancia aparecieron las centrales digitales, menos propensas a fallos, y permitieron controlar más líneas de usuario y realizar las conexiones mucho más rápido. De esta forma, una comunicación por una línea telefónica convencional se realiza de forma analógica en el bucle de abonado, pero de forma digital hasta llegar a la central donde está conectado el abonado destino. La RDSI (Red Digital de Servicios Integrados) supone el último avance: la comunicación digital entre el abonado y la central telefónica.

47.1.1 RDSI

RDSI es una red desarrollada a partir de la red telefónica que proporciona una conexión digital extremo a extremo y que soporta una gran variedad de servicios.

Se denomina “Digital” porque se basa en técnicas digitales, garantizando la integridad de la información y la transmisión de la misma libre de degradaciones o perturbaciones externas; y es “de Servicios Integrados” porque utiliza la misma infraestructura para muchos servicios que tradicionalmente requerían interfaces distintos (télex, voz, conmutación de circuitos, conmutación de paquetes, etc.).

Las características más importantes son:

- Su arquitectura está estratificada en niveles: físico, enlace y red.
- Proporciona conexiones de 64Kbps.
- La señalización va por un canal diferente a la información propiamente dicha. En ciertas ocasiones se utiliza el canal de señalización para enviar información aunque a una velocidad más baja.
- Soporta una gran variedad de aplicaciones, independientemente de si están basadas en conmutación de circuitos o de paquetes.

47.1.1.1 VENTAJAS DE RDSI

Entre las ventajas que ofrece RDSI se pueden destacar:

- Velocidad. Ofrece múltiples canales digitales que pueden operar simultáneamente a través de la misma conexión telefónica entre central y el usuario. Usando un protocolo de agregación de canales se puede alcanzar una velocidad de datos sin comprimir de unos 128 Kbps, en el servicio de acceso básico. Este esquema permite una transferencia de datos a una velocidad mucho mayor que la línea telefónica. Además, el tiempo necesario para establecer una comunicación en RDSI es aproximadamente la mitad del tiempo empleado con una línea analógica.

- Conexión de múltiples dispositivos. Es posible combinar diferentes fuentes de datos digitales y hacer que la información llegue al destino correcto. Como la línea es digital, es fácil controlar el ruido y las interferencias producidas al combinar las señales.
- Señalización. En una conexión RDSI la llamada se establece enviando un paquete de datos especial a través de un canal independiente de los canales para datos. Permite establecer la llamada en un par de segundos.
- Servicios. La RDSI no se limita a ofrecer comunicaciones de voz. Ofrece otros muchos servicios como transmisión de datos informáticos (servicios portadores), télex, facsímile, videoconferencia (usando, por ejemplo, H.320), conexión a Internet y opciones como llamada en espera, identidad del origen, etc.

En función del ancho de banda se distinguen entre RDSI de “banda estrecha” que permite velocidades de 64Kbps o agrupaciones de esta velocidad hasta 1984Kbps y RDSI de banda ancha donde la velocidad mínima a la que se trabaja es 2Mbps, pudiendo llegar hasta los 100Mbps.

47.1.1.2 RDSI DE BANDA ESTRECHA

La RDSI dispone de tres tipos de canales:

- Canal B. Los canales tipo B transmiten información en modo circuito o en modo paquete a 64Kbps y se emplean para transportar cualquier tipo de información de usuario, bien sea voz o datos.
- Canal D. Se utiliza principalmente para enviar información de control, como es el caso de los datos necesarios para establecer una llamada o para liberarla. Estos canales trabajan a 16Kbps o 64kbps según el tipo de servicio contratado.
- Canales H. Combinando varios canales B se obtienen canales tipo H, que también son canales para transportar solo información de usuario pero a velocidades mucho mayores. Hay varios tipos de canales H:
 - Canales H0, que trabajan a 384Kbps (6 canales B).

- Canales H10, que trabajan a 1472Kbps (23 canales B).
- Canales H11, que trabajan a 1536Kbps (24 canales B).
- Canales H12, que trabajan a 1920Kbps (30 canales B).

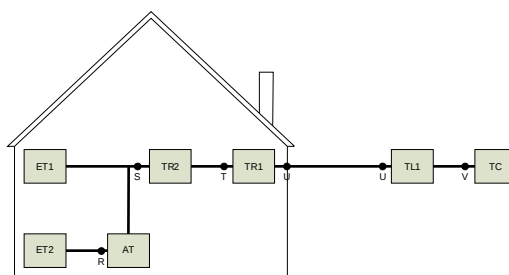
Un usuario puede contactar dos tipos de servicio diferentes con el proveedor telefónico según sus necesidades:

- Acceso básico o BRI (Basic Rate Interface). Proporciona dos canales B y un canal D.
- Acceso primario o PRI (Primary Rate Interface). En Europa el PRI consta de 30 canales B y un canal D. En este caso, los canales B también pueden estar agrupados como 5 canales H0 o un canal H12.

La RDSI ofrece la capacidad de agregar canales para realizar conexiones a mayor velocidad.

En un acceso básico una llamada a 128Kbps son en realidad dos llamadas diferentes a 64Kbps cada una, existiendo un protocolo por encima que permite ver esa llamada como una sola. Muchos fabricantes de hardware para RDSI permiten la agregación de canales utilizando protocolos propios. Para garantizar la compatibilidad entre equipos de diversos fabricantes es conveniente que el hardware soporte el protocolo MPPP (Multilink Point to Point Protocol).

La configuración de referencia se define por agrupaciones funcionales y puntos de referencia o interfaces, como se muestra en la figura:



Las agrupaciones funcionales son:

- TC (Terminación de Central). Situada en la central de conmutación, se encargara del mantenimiento del Acceso del Usuario.
- TL (Terminación de Línea). Situada en la central, se encarga de los aspectos de transmisión.

- TR1 (Terminación de Red nº 1). Dispositivo frontera que separa las instalaciones de usuario de las de la red y convierte los dos hilos de la interfaz U en los cuatro hilos empleados en una interfaz T o S/T. Siempre lo proporciona el proveedor del servicio. En general, realiza funciones del nivel físico.
- TR2 (Terminación de Red nº 2). Convierte la interfaz T en una interfaz S. Hace referencia a una centralita o PABX (Private Automatic Branch Exchange). En el acceso básico el TR2 no existe, con el que el punto de referencia S y el T coinciden, pasándose a llamar este punto S/T.
- ET1 (Equipo Terminal nº 1). Es un terminal específico para RDSI, preparado para la señalización en modo paquete y gestión de canales de información.
- AT (Adaptador de Terminal). Se trata de un equipo RDSI que tiene la capacidad de adaptar interfaces. Convierte las señales de otros equipos no RDSI a señales adecuadas a la interfaz correspondiente, S y/o T.
- ET2 (Equipo Terminal nº 2). Equipos no RDSI que pueden conectarse mediante un AT al bus RDSI.

Los Puntos de Referencia o interfaces son:

- V. Representa la separación entre las funciones de conmutación y transmisión en la central.
- U. En un acceso básico está formado por la línea típica de un par trenzado de hilos procedente de la red telefónica. En un acceso primario está formado por una línea de cable coaxial o fibra óptica que se suele conectar directamente a una central local de distribución o PABX que actúa como TR2.
- T. Representa la separación entre la transmisión de línea y la transmisión en el domicilio del cliente. Consta de cuatro hilos, dos para recibir y dos para enviar datos, permitiendo también una conexión full dúplex.

- S. Representa la interfaz de conexión física de los equipos terminales RDSI y define la estructura de la trama, la gestión del Canal D, la sincronización y las características de transmisión.
- R. Representa una interfaz no normalizada en RDSI.

La RDSI se estructura en tres capas: física, de enlace y red:

- Física. Las funciones más destacadas de este nivel son la codificación de datos digitales para la transmisión a través de la interfaz correspondiente, transmisión full dúplex, formación de la trama, activación y desactivación del circuito físico, etc.
- Enlace. Este nivel emplea principalmente el protocolo LAP-D (Link Access Protocol o protocolo de acceso al enlace). Proporciona al nivel superior un servicio orientado a conexión con transferencia de información confirmada, servicio sin conexión con transferencia de información no confirmada y servicios de administración, que permiten identificar los equipos específicos dentro del bus S/T asociado a una conexión RDSI.
- Red. En esta capa, la Recomendación Q.931 especifica los procedimientos para establecer, mantener y liberar las conexiones en la interfaz usuario-red. Se manejan distintos tipos de mensajes: de establecimiento de llamada, durante la fase de transmisión de información, de liberación de la llamada y otros.

47.1.1.3 RDSI DE BANDA ANCHA

La RDSI de banda ancha representa un término medio entre la conmutación de circuitos pura y la conmutación de paquetes pura. El servicio ofrecido está orientado a conexión, pero internamente se implementa con conmutación de paquetes. La RDSI-BA está basada en la tecnología ATM. Las razones que llevaron a elegir esta tecnología fueron, entre otras, que permite manejar tanto tráfico de velocidad constante como variable y que, a velocidades altas, la conmutación digital de celdas es más fácil que las técnicas tradicionales de multiplexación. Las velocidades que pueden alcanzar RDSI-BA dependen de las tecnologías

concretas usadas en la red y van desde un mínimo de 2 Mbps hasta los 155 o 622Mbps.

En ATM, el flujo de información se organiza en bloques de tamaño fijo y pequeño (53 bytes), llamados celdas. No se garantiza la entrega de todas las celdas, pero las que llegan lo hacen en orden. El modelo ATM también se divide en capas:

- Capa física. Tiene que ver con el medio físico. Se divide en dos subcapas: PDM (Physical Medium Dependent) y TC (Transmisión Convergence).
- Capa ATM. Tiene que ver con las celdas y su transporte.
- Capa de adaptación de ATM (AAL, ATM Adaptation Layer). Permite a los usuarios enviar paquetes mayores que una celda. Se divide en dos subcapas: SAR (Segmentation And Reassembly) y CS (Convergence Sublayer).

ATM se tratará en otro tema más en detalle.

47.1.1.3.1 SERVICIOS RDSI-BA

En la RDSI de Banda Ancha se pueden incorporar distintos tipos de servicios que podemos clasificar en servicios interactivos y servicios de distribución.

Dentro de los servicios interactivos podemos encontrar:

- Servicios conversacionales, como pueden ser:
 - o Videoconferencia
 - o Video vigilancia
 - o Fax de alta velocidad
 - o Transferencia de documentos
- Servicios de mensajería:
 - o Video-mail
 - o Correo con contenido multimedia
- Servicios de consulta:
 - o Videotex
 - o Recuperación de datos, documentos, etc.

Ejemplos de servicios de distribución podrían ser:

- Servicios sin control de presentación:
 - o Televisión
 - o Televisión a la carta
 - o Distribución de documentos
 - o Video bajo demanda
 - o ...
- Servicios con control de presentación:
 - o Video

47.1.2 XDSL

Una Digital Subscriber Line (DSL) es el nombre que identifica a todos los estándares digitales sobre bucle de abonado, un ejemplo es la RDSI. Por su parte xDSL identifica un conjunto de estándares para bucle de abonado sobre hilo de cobre como son (entre otras):

- ADSL (Asymmetrical Digital Subscriber Line)
- SDSL (Symmetrical Digital Subscriber Line)
- HDSL (High data rate Digital Subscriber Line)
- VDSL (Very high rate Digital Subscriber Line)

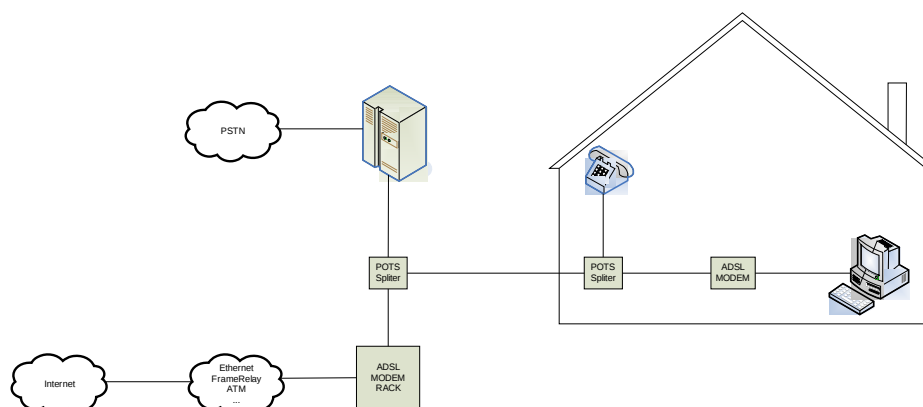
47.1.2.1 ADSL

Proporciona servicios digitales de alta velocidad sobre redes de pares de cobre existentes. Permitiendo trabajar sin interferir con los tradicionales servicios de voz analógica (POTS Plain Old Telephone Service).

Utiliza técnicas eficientes de codificación de línea como QAM. Y soporta nuevos servicios sobre un par trenzado simple, como el acceso a Internet de alta velocidad.

Su ancho de banda asimétrico (64-640 kbit/s upstream, 500 kbit/s - 8 Mbit/s downstream) la hace atractiva para la mayoría de las aplicaciones cliente/servidor como el acceso a Web, acceso a LAN remotas, donde tradicionalmente el cliente recibe mucha más información del servidor de la que genera.

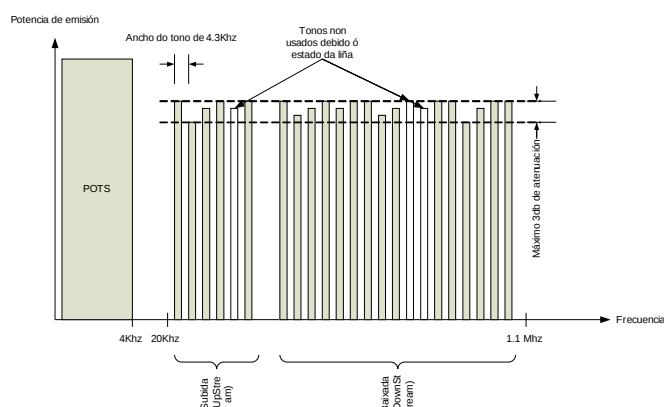
47.1.2.1.1 ARQUITECTURA ADSL



La arquitectura de ADSL hace uso de filtros tanto en el domicilio del abonado como en la central para separar la señal del teléfono y de la conexión de datos, estos filtros se llaman splitters. En el domicilio del abonado el teléfono se conectará directamente a la salida correspondiente del splitter mientras que los equipos de transmisión de datos necesitarán un MODEM ADSL. En la central la salida del splitter correspondiente se conecta a la PSTN (Public Switching Telephone Network o RTC) mientras que la salida de datos se conecta a uno de los módems de la central que está conectado a la red de distribución que a su vez está conectada a Internet.

47.1.2.1.2 NIVEL FÍSICO

El canal se divide en tres bandas diferentes, se utiliza DMT (Discrete Multi-Tone) que permite utilizar diferentes portadoras (codificadas en QAM) en distintas frecuencias:



TEXTOS: Tonos no usados debido al estado de la línea. Bajada.

DMT utiliza a codificación QAM para conseguir codificar más bits en frecuencias

donde la señal presenta menos interferencias. De esta forma se modulan un número variable de bits en cada una de esas portadoras, dependiendo este número de las características del cable de pares, del espectro de frecuencias y de las interferencias en la señal. De este modo, los rateos de velocidad pueden ser optimizados haciendo posible el uso del mismo módem sobre bucles locales con diferentes características.

La velocidad de bajada depende de un buen número de factores, entre ellos:

- Longitud de la línea de cobre.
- Sección del cable.
- Presencia de bobinas de carga, por atenuación en líneas analógicas.
- Interferencias por paradiafonía.

El alcance depende de la velocidad y va desde 2,7 Km. (a la máxima velocidad en el peor caso) hasta 5,5 Km. (la baja velocidad en el mejor caso).

Actualmente este estándar ha evolucionado existiendo ADSL2 y ADSL2+ que proporcionan mayor velocidad (12 Mb en el caso de ADSL2 y 24Mb en el caso de ADSL2+) simplemente usando más espectro de frecuencias.

47.1.2.2 HDSL

HDSL es simplemente una forma mejor de transmitir circuitos T1 o E1 (32 canales de 64Kbs) sobre líneas de pares de cobre. Necesita un menor ancho de banda para transmitir estas líneas y no necesita utilizar repetidores.

Utilizando avanzadas técnicas de modulación, HDSL transmite 1,544 Mbps o 2,048 Mbps utilizando rangos de frecuencia entre 80 Khz. y 240 k.o., bastante menos con los 1,5 MHz necesarios para las E1/T1 tradicionales.

Sobre un cable con un calibre 24 AWG (0,5 mm) la distancia que se puede alcanzar es de aproximadamente 3,7 Km. aunque puede llegar los 4,5 Km., siempre sobre dos

pares de cobre.

Este tipo de tecnología se utiliza para conexiones entre PBX, conexiones entre estaciones de antenas celulares, circuitos digitales, servidores de Internet y Redes de Datos Privadas. Pero no está falta de problemas, siendo los más destacables:

- La existencia de gran cantidad de implementaciones propietarias de HDSL pues el estándar solo contempla las características básicas.
- Los beneficios técnicos son transparentes a los usuarios, pues ellos siguen percibiendo una T1/E1 aunque se podrían alcanzar mejores rendimientos en términos de velocidad y de costes.
- Para distancias mayores de 3,7 Km. se necesitan repetidores.
- La necesidad de utilizar múltiples pares de hilos, reduce la disponibilidad del servicio T1/E1 en un área determinada entre un 50 y 66 por ciento. Además, muchas veces existen problemas para encontrar 2 ó 3 pares libres dentro de la misma ruta.

Al igual que con ADSL, HDSL evolucionó tratando de eliminar los problemas de la primera generación a HDSL2 que simplemente usa menos hilos.

47.1.2.3 SDSL

SDSL (Symmetrical Digital Subscriber Line) puede referirse a:

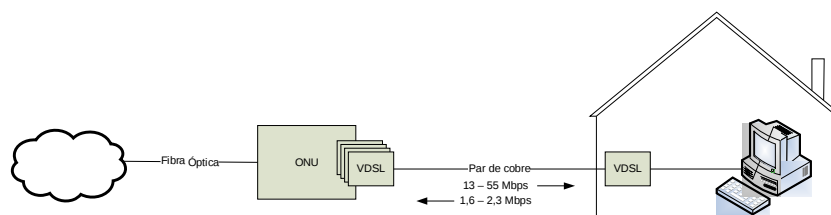
- En un sentido amplio a cualquier tecnología DSL simétrica
- O a un estándar concreto que proporciona servicios T1/E1 (el caso que nos ocupa)

SDSL permite la transmisión de señales T1 o E1 sobre un único par de cobre. Esto supone una gran ventaja sobre HDSL puesto que se pueden usar líneas individuales extendiéndose el servicio a domicilios particulares. La distancia máxima de SDSL es de 3 Km., distancia a la que un ADSL podría operar la 6 Mbps.

47.1.2.4 VDSL

Es una de las más recientes tecnologías de la familia xDSL, confía en que el tendido de cobre será corto ya que las operadoras están instalando cada vez más tramos de F.O. (Fibra Óptica), puesto que quieren ofrecer nuevos

servicios que requieran la combinación de voz, video y audio, lo cual solo es posible con transportes como el ofrecido por ATM. VDSL está preparado para actuar como capa física que dé soporte a redes ATM. Para lograrlo, VDSL incluye una unidad de red óptica (ONU) que se encarga de convertir y concentrar señales VDSL sobre una red de fibra.



Problemas de VDSL:

- Es muy sensible a las interferencias de radio. A las frecuencias a las que trabaja, un bucle de abonado se comporta como una antena receptora para este tipo de señales.
- VDSL fue diseñada para trabajar sobre redes ATM.
- ADSL tiene un coste mucho menor, pues los filtros pueden instalarse en la propia central local. Con VDSL se necesitan ONU residenciales que deben ser instalados y mantenidos por la operadora.

Al igual que con las tecnologías xDSL anteriores VDSL tiene su evolución en VDSL2 capaz de proporcionar 250Mbps de bajada.

47.2 REDES DE TELEFONÍA MÓVIL

47.2.1 GSM

La tecnología GSM pertenece a los sistemas de segunda generación, que al igual que otros como CDMA, TDMA, NADC o PDC se caracterizan porque son digitales. GSM se implantó en Europa y en otros países del resto del mundo, mientras que TDMA y CDMA se implantaron en EEUU, y PDC en Japón.

GSM utiliza multiplexación por división del tiempo (TDM), lo que posibilita que en cada frecuencia se puedan transmitir varias conversaciones; el tiempo de transmisión se divide en pequeños intervalos de tiempo, cada uno de los cuales puede ser utilizado por una transmisión distinta. Además, una misma conversación se lleva a cabo en intervalos de distintas

frecuencias, con lo que no se puede asociar una llamada a una frecuencia. Esto tiene la ventaja de que si una de las frecuencias se ve afectada por una interferencia, una conversación que utilice esta frecuencia solo observará problemas en los intervalos pertenecientes a dicha frecuencia. Esto se denomina TDMA.

El sistema GSM tiene asignadas dos bandas de frecuencias, 900 Mhz (llamado GSM-900) y 1800 Mhz (llamado DCS-1800). En cada una de las bandas, las frecuencias más bajas se usan para el enlace ascendente y las más altas para el descendente. Así, en la banda de los 900 Mhz, las frecuencias comprendidas entre los 890 y 915 Mhz comprenden 125 portadoras, cada una de ellas con un ancho de banda de 200 KHz para transmisiones móvil-estación base. De la misma manera, la banda comprendida entre los 935 y los 960 Mhz se subdivide en otras 125 portadoras de 200 KHz para transmisiones estación base-móvil.

Además, existe también una tercera banda de frecuencia en los 1900 Mhz, en los que GSM opera en algunos países como EEUU.

Cada portadora subdivide en 8 canales lógicos o slots, cada uno de ellos tiene su uso particular: señalización, control de la comunicación o tramas de información.

En GSM, la señalización se realiza por el canal común, según el protocolo SS7.

GSM es un sistema basado en conmutación de circuitos y por tanto es un servicio orientado a conexión, es decir, en toda comunicación habrá 3 etapas diferenciadas: establecimiento, comunicación y liberación. En GSM, lo que se tarifica justo es el establecimiento de un canal.

La tasa de transmisión que se alcanza con GSM es de 9'6 Kbps.

47.2.1.1 ARQUITECTURA DE LA RED GSM

La arquitectura GSM se basa en tres subsistemas diferenciados:

- Subsistema estación base (BSS): Agrupa las máquinas específicas a los aspectos de radio y celulares del GSM. El BSS está en contacto directo que las estaciones móviles a través del interfaz radio. El BSS

incluye dos tipos de elementos: la Estación de Base (BTS, Base Transceiver Station) y el Controlador de Estaciones de Base (BSC, Base Station Controller).

- Subsistema conmutación (NSS): Incluye las funciones básicas de conmutación del GSM, así como las bases de datos necesarias para los datos de usuario y la gestión de la movilidad. La función principal del NSS es gestionar las comunicaciones entre los usuarios GSM y los usuarios de otras redes de telecomunicación. Dentro del NSS, la función básica de conmutación se realiza en la MSC (Mobile services Switching Centre), cuya misión principal es coordinar el establecimiento de llamadas desde y hasta usuarios GSM.
- Subsistema operación y mantenimiento (OMS): Controla y monitoriza el estado general de la red. Se componen de los siguientes elementos:
 - o HLR: Home Location Registry. Existe un solo HLR por compañía. En esta base de datos se guarda la información estática del abonado (servicios contratados, etc.) y dinámica (dónde se localiza el móvil en un determinado momento)
 - o EIR: base de datos utilizada para comprobar la pertenencia del dispositivo móvil a la red del operador, mediante el chequeo del número IMEI, que es un código que identifica unívocamente el móvil, una especie de número de serie del aparato.
 - o AUC: centro de autenticación de usuarios
 - o OMC: Centro de gestión de la red (mantenimiento)

47.2.2 GPRS, HSCSD

GPRS y HSCSD pertenecen a los denominados sistemas de la generación 2'5, que harán de puente entre los de segunda y tercera generación (UMTS, que se verá mas adelante).

47.2.2.1 GPRS

GPRS significa "General Packet Radio Service". Como su nombre indica, se trata de un servicio portador basado en la conmutación de paquetes, que

se realiza utilizando la red GSM actual, aunque necesitan terminales que la soporten.

Las principales características de GPRS son las siguientes:

- Velocidad: la velocidad máxima teórica es de 171'2 Kbps, aunque se habla de una velocidad de conexión máxima en la práctica de 115 Kbps.
- Inmediatez: GPRS facilita las conexiones instantáneas tan pronto como se necesita enviar o recibir información; se puede decir que con GPRS estamos siempre conectados.
- Noticias y mejores aplicaciones: gracias a la mayor velocidad de GPRS.
- Tarificación: GPRS se tarifica por volumen de datos intercambiado, calidad de servicio y tipo de servicio; en GSM por el contrario se tarifica por duración de la llamada.

47.2.2.1.1 ARQUITECTURA DE GPRS

Como dijimos anteriormente, el sistema GPRS se despliega sobre la red GSM existente, aunque requiere de algunos elementos nuevos como:

- El nodo GGSN (Gateway GPRS Support Node): este nodo es la interfaz con las redes de datos externas, como X.25 y las redes IP
- El nodo SGSN (Serving GPRS Support Node): nodo de conmutación de paquetes, al mismo nivel que las centrales convencionales de GSM (las MSC)
- Estructura principal o red troncal GPRS (backbone)

47.2.2.1.2 EDGE O E-GPRS

EDGE responde a las siglas de Evolved (o Enhanced) Data rates for GSM Evolution. No es en sí una nueva arquitectura, si no un avance de la modulación del canal, es decir, es una versión mejorada de GPRS.

Con estas técnicas se consigue hasta 384 Kbps, combinando hasta 8 slots.

47.2.2.2 HSCSD

HSCSD (High Speed Circuit Switched Data) es una especificación homologada por el ETSI (European Telecommunication Standard Institute),

que supone una evolución de GSM, ya que aprovecha dicha infraestructura. Se trata de un servicio multi-slot para la transmisión de datos a alta velocidad mediante circuitos conmutados.

El HSCSD aporta un esquema de codificación mejorado que permite 14'4 Kbps, frente a los 9'6 Kbps de GSM, lo cual posibilita velocidades de transmisión de datos de hasta 57'6 Kbps combinando hasta 4 canales GSM. HSCSD fue desarrollado en paralelo con GPRS pero son servicios de alta velocidad totalmente diferentes. Como su propio nombre indica HSCSD utiliza la conmutación de circuitos a diferencia de GPRS que utiliza la conmutación de paquetes.

La ventaja de HSCSD sobre GPRS es la calidad de servicio garantizada, proporcionada por el canal de comunicación dedicado. Esto, sin embargo, la hace menos eficiente para la transmisión de datos pues la conexión tiene que mantenerse incluso en los momentos en los que no existe transmisión de datos. GPRS hace un uso más eficiente del ancho de banda y permite hacer la tarificación en función de la cantidad de contenido que se recibe y no solo en función del tiempo de conexión.

47.2.3 SISTEMAS DE TERCERA GENERACIÓN: UMTS

UMTS es el tercer escalón en la historia de la telefonía móvil, después de la analógica y la digital. UMTS son las siglas de Universal Mobile Telecommunication System o Sistema Universal de Comunicaciones Móviles. UMTS es un miembro de la familia global IMT-2000 del sistema de comunicaciones móviles de “tercera generación” del UIT (Unión Internacional de Telecomunicaciones). Este sistema es revolucionario ya que por primera vez se trata de un estándar universal.

El funcionamiento también es novedoso, ya que el usuario paga según la cantidad de información que se descargue de la red, y no ya por el tiempo de uso del servicio. De esta forma podremos estar constantemente conectados a la red, lo que permite, por ejemplo, acceder al correo electrónico de forma instantánea.

Esta tecnología permite que los teléfonos transmitan y reciban datos con una velocidad 200 veces superior a la de GSM. La máxima velocidad del

UMTS es 2 Mbits. Este tope puede alcanzarse solamente si la red está al máximo nivel, el usuario está parado y sin móviles a su alrededor.

UMTS también plantea importantes innovaciones con respecto a la arquitectura de red. UMTS R'99 definió una arquitectura que da cabida a redes de acceso GSM y a la red de acceso UMTS (UTRAN), y proponen una red central (CN, Core Network) diseñada como una evolución de la red GSM/GPRS para facilitar la migración de redes GSM/GPRS a UMTS.

UMTS ofrece un nuevo interfaz radio denominado UTRA (UMTS Terrestrial Radio Access). Dicho interfaz está basado en tecnología CDMA (Code Division Multiple Access) permitiendo aumentar considerablemente la velocidad de transferencia de datos, y soporta dos modos de operación el FDD (Frequency Division Duplex) y el TDD (Time Division Duplex). FDD está basada en un esquema de Secuencia Directa CDMA y soporta una velocidad de hasta 384 Kbit/s. El TDD está basado en la multiplexación en tiempo y en código, se diseñó y se optimizó para ser usado en zonas con alta densidad de tráfico, y soporta una velocidad de hasta 2 Mbit/s.

Entre las cosas que nos ofrece UMTS, destacamos su facilidad de uso y bajos costes, nuevos y mejores servicios, acceso rápido, transmisión de paquetes de datos y velocidad de transferencia de datos a pedido, entorno de servicios amigable y consistente, movilidad de cobertura y servicios UMTS disponibles globalmente por satélite.

Su velocidad sumada al soporte inherente del Protocolo de Internet (IP), se combinan para prestar servicios multimedia interactivos y nuevas aplicaciones de banda ancha, tales como servicios de video telefonía y videoconferencia.

47.2.3.1 HSPA

High-Speed Downlink Packet Access (HSDPA) es un protocolo mejorado de la tercera generación que pertenece a la familia High-Speed Packet Access (HSPA) también conocida como 3.5G, 3G+ o turbo 3G. HSDPA permite a las redes UMTS tener un ancho de banda de descarga mayor que actualmente puede ser de 1,8, 3,6, 7,2 y 14,4 Mbps. Ya está disponible también HSPA+

que entrega hasta 84Mbps gracias al uso de varias antenas (MIMO Multiple Input Multiple Output).

High-Speed Uplink Packet Access (HSUPA) es otro de los protocolos HSPA que permite una velocidad de subida de 5,76Mbps. El nombre HSUPA fue acuñado por Nokia, el nombre oficial es Enhanced Uplink (EUL).

47.3 CABLE

Las redes de cable actuales presentan las siguientes características: servicios integrados, alta capacidad, y redundancia. Los servicios que ofrece una red de cable moderna incluyen los siguientes: amplia oferta de canales de TV (terrestres, vía satélite, y de producción propia), video a la carta, PPV, datos e Internet (mediante módem cable), telefonía (básica y RDSI, con opción de acceso a Internet), alquiler de líneas y fibras.

La transmisión de la señal hasta el abonado se lleva a cabo mediante el canal denominado descendente o directo (de 86 a 862 MHz), mientras que las que parten del abonado se realizan a través del canal ascendente o de retorno (de 5 a 65 MHz).

La topología de una red de cable basada en tecnología HFC (Hybrid fibre-coaxial):

- Red troncal primaria: a nivel físico anillos redundantes de fibra óptica, a nivel lógico topología de estrella. Estos anillos comunican la cabecera con los nodos primarios. El respaldo es activo.
- Red secundaria o de distribución: conecta un nodo primario con varios nodos secundarios a través de anillos con arquitectura en estrella formando lóbulos que abarcan 12.000 hogares. Cada lóbulo interconecta 5 o 6 nodos secundarios. Hay redundancia en ruta y equipos. El servicio de telefonía a veces no se proporciona mediante la red HFC (es decir, no presenta telefonía integrada), si no que hace uso de una red paralela de tipo SDH (Synchronous Digital Hierarchy), hablándose entonces de telefonía superpuesta.
- Red terciaria o de dispersión: conecta cada nodo secundario con cada uno de los cuatro nodos ópticos terminales que dependen de él. Cada

nodo óptico terminal cubre un área de 500 hogares. La red de dispersión presenta una disposición en estrella sin redundancia en ruta. En el nodo secundario se realiza la interconexión de las fibras provenientes del nodo primario con las fibras que van hasta los nodos terminales.

- Red de distribución de coaxial: distribuye las señales desde el nodo óptico terminal hasta cada punto de derivación en los edificios a los que da servicio. La distribución se realiza con estructura en árbol, de forma que cada nodo óptico terminal da lugar a 4 ramas de unos 125 hogares aproximadamente. Los nodos ópticos terminales se ubican físicamente en armarios de exterior. El nodo óptico terminal realiza la conversión óptico-eléctrica de las señales transportadas en sentido descendente. De él va a los amplificadores que atacan las cuatro ramas de coaxial que parten del nodo óptico. Cada rama de coaxial alimenta (si es necesario, mediante amplificadores) a una red de derivadores, cuyas salidas están conectadas a las atacadas individuales de abonado. Para el camino de retorno se utiliza la misma infraestructura de red, equipando adecuadamente a los amplificadores.
- Red de atacada de abonado: conecta la red de distribución de coaxial con el punto de terminación de red. Existen dos arquitecturas:
 - o Estrella: un mismo derivador da servicio a todas las viviendas de las diferentes plantas de un edificio.
 - o Árbol: se coloca un derivador en cada planta, del que parten los coaxiales que dan servicio a los abonados de esa planta.La red de atacada de abonado se puede dividir en dos partes: cableado de edificio o verticales, y cableado de vivienda.

Las redes HFC tienen los siguientes puntos singulares:

- Cabecera: está equipada para la prestación del servicio de difusión de televisión. Se puede descomponer en cuatro bloques:

- o Sistemas de recepción y transmisión analógica: compuesto por antenas de recepción, equipos de recepción, equipos para banda base, etapa de codificación, y etapa de modulación y salida.
 - o Sistemas de recepción y transmisión analógica de reserva: antenas de recepción, equipos de recepción, y etapa de modulación.
 - o Sistemas de monitorización.
 - o Sistemas de transmisión óptica.
- Nodo primario: recibe la señal de la red troncal primaria proveniente de la cabecera de red. El nodo primario presenta dos módulos independientes:
 - o El módulo del camino descendente.
 - o El módulo del camino ascendente.
- Nodo secundario: encaminan las señales procedentes del nodo primario (mediante la red troncal secundaria) hasta los nodos ópticos terminales (a través de la red terciaria). Se ubican físicamente en una arqueta, habitualmente junto a uno de sus nodos ópticos terminales.
- Nodo óptico terminal: dan servicio a áreas de aproximadamente 500 hogares. Se ubican en armarios de exterior. Se pueden descomponer en dos grandes bloques:
 - o Canal descendente.
 - o Canal ascendente.
- Terminal direccionable de abonado: permite al cliente acceder a los servicios TV de la red y es instalado en el propio domicilio del abonado. Descodifica los canales correspondientes al servicio contratado por el abonado y permite al cliente interactuar con el sistema.
- Subredes de telefonía y datos:
 - o Subred de datos:
 - Servicios ofrecidos: portadores (alquiler de circuitos digitales), de transmisión de datos (se basan en conmutación de circuitos y conmutación de paquetes o celdas), de acceso a redes

(acceso a Internet y a otros proveedores de contenido multimedia), y de valor añadido.

- Estructura: los equipos que conectan la red de datos con Internet están situados en la cabecera. El nodo primario que reside junto a ésta es el encargado del funcionamiento de los módems cable, a través de los cuales el abonado tiene acceso a la red. Sus elementos son:
 - Router: encamina el tráfico IP entre la red de datos e Internet.
 - Servidor Proxy: actúa a modo de caché.
 - Firewall (cortafuegos): protege la red de datos de ataques externos.
 - Servidores: se encargan de dar diversos servicios: WWW, FTP, IRC, e-mail, DNS, etc.
 - Conmutador ATM multiservicio: permite la interconexión de equipos de diferentes tecnologías.
 - Conmutador LAN: conecta los servidores con el conmutador ATM multiservicio.
 - Conmutador ATM de acceso: como el conmutador ATM multiservicio, pero de menor capacidad.
 - Cabecera de módems cable: la cabecera de módems y los módems cable componen la red de acceso a datos integrada en HFC.
 - Módems cable: se sitúa en el domicilio del abonado, y permite acceso a la red de datos mediante HFC.
- o Red de telefonía:
 - Servicios ofrecidos: telefonía analógica tradicional, acceso digital RDSI básico, acceso digital RDSI primario.
 - Estructura: La red soporta tanto telefonía integrada como superpuesta.

- Centro de conmutación: canaliza todo el tráfico de llamadas.
- Red de acceso mediante telefonía integrada: aprovecha la red HFC de distribución de TV y datos para llegar hasta el cliente. Para realizar el interfaz con la red HFC, son necesarios dos equipos específicos (HDT y MDU).
- Red de acceso mediante telefonía superpuesta: no usa la red HFC. Desde la cabecera se distribuye la señal, mediante fibra óptica hasta los nodos primarios, y desde ellos, hasta los lóbulos de 12.000 hogares de la red SDH.
- Cableado de viviendas.

47.4 PLC

La tecnología Power Line Communications, "PLC", posibilita la transmisión de voz y datos a través de los cables eléctricos, convirtiendo cualquier enchufe de la casa en conexión potencial a todos los servicios de telecomunicaciones. El cliente solo necesitará conectar un pequeño módem para acceder a Internet, telefonía y datos al mismo tiempo y a alta velocidad (banda ancha).

La red eléctrica transporta electricidad a una frecuencia de 50 Hz. En PLC se añaden frecuencias en la banda que va desde 1,6MHz hasta 30MHz para el transporte de los datos. Unos filtros instalados en el transformador de baja tensión separan las frecuencias altas de datos, de la frecuencia de 50Hz de la electricidad.

Power Line Communications emplea una red conocida como High Frequency Conditioned Power Network (HFPCN) para transmitir simultáneamente energía e información. Una serie de unidades acondicionadoras son las que se encargan del filtrado y separación de ambas señales.

En la actualidad no existen estándares tecnológicos para el PLC de acceso. Este es uno de los principales problemas de esta tecnología, al no permitir la interoperabilidad entre los equipos suministrados por los distintos fabricantes. Tampoco existía una regulación en cuanto a la utilización de

frecuencias, hasta 2005. Garantizando ahora la coexistencia de sistemas domésticos (como HomePlug) y las tecnologías de acceso.

Es posible que el precio de la tecnología PLC sea bastante inferior al de los actuales ADSL y Cable en el mismo rango de velocidades lo que la convierte en una tecnología interesante.

Los servicios típicos de telecomunicaciones que podrían ser proporcionados son:

- Telefonía
- Acceso rápido a Internet
- Video bajo demanda

Ventajas de PLC:

- Como la PLC se posicionó como un servicio de tipo IP utilizará routers de paquetes en vez de los de conmutación de circuitos típicos, de los suministradores de telecomunicaciones tradicionales, manteniendo así los costes de los equipos de IT bajos.
- Las compañías eléctricas podrían pues comercializar un servicio básico de conexión a Internet con una suscripción mensual de tarifa plana.
- Esta tecnología se pone virtualmente al alcance de cualquiera,
- Ya existen varias tecnologías que transforman los cables eléctricos existentes en un cableado LAN (Local Area Network)
- PLC podría facilitar a las compañías eléctricas la oportunidad de ofrecer servicios de valor añadido.

Inconvenientes de PLC:

- El número máximo de hogares por transformador. Como las señales de datos de Power Line no pueden sobrevivir a su paso por un transformador, solo se utilizan en la última milla. El modelo europeo de red eléctrica suele colocar un transformador cada 150 hogares aproximadamente.
- Por lo que es necesario que todos los transformadores vengán dotados de servidores de estación base PowerLine.

- Cualquier línea conductora es, por definición, una antena por lo que la instalación eléctrica de una casa actúa como tal, y es muy sensible a las interferencias que se produzcan en las frecuencias de transmisión de datos, alrededor de los 30 MHz.

47.5 REDES RADIO (LMDS, WIMAX),

47.5.1 LMDS

LDMS nace en el contexto de las emergentes tecnologías sin hilos y el creciente interés en IP como una alternativa para proporcionar servicios multimedia al usuario final, junto con el aumento de la demanda de nuevos servicios de telecomunicación orientados a voz y datos (acceso rápido a Internet, etc.)

LDMS (Local Multipoint Distribution Service) es una tecnología de acceso sin hilos de banda ancha o bucle de abonado sin cable. Los sistemas LDMS utilizan ondas radioeléctricas de alta frecuencia para ofrecer servicios multimedia y de difusión a usuarios finales en distancias similares a las alcanzadas con las tecnologías de cable.

Entre las ventajas que ofrece LDMS podemos señalar:

- Rápido despliegue, comparado con las tecnologías de cable: LDMS permite instalar redes rápidamente ya que, por ejemplo, el emplazamiento de las antenas es muy sencillo dado el pequeño tamaño de estas.
- Posibilidad de integrar distintos tipos de tráfico (voz, video, datos,...)
- Alta velocidad de acceso a Internet
- Flexibilidad y modularidad

Como otras características de LDMS, podemos señalar que requiere LoS (Line of Sight), es decir, visión directa entre los dos puntos que se comunican. Las velocidades de acceso que se alcanzan se encuentran en el entorno de los 512 Kbps - 2 Mbps.

El servicio LDMS se presta en dos bandas:

- Banda S: esta banda trabaja en los 3,5 GHz. Es la que se utiliza para el despliegue del bucle de abonado. Tiene un alcance de aproximadamente de 15 Km. y posee un ancho de banda de 20 Mhz.
- Banda K: trabaja en los 26 GHz. Es la banda utilizada para el acceso de banda ancha. Disponen de un alcance menor que la banda S (alrededor de los 3 Km.), pero un mayor ancho de banda (unos 56 Mhz).

La comunicación en LDMS se establece mediante radiodifusión punto-multipunto: las señales viajan desde o hasta una estación central, hasta o desde los diferentes puntos de recepción distribuidos en la zona de cobertura.

LDMS utiliza modulación QPSK (Cuadratura Phase Shift Keying), que permite reducir las interferencias y aumentar la reutilización del espectro, alcanzando un ancho de banda cercano a 1 Gbps.

47.5.2 WiMAX

WiMAX (Worldwide Interoperability for Microwave Access) es un protocolo de telecomunicaciones que proporciona acceso a Internet en puntos fijos o móviles.

La actual revisión de WiMAX permite hasta 40Mbps, con la nueva versión (IEEE 802.16m) se esperan velocidades de hasta 1 Gbps.

El nombre WiMAX fue creado por el WiMAX Forum que fue fundado en junio de 2001 para fomentar la interoperabilidad del estándar. Este foro describe WiMAX como una tecnología basada en estándares permitiendo el acceso de banda ancha de última milla como alternativa al cable y a las xDSL.

El estándar 802.16 Broadband Wireless Access (BWA) define:

- Capa 1 - Capa física: La versión original de IEEE 802.16 especifica una capa física que opera el rango entre los 10 y los 66GHz. 802.16a (actualización de 2004) añadió la posibilidad de operar entre 2 y 11 GHz. En 2005 la versión 802.16e-2005 vio la luz usando SOFDMA (Scalable Orthogonal Frequency-Division Multiple Access) en vez de la original OFDM (Orthogonal Frequency División Multiplexing). 802.16e también define el uso de varias antenas con MIMO.

- Capa 2 - Capa de acceso al medio (MAC): Usa un algoritmo de planificación para lo cual la estación del abonado necesita competir solo una vez: para conectarse a la red. La ventana de tiempo puede alargarse o contraerse, pero permanece asignada al abonado. El algoritmo es estable en situaciones de sobrecarga y gran número de abonados permitiendo a la estación base el control de la calidad del servicio (QoS).
- Movilidad
- Características opcionales y obligatorias del enlace de radio

47.6 SATÉLITE

El acceso a Internet por satélite puede obtenerse en cualquier parte del mundo usando satélites LEO (Low Earth Orbit) aportando una relativamente baja latencia pero baja velocidad, o satélites geoestacionarios aportando mayor velocidad pero también mayor latencia y no pudiendo llegar a ciertas partes de los polos. Las desventajas de este sistema no se quedan ahí (alta latencia) si no que también incluyen problemas de cobertura cuando llueve, además requiere línea directa de visión al satélite (en un terreno escarpado esto puede ser un problema).

El equipo del cliente para una comunicación de satélite requiere la instalación de una antena parabólica de un tamaño dependiente de la tecnología concreta, del satélite y del modo en que se use (comunicación uni o bidireccional,...) además de un MÓDEM específico.

Existen distintas técnicas usadas para compartir cada portadora (TDMA, SCPC,...) aportando velocidades de hasta 40Mbps de descarga.

Los típicos modos de comunicación son:

- Comunicación bidireccional por satélite. En este caso tanto la subida como la bajada se produce usando el satélite, requiriendo una muy precisa orientación de la antena.
- Comunicación unidirección más conexión terrestre. En este caso la antena solo recibe la señal del satélite, y el envío de datos se produce por una línea terrestre (RTC, GSM, GPRS,...). Tiene la ventaja sobre el

modelo anterior de que la antena no necesita estar orientada de manera tan precisa y que, por lo tanto, es mejor para instalaciones móviles.

- Comunicación unidireccional / multicast, sin retorno. Dentro de esta modalidad tenemos los servicios de multicast por IP que no requieren retorno (además de la transmisión de audio y video).

47.7 LÍNEAS PUNTO A PUNTO

Una línea punto a punto o línea personal (como contraposición a una VPN) es una línea física entre dos ubicaciones de forma transparente, de modo que una línea punto a punto desde una ubicación remota funciona de la misma manera que si estuviese conectada en la ubicación de destino. Tradicionalmente cuando se contrataba una línea punto a punto se especificaban las características y velocidad de la misma usando múltiplos del DS0, desde un DS0 (64Kbps) hasta un T1/Y1 (1,5Mbps) o DS-3 (672 canales de 64Kbps). Los operadores usaban conmutación de circuitos o circuitos virtuales con tecnologías como X.25.

En la actualidad estas líneas se suelen crear como una VPN dentro de las redes del operador, por ejemplo usando MetroEthernet y MPLS.

47.7.1 X.25

X.25 es un estándar para el acceso a redes públicas de conmutación de paquetes. No especifica como está implementada la red interiormente aunque el protocolo interno suele ser parecido a X.25. Implementa un servicio de circuito virtual externo.

El servicio que ofrece es orientado a conexión, fiable, en el sentido de que no duplica, ni pierde ni desordena, y ofrece multiplexación, esto es, a través de un único interfaz se mantienen abiertas distintas comunicaciones.

Los elementos usados por X.25 se denominan:

- DTE (Data Terminal Equipment): Es el equipo final de usuario (PC con placa X.25 por ejemplo).

- DCE (Data Circuit Terminating Equipment): Podemos interpretarlo como un nodo local. A nivel de enlace (LAPB) las conexiones se establecen DTE-DCE. Con el nivel de red, ampliamos las comunicaciones más allá del DCE, que hace de interconexión.

X.25 define 3 niveles:

- Nivel Físico:

Existen dos posibilidades:

- X.21: Se utiliza para el acceso a redes de conmutación digital. (Similares a las de telefonía digital.)
- X.21bis: Se emplea para el acceso a través de un enlace punto a punto. (Similar a RS-232 en modo síncrono.)

En cuanto a las características mecánicas, se usan conectores Canon de 15 pines o de 25 pines.

Las velocidades van entre los 64kbps y los 2Mbps, velocidades que pueden parecer bajas y, de hecho, así son. X.25 presenta un problema de baja eficiencia por la exagerada protección contra errores que implementa y que con las redes actuales no tiene sentido.

- Nivel de Enlace (LAP-B):

En X.25, este nivel queda implementado con el protocolo LAP-B (Link Access Procedure - B) que es un protocolo de enlace con rechazo simple y en el cual las tramas de información pueden ser utilizadas como tramas de control.

- Nivel de Paquete (PLP):

Este nivel está especificado por el PLP (Packet Layer Protocol) que es un protocolo de acceso a nivel de red y que proporciona servicios al nivel superior.

Permite establecer circuitos virtuales (CV): Que podríamos definir como la asociación lógica entre usuarios para comunicarse entre ellos. Existen dos tipos de CV:

- Conmutados (CVC): Hay que realizar un diálogo previo a la transmisión con el nodo local para establecerlos.
- Permanentes (CVP): Están establecidos de antemano (por contrato), así que no hace falta fase de establecimiento. Son muy útiles si se transmite mucho y con mucha frecuencia hacia un mismo destino.

47.7.2 FRAMERELAY

Es posible usar FrameRelay como tecnología de soporte para conseguir redes punto a punto. Esta tecnología se explica en otro tema.

47.7.3 METROETHERNET

Es posible usar MetroEthernet como tecnología de soporte para conseguir redes punto a punto. Esta tecnología se explicará más adelante en este mismo tema.

47.8 METROETHERNET

MetroEthernet es una red tipo MAN (está diseñada para cubrir un área metropolitana) basada en el muy conocido estándar Ethernet. El uso habitual de MetroEthernet es servir de red de acceso para conectarse a Internet o servir de red de interconexión de varias oficinas de una compañía.

Habitualmente el proveedor de una conexión MetroEthernet proporcionará la misma por fibra óptica terminando en un equipo que habitualmente tiene capacidades no solo de nivel 2 sino de nivel 3 (red).

Esta tecnología puede desplegarse de varias formas atendiendo a la base usada para MAN que la soporta:

- Ethernet pura, toda la red está basada en Ethernet, sin ninguna otra tecnología de soporte. Esta opción aporta una gran simplicidad y bajo coste, pero tiene graves problemas de fiabilidad y de escalabilidad por lo que está limitada a pequeños despliegues.
- MetroEthernet basadas en redes SDH ya existentes, con las limitaciones que imponen SDH en el manejo del ancho de banda.

- Y, por último, MetroEthernet basadas en MPLS. Esta es la opción más cara pero la más escalable y fiable siendo la típica a desplegar por operadores (de no tener una red SDH existente).

47.8.1 MAN BASADA EN ETHERNET

Un despliegue basado solo en Ethernet hace solo uso de switches de nivel 2. Esto permite un diseño y configuración muy simples a un bajo coste. Este tipo de despliegue solo fue posible tras la incorporación de las VLAN (Virtual LAN) aportando la posibilidad de “punto a punto” y “multipunto a multipunto” combinadas con VLAN Stacking (también conocida como VLAN Tunneling) y VLAN Translation ya que previamente no era posible aislar el tráfico de cada usuario (dada la naturaleza de Ethernet) para formar circuitos.

VLAN Stacking permite el uso de varias LANs virtuales sobre el mismo circuito de la red troncal gracias al uso de dos identificadores: uno para red troncal y otro para la red Ethernet (existiendo 4096 identificadores distintos según el estándar 802.1Q, que no 4096 VLAN distintas).

VLAN Translation permite convertir un identificador de VLAN en otro de forma que el identificador usado en una parte de la red sea distinto al usado en otra, evitando de esta forma posibles conflictos entre identificadores de distintos usuarios.

47.8.2 MAN BASADA EN SDH

Una Ethernet MAN basada en SDH (Synchronous Digital Hierarchy) es un paso intermedio entre redes tradicionales (basadas en división de tiempos) y redes más modernas (como Ethernet). En este modelo la infraestructura SDH existente es utilizada para transportar conexiones Ethernet de alta velocidad aportando una gran fiabilidad gracias a los mecanismos intrínsecos de las redes SDH (con un tiempo de recuperación inferior a 50 ms).

Este tipo de implantaciones se limitan a los casos donde ya existe una red SDH debido al alto coste de los equipos SDH y las limitaciones de SDH para gestionar el tráfico (velocidad, ruta,...) llevando muchas veces a la

instalación de switches Ethernet en la frontera SDH para aliviar parte de estas limitaciones

47.8.3 MAN BASADA EN MPLS

En este caso las tramas Ethernet enviadas por el usuario son empaquetadas en MPLS que transmite sus datos sobre (habitualmente) Ethernet, creando una pila Ethernet sobre MPLS sobre Ethernet (aunque podría haber otro protocolo por debajo).

Este despliegue usa LDP (Label Distribution Protocol) punto a punto para la etiqueta interna (etiqueta del VC) y RSVP-TE (Resource reSerVation Protocol-Traffic Engineering) o LDP para la etiqueta externa usada en la red.

Uno de los mecanismos de restoración de MetroEthernet basadas en MPLS es Fast ReRoute (FRR) que permite un tiempo de restoración inferior a los 50ms. Esto es una de las cosas que más hay que tener en cuenta a la hora de decidirnos por MetroEthernet basadas en MPLS frente aquellas basadas en Ethernet, ya que si tenemos un tiempo de restoración equivalente usando una solución Ethernet pura no merece la pena introducir una basada en MPLS.

47.9 BIBLIOGRAFÍA

José Manuel Huidrobo. Todo sobre comunicaciones. PARANINFO, 1998

José Manuel Huidrobo. Manual de Telefonía. PARANINFO, 1996

Andrew S. Tanenbaum. Redes de computadoras. PRENTICE HALL, 1997

Autor: Matías Villanueva Sampayo

Director de Informática Asociación Provincial de Pensionistas y Jubilados de A Coruña

Colegiado del CPEIG

48. TECNOLOGÍAS DE TRANSPORTE: FRAME RELAY, ATM, DWDM, MPLS. REDES DE FIBRA ÓPTICA. REDES DE NUEVA GENERACIÓN (NGN).

Tema 48. Tecnologías de transporte: Frame Relay, ATM, DWDM, MPLS. Redes de fibra óptica. Redes de nueva generación (NGN).

48.1 Tecnologías de transporte

48.1.1 Frame Relay

48.1.1.1 Arquitectura de protocolos

48.1.1.1.1 Protocolo LAPF

48.1.1.1.2 Direccionamiento

48.1.1.1.3 Control de la congestión

48.1.1.1.4 Tipos de tráfico transportado

48.1.1.1.5 Ventajas

48.1.2 ATM

48.1.2.1 Principios de operación

48.1.2.2 Capas de ATM

48.1.2.2.1 Capa física

48.1.2.2.2 Capa ATM

48.1.2.2.2.1 Parámetros del tráfico

48.1.2.2.2.2 Clases de servicio

48.1.2.2.2.3 Asignación de ancho de banda y control de la congestión

48.1.2.2.3 Capa de adaptación (AAL)

48.1.2.2.3.1 Estructura de la capa AAL

48.1.3 DWDM

48.1.3.1 Demultiplexadores

48.1.3.2 Erbium Doped Fiber Amplifier

48.1.4 MPLS

48.1.4.1 Funciones de MPLS

48.1.4.2 LSRS y LERS

48.1.4.3 FEC

48.1.4.4 Etiquetas

48.1.4.5 Distribución de etiquetas

48.1.4.6 LSP

48.1.4.7 Pila de etiquetas

48.2 Redes de fibra óptica

48.2.1 Jerarquía Digital Plesiócrons (PDH)

48.2.2 Jerarquía Digital Síncrona (SDH) / SONET

48.2.2.1 Frame SDH / SONET

48.2.2.1.1 Framing

48.2.2.1.2 Estructura del frame STM-1

48.3 Redes de nueva generación (NGN)

48.3.1 Tecnologías de soporte

48.4 Bibliografía

48.1 TECNOLOGÍAS DE TRANSPORTE

48.1.1 FRAME RELAY

Frame relay es un protocolo de transmisión de paquetes de datos en ráfagas de alta velocidad a través de una red digital fragmentados en unidades de transmisión llamadas Frames. Requiere una conexión exclusiva durante el período de transmisión.

Frame relay es una tecnología de paquete-rápido ya que el chequeo de errores no ocurre en ningún nodo de la transmisión. Son los extremos los responsables de este chequeo de errores. (Sin embargo, debido a que los errores en redes digitales son extremadamente menos frecuentes en comparación con las redes analógicas, esto no supone un verdadero inconveniente).

A diferencia de los paquetes que son de tamaño fijo, Frame Relay transmite Frames que son de tamaño variable (mil o más bytes).

El estándar de Frame Relay (ITU-T I.122) es una extensión del estándar ISDN. Implementa varios interfaces físicos como V.35 para velocidades menores de 2 Mb y G.703 para 2 Mb.

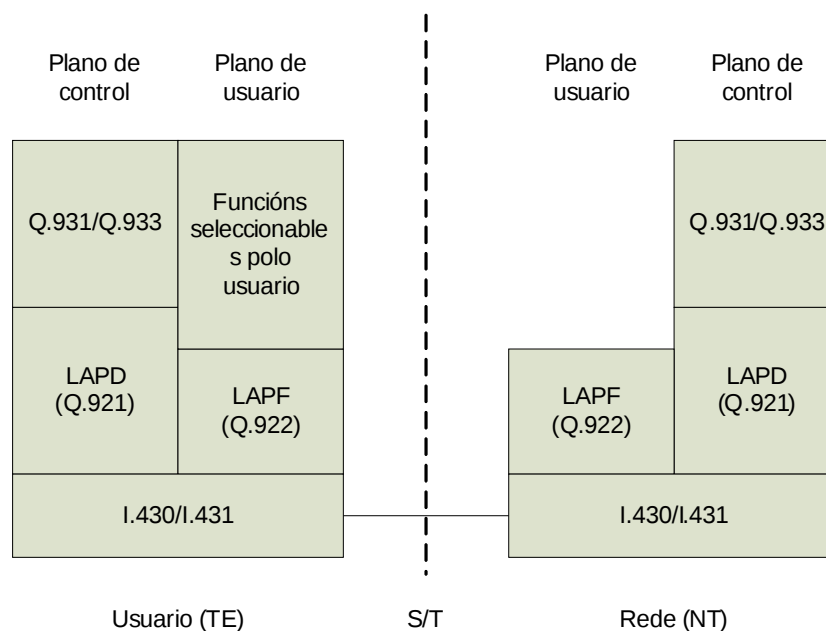
Una conexión Frame Relay es conocida como una conexión virtual. Una conexión virtual permanente es exclusiva al par origen-destino y puede transmitir por encima de 1,544 Mbps, dependiendo de las capacidades del

par origen-destino. Es posible también una conexión virtual conmutada usando la red pública y puede proporcionar elevados anchos de banda.

48.1.1.1 ARQUITECTURA DE PROTOCOLOS

En Frame Relay se consideran dos planos de operación:

- Plano de control (C): Involucrado en el establecimiento y liberación de conexiones lógicas. Los protocolos de este plano se implementan entre el usuario y la red. Es similar a la señalización en canales de servicios de conmutación de circuitos, ya que usa un canal lógico separado para la información de control. En la capa de enlace se usa el protocolo LAPD (Q.921) para proporcionar un servicio de control de datos fiable, mediante un control de flujo y de errores entre la red y el usuario. Este servicio de enlace de datos usa para el intercambio de mensajes de control el protocolo Q.931.
- Plano de usuario (U): Responsable de la transferencia de datos extremo a extremo mediante el protocolo LAPF (Procedimiento de Acceso al Enlace para Servicios en Modo Trama) definido en el estándar Q.922.



TEXTO: FUNCIONES SECCIONABLES POR EL USUARIO. RED

48.1.1.1.1 PROTOCOLO LAPF

Permite la retransmisión de tramas como un servicio orientado a conexión de la capa de enlace con las siguientes propiedades:

- Envío secuencial de las tramas a partir de la información de direccionamiento existente en la cabecera de control de cada trama.
- Existe una probabilidad pequeña de pérdida de tramas.
- Reduce al mínimo el trabajo de la red.

El formato de trama de LAPF de funcionamiento mínimo (conocido como protocolo central LAPF) es similar al LAPD y LAPB con una salvedad: no existe campo de control, lo que tiene las siguientes implicaciones:

- Existe un único tipo de trama, usada para transportar datos de usuario. No existen tramas de control.
- No es posible el uso de señalización en banda; una conexión lógica solo puede transmitir datos de usuario.
- No es posible llevar a cabo control de errores dado que no existen números de secuencia.
- Los campos indicador y secuencia de verificación de trama (FCS), actúan como en LAPD y LAPB. El campo de información contiene datos de capas superiores. Si el usuario decide implementar funciones adicionales de control de enlace de datos extremo a extremo, debe incluirse en este campo una trama de enlace de datos.

48.1.1.1.2 DIRECCIONAMIENTO

El campo de dirección tiene implícitamente una longitud de 2 octetos, y puede ampliarse a 3 o 4 octetos (se indica mediante los bits de ampliación del campo de dirección (EA)). Este campo contiene un identificador de conexión de enlace de datos (DLCI) de 10, 17 o 24 bits. El DLCI proporciona la misma función que el número de circuito virtual en X.25: permite la multiplexación de varias conexiones lógicas de retransmisión de tramas a través de un único enlace físico. Como en X.25, el identificador de conexión solo tiene significado local.

La función realizada por cualquier red que soporte la técnica de retransmisión de tramas, consiste en el encaminamiento de las tramas de acuerdo con sus valores DLCI. Para esta función existe un gestor de tramas encargado de tomar las decisiones de encaminamiento. Esta operación puede involucrar a múltiples gestores de tramas interconectados.

48.1.1.1.3 CONTROL DE LA CONGESTIÓN

Se utilizan dos tipos de señalización para el control de la congestión:

- Señalización implícita: se produce cuando la red descarta tramas, hecho que es detectado por los protocolos de nivel superior en el interfaz de usuario.
- Señalización explícita: es de carácter opcional y constituye una señalización de la red al interfaz de usuario mediante dos bits. Ambos bits permiten que los dispositivos finales regulen la velocidad de transmisión de información a la red hasta que la congestión desaparezca. Los bits son el BECN (congestión en el sentido opuesto a la trama) y el FECN (congestión en el sentido de la trama).

Adicionalmente, existe otro mecanismo de control de la congestión (CLLM, “Consolidated Link Layer Management”), consistente en mensajes que la red envía a los dispositivos de acceso con códigos indicadores de las causas de la congestión, así como una lista de todos los DLCI’s que deben reducir su tráfico para disminuir el nivel de congestión.

En Frame Relay se definen dos clases de tráfico por Circuito Virtual Permanente:

- Clase de Caudal o CIR (Committed Information Rate): se define como el caudal de información que la Red se compromete a transmitir expresado en bit/sg. En un dimensionamiento correcto, debe corresponder a un tráfico “normal” o promedio. Se recomienda que no supere el 75 % de la velocidad de la línea, aun cuando hay poca simultaneidad entre los Circuitos Virtuales, se puede superar con la sobrecontratación que se recomienda no sobrepase del 200%.

- Exceso de Tráfico o EIR (Excess Information Rate): sin contratación, y que va dirigido a permitir la transmisión de ráfagas de gran intensidad de tráfico, sin coste adicional: se define como la cantidad de información en exceso del CIR contratado, que la Red es capaz de gestionar durante un período de tiempo definido. Esta clase de tráfico, expresado en bit/sg, es señalada por la Red como de menor prioridad (DE=1), y en condiciones normales será retransmitida y en condiciones de congestión puede ser descartada.

Para los Circuitos Virtuales Conmutados se define un CIR y un EIR Total Agregado que engloba a todos los CVC establecidos.

48.1.1.1.4 TIPOS DE TRÁFICO TRANSPORTADO

La necesidad de nuevas facilidades para las comunicaciones de área extendida, en particular para las comunicaciones de datos entre redes locales, impulsó enormemente el desarrollo y utilización de Frame Relay, debido a que satisface las dos características predominantes de este tipo de tráfico:

- Tráfico a ráfaga e impulsivo, que exigiría dimensionar en exceso el enlace para atender los picos de demanda. Frame Relay soluciona este problema, ya que requiere una pequeña cantidad de ancho de banda permanentemente reservada vía un circuito virtual permanente, mientras que dinámicamente, y siempre que exista ancho de banda disponible, es posible asignar mayor velocidad a la conexión para atender picos de demanda.
- La necesidad de interconexión remota de LANs incrementa la necesidad de mallado de las redes WAN resultantes. Frame Relay evita la necesidad de numerosos enlaces físicos, permitiendo la definición de múltiples circuitos virtuales permanentes a diferentes destinos, a través de un mismo puerto dedicado a un enlace físico.

48.1.1.1.5 VENTAJAS

Ahorro en los costes de telecomunicaciones: Con el servicio Frame Relay los usuarios podrán transportar simultáneamente, compartiendo los

misimos recursos de red, el tráfico perteneciente a múltiples comunicaciones y aplicaciones, y hacia diferentes destinos.

Tecnología punta y altas prestaciones: Frame Relay proporciona alta capacidad de transmisión de datos por la utilización de nodos de red de alta tecnología y bajos retardos, como consecuencia de la construcción de red (backbone) sobre enlaces a 34 Mbps. y de los criterios de encaminamiento de la Red de Datos, orientados a minimizar el número de nodos de tránsito.

Flexibilidad del servicio : Frame Relay es una solución adaptable a las necesidades cambiantes, ya que se basa en circuitos virtuales permanentes (CVP), que es el concepto de Red Pública de Datos, equivalente al circuito punto a punto en una red personal. Sobre una interfaz de acceso a la red se pueden establecer simultáneamente múltiples circuitos virtuales permanentes distintos, lo que permite una fácil incorporación de nuevas sedes a la Red de Cliente.

Servicio normalizado: Frame Relay es un servicio normalizado según los estándares y consejos de UIT -T, ANSI y Frame Relay Forum, con el que queda garantizada la interoperatibilidad con cualquier otro producto Frame Relay asimismo normalizado.

48.1.2 ATM

Asynchronous Transfer Mode (ATM) es una técnica de conmutación que lleva a cabo la transmisión de datos por medio de paquetes (celdas), permite la multiplexación de varias conexiones lógicas sobre una única interfaz física y se trata de una técnica de conmutación de paquetes orientada a conexión.

El protocolo de ATM tiene una mínima capacidad de control de errores, de flujo y un tamaño de paquete fijo (celda) con el que facilita el uso de nodos de conmutación a velocidades elevadas.

Sus principales características son:

- Capacidad de integración de diverso tipo de tráfico.
- Asignación dinámica y flexible del ancho de banda.

- Optimización del compromiso entre caudal y latencia.
- Ganancia estadística: capacidad de optimizar la relación entre la suma de las velocidades de pico de las fuentes y la velocidad del enlace.

48.1.2.1 PRINCIPIOS DE OPERACIÓN

Las conexiones lógicas en ATM están relacionadas con las conexiones de canales virtuales (VCC, “Virtual Channel Connection”). Una VCC es la unidad básica de conmutación en una red ATM. Una VCC se establece entre dos usuarios finales a través de la red, intercambiándose celdas de tamaño fijo a través de la conexión de un flujo full-duplex y de velocidad variable. Las VCC se utilizan también para señalización de control y gestión de red y encaminamiento.

Se introdujo una segunda capa de procesamiento en ATM para gestionar el concepto de camino virtual. Una conexión de camino virtual (VPC, “Virtual Path Connection”) es un conjunto de VCC con los mismos extremos, de manera que todas las celdas fluyendo a través de las VCC de una misma VPC se conmutan conjuntamente.

La técnica de camino virtual ayuda a contener el coste de control agrupando en una sola unidad conexiones que comparten caminos comunes a través de la red. Las acciones de la gestión de red pueden ser aplicadas a un pequeño número de grupos de conexiones, en lugar de a un gran número de conexiones individuales.

48.1.2.2 CAPAS DE ATM

Las normalizaciones ITU-U para ATM se basan en una arquitectura donde se contemplan los siguientes niveles:

- Capa física: Especifica el medio de transmisión y un esquema de codificación de la señal. Dividiéndose en dos capas:
 - Subcapa dependiente del medio físico (PMD): que lleva a cabo funciones de transmisión y temporización de bits.

- Subcapa de Convergencia de Transmisión (TC): responsable de las funciones relacionadas con la transmisión de células como control de HEC, delimitación de celdas, etc.
- Capa ATM: Define la transmisión de datos en celdas de tamaño fijo, al tiempo que establece el uso de conexiones lógicas. Realiza funciones de multiplexación de celdas y control de flujo.
- Capa de adaptación ATM (AAL): Capa de adaptación para admitir compatibilidad con protocolos de transferencia de información no basados en ATM. Se divide en dos:
 - Subcapa de Convergencia (CS).
 - Subcapa de Segmentación y reensamblado (SAR).

48.1.2.2.1 CAPA FÍSICA

La función básica del nivel físico es la codificación/decodificación de la información en formato eléctrico u óptico para la transmisión/recepción sobre el medio físico de comunicación utilizado. Otras funciones proporcionadas por este nivel son la desalineación de celdas y generación y proceso del checksum para el control de errores en la cabecera.

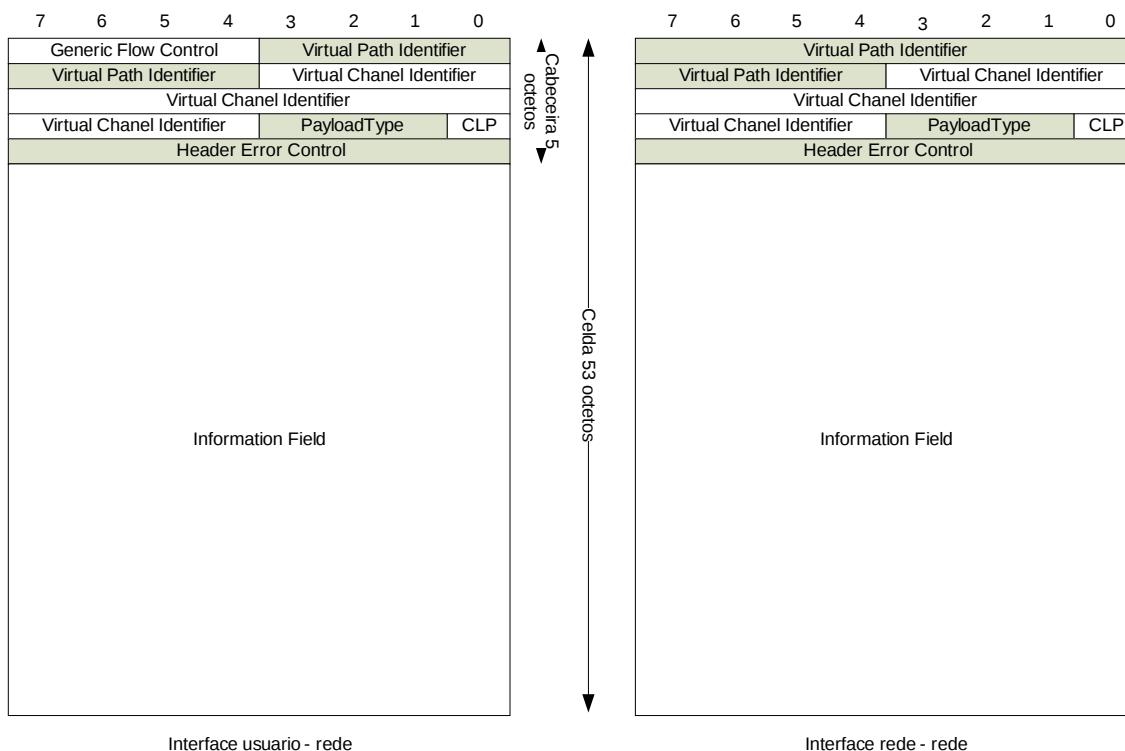
Las recomendaciones ITU-T detallan la velocidad de transmisión y las técnicas de sincronización para la transmisión de celdas ATM. Las principales propuestas de capas físicas en redes ATM son las siguientes:

- ATM sobre SDH: STM-1 (155,52) y STM-4 (622,08)
- ATM sobre PDH: E1 (2,048), DS1 (1,548), DS2 (6,312), E3 (34,368), E4 (139,264) y DS3 (44,736).
- ATM a 100 Mbps sobre FDDI.
- ATM a 25,6 Mbps (propuesta por IBM).

48.1.2.2.2 CAPA ATM

El modo de transferencia asíncrono utiliza celdas de tamaño fijo, que constan de 5 octetos de cabecera y un campo de información de 48 octetos. La capa ATM es la encargada de incorporar la cabecera de 5 octetos al campo de información. La cabecera tiene el siguiente formato:

- Control de Flujo Genérico (GFC, “Generic Flow Control”). Se utiliza solo en el interfaz UNI (User-Network Interface).
- Identificador de camino Virtual (VPI, “Virtual Path Identifier”) e Identificador de Canal Virtual (VCI, “Virtual Channel Identifier”).
- Indicador de Tipo de Carga Útil (PTI, “Payload Type Indicator”). Indica si se trata de datos de usuario, información de gestión, información OAM, etc.
- Prioridad de Pérdida de Celda (CLP, “Cell Loss Priority”). Las celdas marcadas son las primeras en ser descartadas en caso de congestión.
- Control de Errores de Cabecera (“Checksum”).



48.1.2.2.1 PARÁMETROS DE TRÁFICO

Cuando se establece una conexión ATM se constituye un “Contrato de tráfico” en el que se especifican los parámetros de tráfico y los de QoS, entre los más significativos están:

- PCR (“Peak Cell Rate”): Tasa máxima de celdas permitida sobre el circuito.

- MCR (“Minimun Cell Rate”): Mínima tasa de celdas sobre el circuito garantizada por el proveedor del servicio.
- CDVT (“Cell Delay Variation Tolerance”): Nivel de tolerancia para la diferencia entre la celda con el mínimo retardo y la celda con el máximo retardo.
- SCR (“Sustained Cell Rate”): Tasa media de transmisión de celdas que se mantendrá durante la duración de una transmisión.
- BT (“Burst Tolerance”): Límite que la transmisión puede alcanzar en su nivel más alto (PCR).

Se garantiza una calidad de servicio con respecto a un mínimo ancho de banda disponible, la cantidad de retardo que afectará a la transmisión y la máxima pérdida de celdas que se producirá en esta.

48.1.2.2.2 CLASES DE SERVICIO

A partir de estas especificaciones iniciales del ITU, se definieron cinco clases de servicio que la red ATM debería proporcionar (no es obligatorio):

- CBR (“Constant Bit Rate”): Es un servicio determinístico, diseñado para soportar emulación de circuitos, tráfico de voz y video (por ejemplo, MPEG/JPEG) en tasa constante de bits. Proporciona ancho de banda reservado, garantizando mínima pérdida de celdas y mínimas variaciones en retardos. El servicio CBR proporciona ancho de banda reservado incluso el PCR especificado para el circuito. Con CBR el usuario debe declarar el PCR y el CDTV en el momento de establecer la conexión.
- VBR (“Variable Bit Rate”): Se definieron dos tipos:
 - VBR-RT (“Real Time”), proporciona un estrecho control de los retardos para la transmisión de información como video y voz sin silencios.
 - VBR-NRT (“No Real Time”) tiene menos exigencias que el anterior, respecto a las variaciones en retardos y se desarrolló para la transmisión de datos transaccionales.

El servicio VBR también requiere la especificación del PCR, si bien con un comportamiento diferente: el usuario puede utilizar el canal por arriba del SCR (hasta el PCR) solo durante cortos períodos de tiempo determinados por el parámetro BT, pero debe mantener el SCR como una tasa media. Si el usuario sobrepasa el SCR durante un período de tiempo, a esto le seguirá un período similar por debajo del SCR. Si el usuario sobrepasa el PCR, esto se seguirá por un período de inactividad antes de que el usuario pueda sobrepasar el SCR de nuevo. Con VBR el usuario debe declarar PCR, CDVT, SCR y BT.

- UBR (“Unspecified Bit Rate”): Se diseñó para permitir el uso de ancho de banda excedente no utilizado para los servicios CBR y VBR. No ofrece garantías en cuanto a la pérdida de celdas o variaciones en retardos; es decir, no incluye ningún mecanismo de control en el caso de congestión en la red. Con UBR no hay descriptores de tráfico, ni garantías de calidad de servicio ni mecanismos de realimentación en caso de congestión en la red. La estación puede enviar tráfico cuando lo necesite y la red lo aceptará; eso sí, en caso de congestión, la estación no es notificada de ningún modo y el conmutador eliminará celdas cuando sus buffers estén llenos. Esto significa que la tasa potencial de pérdida de celdas con UBR puede ser inaceptablemente alta.
- ABR (“Available Bit Rate”): Al igual que UBR, se diseñó para aprovechar el ancho de banda excedente pero, al contrario que aquel, implementa mecanismos de control y control en caso de congestión en la red. ABR se concibió para transportar el tráfico a ráfagas sin las limitaciones de calidad de servicio de UBR, básicamente aplicaciones que no funcionen en tiempo real y por lo tanto poco sensibles a retardos. Utiliza básicamente los descriptores PCR y MCR; el usuario se compromete a no enviar información más rápido que el PCR y la red a proporcionar como mínimo el MCR requerido. El usuario no está obligado a especificar PCR y MCR; en

ausencia de tal especificación, los valores por defecto serían el PCR a velocidad de acceso y el MCR a cero. Si se cumplen estos parámetros descriptores de tráfico, se garantiza la calidad de servicio en cuanto a mínimo nivel de pérdida de celdas y mínimo ancho de banda asegurado; el retardo de celdas será minimizado, pero no existe garantía absoluta respecto al retardo para el servicio ABR. Hay otro tipo de servicio en estudio por el ATM Forum (VBR+) que, como el ABR, contempla un sistema de realimentación para control de la congestión en la red pero, adicionalmente, proporciona además garantías en cuanto a los retardos.

48.1.2.2.3 ASIGNACIÓN DE ANCHO DE BANDA Y CONTROL DE CONGESTIÓN

Una red ATM debe garantizar unos determinados parámetros de QoS, además de proporcionar ganancia estadística. Para conseguirlo utiliza métodos preventivos, denominados Control de Admisión de Conexión y de monitorización posterior, mediante una función de policía (UPC) que emplea diversos algoritmos para este fin.

También existen métodos reactivos como el CLP (Cell Loss Priority) o el GFC (Generic Flow Control) que controla el tráfico del usuario a la red.

Para el control de la congestión existen dos opciones:

- Control basado en créditos: el extremo receptor emite créditos, que indican el número de celdas que puede enviar el emisor, útil en entornos de área local.
- Control basado en la velocidad: basado en mensajes EFCI (Explicit Forward Congestion Indication), las estaciones y conmutadores ajustan la velocidad dinámicamente. Esta es la técnica más ampliamente utilizada.

48.1.2.2.3 CAPA DE ADAPTACIÓN (AAL)

La función básica del nivel de adaptación ATM (AAL) es proporcionar el enlace entre los servicios requeridos por los niveles superiores de red y el nivel ATM.

Hasta el momento, el ITU-T definió para la AAL cuatro clases de servicio, respondiendo esta clasificación a tres parámetros básicos: la relación de tiempo entre la fuente y el destino, tasa de bits constante o variable y modo de conexión. Las clases definidas son las siguientes:

Clase	A		B C	D
Relación origen / destino	Sí	Sí	No	No
Velocidad	Constante	Variable	Variable	Variable
Orientado a conexión	Sí	Sí	Sí	No

48.1.2.2.3.1 ESTRUCTURA DE LA CAPA AAL

La capa AAL está organizada en dos subcapas:

- Subcapa de segmentación y reensamblado (SAR): Segmenta la información de las capas superiores para construir la carga útil de las celdas ATM y recíprocamente reensambla los campos de información de las celdas en unidades de información para las capas superiores.
- Subcapa de convergencia (CS): tiene como misión realizar funciones específicas para cada servicio, como el tratamiento de la variación del retardo de celda, sincronización extremo a extremo, tratamiento de celdas mal insertadas o perdidas. Existen, por tanto, diferentes CS sobre la subcapa SAR. Debido a la gran cantidad de servicios propuestos sobre ATM, fue necesario distinguir entre una parte común CS (CPCS) y una parte específica de servicio (SSCS).

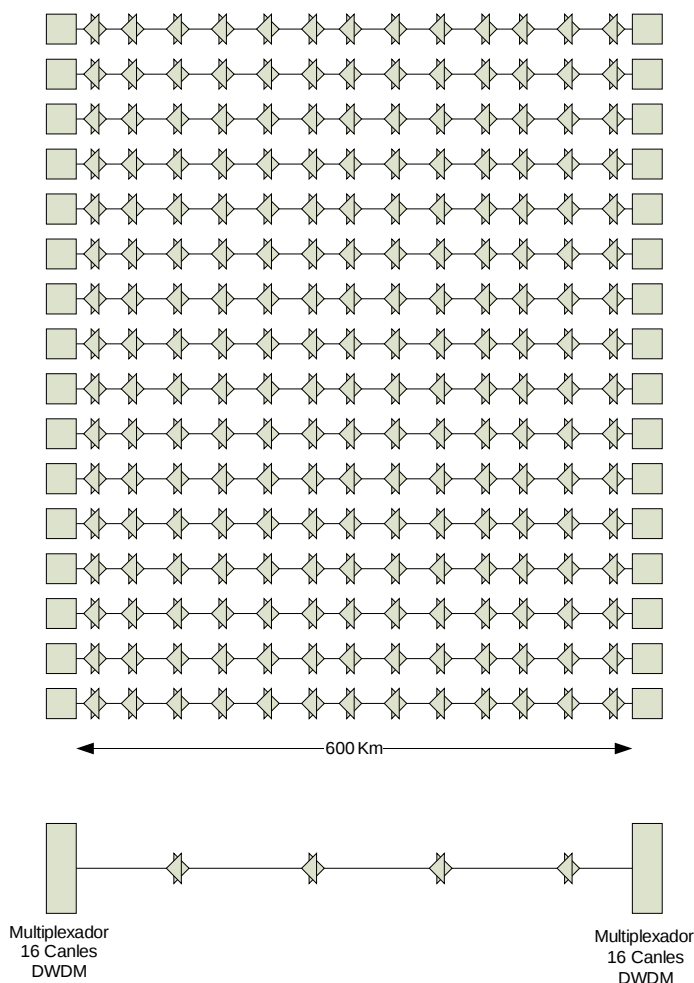
Inicialmente, el ITU-T recomendó cuatro tipos de protocolos AAL para soportar las cuatro clases de servicio definidas, los protocolos AAL de tipo 1, 2, 3, y 4. Así, el tráfico de clase 1 utilizará el protocolo AAL-1, el de clase 2 el AAL-2, y los de clase 3 y 4 el protocolo AAL-3/4. Siendo los protocolos de las clases 3 y 4 un protocolo único.

Debido a la complejidad del protocolo AAL-3/4 se propuso como alternativa el AAL-5, a veces denominado SEAL ("Simple and Efficient Adaptation

Layer“). En consecuencia, las clases de tráfico 3 y 4 pueden utilizar el protocolo AAL-3/4 o el AAL-5.

48.1.3 DWDM

La tecnología DWDM usa una composición óptica de la señal de distintos flujos de datos cada uno de los cuales en su propia longitud de onda óptica. A pesar de que la división y multiplexado usando el espectro óptico es una tecnología que se conoce desde hace tiempo, sus primeras aplicaciones restringían su uso a proveer dos longitudes de onda muy gruesas y muy separadas o la construcción de componentes capaces de hasta 4 canales. Solo recientemente la tecnología evolucionó hasta el punto de poder empaquetar e integrar en un sistema de transmisión una alta densidad de canales paralelos, simultáneos, a una frecuencia extremadamente alta (192 – 200 Terahertz). Conforme al plan de canales del ITU, este sistema asegura la interoperabilidad con otros equipos y permite a los operadores posicionarse bien para desplegar soluciones ópticas en su red. El sistema de 16 canales proporciona básicamente un cable virtual con 16 fibras.



Para transmitir 40Gb/s a 600 Km. usando un sistema tradicional requerimos 16 pares de fibra óptica con regeneradores cada 35 Km. con un total de 272 regeneradores. Un sistema DWDM de 16 canales usa solo un par de fibra óptica y 4 amplificadores posicionados cada 120Km.

La forma más común de DWDM usa un par de fibra (una para transmitir y otra para recibir). Aunque existen sistemas que solo usan una fibra para transmitir y recibir, estos sistemas deben sacrificar un poco de la capacidad de la fibra óptica para una banda de guardia y evitar así la mezcla de canales reduciendo también el rendimiento de los amplificadores.

Adicionalmente, existe un gran riesgo de que los reflejos producidos durante el mantenimiento o reparación puedan dañar los amplificadores.

La disponibilidad de tecnologías maduras de soporte como los multiplexadores precisos y los EDFA (Erbium Doped Fiber Amplifiers)

permitió la disponibilidad comercial de sistemas DWDM con ocho, dieciséis, o incluso un mayor número de canales.

48.1.3.1 DEMULTIPLEXADORES

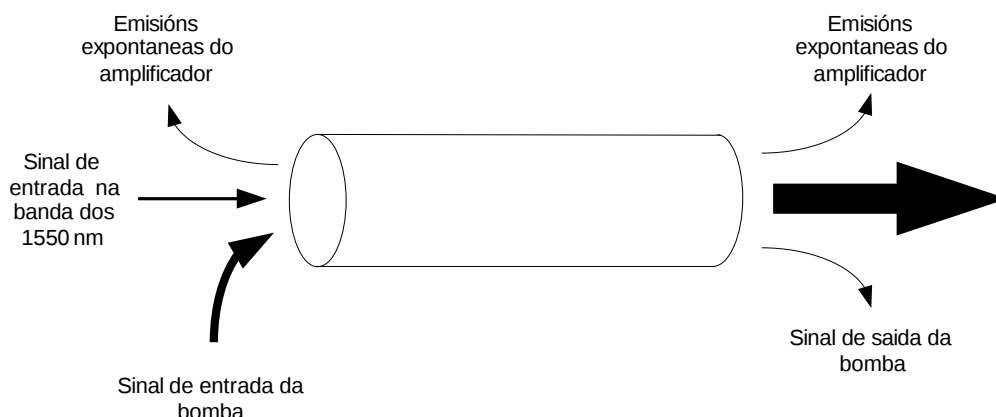
Con señales tan precisas y densas como las usadas en DWDM, tiene que existir una forma que aporte una precisa separación de las señales, o filtrado, en el receptor óptico. Esta solución también tiene que ser fácil de implementar y no requerir mantenimiento. Los sistemas primitivos de filtrado eran o demasiado imprecisos para DWDM o demasiado sensibles a variaciones de temperatura y polarización, demasiado vulnerables a cruces de comunicaciones en canales adyacentes o demasiado caros. Esto restringió la evolución de DWDM. Para conseguir satisfacer los requisitos de alto rendimiento, se desarrolló una nueva tecnología de filtrado que hizo DWDM posible a un coste aceptable: la fibra con rejilla de Bragg.

El nuevo componente de filtro (fibra con rejilla) consiste en una determinada longitud de fibra óptica donde el índice de refracción del núcleo fue permanentemente modificado en puntos equidistantes, generalmente por exposición a un patrón de interferencia ultravioleta. El resultado es un componente que refleja la luz dependiendo de la longitud de onda y es útil para separar longitudes de onda. En otras palabras, la rejilla la crea un filtro altamente selectivo para una longitud de onda muy estrecha que funciona de forma similar a un espejo y aporta mayor selectividad de longitud de onda que cualquier otra tecnología. Como este es un dispositivo pasivo, fabricado en fibra de vidrio, es fuerte y duradero.

48.1.3.2 ERBIUM DOPED FIBER AMPLIFIER

La llegada del EDFA permitió el desarrollo de sistemas DWDM comerciales proporcionando una forma de amplificar todas las longitudes de onda al mismo tiempo. Esta amplificación óptica se hace incorporando iones de Erblio en el núcleo de una fibra especial en un proceso conocido como dopado. Se usan bombas ópticas láser para transferir altos niveles de energía a la fibra especial, energizando los iones de Erblio que luego aumentan a las señales ópticas que pasan por la fibra. La estructura

atómica del Erblio proporciona amplificación a los grandes rangos del espectro que se requieren para DWDM.



TEXTO: Emisiones espontáneas del amplificador. Señal de entrada en la banda de los 1550 nm. Señal de entrada de la bomba. Señal de salida de la bomba

En vez de múltiples regeneradores electrónicos, que requieren que la señal óptica sea convertida a señal electrónica y viceversa, el EDFA amplifica directamente las señales ópticas. De esta forma, la señal puede ser enviada hasta 600 Km. sin regeneración y hasta 120Km. entre amplificadores en un sistema DWDM disponible comercialmente.

48.1.4 MPLS

MPLS (MultiProtocol Label Switching) es una solución versátil para resolver los problemas que afrontan las redes actuales de velocidad, escalabilidad, gestión de la calidad de servicio (QoS) e ingeniería del tráfico. MPLS emergió como una solución elegante para aportar la gestión de ancho de banda y requerimientos de servicio para la nueva generación de redes troncales basadas en IP. MPLS resuelve problemas relacionados con la escalabilidad y encaminamiento (basados en QoS y métricas de la calidad de servicio) y puede existir sobre redes ATM y Frame Relay ya existentes.

48.1.4.1 FUNCIONES DE MPLS

MPLS realiza las siguientes funciones:

- Especifica mecanismos para gestionar los flujos de tráfico de varias granularidades, como los flujos entre diferente hardware, maquinas o incluso entre diferentes aplicaciones.
- Se mantiene independiente de los protocolos de las capas 2 y 3.
- Aporta un método para mapear direcciones IP a simples etiquetas de tamaño fijo, usadas por diferentes tecnologías.
- Se integra con protocolos existentes como RSVP (Resource Reservation Protocol) y OSPF (Open Shortest Path First).
- Da soporte a IP, ATM y Frame Relay.

En MPLS la transmisión de datos se produce en LSPs (Label Switching Paths). Un LSP es una secuencia de etiquetas para cada uno de los nodos a lo largo del camino, desde el origen hasta el destino. Los LSPs se establecen antes de la transmisión de los datos (establecimiento por control) o ante la detección de un determinado flujo de datos (establecimiento por datos).

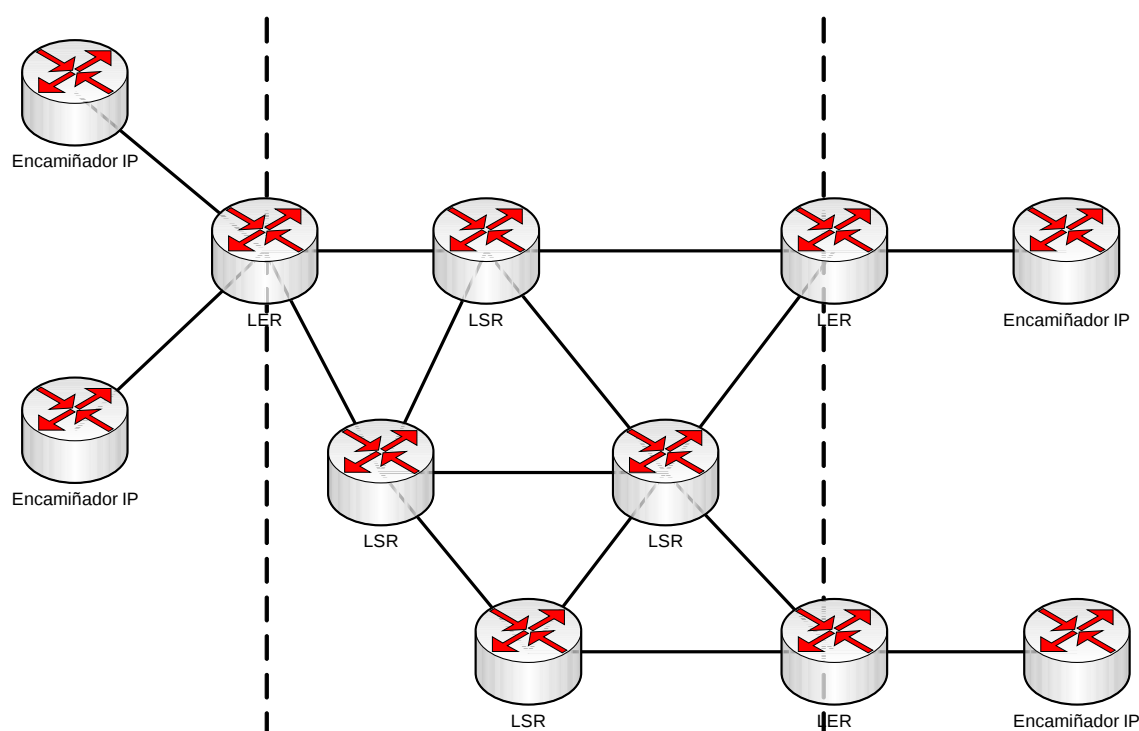
Las etiquetas (que son identificadores específicos de los protocolos subyacentes) se distribuyen usando LDP (Label Distribution Protocol) o RSVP o acompañando los datos de protocolos de encaminamiento como el BGP (Border Gateway Protocol) y OSPF. Cada paquete de datos encapsula y transporta las etiquetas durante su trayecto desde el origen hasta el destino. La alta velocidad de conmutación es posible por la longitud fija de las etiquetas y porque estas son insertadas al principio del paquete o celda y esto permite que hardware específico las use para conmutar paquetes a alta velocidad entre distintos enlaces.

48.1.4.2 LSRS Y LERS

Los dispositivos que participan en los mecanismos del protocolo MPLS pueden clasificarse en LERs (Label Edge Routers) y LSRs (Label Switching Routers).

Un LSR es un encaminador de alta velocidad en el núcleo de una red MPLS que participa en el establecimiento de los LSPs usando el protocolo de señales adecuado y proporciona conmutación de alta velocidad de los datos basándose en los caminos establecidos.

Un LER es un dispositivo que opera en el límite entre la red de acceso y de la red MPLS. LERs soportan múltiples puertos conectados a diferentes redes (Frame Relay, ATM, Ethernet,...) y envía el tráfico a la red MPLS después de establecer su LSP, también distribuye el tráfico a la red de acceso en el proceso inverso. El LER juega un papel muy importante en la asignación y renovación de etiquetas, cuando el tráfico entra o sale de una red MPLS.



TEXTO: Encaminador

48.1.4.3 FEC

La FEC (Forward Equivalent Class) es la representación de un grupo de paquetes que comparten los mismos requisitos de transporte. Todos los paquetes de este grupo reciben el mismo tratamiento en su ruta hacia el destino. Al contrario que IP, en MPLS, la asignación de un determinado paquete a un FEC se realiza solo una vez, cuando el paquete entra en la red. Los FECs están basados en los requisitos del servicio para un conjunto de paquetes o simplemente en un determinado prefijo de red. Cada LSR construye una tabla para saber cómo un paquete debe ser enviado. Esta

tabla, llamada LIB (Label Information Base) se componen de relaciones FEC – etiqueta.

48.1.4.4 ETIQUETAS

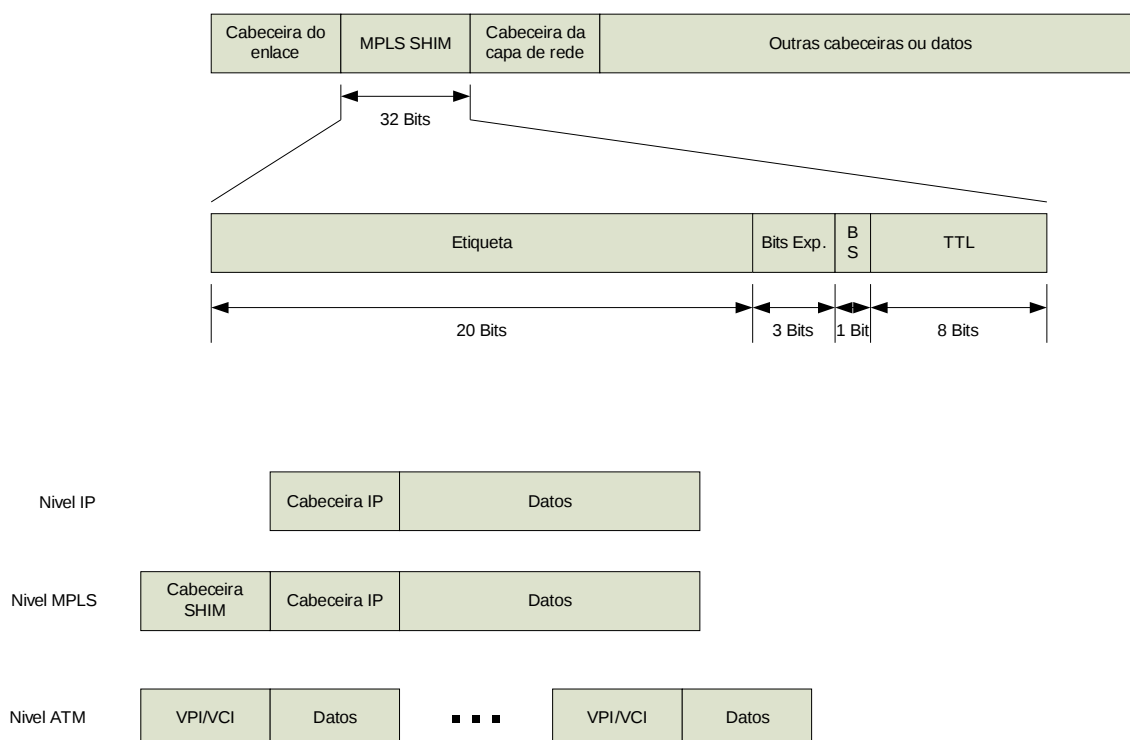
Una etiqueta en su forma más simple, identifica el camino que debe recorrer un paquete. Las etiquetas se encapsulan en una cabecera de nivel 2 junto con el paquete. El encaminador que lo recibe, examina el paquete para obtener su etiqueta para determinar el siguiente salto. Una vez que el paquete está etiquetado, el resto del camino por la red troncal se basa en conmutación por etiquetas. Los valores de las etiquetas solo tienen valor local, esto quiere decir que solo pertenecen a saltos entre LSRs concretos. Cuando un paquete se clasifica como un FEC nuevo o existente, se le asigna una etiqueta. Los valores de la etiqueta se derivan de la capa de enlace inferior (DLCI para Frame Relay, VPI/ VCI para ATM,...).

Las etiquetas se enlazan con los FEC como resultado de un evento o política que indica la necesidad de ese enlace. Estos eventos pueden tener como origen las señales de control o las propias de transmisión de datos siendo esta última la mejor opción por sus propiedades de escalado.

La asignación de etiquetas se basa en criterios de encaminado como:

- Destino Unicast
- Ingeniería de tráfico
- Multicast
- VPN (Virtual Private Network)
- QoS

En la siguiente imagen podemos ver la estructura de una etiqueta MPLS y un ejemplo del proceso desde IP hasta la capa de enlace (en este caso sobre ATM).



TEXTO: CABECERA

48.1.4.5 DISTRIBUCIÓN DE ETIQUETAS

MPLS no imponen un solo método de distribución de etiquetas. Existen protocolos de encaminado, como BGP y RSVP que fueron mejorados para poder incorporar (usando el método *poggyback*) la información de las etiquetas junto con la información del protocolo. El IETF (Internet Engineering Task Force) también definió un protocolo llamado LDP (Label Distribution Protocol) para gestionar las etiquetas. Extensiones de LDP permiten definir rutas explícitas basadas en requisitos de Qos. Estas extensiones están recogidas en la definición del protocolo CR-LSP (Constraint-based Routing-LDP).

Un resumen de los varios esquemas para el intercambio de etiquetas es el siguiente:

- LDP: mapea direcciones de unicast IP a etiquetas.
- RSVP, CR-LDP: se usan para ingeniería del tráfico y reserva de recursos.

- PIM (Protocol Independent Multicast): se usa para mapear multicasts a etiquetas.
- BGP: etiquetas externas (VPN)

48.1.4.6 LSP

Una colección de dispositivos MPLS se define como un dominio MPLS.

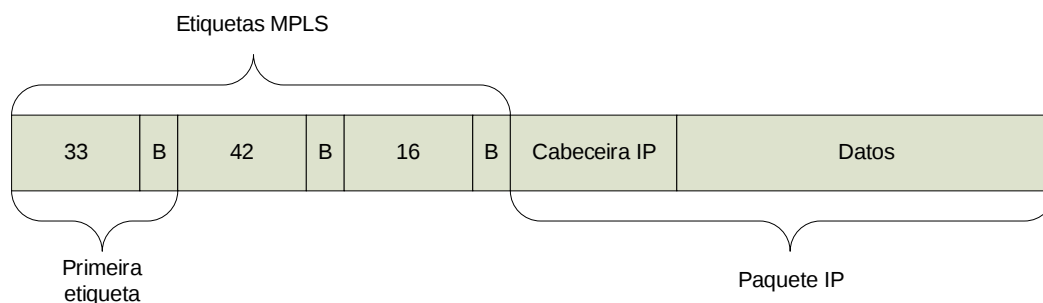
Dentro de un dominio MPLS se fija un camino para un paquete basándose en su FEC. El LSP se fija antes de la transmisión de los datos usando una de estas dos opciones:

- Encaminado salto a salto (hop-by-hop): cada LSR selecciona independientemente el siguiente salto para un FEC determinado. Esta es una metodología muy similar a la usada en redes IP. El LSR usa los protocolos de encaminamiento disponibles como OSPF, etc.
- Encaminado explícito (ER-LSP): El LSR de entrada (el LSR donde el flujo de datos comienza en la red) especifica una lista de nodos que el ER-LSP atraviesa. El camino podría ser no excelente. Los recursos necesarios podrían ser reservados para garantizar la QoS. Esto facilita la ingeniería de tráfico en la red, y permite que servicios diferentes sean dados usando flujos basados en métodos de políticas o gestión de red.

Un LSP para un determinado FEC es unidireccional en naturaleza, el tráfico de retorno tendrá que usar otro LSP.

48.1.4.7 PILA DE ETIQUETAS

El apilado de etiquetas (Label Stack) es un mecanismo que permite la operación jerárquica dentro de un dominio MPLS. Básicamente permite al MPLS ser usado simultáneamente para el encaminado a nivel fino (entre encaminadores individuales dentro de un ISP) y en un nivel grueso (dominio a dominio). Cada nivel, en una pila de etiquetas, pertenece a un nivel jerárquico. Esto facilita el uso de túneles en MPLS.



TEXTO: CABECERA. PRIMERA ETIQUETA

48.2 REDES DE FIBRA ÓPTICA

48.2.1 JERARQUÍA DIGITAL PLESIÓCRONA (PDH)

A PDH (Plesiochronous Digital Hierarchy) es una tecnología usada en redes de telecomunicaciones para transportar una gran cantidad de datos sobre redes de fibra óptica o radioenlaces. El término alude a que las diferentes partes de la red funcionan de forma casi sincronizada, pero no totalmente. La mayor parte de los operadores están actualizando PDH a SDH o SONET (capaces de transmitir a más velocidad) si no la reemplazan directamente por una tecnología completamente distinta.

PDH permite la transmisión de datos a una velocidad similar entre las transmisiones pero permitiendo variaciones sobre la velocidad nominal, ya que no hay una sincronización exacta dentro de la red.

La velocidad de transferencia básica es de 2 Mb/s, para la transferencia de voz está dividida en 30 canales de 64Kb/s y dos canales para señalización y sincronización; además todo el enlace (2Mb/s) se puede usar para transmitir datos.

La velocidad de transmisión está controlada por un reloj en el equipo que envía los datos; esta velocidad puede variar 50 ppm desde los 2 Mb/s esto quiere decir que las distintas transmisiones pueden estar sucediendo a diferentes velocidades (y probablemente lo están).

Para transmitir varios flujos de datos desde un origen, estos se multiplexan en grupos de 4 de forma que primero se transmite el bit 1 del flujo 1, luego el bit 1 del flujo 2, luego el bit 1 del flujo 3, luego el bit 1 del flujo 4 y así sucesivamente. El transmisor también añade información para poder

reconstruir el flujo cuando se recibe. Como los flujos de datos transmitidos pueden no estar siendo recibidos a la misma velocidad en el multiplexador de origen, este supone que los está recibiendo a la máxima velocidad posible. Esta suposición provoca que a veces no se haya recibido el bit correspondiente de un flujo, esta situación debe ser notificada al multiplexador de destino para que este pueda reconstruir los flujos a la velocidad correcta.

La velocidad resultante de la multiplexación descrita es de 8.448 kbit/s, técnicas similares permiten combinar 4 streams de 8 Mb/s más bit de relleno (proporcionando 34 Mb/s), 4 streams de 34Mb/s (proporcionando 140Mb/s) y 4 streams de 140 Mb/s (proporcionando 565Mb/s). 565 Mbit/s es la velocidad típica para transmitir datos sobre fibra óptica para largas distancias.

48.2.2 JERARQUÍA DIGITAL SÍNCRONA (SDH) / SONET

Synchronous optical networking (SONET) y Synchronous Digital Hierarchy (SDH) son protocolos de multiplexación que transmiten varios streams sobre una red de fibra óptica, aunque también se pueden usar sobre interfaces eléctricos (a menor velocidad). Esta técnica se desarrolló para reemplazar PDH en la tarea de transportar un ancho número de llamadas de teléfono y tráfico de datos sobre la misma fibra en problemas de señalización. La mayor diferencia con PDH es que SDH / SONET está sincronizada usando relojes atómicos reduciendo la necesidad de buffers en la red y aprovechándola mejor.

SONET y SDH, son básicamente idénticos, y, aunque SONET (ANSI T1.105) es anterior, dado que solo se utiliza en Canadá y EEUU mientras que SDH (ITU G.707, G.783, G.784 y G.803) se utiliza en el resto del mundo, SONET se considera una variación de SDH. Dada la gran similitud entre ellos es extremadamente fácil la interconexión entre los dos a cualquier velocidad.

48.2.2.1 FRAME SDH / SONET

La unidad básica para la transmisión en SDH es la Synchronous Transport Module, level 1 (STM-1), que se transmite a 155,52Mb/s. SONET cambia el nombre de esta estructura a Synchronous Transport Signal 3 concatenated

(STS-3c) u OC-3c dependiendo si la señal se transporta eléctrica (STS) u ópticamente (OC) pero su funcionalidad, velocidad y tamaño son iguales a STM-1.

SONET proporciona otra unidad STS-1 u OC-1 que opera a 51,84Mb/s (un tercio de STM-1) esto busca poder transmitir un canal DS-3 estándar (672 canales de 64Kb/s para voz).

48.2.2.1.1 FRAMING

En tecnologías como Ethernet la trama consiste en una cabecera y un conjunto de datos, la cabecera se transmite primero, seguida de los datos y posiblemente de una cola que contiene el CRC o equivalente. En SDH esto se modifica ligeramente, la cabecera se denomina overhead y en vez de ser transmitida antes que el resto de los datos es entrelazada con ellos durante la transmisión: se transmite parte de la cabecera, luego parte de los datos,... hasta que se transmite todo el frame.

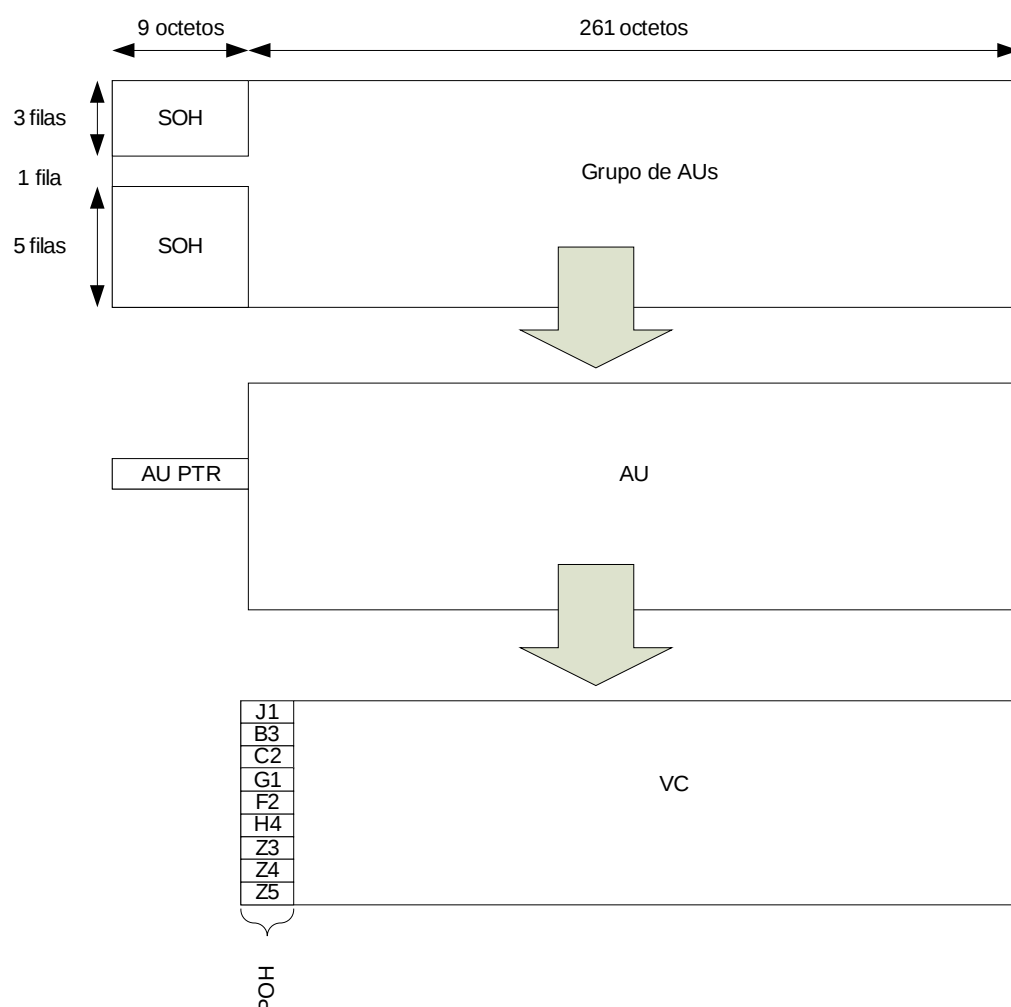
En el caso de STS-1, cada frame está compuesto de 810 octetos, mientras que en el caso de STM-1/STS-3 cada frame está compuesto de 2.430 octetos. STS-1 transmite 3 octetos de overhead seguidos de 87 de datos durante nueve veces hasta transmitir los 810 octetos en 125 microsegundos. En el caso de STM-1 (que opera a tres veces la velocidad de STS-1) se transmiten 9 octetos de overhead y 261 de datos, también 9 veces hasta que se transmite en los 2.430 octetos llevando también 125 microsegundos. Esto suele representarse gráficamente dibujando el frame como un bloque de 90 columnas y 9 filas para STS-1 y 270 columnas y 9 filas para STM-1 de esta forma la representación alinea toda la overhead y todos los datos de la payload.

La estructura interna de la overhead y de los datos transmitidos dentro del frame varía ligeramente para SONET y SDH, usando también diferentes nombres para describir estructuras.

48.2.2.1.2 ESTRUCTURA DEL FRAME STM-1

La Overhead Section y los Administrative Unit Pointers ocupan las 9 primeras columnas del frame. Estos punteros (los bytes H1, H2 y H3) identifican AUs (Administrative Units) dentro de la carga útil. Cada una de

estas unidades administrativas puede albergar uno o varios Virtual Containers (VC) que a su vez contienen una descripción del camino (Path OverHead, POH) y datos. La primera columna es para el POH y el resto son para datos que pueden ser a su vez otros VC. Las unidades administrativas pueden tener cualquier tipo de alineación y es esta alineación la que es indicada por el puntero de la fila 4.



Los componentes del frame son:

- Overhead conteniendo:
 - o SOH (Section OverHead) contiene información para el sistema de transmisión (para control de calidad, detección de fallas,...) y está dividida en dos partes:

- RSOH (Regenerator Section Overhead) también conocida como Section overhead: compuesta por 27 octetos que contiene información sobre la estructura del frame.
- MSOH (Multiplex Section Overhead) también conocida por Line overhead: está compuesta por 45 octetos que contiene información sobre corrección de errores y mensajes Automatic Protection Switching (como podrían ser: alarmas y mensajes de mantenimiento)
 - o Puntero AU: Apunta a la localización del byte J1 en los datos (el primer byte del VC).
- Datos Path: los datos transmitidos de extremo a extremo se llaman datos path y están compuestos de 2 elementos:
 - o POH (Path OverHead): nueve octetos para señalización extremo a extremo.
 - o Datos de usuario: 2340 octetos de datos

48.3 REDES DE NUEVA GENERACIÓN (NGN)

Según el ITU-T, una NGN es una red basada en paquetes que puede proporcionar servicios, incluyendo servicios de telecomunicaciones, y capaz de usar varias tecnologías de banda ancha que incorporen capacidades de calidad de servicio. En estas redes las funciones relacionadas con el servicio deben ser independientes de la tecnología de transporte usada. Ofrecen un acceso sin restricciones al usuario a diferentes proveedores de servicio. Soporta la movilidad, lo que permitirá un acopio de servicio consistente y ubicuo a los usuarios.

Desde un punto de vista práctico, NGN implica tres cambios en la arquitectura:

- En la red troncal, NGN implica la consolidación de diversas redes de transporte, cada una de las cuales construida históricamente para un servicio diferente en una sola red troncal de transporte (normalmente basada en IP y Ethernet). Implica entre otras, la migración de la voz desde una arquitectura de conmutación de circuitos (RTC) a VoIP, y

también la migración de servicios como X.25 y Frame Relay (ya sea una migración comercial a nivel de usuario con servicios como VPN sobre IP, o la migración técnica emulando estos servicios pero sobre la NGN).

- En la red de acceso por par de cobre, NGN implica la migración desde el sistema dual con la voz independiente del xDSL en la central a la que llega el bucle de abonado a una configuración donde los DSLAMs (Digital Subscriber Line Access Multiplexer, el punto donde se concentran todas a las conexiones DSL de la central) integran puertos de voz o VoIP, posibilitando la eliminación de la infraestructura de conmutación de voz.
- En la red de acceso de cable, la convergencia NGN implica la migración de la voz de servicios CBR a estándares de VoIP y SIP.

En una NGN existe una mayor distancia entre la parte de la red que proporciona el transporte (conectividad) y los servicios que se ejecutan sobre este. Esto tiene como consecuencia que cada vez que un operador quiere dar un nuevo servicio solo tiene que definir el nivel de la capa de servicios sin preocuparse por el transporte. Cada vez más los servicios (incluyendo los de voz) tienden a ser independientes de la red de acceso y residen más en los equipos de usuario final (PC, Set-Top Box,...).

48.3.1 TECNOLOGÍAS DE SOPORTE

Las redes de nueva generación están basadas en tecnologías como IP y MPLS. A nivel de aplicación SIP (Session Initiation Protocol) está reemplazando a H.323. Aunque originalmente H.323 era el protocolo de VoIP / videoconferencia /... sobre redes IP más popular, a sus limitaciones para atravesar NAT (Network address translation) y firewalls reducen su implantación a nivel del bucle de abonado. Son estas algunas de las razones (junto con la complejidad de H.323) que están llevando a la implantación de SIP, sobre todo en el bucle de abonado. Sin embargo, en las redes de operador (donde todo está bajo su control) muchos de ellos usan H.323 para a sus redes troncales.

Con los nuevos cambios introducidos en H.323 es posible que dispositivos H.323 atraviesen NAT y firewalls fácilmente, esta circunstancia puede propiciar que H.323 pueda volver a ser usado en entornos donde esto sea necesario.

Como contrapartida muchos operadores están investigando y dando soporte a IMS (IP Multimedia Subsystem, una arquitectura estandarizada para servicios multimedia en Internet definida por el ETSI y la 3GPP) que daría a SIP la oportunidad de ser el protocolo más usado.

Para aplicaciones de voz el dispositivo más importante de la NGN y el Softswitch (este nombre y sus funciones aún son muy dependientes del fabricante), un dispositivo que controla las llamadas VoIP permitiendo la correcta integración de diferentes protocolos dentro de la NGN. Su función principal es crear la interfaz a las redes telefónicas existentes (RTC).

Uno de los términos más comúnmente usados es el de GateKeeper, que originalmente se refería a un dispositivo que transformaba voz y datos desde sus formatos analógicos a IP. Cuando este dispositivo comenzó a usar Media Gateway Control Protocol pasó a llamarse Media Gateway Controller (MGC).

Un Agente (Call Agent, SIP Agent,...) es un nombre general para dispositivos capaces de controlar llamadas.

48.4 BIBLIOGRAFÍA

- MultiProtocol Label Switching – The International Engineering Consortium
- Dense Wavelength Division Multiplexing - ATG's Communications & Networking Technology

Autor: Matías Villanueva Sampayo

Director de Informática Asociación Provincial de Pensionistas y Jubilados de A Coruña

Colegiado del CPEIG

49. TECNOLOGÍAS SIN HILOS: BLUETOOTH, WIBREE, WIRELESS USB, WI-FI. RFID. TECNOLOGÍAS MÓVILES.

Tema 49. Tecnologías sin hilos: Bluetooth, WiBree, Wireless USB, Wi-Fi. RFID. Tecnologías móviles

49.1 Tecnologías sin hilos

49.1.1 Bluetooth

49.1.1.1 Funcionamiento de Bluetooth

49.1.1.1.1 Especificaciones y características

49.1.1.1.1.1 Versión 1.0 y 1.0B

49.1.1.1.1.2 Versión 1.1

49.1.1.1.1.3 Versión 1.2

49.1.1.1.1.4 Versión 2.0 + EDR

49.1.1.1.1.5 Versión 2.1 + EDR

49.1.1.1.1.6 Versión 3.0 + HS

49.1.1.1.1.7 Versión 4.0

49.1.1.1.2 Pila de protocolos

49.1.1.1.2.1 Capa de banda base e interfaz de radio

49.1.1.1.2.2 Capa del protocolo de gestión de enlace (LMP)

49.1.1.1.2.3 Interfaz de controlador Host (HCI)

49.1.1.1.2.4 Capa del protocolo de adaptación y control del enlace lógico (L2CAP)

49.1.1.1.2.5 Capa del protocolo de descubrimiento de servicios (SDP)

49.1.1.1.2.6 Capa RFCOMM

49.1.1.1.2.7 Comandos AT

49.1.2 WiBree

49.1.3 Wireless USB

49.1.3.1 Descripción del sistema

49.1.3.1.1 Topología

49.1.3.1.1.1 USB host

49.1.3.1.1.2 Dispositivos Wireless USB

49.1.3.1.1.3 Interfaz física

- 49.1.3.1.1.3.1 Velocidades de la capa física
- 49.1.3.1.1.3.2 Soporte de canales
- 49.1.3.1.1.3.3 Selección de canal
- 49.1.3.1.1.4 Gestión de energía
- 49.1.3.1.1.5 Protocolo de bus
- 49.1.3.1.1.6 Robustez
 - 49.1.3.1.1.6.1 Gestión de los errores
- 49.1.3.1.1.7 Seguridad
- 49.1.3.1.1.8 Configuración
 - 49.1.3.1.1.8.1 Conexión de dispositivos Wireless USB
 - 49.1.3.1.1.8.2 Desconexión
 - 49.1.3.1.1.8.3 Enumeración
- 49.1.3.1.1.9 Tipos de flujos de datos
- 49.1.3.1.1.10 Dispositivos Wireless USB
 - 49.1.3.1.1.10.1 Características de los dispositivos
 - 49.1.3.1.1.10.2 Dispositivos y capa MAC
- 49.1.3.1.1.11 Hardware y software del host
- 49.1.4 Wi-Fi
 - 49.1.4.1 Descripción del sistema
 - 49.1.4.1.1 Capa física (PHY)
 - 49.1.4.1.1.1 Infrarrojos
 - 49.1.4.1.1.2 FHSS
 - 49.1.4.1.1.3 DSSS
 - 49.1.4.1.1.4 Tramas de la capa física
 - 49.1.4.1.2 Capa de acceso al medio (MAC)
 - 49.1.4.1.2.1 Tramas del nivel MAC
- 49.2 RFID
 - 49.2.1 Principios de RFID
 - 49.2.2 Componentes y operación
- 49.3 Tecnologías móviles

49.3.1 Android

49.3.2 Meego

49.3.3 Symbian

49.3.4 Windows Phone 7

49.4 Bibliografía

49.1 TECNOLOGÍAS SIN HILOS

49.1.1 BLUETOOTH

Es una tecnología sin hilos de corto alcance (PAN) diseñada para sustituir los cables entre dispositivos que se convirtió en la solución sin hilos ideal para conectar teléfonos móviles con portátiles para su conexión a Internet, o para que otros organizadores de mano, como PDAs puedan conectarse al PC para coordinar sus contactos, e incluso para poder imprimir desde un ordenador sin necesidad de cables.

Las características intrínsecas de las tecnologías con bluetooth permiten establecer conexiones seguras, con capacidad de encriptación del canal, autenticación de la red y otros parámetros de seguridad como la localización y dispositivo del usuario.

49.1.1.1 FUNCIONAMIENTO DE BLUETOOTH

Bluetooth trabaja en el rango de frecuencias de 2.4 a 2.48 Ghz, con espectro ensanchado (widespread) y saltos de frecuencia (frequency hopping), con posibilidad de transmitir en full-duplex con un máximo de 1600 saltos/seg. Los saltos de frecuencia se realizan entre un total de 79 frecuencias con intervalos de 1Mhz, lo cual permite brindar seguridad y robustez. La frecuencia en la cual trabaja le permite atravesar paredes, por lo cual es ideal tanto para el móvil, como en oficinas.

La potencia de salida para transmitir a una distancia máxima de 10m es 1-2,5 mW, mientras que la versión de largo alcance, hasta 100m, transmite a 100 mW.

Para lograr alcanzar el objetivo de bajo consumo y bajo coste, se diseñó una solución integrada en un solo chip. De esta manera, se logró crear una

solución de 9x9mm y que consume aproximadamente 97% menos energía que un teléfono celular común.

Cada una de los cuatro canales de voz en la especificación Bluetooth puede soportar una tasa de transferencia de 64 Kb/s en cada sentido, lo cual es suficientemente adecuada para la transmisión de voz. Un canal de datos asíncrono puede transmitir 721 Kb/s en una dirección y 56 Kb/s en la dirección contraria, sin embargo, para una conexión asíncrona es posible soportar 432,6 Kb/s en ambas direcciones si el enlace es simétrico.

Para relacionarse e intercambiar información los dispositivos Bluetooth ofrecen distintos servicios, llamados técnicamente Perfiles, entre estos perfiles se encuentran el Acceso a Redes locales (LAN), Acceso Telefónico, Fax, Transferencia de Archivos, Sincronización, Intercomunicador, o Telefonía sin hilos, entre otros. De esta

forma cuando dos dispositivos se comunican por primera vez intercambian esta información para conocer sus posibilidades de intercomunicación.

Las compañías mas destacadas en el desarrollo de esta tecnología fueron Ericsson y Nokia. La primera versión del estándar Bluetooth se lanzó en mayo de 1998. Esta tecnología sin hilos tenía una velocidad de transferencia de datos de 1Mbps y cuenta con un alcance máximo de 100 metros. Sin embargo, la versión más utilizada es la de alcance 10 metros, ya que el consumo eléctrico aumenta rápidamente con una mayor potencia de transmisión.

49.1.1.1.1 ESPECIFICACIÓN Y CARACTERÍSTICAS

Tras el diseño de la primera especificación en 1994 la especificación fue ratificada por el SIG (Bluetooth Special Interest Group) en 1998 y desde entonces evolucionó en varias versiones hasta la actualidad. Todas estas versiones incluyen la compatibilidad con los dispositivos de las versiones anteriores.

49.1.1.1.1.1 VERSIÓN 1.0 Y 1.0B

Estas versiones tuvieron muchos problemas sobre todo en lo que a interoperabilidad entre fabricantes se refiere.

También obligaba a incluir la dirección física en la transmisión durante el proceso de conexión lo cual era contraproducente para algunos de los servicios planificados.

49.1.1.1.1.2 VERSIÓN 1.1

Fue establecida como estándar 802.15.1-2002 por el IEEE corrigiendo muchos errores de la versión 1.0B y añadiendo soporte para canal son encriptados y RSSI (Received Signal Strength Indicator).

49.1.1.1.1.3 VERSIÓN 1.2

Los avances de esta versión incluyen:

- Mayor velocidad de conexión y búsqueda (Discovery).
- Uso de AFH (Adaptive Frequency-Hopping) que mejora la resistencia a interferencias evitando el uso de frecuencias muy ocupadas en la secuencia de saltos.
- Mayor velocidad de transmisión, en la práctica hasta 721 kbit/s.
- Uso de eSCO (Extended Synchronous Connections) que mejora la calidad de los enlaces de voz permitiendo la retransmisión de paquetes corruptos y, opcionalmente, pudiendo incrementar la latencia para mejorar el soporte para la transferencia de datos concurrente.
- Soporte del HCI (Host Controller Interface) para UARTs de 3 hilos.
- Estandarizado como IEEE 802.15.1-2005.
- Introducción de modos de control de flujo y retransmisión para L2CAP.

49.1.1.1.1.4 VERSIÓN 2.0 + EDR

La principal diferencia con la versión anterior es la posibilidad de uso de EDR (Enhanced Data Rate) como modo de transferencia rápido, siendo la velocidad nominal de 3 Mbit/s aunque la velocidad práctica real sea de 2.1 Mb/s. EDR es opcional en la especificación por lo que pueden existir dispositivos de la versión 2.0 que no soporten EDR.

49.1.1.1.1.5 VERSIÓN 2.1 + EDR

Esta versión fue adoptada por el SIG en el 2007 siendo su mayor aportación al estándar el SSP (Secure Simple Pairing) que mejora la experiencia de emparejamiento de los dispositivos Bluetooth mientras mejora la seguridad.

49.1.1.1.1.6 VERSIÓN 3.0 + HS

Esta versión es del 2009 soportando en teoría velocidades de hasta 24Mb/s, pero no sobre el enlace Bluetooth sino que Bluetooth se usa para negociar el establecimiento de un enlace 802.11 sobre el que se transfieren los datos.

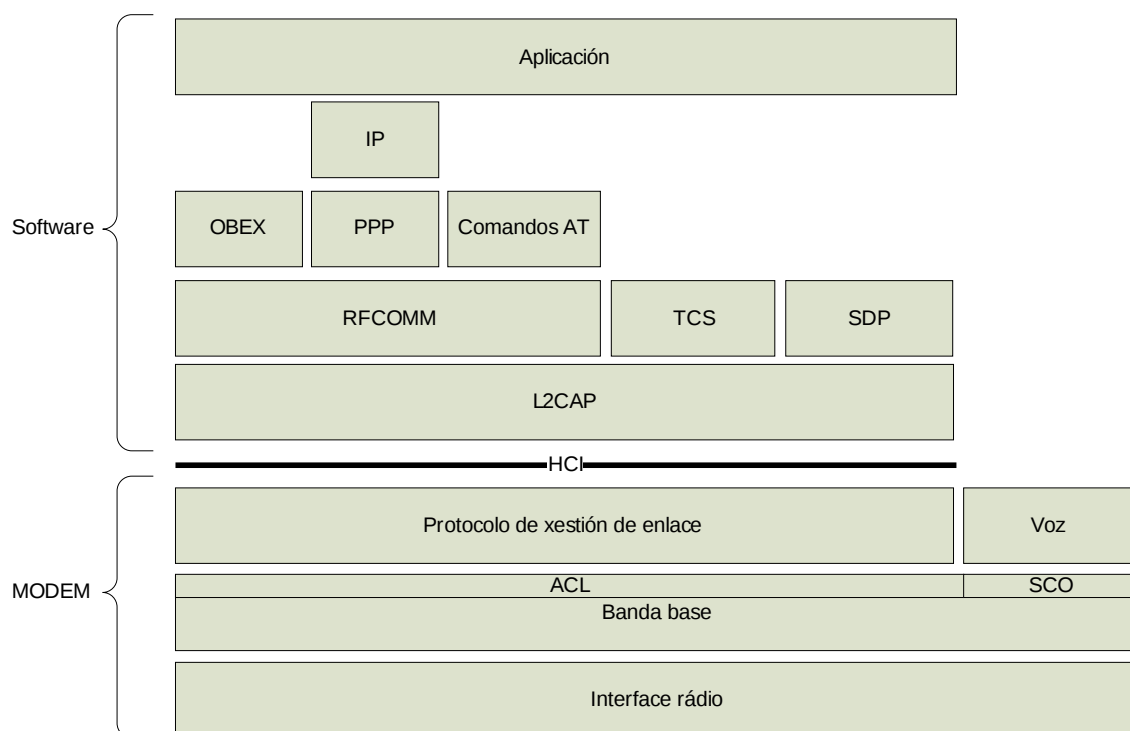
49.1.1.1.1.7 VERSIÓN 4.0

Esta versión data de junio de 2010 e incluye tres sabores del protocolo: Classic Bluetooth, Bluetooth high speed y Bluetooth low energy. Bluetooth high speed está basado en WiFi y Classic Bluetooth está compuesto por los protocolos de versiones anteriores.

Por su parte, Bluetooth low energy define una nueva pila de protocolo para la creación rápida de enlaces simple y fue diseñado para ejecutarse en dispositivos de muy bajo consumo.

49.1.1.1.2 PILA DE PROTOCOLOS

De una forma básica podemos ver la pila de protocolos Bluetooth en la imagen siguiente.



49.1.1.1.2.1 CAPA DE BANDA BASE E INTERFAZ DE RADIO

En la base de la pila de protocolos Bluetooth se encuentran la capa de banda base y el interfaz de radio. Su función principal es permitir el enlace físico por radiofrecuencia (RF) entre unidades Bluetooth realizando tareas de modulación y demodulación de los datos en señales RF que se transmiten por los aires.

El nivel de banda base proporciona dos tipos de enlace físico:

- ACL (Asynchronous ConnectionLess) para enlaces asíncronos sin conexión.
- SCO (Synchronous Connection-Oriented) para enlaces síncronos orientados a conexión.

49.1.1.1.2.2 CAPA DEL PROTOCOLO DE GESTIÓN DE ENLACE (LMP)

La capa LMP es la responsable de la configuración y control del enlace entre dispositivos Bluetooth, incluyendo el control y negociación del tamaño de los paquetes.

49.1.1.1.2.3 INTERFAZ DE CONTROLADOR HOST (HCI)

La capa HCI (Host Controller Interface) actúa como frontera entre las capas de protocolo relativas al hardware (módulo Bluetooth) y las relativas al

software (host Bluetooth). Proporciona una interfaz de comandos para la comunicación entre el host y el firmware del módulo Bluetooth y permite disponer de una capa de acceso homogénea para todos los módulos Bluetooth, aunque sean de distintos fabricantes.

49.1.1.1.2.4 CAPA DEL PROTOCOLO DE ADAPTACIÓN Y CONTROL DEL ENLACE LÓGICO (L2CAP)

La especificación Bluetooth incluye el protocolo L2CAP (Logical Link Control and Adaptation Protocol), que se encarga de la multiplexación de protocolos, ya que el protocolo de banda base no soporta un campo tipo para identificar el protocolo de nivel superior al que quiere transmitir la información, por ejemplo SDP, RFCOMM y TCS.

Otra función que se realiza en el nivel L2CAP es la segmentación y recomposición de paquetes, necesaria para permitir la utilización de protocolos que utilicen paquetes de mayor tamaño que los soportados por la capa de banda base.

49.1.1.1.2.5 CAPA DEL PROTOCOLO DE DESCUBRIMIENTO DE SERVICIOS (SDP)

El descubrimiento de servicios hace referencia a la capacidad de buscar y encontrar servicios disponibles en dispositivos Bluetooth. A través de los servicios, de los dispositivos pueden ejecutar aplicaciones comunes e intercambiar datos.

49.1.1.1.2.6 CAPA RFCOMM

El protocolo RFCOMM (Radio Frequency Communication) es un protocolo de emulación de línea serie basado en el estándar ETSI TS 07.10. Proporciona una emulación de los puertos serie RS-232 sobre el protocolo L2CAP.

49.1.1.1.2.7 COMANDOS AT

Los comandos AT son instrucciones codificadas que conforman un lenguaje de comunicación entre el hombre y un terminal módem. Los comandos AT se denominan así por la abreviatura de attention.

49.1.2 WIBREE

En 2001, investigadores Nokia determinan que existen varios escenarios no cubiertos por los sistemas sin hilos de la época. Para solucionar este

problema Nokia Research Center comenzó a desarrollar una tecnologías en hilos adaptada desde el estándar Bluetooth que proporcionara un dispositivo de más bajo consumo y precio pero sin ser muy distinto a un Bluetooth. El resultado fue publicado en 2004 usando el nombre Bluetooth Low End Extension, y tras más desarrollo la tecnología fue publicada con el nombre de WiBree en octubre de 2006. Tras una negociación con el SIG de Bluetooth, en junio de 2007 se acordó que WiBree sería incluido en una futura especificación de BlueTooth como Bluetooth ultra-low-power que hoy se conoce como Bluetooth low energy (presenta en la especificación Bluetooth 4.0).

BLE (Bluetooth Low Energy) opera en el mismo rango de frecuencias que Classic Bluetooth (2402-2480 MHz) pero usa un conjunto de canales distinto, en vez de usar los 79 canales de 1Mhz. BLE usa 40 canales de 2 Mhz.

BLE fue diseñado para permitir dos alternativas: modo simple y modo dual. Los dispositivos sencillos, como sensores, relojes, etc. están basados en el modo simple permitiendo solo BLE, mientras que los dispositivos de modo dual combinan BLE con Classic Bluetooth en la misma circuitería.

A pesar de que Classic Bluetooth y BLE pueden coexistir no son compatibles entre sí. Podemos ver las principales diferencias en la siguiente tabla.

	Classic Bluetooth	Bluetooth Low Energy
Alcance	100 m	200 m
Velocidad de la transmisión	1-3 Mb/s	1 Mb/s
Velocidad aprovechable	0.7-2.1 Mb/s	0.26 Mb/s
Latencia típica	100 ms	6 ms
Capacidad para voz	Sí	No
Topología	Malla	Etrella - Bus
Consumo	1mW	0,01 a 0,5mW
Pico de consumo de corriente	<30mA	<20mA

49.1.3 WIRELESS USB

Wireless USB es un protocolo de comunicación sin hilos de alta velocidad y reducido alcance basado en la plataforma común de radio UWB (Ultra-WideBand) y siendo capaz de transmitir a 480Mb/s hasta una distancia de 3 metros y a 11Mb/s hasta una distancia de 10 metros. Fue diseñado para operar en el rango de frecuencias entre 3.1 y 10.6 Ghz aunque las regulaciones de cada país pueden limitar este rango.

Sin embargo, aunque existe una gran excitación sobre Wireless USB es soporte de los grandes fabricantes, no acaba de despegar. A pesar de que técnicamente Wireless USB tiene muchas ventajas sobre BlueTooth y WiFi (sus principales competidores) estas otras tecnologías ya tenían su posición en el mercado y no había espacio para una nueva.

49.1.3.1 DESCRIPCIÓN DEL SISTEMA

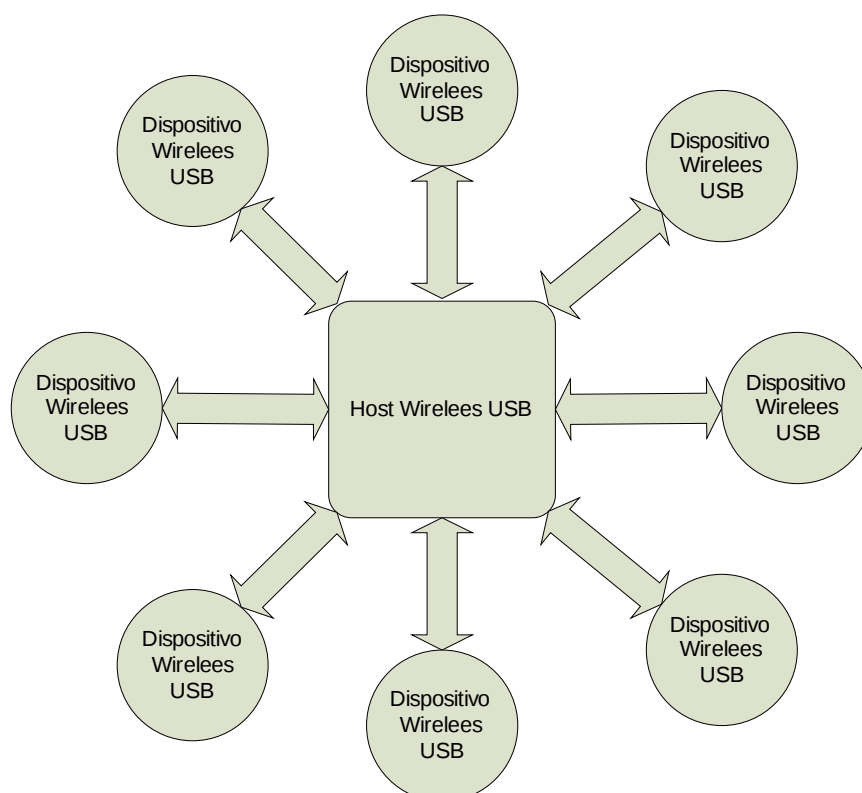
Un sistema USB esta compuesto por un host y un número indeterminado de dispositivos funcionando en la misma conexión lógica y puede ser descrito por 3 áreas:

- Interconexión USB
- Dispositivos USB
- Host USB

En este documento nos centraremos en la descripción de la Interconexión USB.

49.1.3.1.1 TOPOLOGÍA

Wireless USB conecta dispositivos usando un modelo de “conectarse al concentrador y hablar” (“hub and spoke”). El host es el concentrador en el centro de la topología y cada dispositivo se encuentra al final de una conexión punto a punto con el host. Un host puede soportar hasta 127 dispositivos debido a que Wireless USB no tiene un interfaz físico para cada puerto (conector como el del USB) no hay necesidad de instalar ningún dispositivo para expandir los puertos.



49.1.3.1.1.1 USB HOST

Solo hay un host en cualquier sistema USB. La interfaz con el ordenador host se llama Host Controller y están conectados a los PCs usando buses internos como el PCI. El Host Controller puede estar implementado como una combinación de hardware, firmware y software.

Los adaptadores que usan cables y se conectan directamente al PC usando USB se conocen como Host Wire Adapter, estos dispositivos proporcionan capacidad de Host Wireless USB al PC.

Los adaptadores que proporcionan conexiones USB pero se conectan al host usando Wireless USB se llaman Device Wire Adapters y normalmente usan conectores USB tipo A.

Hay que tener en cuenta que cada uno de estos adaptadores crea un nuevo sistema USB con un host (el adaptador) y uno o varios dispositivos USB.

49.1.3.1.1.2 DISPOSITIVOS WIRELESS USB

Los dispositivos USB pueden adoptar una de las siguientes formas:

- Funciones: proporcionan capacidades al sistema como impresoras, cámaras digitales,...

- Device Wire Adapter: ya descrito más arriba.

Los dispositivos Wireless USB proporcionan una interfaz estándar en términos de:

- Su comprensión del protocolo Wireless USB
- Su respuesta a operaciones USB estándar como confirmación o reinicialización
- Su capacidad de proporcionar información descriptiva

49.1.3.1.1.3 INTERFAZ FÍSICA

49.1.3.1.1.3.1 VELOCIDADES DE LA CAPA FÍSICA

La capa física de Wireless USB está descrita en la especificación UWB PHY de la WiMedia Alliance y soporta velocidades de transmisión de 53,3, 80, 106,7, 200, 320, 400, y 480Mb/s con múltiples canales.

PHY aporta también esquemas de detección y corrección de errores para proporcionar un canal de comunicación tan robusto como sea posible.

Las velocidades de 53,3, 106,7 y 200 son obligatorias para los dispositivos Wireless USB, el resto de velocidades son opcionales.

Los host Wireless USB están obligados a implementar todas las velocidades descritas.

49.1.3.1.1.3.2 SOPORTE DE CANALES

Todas las implementaciones Wireless USB deben soportar los canales PHY de la 9 a la 15 (Band Group 1, Códigos TF 1-7) se está permitiendo por las regulaciones nacionales. En la versión 1.1 se deben soportar Band Group 3 o Band Group 6 (todos los códigos TF) y en el caso de los hosts también a las usadas en la versión 1.0.

49.1.3.1.1.3.3 SELECCIÓN DE CANAL

Las implementaciones de Wireless USB deben soportar un canal inicial para encontrar otros dispositivos y, después de esta búsqueda, pueden moverse a otro canal.

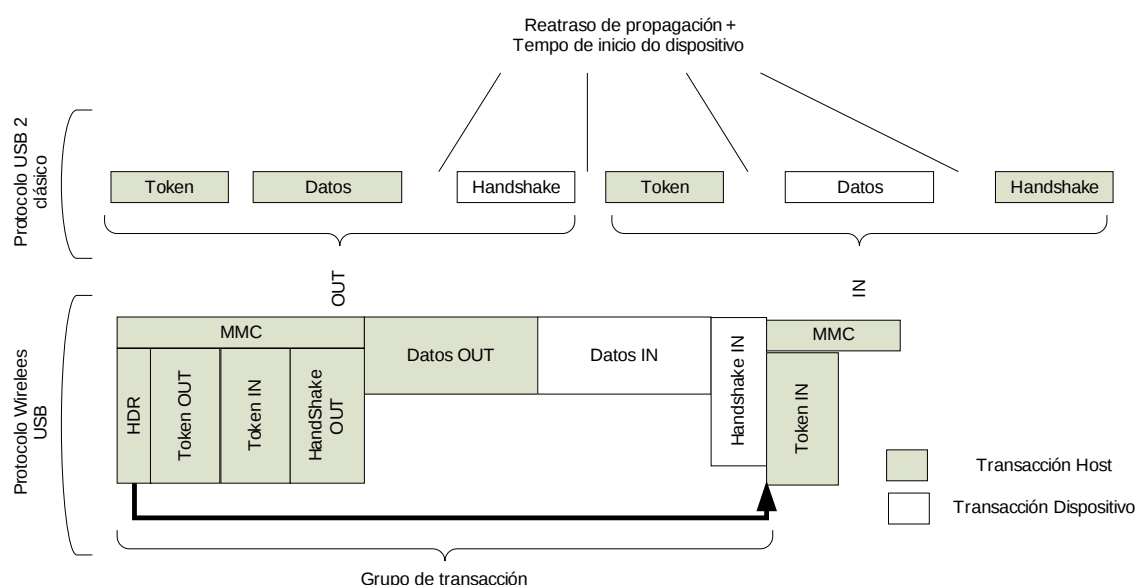
49.1.3.1.1.4 GESTIÓN DE LA ENERGÍA

Un host Wireless USB puede tener un sistema de gestión de la energía independiente del USB. El software del sistema USB interactuará con el

gestor de energía del host para procesar los eventos tales como la suspensión. Además, los dispositivos USB implementarán características adicionales para la gestión de la energía que pueden ser usadas por el software del sistema.

49.1.3.1.1.5 PROTOCOLO DEL BUS

Lógicamente Wireless USB es un protocolo basado en TDMA similar al de USB. El Host Controller inicia todas las transmisiones de datos. De la misma forma que en el USB de cable, cada transferencia está compuesta de 3 “paquetes”: token, datos y handshake. Sin embargo, para mejorar la eficiencia de la capa física eliminando transmisiones constantes entre el emisor y el receptor, los hosts combinan información de múltiples tokens en un solo paquete. En ese paquete el host indica el tiempo apropiado para que los dispositivos escuchen un paquete OUT o para que transmitan un paquete IN o handshake.



De la misma forma que en USB, el modelo de transferencia de datos entre un origen y un destino se llama pipe.

Wireless USB define un nuevo máximo tamaño de paquete para algunas transmisiones con el objetivo de mejorar el rendimiento y el consumo.

49.1.3.1.1.6 ROBUSTEZ

Hay varios atributos de Wireless USB que contribuyen a su robustez:

- La capa física está diseñada para una comunicación fiable y robusta con detección y corrección de errores.
- Detección de conexiones y desconexiones y configuración de recursos en el sistema
- Autorrecuperación en el propio protocolo usando timeouts para paquetes perdidos y corruptos
- Control de flujo metiendo en un buffer y reintentando

49.1.3.1.1.6.1 GESTIÓN DE LOS ERRORES

El protocolo permite la gestión de errores tanto en hardware como en software.

La gestión de errores en hardware incluye el informe y envío de transferencias fallidas. Un host reintentará una transmisión en la que se encuentren errores hasta un número limitado de veces antes de informar al software del fallo.

El software puede recuperarse de ese fallo en una forma que es dependiente de la implementación.

49.1.3.1.1.7 SEGURIDAD

Todos los hosts y todos los dispositivos Wireless USB deben soportar el nivel de seguridad definido en la especificación. El mecanismo de seguridad se asegura de que ambos, host y dispositivo, son capaces de autenticarse uno al otro (impidiendo un ataque de man-in-the-middle) y de que las comunicaciones son privadas.

La seguridad se base en encriptación AES-128/CCM, las comunicaciones entre el host y el dispositivo usan claves que solo el host y el dispositivo poseen una vez que están autenticados uno en el otro.

49.1.3.1.1.8 CONFIGURACIÓN

De igual forma que con el USB, Wireless USB soporta dispositivos conectándose y desconectándose del host por lo que el software del sistema debe soportar esta circunstancia.

49.1.3.1.1.8.1 CONEXIÓN DE DISPOSITIVOS WIRELESS USB

A diferencia de USB, un dispositivo Wireless Usb se conecta a un host enviando un mensaje en un momento determinado. El host y el dispositivo se autentican entre ellos usando sus identificadores únicos y las claves de seguridad apropiadas.

Después de que el dispositivo y el host se hayan autenticado y autorizado, el host le asigna una dirección USB única al dispositivo y notifica al software del sistema de la conexión del dispositivo.

49.1.3.1.1.8.2 DESCONEXIÓN

La desconexión de los dispositivos puede ser realizada de forma explícita por el host o el dispositivo usando los mecanismos definidos en el protocolo. La desconexión también se produce si el host no puede comunicarse con el dispositivo por un largo periodo de tiempo.

49.1.3.1.1.8.3 ENENUMERACIÓN

Esta actividad permite identificar y asignar direcciones únicas a los dispositivos conectados al bus lógico. Dado que Wireless USB permite a los dispositivos conectarse o desconectarse del bus lógico en cualquier momento, la enumeración es una tarea continua del software del sistema USB. Adicionalmente la enumeración de Wireless USB permite también la detección y procesamiento de las desconexiones.

49.1.3.1.1.9 TIPOS DE FLUJOS DE DATOS

Wireless USB soporta los mismos tipos de transferencia y “pipes” que USB. Debido a su mayor nivel de error (por razones del medio de transmisión), el protocolo de Wireless USB define diferentes mecanismos para realizar las transmisiones, estos mecanismos incluyen handshakes durante la recepción de datos y el uso de buffers para permitir una cierta confianza en el pipe.

La asignación de ancho de banda se realiza de forma similar a USB.

49.1.3.1.1.10 DISPOSITIVOS WIRELESS USB

De la misma forma que los dispositivos USB, los dispositivos Wireless USB están divididos en clases de dispositivos tales como interfaz humana, impresoras o dispositivos de almacenamiento. Los dispositivos Wireless USB tienen que almacenar la información necesaria para su identificación y

configuración. También se requiere de ellos que muestren un comportamiento consistente con los estados USB definidos.

Una cosa importante es que los concentradores no son dispositivos Wireless USB ya que el propio host soporta 127 dispositivos.

49.1.3.1.1.10.1 CARACTERÍSTICAS DE LOS DISPOSITIVOS

De la misma forma que en USB, todos los dispositivos Wireless USB son accesibles usando una dirección USB que es asignada cuando el dispositivo se conecta y sufre el proceso de enumeración. Cada dispositivo USB soporta adicionalmente uno o varios “pipes” por los que el host puede comunicarse con él. Todos los dispositivos deben soportar un “pipe” especial al que se había conectado el “pipe” de control USB del dispositivo. Todos los dispositivos soportan un mecanismo de acceso a la información a través de este “pipe” de control. Asociado a este “pipe” está la información requerida para describir por completo el dispositivo USB.

49.1.3.1.1.10.2 DISPOSITIVOS Y CAPA MAC

Los dispositivos deben implementar una capa MAC que se comporte adecuadamente.

49.1.3.1.1.11 HARDWARE Y SOFTWARE DEL HOST

El host posee unas responsabilidades mayores que en el caso de USB. El host Wireless USB debe comportarse de forma responsable con respeto a la capa MAC y es posible que tengan que compartir la UWB con otras aplicaciones del host, como por ejemplo en un PC el acceso radio puede ser compartido entre Wireless USB y la conexión de red.

Los hosts son también responsables de conectarse a otros dispositivos UWB (incluyendo otros hosts Wireless USB) de forma ordenada para reducir la interferencia y mejorar el uso de ancho de banda.

La especificación de hosts Wireless USB cubre hosts implementados como parte de Pcs, en el caso de otros dispositivos que no se conforman a este estándar (dispositivos portátiles, embebidos,...) pueden elegir implementar un subconjunto de los requisitos.

49.1.4 WI-FI

Hoy en día existen varias tecnologías y estándares para las comunicaciones de redes de área local sin hilos.

Estos estándares, definen una red formada por un medio inalámbrico compartido y transmisión encriptada de la información.

IEEE 802.11 es un estándar para redes inalámbricas definido por la organización Institute of Electrical and Electronics Engineers (IEEE), instituto de investigación y desarrollo, de gran reconocimiento y prestigio, cuyos miembros pertenecen a decenas de países entre profesores y profesionales de las nuevas tecnologías.

El estándar IEEE 802.11 es un estándar en continua evolución, debido a que existen cantidad de grupos de investigación, trabajando en paralelo para mejorar el estándar, a partir de las especificaciones originales.

En la actualidad coexisten principalmente los siguientes estándares:

- 802.11b: Este estándar especifica transmisiones en la banda de frecuencias de los 2.4GHz, con velocidades de incluso 11 Mbps.
- 802.11a: Este estándar, posterior al 802.11b, especifica transmisiones en la banda de los 5 GHz (una banda con menos ruido que la de los 2.4 GHz) y con una velocidad de hasta 54 Mbps. Posee una menor cobertura que 802.11b.
- 802.11g: Especifica transmisiones de hasta 54 Mbps en la banda de los 2.4GHz y asegura la compatibilidad con los dispositivos 802.11b.
- 802.11n: Aprobado en el 2009 especifica velocidades de transmisión de hasta 600Mb/s.

La alianza WI-FI (Wireless Fidelity) es una organización sin ánimo de lucro formada en 1999 para certificar la interoperabilidad de los productos 802.11 y para promocionarlos con un estándar global de WLAN en todos los segmentos de mercado. Hoy en día, existen más de 500 productos certificados, principalmente en 802.11b/g.

Se trata de una especificación en continua evolución con posibilidad de adaptarse a nuevos requerimientos y demandas de usuario en el futuro.

49.1.4.1 DESCRIPCIÓN DEL SISTEMA

El estándar permite el uso de varios medios y técnicas para establecer conexiones. Incluso el estándar original permite usar infrarrojos y espectro ensanchado, tanto en salto de frecuencias como secuencia directa, con la ventaja de usar una capa de acceso al medio (MAC) común. Esto proporciona mucha flexibilidad a los desarrolladores e investigadores, que pueden olvidarse de ciertos aspectos ya que no existe dependencia directa entre ellos.

Los estándares de IEEE 802.11 son de libre distribución y cualquier persona puede ir a la página Web del IEEE y descargarlos. Estos estándares sólo definen especificaciones para las capas físicas y de acceso al medio y para nada tratan modos o tecnologías a usar para la implementación final. Esto debe permitir y facilitar la interoperabilidad entre fabricantes de dispositivos IEEE 802.11 y para asegurarse de eso se creó una alianza denominada WECA para crear y definir procedimientos para conseguir certificados de interoperabilidad y de cumplir las especificaciones, todo dentro de un estándar llamado WiFi (Wireless Fidelity). El nombre además es un indicativo del enfoque doméstico y muy enfocado hacia el usuario final.

El bloque constructivo básico de una red inalámbrica 802.11 es el denominado conjunto de servicio básico (BSS, Basic Service Set), que es un área geográfica en la que las estaciones sin hilos se pueden comunicar.

El tipo más sencillo de BSS consiste en dos o más equipos que entran dentro de las áreas de transmisión respectivas. Este proceso por el que los dispositivos entran en un BSS se denomina asociación.

49.1.4.1.1 CAPA FÍSICA (PHY)

La capa física en cualquier red define la modulación y características de señalización para la transmisión de datos en ese medio. Para poder transmitir en redes sin hilos en bandas sin licencia se necesita usar técnicas de espectro ensanchado, definidas en los requerimientos de casi todos los países.

En el estándar IEEE 802.11 se definen tres medios de nivel físico. Uno usa señales de infrarrojos y los otros dos utilizan señales de radio frecuencia (RF).

Los medios de RF 802.11 funcionan en la banda de 2.4Ghz, con un ancho de banda de 83Mhz entre 2.400 y 2.483 GHz, aunque en España tan solo tenemos 23Mhz, como Francia y Japón. Además, hay definiciones de potencia máxima de transmisión definidas por los distintos organismos de regulación. En EEUU se define una potencia máxima de 1W, para Europa 10mW cada 1 Mhz y para Japón 10mW.

Las definiciones para la transmisión por radiofrecuencia en los estándares son de espectro ensanchado por salto en frecuencias (FHSS) y espectro ensanchado por secuencia directa (DSSS). Ambos están definidos para trabajar en la banda de 2.4Ghz, y DSSS además tiene una variante en la banda de los 5Ghz, que consigue mayores velocidades de transmisión.

49.1.4.1.1.1 INFRARROJOS

Las comunicaciones por infrarrojos utilizan frecuencias entre 850 y 950 nanómetros, justo por debajo del espectro de la luz visible. La implementación IEEE 802.11 de infrarrojos, a diferencia de la mayoría de los medios infrarrojos, no requiere comunicación de visión directa, puede funcionar mediante señales reflejadas.

Sin embargo, debido su limitado alcance comparado con los medios de RF y a que solo puede funcionar adecuadamente en un ambiente interior cuando las superficies proporcionan una buena reflexión de las señales, es raro que se implemente en las redes sin hilos. Además imponen más restricciones en la ubicación física del dispositivo que FHSS o DSSS.

49.1.4.1.1.2 FHSS

FHSS (Frequency-Hopping Spread Spectrum) se refiere a un sistema que periódicamente cambia las frecuencias en las que transmite. Se utiliza la banda entera lo que contribuye a aumentar la seguridad frente a escuchas al tiempo que ayuda a suprimir el ruido o las interferencias.

FHSS tiene 22 patrones de saltos predefinidos usando 79 canales de 1Mhz a un mínimo de 2.5 saltos por segundo, y para resolver los problemas de

sincronización, para que tanto transmisor como receptor salten a la vez, se definen paquetes de sincronización.

La velocidad de los cambios de frecuencia es independiente de la velocidad de bit de transmisión de datos. Si la velocidad del salto de frecuencia es menor que la velocidad de bit de la señal, la tecnología se denomina sistema de salto lento, y si es mayor se denomina sistema de salto rápido.

Para la modulación FHSS usa FSK gaussiano de 2 o 4 niveles. Las velocidades típicas conseguidas son de 1 y 2 Mbps para FHSS.

49.1.4.1.1.3 DSSS

DSSS (Direct Sequence Spread Spectrum) trabaja en un canal fijo y preconfigurado, lo que le permite obtener mayores tasas de transferencia, pero con la desventaja de ser más sensible a interferencia y a señales procedentes de otros dispositivos que usen la misma frecuencia. Es posible tener tres puntos de acceso con tres canales diferentes, sin solapar en un mismo emplazamiento y sin tener en cuenta ningún tipo de planificación. Aún para más de tres puntos de acceso es necesaria cierta planificación, para poder mantener las velocidades, puesto que el solape de celdas y frecuencias tendrá un deterioro sobre el rendimiento.

Las modulaciones usadas para DSSS son BPSK y DQPSK para el estándar original. Para 11b, que permite conseguir 11Mbps, se utiliza CCK.

Además, se definió una variante de IEEE 802.11, que permite conseguir 54Mbps en la banda de 5Ghz, con un ancho de banda de hasta 300MHz y usando una modulación OFDM.

Esta misma modulación es la utilizada por 802.11g y 802.11n.

49.1.4.1.1.4 TRAMAS DE LA CAPA FÍSICA

En lugar de tener un esquema de señalización relativamente sencillo como en Ethernet y Token Ring que utilizan Manchester y Manchester diferencial respectivamente, los medios que funcionan en 802.11 tienen su propio formato de tramas, que encapsulan las tramas generadas en el nivel de enlace de datos.

La trama de FHSS contiene los siguientes campos:

- Preámbulo (10 bytes): contiene 80 bits de 1 y 0 alternos utilizados por el receptor para detectar la señal y sincronizar los tiempos.
- Delimitador de comienzo de trama (SFD) (2 bytes): indica el comienzo de la trama.
- Longitud (12 bits): indica el tamaño del campo de datos.
- Señalización (4 bits): contiene un bit para indicar si se está utilizando la velocidad de 1 o 2 Mbps. Los otros 3 bits se reservan para uso futuro. Solo el campo de datos se puede transmitir a 2 Mbps.
- CRC (2 bytes): contiene un valor de comprobación de redundancia cíclica.
- Datos (de 0 a 4.095 bytes): contiene la trama del nivel de enlace de datos que se transmite.

La trama DSSS contiene los siguientes campos:

- Preámbulo (16 bytes): contiene 128 bits que el sistema receptor utiliza para ajustarse a la señal entrante.
- Delimitador de comienzo de trama (SFD) (2 bytes): indica el comienzo de la trama.
- Señal (1 byte): especifica la velocidad de transmisión.
- Servicio (1 byte): contiene el valor hexadecimal 00 que indica que el sistema cumple con el estándar 802.11
- Longitud (2 bytes): indica el tamaño del campo de datos.
- CRC (2 bytes): contiene un valor de comprobación de redundancia cíclica.
- Datos (variable): contiene la trama del nivel de enlace de datos que se transmite.

La trama de infrarrojos contiene los siguientes campos:

- Delimitador de comienzo de trama (SFD) (2 ranuras): indica el comienzo de la trama.
- Velocidad de datos (3 ranuras): especifica la velocidad de transmisión.

- Ajuste del nivel de DC (DCLA) (32 ranuras): utilizado por el receptor para estabilizar el nivel DC después de transmitir los campos precedentes.
- Longitud (12 bits): indica el tamaño del campo de datos.
- CRC (2 bytes): contiene un valor de comprobación de redundancia cíclica.
- Sincronización (SYNC) (entre 57 y 73 ranuras): utilizadas por el sistema receptor para sincronizar el tiempo y opcionalmente para estimar la relación señal/ruido.
- Datos (de 0 a 2.500 bytes): contiene la trama del nivel de enlace de datos que se transmite.

49.1.4.1.2 CAPA DE ACCESO AL MEDIO (MAC)

La especificación de la capa MAC del IEEE 802.11 tiene muchas similitudes con el estándar de Ethernet cableado (IEEE 802.3). El protocolo del 802.11 es un esquema de protocolo conocido como detección de portadora, acceso múltiple, evitando colisiones (CSMA/QUE). Este protocolo evita las colisiones, en vez de detectarlas como el algoritmo de 802.3 (CSMA/CD). Es extremadamente difícil detectar colisiones en una red de transmisión de radiofrecuencias y de ahí que se trate de evitar las colisiones.

La capa MAC opera junto con la capa física muestreando la energía del medio de transmisión de datos. El protocolo CSMA/CA permite opciones para que se pueda minimizar las colisiones usando tramas de transmisión RTS/CTS (Request-to-send/Clear-to-send), datos y reconocimientos de una manera secuencial. En estas tramas se suelen incorporar datos de duración de los envíos con el objetivo de asegurar que esos envíos no van a ser interrumpidos: los demás nodos saben que deben estar callados durante ese intervalo de tiempo. Todo eso además se asegura y confirma con tramas de reconocimiento (ACK).

Pero un problema común a cualquier WLAN es el problema de los nodos ocultos. Esto puede llegar a reducir las prestaciones en un 40% en una WLAN con alta carga. Se produce cuando un nodo no puede escuchar

transmisiones de un nodo y trata de transmitir a un nodo que sí puede escucharlos, allí se pueden generar muchas colisiones.

Algunos avances se incluyeron para evitar el problema con el uso de RTS/CTS de una manera inteligente.

Además, se utilizan tiempos entre tramas para evitar colisiones, esto, a parte de evitar colisiones, permite además cierto uso de clases de calidad o por lo menos de preferencia de un tráfico sobre otro, utilizando funciones de coordinación puntual y de permitir el acceso al medio de tráfico prioritario antes que a los demás.

49.1.4.1.2.1 TRAMAS DEL NIVEL MAC

El estándar 802.11 define tres tipos básicos de tramas en este nivel:

- Tramas de datos: se usan para transmitir datos de los niveles superiores entre estaciones.
- Tramas de administración: se usan para el intercambio de información para realizar funciones de red como la autenticación y la asociación.
- Tramas de control: se usan para regular el acceso al medio y para reconocimiento de las tramas de datos transmitidas.

Una trama MAC genérica contiene los siguientes campos:

- Control de la trama (2 bytes): contiene 11 subcampos que habilitan las distintas funciones del protocolo:
 - Versión del protocolo (2 bits): especifica la versión del estándar que se está utilizando.
 - Tipo (2 bits): indica si la trama es de administración (00), control (01) o datos (10).
 - Subtipo (4 bits): identifica la función específica de la trama.
 - La DS (1 bit): un valor de 1 indica que la trama se transmite al sistema de distribución a través de un punto de acceso.
 - Desde DS (1 bit): un valor de 1 indica que la trama se recibió de un sistema de distribución.



- Más fragmentos (1 bit): un valor de 1 indica que el paquete contiene un fragmento de una trama y que hay más fragmentos para su transmisión.
- Reintento (1 bit): un valor de 1 indica que la trama se está retransmitiendo debido a una falta de recepción de un ack.
- Administración de energía (1 bit): un valor de 0 indica que la estación está funcionando en modo activo; un valor de 1 en modo ahorro de energía.
- Más datos (1 bit): si vale 1 indica que el AP tiene más paquetes almacenados para la estación y en espera de transmisión.
- WEP (1 bit): si vale 1 indica que el cuerpo de la trama se cifró utilizando WEP.
- Orden (1 bit): si vale 1 indica que la trama de datos se está transmitiendo utilizando la clase de servicio estrictamente ordenado.
- Duración/AID (2 bytes): en las tramas de control de sondeo de energía contiene la identidad de asociación (AID) de la estación transmisora. En el resto de las tramas contiene el tiempo (en microsegundos) necesario para transmitir una trama más el intervalo entre tramas.
- Dirección 1 (6 bytes): contiene una dirección que identifica al receptor de la trama, dependiendo de los valores de los subcampos A DS y Desde DS.
- Dirección 2 (6 bytes): contiene una dirección, dependiendo de los valores de los subcampos A DS y Desde DS.
- Dirección 3 (6 bytes): contiene una dirección, dependiendo de los valores de los subcampos A DS y Desde DS.
- Control de secuencia (2 bytes): contiene dos subcampos:
 - Número de fragmento (4 bits): contiene un valor que identifica un fragmento particular en una secuencia.

- Número de secuencia (12 bits): contiene un valor que identifica los fragmentos de la secuencia que componen el conjunto de datos.
- Dirección 4 (6 bytes): contiene una dirección, dependiendo de los valores de los subcampos A DS y Desde DS.
- Cuerpo de la trama (0 a 2.312 bytes): contiene la información que se está transmitiendo a la estación receptora.
- Secuencia de verificación de trama (4 bytes): contiene un valor CRC.

Los cinco tipos de dirección del subnivel MAC son:

- Dirección del emisor (TA): una dirección MAC individual que identifica al sistema que transmitió la información que va en el cuerpo de la trama en medio sin hilos actual (un AP).
- Dirección del receptor (RA): una dirección MAC individual o de grupo que identifica al receptor inmediato de la información en el cuerpo de la trama en medio inalámbrico actual (un AP).
- Dirección destino (DA): una dirección MAC individual o de grupo que identifica al receptor final de una unidad de datos de servicio.
- Dirección origen (SA): una dirección MAC individual que identifica al sistema que generó la información que va en el cuerpo de la trama.
- ID del conjunto de servicio básico (BSSID): en una red ad hoc el BSSID es un valor generado aleatoriamente durante la creación del BSS; en una red con infraestructura es la dirección MAC de la estación que funciona como AP del BSS.

49.2 RFID

RFID (Radio-frequency identification) es una tecnología que usa la comunicación mediante ondas de radio para transferir datos entre un lector y una etiqueta electrónica adherida a un objeto con el propósito de identificación o seguimiento.

Una etiqueta pasiva de RFID (una sin alimentación propia) se puede leer con un lector RFID si se aproxima suficientemente.

49.2.1 PRINCIPIOS DE RFID

Existen muchos tipos de RFID, pero en el mayor nivel de abstracción podemos dividirlos en dos clases: activo y pasivo.

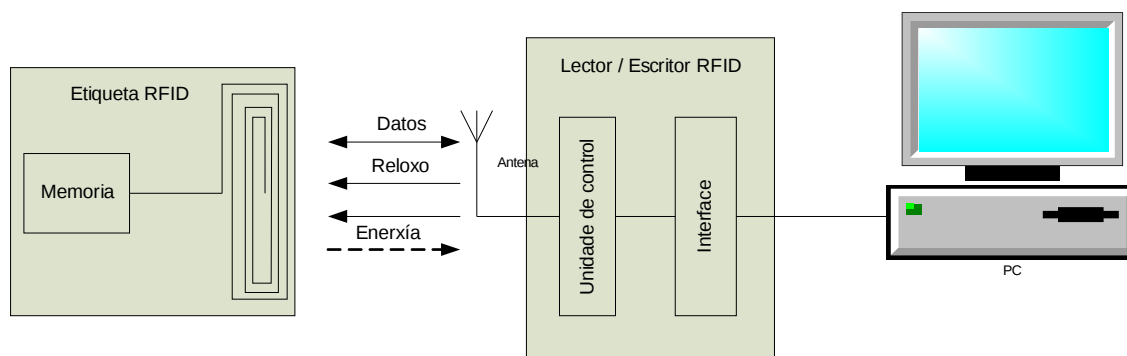
Las etiquetas activas requieren energía de una fuente, están o conectadas a la red eléctrica o a unas baterías. En el caso de usar baterías la vida de la etiqueta está limitada por la duración de estas contra el número de lecturas que sufrirá el dispositivo. Un ejemplo de etiqueta activa es el transpondedor de un avión que identifica a su nación de origen.

Sin embargo, las baterías hacen que el coste, tamaño y duración de las etiquetas activas sea poco práctica. Las etiquetas RFID pasivas son interesantes porque no necesitan mantenimiento, tienen un período de vida indeterminado y son suficientemente pequeñas como para caber en una etiqueta adhesiva.

Una etiqueta pasiva está compuesta por 3 elementos: una antena, un chip conectado a la antena y algún tipo de encapsulación. El lector de etiquetas es el responsable de aportar la energía y comunicarse con la etiqueta para leer a su ID (el chip de la etiqueta coordina este proceso). La encapsulación mantiene la integridad física de la etiqueta y protege la antena y el chip de las condiciones ambiente. Esta encapsulación puede ser un cristal o una lámina de plástico con adhesivo por una de las caras para permitir su adherencia a una superficie.

Existen dos aproximaciones fundamentales distintas para transmitir energía a la etiqueta desde el lector: inducción magnética y captura de onda electromagnética (EM). Estos dos diseños toman como ventaja las propiedades EM asociadas con una antena con una potencia típica desde 10 micro vatios hasta 1 mili vatio (podemos compararlo con el consumo de un procesador Intel XScale que es de 500 mili vatios o con el consumo de un procesador Intel Pentium 4 de 50 vatios).

49.2.2 COMPONENTES Y OPERACIÓN



TEXTO: RELOJ. ENERGÍA. INTERFAZ

Un sistema RFID tiene los siguientes componentes:

- Una etiqueta RFID que almacena cierta información (las más típicas son de 2KB pero las hay de muchos tamaños)
- Un lector RFID que emite en una determinada frecuencia y es capaz de detectar la respuesta de la etiqueta
- Un equipo capaz de interpretar la información de la etiqueta

La operación del sistema es muy sencilla:

- El lector RFID emite señales de radio a una determinada frecuencia con el objetivo de activar la etiqueta RFID y leer o escribir en ella
- Cuando una etiqueta RFID pasa por el rango de acción del lector RFID, este detecta la señal de la etiqueta
- El lector se comunica con la etiqueta (con el propósito concreto para el cual se crea ese sistema, identificación del producto, pago sin hilos, ...)

49.3 TECNOLOGÍAS MÓVILES

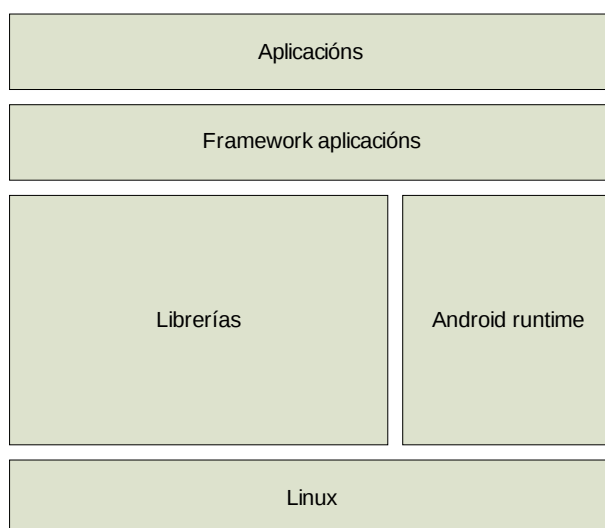
49.3.1 ANDROID

Android es una pila de software para dispositivos móviles que incluye el sistema operativo basado en Linux, un middleware y aplicaciones clavy siendo la plataforma para móviles más vendida.

Google compró la compañía que comenzó el desarrollo del producto en 2005 y junto con otros miembros de la Open Handset Alliance colaboró en

su desarrollo y publicación y en la actualidad AOSP (Android Open Source Project) lleva su mantenimiento y desarrollo futuro.

A grandes rasgos la estructura de Android puede verse en la figura siguiente.



- **Aplicaciones:** Android permite desarrollar aplicaciones e interfaces de usuario específicas para productos específicos
- **Framework aplicaciones:** Permite extender la funcionalidad por arriba de la de un dispositivo de mano dando soporte a las aplicaciones y permitiendo definir clases específicas para una industria o producto.
- **Librerías:** Optimizadas para un hardware determinado.
- **Android runtime:** Optimización de la VM Dalvik de Java para distintas CPU's y SoC.
- **Linux:** Sistema operativo base preparado para distintas CPU's y chipsets.

49.3.2 MEEGO

MeeGo es un sistema operativo basado en Linux y orientado a dispositivos móviles. Aunque está principalmente orientado a dispositivos móviles y appliances en el mercado de electrónica de consumo, MeeGo está diseñado para actuar como sistema operativo para otras plataformas hardware como netbooks, tablets, televisiones,... En la actualidad MeeGo está amparada por la Linux Foundation.

49.3.3 SYMBIAN

Symbian es otro sistema operativo y plataforma computacional para smartphones mantenido por Nokia. La plataforma Symbian es la sucesora de Symbian OS de la Nokia Series 60, a diferencia de Symbian OS, que requería una interfaz de usuario adicional, Symbian incluye componentes de interfaz de usuario basados en la 5ª edición de S60. La última versión de Symbian (Symbian ^3) se lanzó a finales de 2010 con el Nokia N8. Symbian solo está preparado para ejecutarse en procesadores ARM aunque existe una versión para procesadores x86 que no fue lanzada. Los dispositivos Symbian incluyen un 29,2% de los smartphones.

49.3.4 WINDOWS PHONE 7

Windows Phone 7 (anteriormente Windows Phone 7 Series) es un sistema operativo móvil desarrollado por Microsoft y es el sucesor de su Windows Mobile platform. A diferencia de su predecesor está orientado al mercado de consumo en vez de al mercado empresarial.

Con Windows Phone 7 Microsoft ofrece un nuevo interfaz de usuario con su nuevo lenguaje Metro, integra el sistema operativo con servicios de terceras partes y de la propia Microsoft, y controla el hardware en el que se ejecuta.

49.4 BIBLIOGRAFÍA

- Wireless Universal Serial Bus Specification 1.1 (2010)
- GAST, Matthew S. 802.11 Wireless Networks: The Definitive Guide. O'Reilly & Associates; 1st edition (2002)
- GEIER, James T. y Geier, Jim. Wireless LANs (2nd Edition). Sams; 2nd edition (2001)
- FLICKENGER, Rob. Building Wireless Community Networks. O'Reilly & Associates; 1st edition (2001)
- Roy Want. An Introduction to RFID Technology

Autor: Matías Villanueva Sampayo

Director de Informática Asociación Provincial de Pensionistas y Jubilados de
A Coruña
Colegiado del CPEIG



**50. PROTOCOLO TCP/IP:
DIRECCIONAMIENTO Y
SISTEMAS DE NOMBRES DE
DOMINIO. PROTOCOLOS IP,
ICMP, TCP, UDP.
ENCAMINAMIENTO.
APLICACIONES BÁSICAS:
TELNET, FTP (TFTP) Y SMTP.**

Tema 50. Protocolo TCP/IP: Enderezamiento y sistemas de nombres de dominio. Protocolos IP, ICMP, TCP, UDP. Encaminamiento. Aplicaciones básicas: Telnet, FTP (TFTP) y SMTP.

50.1 Protocolo TCP/IP

50.1.1 Enderezamiento y sistemas de nombres de dominio

50.1.1.1 Enderezamiento IP

50.1.1.1.1 Subredes

50.1.1.1.2 Máscaras de red

50.1.1.1.3 Direcciones IPV6

50.1.1.2 DNS

50.1.1.2.1 Estructura del DNS

50.1.1.2.2 Sintaxis de nombres de dominio

50.1.1.2.3 Servidores de nombres

50.1.1.2.4 Resolución de nombres

50.1.1.2.4.1 Dependencias circulares

50.1.1.2.4.2 TTL

50.1.1.2.4.3 Búsqueda inversa

50.1.1.2.5 Estructura de los registros DNS

50.1.2 Protocolos IP, ICMP, TCP, UDP

50.1.2.1 Capas del modelo TCP/IP

50.1.2.2 Protocolo IP

50.1.2.2.1 Datagrama IP

50.1.2.3 ICMP protocolo de control de mensajes de Internet

50.1.2.4 ARP. Protocolo de resolución de direcciones

50.1.2.5 RARP. Protocolo de resolución de direcciones inverso

50.1.2.6 Protocolo TCP

50.1.2.6.1 Segmento TCP

50.1.2.6.2 Conexiones TCP

50.1.2.6.3 Detección de errores

50.1.2.6.4 Control de flujo

50.1.2.6.5 Control de congestión

50.1.2.7 Protocolo UDP

50.1.2.7.1 Datagrama UDP

50.1.3 Encaminamiento

50.1.3.1 CIDR

50.1.3.2 OSPF

50.1.3.3 BGP

50.1.4 Aplicaciones básicas: Telnet, FTP (TFTP) y SMTP

50.1.4.1 TELNET

50.1.4.2 FTP

50.1.4.2.1 TFTP

50.1.4.3 SMTP

50.2 Bibliografía

50.1 PROTOCOLO TCP/IP

El alumbramiento del modelo TCP/IP se remonta a la red ARPANET. Esta era una red de investigación controlada por el Departamento de Defensa de EE.UU. Poco a poco fueron conectándose instituciones, mediante el uso de líneas de la red telefónica. La necesidad de buscar una arquitectura de referencia nueva surgió cuando empezaron a añadirse redes de satélite y radio con los consiguientes problemas de interactuar con los protocolos existentes. Uno de los principales objetivos de esta nueva arquitectura fue la capacidad de conexión de múltiples redes entre sí desembocando en lo que hoy conocemos cómo modelo TCP/IP.

TCP/IP tiene una mayor aplicación que el modelo OSI, ya que se desarrolló antes y se implantó TCP/IP mientras se esperaba al protocolo OSI. Además, como todas las especificaciones asociadas a los protocolos TCP/IP son de dominio público, y por lo tanto no hay que pagar nada para usarlos, fueron utilizados extensivamente por entidades comerciales y públicas para crear entornos de redes abiertos.

Las ventajas de TCP/IP son:

- Agrupa redes, creando una red mayor llamada Internet.

- Es independiente del hardware de los nodos, del sistema operativo y de la tecnología del medio y del enlace.
- Ofrece capacidad de encaminamiento adaptativo, transparente al usuario.
- Es el software de red más disponible universalmente.

Las diferencias con el modelo OSI son:

- Mientras que en OSI la distinción entre los conceptos de servicio, interfaz y protocolo es clara, en TCP/IP no existía esta distinción inicialmente. Posteriormente, se intentó ajustar esto para acercarse más a OSI.
- OSI se desarrolló antes de que se hubiesen definido los protocolos, mientras que TCP/IP fue, en realidad, el resultado de los protocolos existentes.
- Una diferencia clara es que OSI cuenta con siete capas bien definidas y TCP/IP sólo tiene 4.
- El modelo OSI considera los dos tipos de comunicación, orientada y no orientada a conexión, en la capa de red. Sin embargo, en la capa de transporte, ofrece sólo orientada a conexión. Por otro lado, el modelo TCP/IP en la capa de red sólo soporta comunicaciones no orientadas a conexión pero considera ambos modos en la capa de transporte.

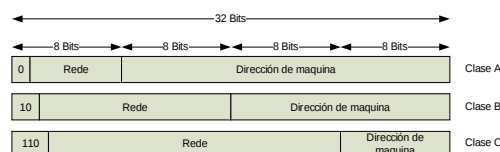
50.1.1 ENDEREZAMIENTO Y SISTEMAS DE NOMBRES DE DOMINIO

50.1.1.1 ENDEREZAMIENTO IP

Cada nodo de la red tiene una dirección IP única, formada por el número de la red y el número del nodo. La asignación de direcciones IP está regulada por la ICANN (Internet Corporation for Assigned Names and Numbers) para evitar que una misma dirección sea usada por varias máquinas.

Una dirección IP en su versión 4 consta de 32 bits de longitud y generalmente se escribe como concatenación de 4 bytes en formato decimal separados por puntos.

Tradicionalmente las direcciones se agrupan en clases que podemos ver en la siguiente imagen.



Además, históricamente existen las clases D (para multicast) y E (originalmente reservada para uso futuro).

Hay determinadas direcciones reservadas, estas son:

- 0.0.0.0 Esta IP es utilizada por las estaciones cuando aún no tienen una IP asignada.
- La dirección de la red se representa por una dirección IP donde la primera parte es la parte de red y el resto de bits están a 0.
- 127.X.X.X Red se loopback (acceso a la propia máquina desde la propia máquina) siendo la dirección predilecta para este fin 127.0.0.1 aunque todas funcionan de la misma forma.
- 255.255.255.255 Es la dirección de broadcast (normalmente no retransmitido por los encaminadores). De forma equivalente a dirección de broadcast para la red y de la dirección de la red con el resto de bits a 1.

Cuando el número de red va todo a ceros se asume que esa dirección se refiere a la red actual.

No todas las direcciones son únicas en la red (estas direcciones son conocidas como IPs públicas) si no que existe en una serie de rangos reservados para su uso en registro:

- Para la clase A: de 10.0.0.0 a 10.255.255.255 (8 bits red, 24 bits estación).
- Para la clase B: 172.16.0.0 a 172.31.255.255 (16 bits red, 16 bits estación). 16 redes clase B contiguas, uso en universidades y grandes compañías.
- Para la clase C: 192.168.0.0 a 192.168.255.255 (24 bits red, 8 bits estación). 256 redes clase C contiguas, uso de compañías medias y pequeñas.

50.1.1.1.1 SUBREDES

Todos los ordenadores de una red deben tener el mismo número de red. Esta característica puede llegar a ser un problema a medida que crecen las redes. La solución a este problema es la división de una red en varias partes o subredes. Desde el punto de vista del mundo exterior las subredes no son visibles, si no que se ve la red como un todo.

La parte de la dirección que define el número de red permanece igual una vez dividida, pero el número de estación se divide en número de subred y número de estación.

50.1.1.1.2 MÁSCARAS DE RED

La herramienta que permite obtener la dirección de red de una dirección IP dada es la máscara de red. Es una especie de dirección IP especial que, en binario, tiene todos los bits que definen la red puestos a 1 y los bits correspondientes al host puestos a 0. Así, las máscaras de red de los diferentes tipos de redes principales son:

- Red de clase A: Máscara de red = 255.0.0.0
- Red de clase B: Máscara de red = 255.255.0.0
- Red de clase C: Máscara de red = 255.255.255.0

La máscara de red posee la propiedad de que cuando se combina, mediante una operación AND lógica, con la dirección IP de un host se obtiene la dirección propia de la red en la que se encuentra el mismo. En las redes donde existen definidas subredes se aplica el concepto de máscara de subred, que es el resultado de poner a 1 todos los bits que representan red o subred y a 0 todos los bits que representan una estación.

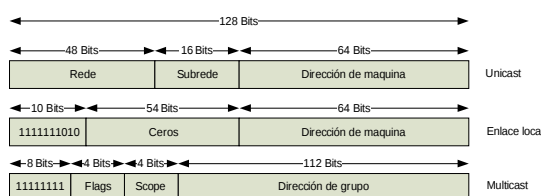
50.1.1.1.3 DIRECCIONES IPV6

A diferencia de IPv4, que utiliza una dirección IP de 32 bits, las direcciones IPv6 están compuestas de 128 bits, ampliando enormemente la capacidad de direcciones del protocolo IP.

De similar forma que las direcciones IPv4 las direcciones IPv6 se agrupan en 8 números de 4 dígitos hexadecimales separados entre sí por dos puntos (:). Cuando uno de estos números es todo ceros, se puede omitir en la escritura de la dirección.

Existen 3 tipos de direcciones:

- Unicast, que identifica un único interfaz de red. El protocolo IP entrega los paquetes enviados a una dirección unicast a la interfaz específica.
- Anycast, que es asignada a un grupo de interfaces, normalmente de nodos diferentes. Un paquete enviado a una dirección anycast se entrega sólo a uno de los miembros, normalmente el host con menos coste, según la definición de métrica del protocolo de encaminamiento. Las direcciones anycast no se identifican fácilmente pues tienen el mismo formato que las unicast, diferenciándose sólo por estar presente en varios puntos de la red. Casi cualquier dirección unicast puede utilizarse como dirección anycast.
- Multicast, que también es utilizada por múltiples hosts, que consiguen la dirección multicast participando del protocolo de multidifusión (multicast) entre los routers de red. Un paquete enviado a una dirección multicast es entregado a todos los interfaces que se unieron al grupo multicast correspondiente.



50.1.1.2 DNS

El sistema de nombres de dominio (DNS, por sus siglas en inglés: Domain Name System) es un sistema de nombres jerárquico y distribuido para equipos, servicios o cualquier tipo de recurso conectado a Internet. Su función más importante es traducir los nombres comprensibles por los usuarios a direcciones IP numéricas con el propósito de localizarlos en la red.

50.1.1.2.1 ESTRUCTURA DEL DNS

El espacio de nombres está organizado en árbol con cada nodo u hoja en el árbol conteniendo cero o más registros de recursos (siendo estos los que almacenan la información correspondiente al nombre de dominio).

Una zona DNS consiste en uno o varios dominios y subdominios dependiendo de la autoridad delegada en ese gestor. Esta autoridad puede dividirse creando más zonas (que normalmente se ocuparán de subdominios) cuya autoridad será asumida por otra entidad, perdiendo la original la autoridad sobre estas nuevas zonas.

50.1.1.2.2 SINTAXIS DE NOMBRES DE DOMINIO

La descripción de las reglas de nombrado para los dominios aparece en los RFC 1035, RFC 1123, y RFC 2181. Un nombre de dominio consiste en una o varias partes, llamadas etiquetas, que son concatenadas de forma jerárquica y separadas entre sí por puntos.

Las reglas para construir el nombre son:

- La etiqueta situada al final derecho del nombre se llama TLD (Top-Level Domain) y tiene que pertenecer a uno de los TLD definidos.
- La jerarquía desciende de derecha a izquierda, de forma que con cada etiqueta se especifica una división en el árbol. Existe un límite de 127 niveles en el árbol jerárquico.
- Cada etiqueta puede tener hasta 63 caracteres y el nombre completo del dominio no puede sobrepasar los 255 octetos (incluyendo un punto como representación del máximo nivel, lo que hace que el nombre de dominio más grande pueda contener 253 caracteres).
- Los nombres de dominio almacenados en DNS pueden estar compuestos de cualquier carácter almacenable en un octeto. Aunque los nombres que se permiten en la zona raíz y en la mayoría de las subzonas limitan esto, permitiendo sólo un subconjunto de los caracteres ASCII que incluye de la a a la z, de la A a la Z, del 0 al 9 y el guión. Los nombres de dominio no distinguen entre mayúsculas y minúsculas y las etiquetas no pueden comenzar ni acabar en un guión.
- Un nombre de equipo es aquel nombre de dominio que tiene asociada por lo menos una IP, independientemente de su nivel.

50.1.1.2.3 SERVIDORES DE NOMBRES

El Sistema de Nombres de Dominio está soportado por una base de datos distribuida y jerárquica accesible usando el paradigma cliente-servidor. Los nodos de esta base distribuida se llaman servidores de nombres.

Cada dominio tiene sus datos almacenados en un servidor de nombres autoritativo que contiene los datos de ese dominio y los servidores de dominio subordinados a él. En la cúspide de la jerarquía están los servidores de nombres raíz (que contienen la información de los TLD).

Existen dos tipos de servidores de nombres:

- **Servidor de nombres autoritativo:** este tipo de servidor responde con los datos configurados por una fuente original (como puede ser el administrador del dominio o algún método dinámico, pero no por consultas a otro servidor de nombres). Dependiendo de la fuente que se use para actualizarse, existen dos tipos de servidores:
 - **Maestros:** Recogen la configuración directamente del administrador del dominio.
 - **Esclavos:** Mantienen una copia de la base de datos de su servidor maestro que obtienen usando un mecanismo automático del protocolo DNS.

Toda zona DNS debe tener por lo menos un servidor de nombres autoritativo que debe estar almacenado en un registro DNS en la zona padre. Normalmente se usan dos servidores (referidos como Primario y Secundario) para cada zona solamente distinguidos por la prioridad almacenada en sus registros (la especificación técnica DNS en sí no tiene ninguna referencia a estos términos) y que suelen corresponder a un maestro (el Primario) y a un esclavo (el Secundario). Cuando un servidor autoritativo responde a una petición de uno de sus dominios marca la respuesta con el bit AA (Authoritative Answer) para indicarlo.

- **Servidores recursivos y de caché:** Aunque teóricamente los servidores autoritativos deberían ser suficientes, si sólo existieran estos una petición debería viajar de forma recursiva desde la zona raíz. La forma

para corregir esto y reducir el tráfico DNS y mejorar el rendimiento fue la creación de servidores de nombres que almacenan una caché con los resultados previos y que tienen la capacidad de recurrir recursivamente a los servidores autoritativos para resolver peticiones.

50.1.1.2.4 RESOLUCIÓN DE NOMBRES

Como ya se comentó anteriormente, el proceso para resolver un nombre implica realizar una serie de peticiones comenzando con la etiqueta a la derecha. Más en detalle este proceso implica:

1. Un equipo debe tener configurada una caché inicial (llamada hint) con las direcciones de los servidores raíz. Esta caché debe ser actualizada a mano por el administrador de los equipos.
2. Una petición a uno de los servidores raíz para obtener la dirección del servidor de nombres del TLD.
3. Una petición al servidor de nombres del TLD para obtener la dirección del servidor de nombres autoritativo del dominio en el siguiente nivel.
4. El paso anterior se repetirá para cada etiqueta en el nombre hasta que en el último paso obtenemos la dirección IP.

50.1.1.2.4.1 DEPENDENCIAS CIRCULARES

Los servidores de nombres a los que se delega una zona se identifican por nombre, no por IP (en el registro NS), provocando que haya que resolver otro nombre. Esto puede llevar a que se produzca una dependencia circular (por ejemplo: tratar de resolver un dominio para lo cual se tiene que resolver el nombre de su servidor de nombres, que está dentro de ese dominio). Para resolver esto, los servidores de nombres almacenan registros denominados “glue” (pegamento) que a su vez almacenan una o varias IP's de esos servidores de nombres autoritativos, el servidor que delega proporciona este “pegamento” como registros en la sección adicional de la respuesta DNS pero con el nombre del servidor de nombres al que se delega en el campo correspondiente de la respuesta.

50.1.1.2.4.2 TTL

Para evitar peticiones continuas del mismo nombre, se diseñó un mecanismo para guardar una caché de los registros DNS durante un tiempo

limitado, este tiempo se denomina TTL (Time To Live) y está asociado a todos los registros DNS pudiendo ir desde no permitir el caché hasta 68 años.

Una consecuencia de esta característica es que un cambio en un registro DNS no se propaga de forma automática a toda la red, si no que tarda el tiempo expresado en el TTL en actualizarse.

La correcta forma de seleccionar el TTL para un determinado registro está definida en el RFC 1912.

Existe también la posibilidad de hacer cache negativa (guardar la no existencia de un determinado registro), el TTL de esta caché negativa está determinado por el servidor de nombres autoritativo para esa zona, que incluye en la respuesta negativa el registro SOA (Start Of Authority) en el que se especifica el mínimo tiempo de TTL que combinado con el TTL del propio registro SOA define el TTL de la caché negativa.

50.1.1.2.4.3 BÚSQUEDA INVERSA

Existe la posibilidad de buscar el nombre asociado a una determinada dirección IP. Hay que tener en cuenta que puede haber varios nombres asociados a una dirección IP. Los servidores DNS mantienen la información de las direcciones IP en registros PTR (Pointer) dentro del TLD arpa (in-addr.arpa para IPv4 e ipv6.arpa para IPv6) invirtiendo el orden de los números de la IP (193.144.100.12 esta estará almacenada como 12.100.144.193.in-addr.arpa).

50.1.1.2.5 ESTRUCTURA DE LOS REGISTROS DNS

La base de datos de los registros DNS sigue una estructura de lista de registros, donde cada registro contiene:

- Nombre: el nombre completo del dominio en el árbol. Tiene un tamaño variable.
- Tipo: indicando el tipo de registro que define el formato y el posible uso de los datos del registro. Tiene una longitud de 2 octetos. Los tipos más importantes son:
 - o A: Registro de dirección (IP), asocia un nombre a una dirección IP.

- o MX: Registro de correo electrónico asocia un nombre de dominio a un nombre del servidor de correo electrónico para ese dominio.
- o CNAME: Registro de alias. Asocia un nombre a otro (cadena que debería acabar en un registro de tipo A).
- o NS: Registro de delegación de una zona a un nombre de servidor.
- Clase: Indica la clase del registro. Tiene una longitud de 2 octetos y suele tener el valor de IN (para los registros de Internet) pero también puede tener los valores CN (Chaos) y HS (Hesiod). Cada clase es independiente en lo que a espacio de nombres se refiere.
- TTL: Time To Live. Tiene una longitud de 4 octetos.
- Datos: Contiene los datos relevantes para ese registro, dependiendo del tipo de registro estos datos son distinto si tienen distinto formato. Tiene una longitud variable.

50.1.2 PROTOCOLOS IP, ICMP, TCP, UDP

50.1.2.1 CAPAS DEL MODELO TCP/IP

La arquitectura del modelo TCP/IP consta de 4 capas:

- Aplicación. Proporciona comunicación entre procesos o aplicaciones en ordenadores distintos. Contiene todos los protocolos de alto nivel.
- Transporte. Al igual que la capa de transporte de OSI, permite que se pueda establecer una comunicación entre las entidades pares de los nodos origen y destino. Proporciona, por tanto, transferencia de datos extremo a extremo, asegurando que los datos llegan en el mismo orden en que fueron enviados y sin errores. Esta capa también puede incluir mecanismos de seguridad. Se puede resumir la funcionalidad de la capa de transporte como calidad de servicio. En este nivel se definen dos protocolos importantes, que se explican en detalle más adelante:
 - o TCP: Protocolo orientado a conexión que proporciona entrega fiable de mensajes entre máquinas. Realiza control de flujo para que un emisor rápido no pueda saturar a un receptor lento.
 - o UDP: Protocolo sin conexión y no fiable. Se utiliza en aplicaciones donde la entrega rápida es más importante que la entrega precisa,

como transmisión de voz y video, y en aplicaciones de consulta de petición y respuesta.

- Red. Esta capa es el eje de la arquitectura y permite que los nodos inyecten paquetes en cualquier red y los hagan viajar de forma independiente de su destino, sin importar si está en la misma red, o si hay otras redes entre ellas. Su misión principal, por tanto, es el encaminamiento de los paquetes, pero sin garantía de que lleguen al extremo final ni de que lo hagan en el mismo orden en el que se enviaron. Si se desea una entrega ordenada, las capas superiores deben reordenar los paquetes. En este nivel se define un formato de paquete y el protocolo IP, que se detalla seguidamente.
- Capa del nodo a la red. El modelo TCP/IP no dice mucho de lo que sucede bajo la capa de red, existe un gran vacío. Esta abstracción de la topología de red pone en relieve la capacidad de la capa de red de soportar cualquier tipo de red por debajo. Lo que está claro es que debe permitir que un nodo se conecte a la red para que pueda enviar por ella paquetes IP. El protocolo que regula esta conexión puede variar de un nodo a otro.

50.1.2.2 PROTOCOLO IP

IP proporciona un servicio de distribución de paquetes caracterizado por:

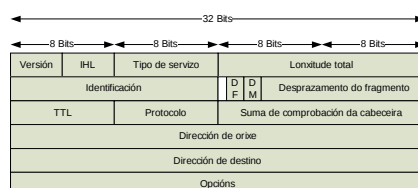
- Transmisión de datos en datagramas (paquetes IP).
- No está orientado a conexión, por lo que los paquetes son tratados de forma independiente y cada uno puede seguir una trayectoria diferente en su viaje hacia el host destino.
- No es fiable, por lo que no garantiza la entrega de los paquetes, ni la entrega en secuencia, ni la entrega única. Esto es responsabilidad del protocolo TCP de la capa superior.
- No implementa control de errores ni control de congestión.
- Puede fragmentar los paquetes si es necesario.
- Direcciona los paquetes empleando direcciones lógicas IP de 32 bits (en IPv4).

- Verifica la integridad del paquete en sí, no de los datos que contiene.

50.1.2.2.1 DATAGRAMA IP

Los datos proporcionados por la capa de transporte son divididos en datagramas y transmitidos a través de la capa de red. A lo largo del camino pueden ser fragmentados en unidades más pequeñas para atravesar una red o subred cuya MTU (Unidad de Transferencia Máxima) sea más pequeña que el paquete. En la máquina destino, estas unidades son reensambladas para volver a tener el datagrama original que es entregado a la capa de transporte.

Un datagrama IP está formado por un cuerpo y una cabecera. El cuerpo se corresponde con el segmento TCP/UDP de la capa de transporte. La cabecera tiene una parte fija de 20 bytes y una parte opcional de longitud variable. En la siguiente figura puede verse la estructura de dicha cabecera.



TEXTO: Tipo de Servicio. Longitud total. Desplazamiento de fragmento. Suma de comprobación de la cabecera. Dirección de origen. Opciones

- Versión (4 bits). Indica la versión del protocolo al que pertenece el datagrama. El propósito de este campo es permitir la evolución del protocolo y que durante la transición entre las versiones se pueda ejecutar en unas máquinas la versión vieja y en otras la versión nueva. Actualmente hay dos versiones: la 4 (Ipv4) y la 6 (Ipv6).
- IHL (Internet Header Length) (4 bits). Indica la longitud de la cabecera en palabras de 32 bits, ya que esta no tiene una longitud constante. Si no hay opciones, este valor es mínimo e igual a 5. El valor máximo es 15 (4 bits a "1", "1111"=15 en decimal). Como cada palabra equivale a 4 bytes, al tamaño máximo de la cabecera es de 60 bytes y, por tanto, de 40 bytes el campo de opciones.

- Tipo de servicio (8 bits). La subred ofrece distintos grados de confiabilidad y seguridad. Con este campo el host puede indicarle a la subred el tipo de servicio que quiere, combinando fiabilidad y seguridad. Este campo contiene, su vez, de izquierda la derecha:
 - o Campo de precedencia (3 bits): Indica la prioridad, de 0 (normal) a 7 (paquete de control de red).
 - o Tres bits indicadores: D (Delay=retardo), T (Throughput=rendimiento) y R (Reliability=fiabilidad), que permiten especificar qué interesa más.
 - o Dos bits no usados.
- Longitud total (16 bits). Longitud total en octetos del datagrama, incluyendo cabecera y datos. La longitud teórica máxima es 65535 bytes (64 Kbytes) pero en la práctica los datagramas son de unos 1500 bytes. Este tamaño máximo será insuficiente en las redes futuras de alta velocidad. Internet no limita los datagramas a un tamaño específico pero sugiere que redes y encaminadores estén preparados para manejar datagramas a partir de 576 octetos.
- Identificación (16 bits). Cuando se transmite un datagrama a través de Internet puede ser necesario fragmentarlo en unidades más pequeñas a lo largo del camino. Este campo permite al host destino determinar a qué datagrama pertenece un fragmento recién llegado, ya que todos los fragmentos de un mismo datagrama contienen el mismo valor de identificación.
- 1 bit sin uso actualmente.
- Bit DF (Don't Fragment). Puesto a "1", indica a los encaminadores que no pueden fragmentar el datagrama porque el destino no va a poder unir las piezas de nuevo. Si es demasiado grande y no se puede enviar, se descarta y se envía al origen un mensaje de error.
- Bit MF (More Fragment). Este bit está a "1" en todos los fragmentos de un datagrama excepto en el último. De esta forma, se sabe cuándo llegaron todos los fragmentos.

- Desplazamiento del fragmento (13 bits). Indica en qué posición del datagrama original, medido en unidades de 8 octetos (64 bits), se encuentra el fragmento actual. Todos los fragmentos, menos el último del datagrama, deben tener una longitud múltiplo de 8 bytes. Puede haber 8192 fragmentos como máximo por datagrama.
- TTL el tiempo de vida (8 bits). Contador que sirve para limitar la vida de un paquete. Teóricamente, cuenta el tiempo en segundos, permitiendo una vida máxima de 255 segundos (“11111111”=255 en decimal). Debe disminuirse en cada salto. En la práctica, simplemente cuenta saltos. Cuando el contador llega a 0 el paquete se descarta y se envía al host origen un paquete de aviso. Este campo evita que los paquetes estén dando vueltas siempre por la red.
- Protocolo (8 bits). Indica la entidad de la capa de transporte a la que debe entregarse el datagrama una vez que la capa de red del host destino lo ensambla por completo.
- Suma de comprobación de la cabecera (16 bits). Verifica sólo la cabecera y es útil para la detección de errores generados por palabras de memoria en mal estado en un encaminador.
- Dirección de origen y dirección de destino (32 bits, cada una). Indican la dirección IP origen y la dirección IP destino.
- Opciones (de 0 a 40 bytes). Las opciones son de longitud variable. Empiezan con un código de 1 byte, que identifica la opción. A continuación, sólo para algunas opciones, 1 byte que indica la longitud de la opción. Finalmente, uno o más bytes de datos. El campo de opciones se llena para obtener palabras completas o, lo que es lo mismo, múltiplos de 4 bytes. Las opciones las eligen las aplicaciones de origen, aún es bastante raro usarlas. Actualmente hay 5 opciones definidas:
 - o Seguridad: Permite añadir una etiqueta para indicar lo secreta que es la información que contiene el datagrama. En la práctica, los encaminadores ignoran esta opción.

- o Encaminamiento estricto desde el origen: Indica la trayectoria completa a seguir como secuencia de direcciones IP. Esta opción es usada por los administradores para hacer mediciones de tiempo.
- o Encaminamiento libre desde el origen: Indica una lista de encaminadores por los que tiene que pasar el paquete, en el orden especificado, pero puede pasar a través de otros encaminadores en el camino. Es de utilidad cuando las consideraciones políticas o económicas dictan pasar o evitar ciertos países.
- o Registrar ruta: Indica a los encaminadores por los que pasa el datagrama que agreguen su dirección IP de 32 bits en el campo de opciones para conocer la ruta que siguió el datagrama.
- o Marca de tiempo: Como la opción anterior, pero además el encaminador también tiene que registrar una marca de tiempo de 32 bits, expresada en milisegundos, de acuerdo con cada reloj local. Ambas opciones se utilizan principalmente para la búsqueda de fallos en los algoritmos de encaminamiento.

50.1.2.3 ICMP PROTOCOLO DE CONTROL DE MENSAJES DE INTERNET

Cuando ocurre algún suceso, ICMP (Internet Control Message Protocol) es el protocolo encargado de informar del mismo. No toma ninguna decisión al respecto, esto es tarea de las capas superiores. Los mensajes de ICMP se encapsulan dentro del campo de datos de los paquetes IP.

El mensaje ICMP tiene tres campos fijos y a continuación, el cuerpo del mensaje que varía en función del tipo. Los campos obligatorios son:

- Tipo (8 bits). Se utiliza para distinguir los tipos de mensajes ICMP, descritos más abajo, y determinar su formato.
- Código (8 bits). En algunos mensajes ICMP se utiliza este campo para distinguir distintos subtipos dentro de un tipo de mensaje, es decir, para ofrecer una descripción concreta del error que se produjo.
- Checksum (16 bits). Código de protección contra errores de transmisión.

Existen diversos tipos de mensajes ICMP. Por un lado, están los mensajes informativos. Todos ellos contienen, además de los 3 campos fijos, un identificador de 16 bits y un número de secuencia, también de 16 bits. Los mensajes informativos más importantes son los siguientes:

- Solicitud de eco (Tipo 8). Permite detectar si un destino concreto es alcanzable y está vivo. Cuando se envía un mensaje de este tipo se espera que el destino devuelva un mensaje de respuesta de eco. Lleva un campo de Datos opcional con un número de bytes variables que fija el host peticionario.
- Respuesta de eco (Tipo 0). Mensaje que se devuelve cuando se recibe un mensaje de Solicitud de eco conteniendo los datos enviados por el peticionario.
- Solicitud de marca de tiempo (Tipo 13). Misma funcionalidad que el mensaje Solicitud de eco pero indica al receptor que debe añadir información adicional de tiempos en el mensaje de respuesta.
- Respuesta de marca de tiempo (Tipo 14). Parecido al mensaje de Respuesta de eco pero además almacena el tiempo de llegada del mensaje de Solicitud de marca de tiempo y el tiempo de partida del mensaje de respuesta.
- Solicitud de máscara de dirección (Tipo 17). Lo utiliza un host cuando se reinicia en una red y no conoce cuántos bits se asignaron a la máscara de subred.
- Respuesta de máscara de dirección (Tipo 18).

El resto son mensajes de error. Todos ellos contienen, además de los 3 campos fijos, el encabezado y los 8 primeros bytes del datagrama que ocasionó el error. Los mensajes de error más importantes son los siguientes:

- Destino inalcanzable (Tipo 3). Este tipo de mensaje se utiliza ante varias situaciones. El campo de código describe el error concreto que se produjo.
 - o Código=0: no se puede encontrar la red destino del mensaje.

- o Código=1: host o aplicación destino inalcanzable.
- o Código=2: campo de protocolo del datagrama no coincide con ninguno de los protocolos del host destino.
- o Código=3: no se puede llegar al puerto destino o la aplicación destino no está libre.
- o Código=4: cuando una red no puede transportar un paquete IP demasiado grande para ella pero lleva el bit DF activado, indicando que no se permite fragmentación.
- o Código=5: ruta de origen no es correcta.
- o Código=6: no se conoce la red destino.
- o Código=7: no se conoce el host destino.
- o Código=8: el host origen está aislado.
- o Código=9: la comunicación con la red destino está prohibida por razones administrativas.
- o Código=10: la comunicación con el host destino está prohibida por razones administrativas.
- o Código=11: no se puede llegar a la red destino debido al Tipo de servicio.
- o Código=12: no se puede llegar al host destino debido al Tipo de servicio.
- Tiempo sobrepasado (Tipo 11). Cuando existe una alta congestión en la red o los paquetes están vagando por la red en bucle, llega un momento en que el contador de tiempo de vida del paquete llega a 0.
 - o Código = 0: tiempo sobrepasado (TTL alcanzó 0)
 - o Código = 1: finaliza el tiempo sin que se hubiesen recibido todos los fragmentos de un datagrama
- Problema de parámetro (Tipo 12). Indica que algún campo de la cabecera tiene un valor ilegal, que el tamaño del datagrama es incorrecto o que falta algún campo obligatorio, debido a un fallo del software de IP en el host emisor o en alguno de los encaminadores por los que pasó el mensaje. Este mensaje incluye un campo

Indicador de 8 bits que apunta al campo del encabezado IP que generó el problema.

- Supresión de origen (Tipo 4). Cuando un host envía muchos paquetes se le envía un mensaje de este tipo con la intención de que reduzca. En la actualidad apenas se usa, ya que incrementa la posibilidad de congestión en la red.
- Redireccionamiento (Tipo 5). Cuando un encaminador detecta que un paquete puede estar mal encaminado envía un mensaje de este tipo al host emisor del paquete para avisarlo del posible error y para que modifique sus tablas de encaminamento, si procede.

50.1.2.4 ARP. PROTOCOLO DE RESOLUCIÓN DE DIRECCIONES

El hardware de la capa de enlace de datos no entiende las direcciones IP, es necesario que sean traducidas a direcciones físicas. Una posible solución es tener un archivo de configuración en algún lugar del sistema que proyecte las direcciones IP en direcciones físicas. Sin embargo, en organizaciones con miles de hosts, el mantenimiento y gestión de estos archivos supondría mucho tiempo y sería muy susceptible a errores. Una solución más sencilla la ofrece el protocolo de resolución de direcciones, ARP (Address Resolution Protocol). Cuando un host quiere enviar un paquete a otro del cual solo conoce la dirección IP, envía un paquete ARP a la red con la dirección IP que se quiere resolver. La difusión llegará a cada host de la red, que revisará su propia dirección IP, y sólo aquel que coincida responderá con su dirección física. El host de origen añade esta nueva entrada a su tabla ARP.

50.1.2.5 RARP. PROTOCOLO DE RESOLUCIÓN DE DIRECCIONES INVERSO

A veces se produce el caso inverso al anterior. Es decir, se necesita conocer la dirección IP dada una dirección física. Esto ocurre, por ejemplo, cuando se inicia una máquina sin disco que normalmente recibe la imagen binaria de su sistema operativo de un servidor de archivos remoto, pero desconoce su dirección de IP.

El protocolo de resolución de direcciones inverso RARP (Reverse Address Resolution Protocol) permite que un host recién iniciado difunda su dirección física para preguntar si alguien en la red conoce la dirección IP asociada a ella. Cuando el servidor RARP recibe esta solicitud busca la dirección física en sus archivos de configuración y le envía la dirección de IP correspondiente.

50.1.2.6 PROTOCOLO TCP

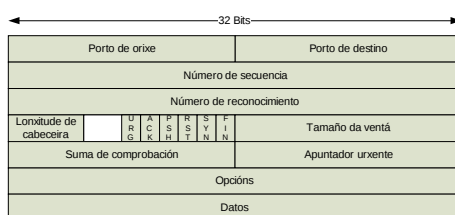
TCP (Transmisión Control Protocol) se diseñó específicamente para enviar una secuencia de bytes fiable a través de una red no fiable. Sus características principales son:

- Es un protocolo orientado a conexión. TCP establece una conexión entre un socket de la máquina transmisora y un socket de la máquina receptora. Un socket es un punto terminal al que se le asigna un número de socket formado por la dirección IP del host y un número de 16 bits local a ese host, llamado puerto. Una vez establecida la conexión se pueden transferir datos entre el origen y el destino. Aunque cada paquete enviado desde el host origen puede viajar por un camino o ruta diferente hasta llegar al host destino, por medio del protocolo IP, TCP consigue que parezca que existe un único circuito de comunicación entre ambos hosts.
- Es un protocolo fiable.
- Es un protocolo de flujo no estructurado, con posibilidad de enviar información de control junto a los datos.
- Es un protocolo con transferencia de memoria intermedia. Con el objeto de minimizar el tráfico de red y conseguir una transferencia eficiente, se van almacenando los datos del flujo de transmisión hasta completar un paquete lo suficientemente largo como para ser enviado. En el destino, se almacenan los datos recibidos hasta completar una secuencia completa y correcta para pasarla al proceso de aplicación destino.

- Usa conexiones full-dúplex, es decir, el tráfico puede ir en ambos sentidos al mismo tiempo.

50.1.2.6.1 SEGMENTO TCP

Cada segmento comienza con una cabecera de formato fijo de 20 bytes. Esta puede ir seguida de opciones de cabecera. Tras las opciones, si las hay, se encuentran los datos. También puede haber segmentos sin datos, usados normalmente para acuses de recibo y mensajes de control. El formato de la cabecera TCP es el siguiente:



TEXTO: Puerto de origen. Puerto de destino. Longitud de cabecera. Tamaño de la ventana. Apuntador urgente. Opciones

- Puerto de origen y puerto de destino (16 bits cada uno). Identifican los puntos terminales locales de la conexión. Cada host puede decidir la forma de asignar sus propios puertos, comenzando por el 256.
- Número de secuencia (32 bits). Indica el primer byte de datos que hay en el segmento.
- Número de acuse de recibo (32 bits). Especifica el siguiente byte esperado, no el último byte recibido correctamente. Para que este campo se tenga en cuenta el bit ACK debe estar activado ("1").
- Longitud de cabecera TCP. Cantidad de palabras de 32 bits. Es precisa, ya que el campo de opciones es de longitud variable. El tamaño de la cabecera completa puede oscilar entre 5 y 60 bytes.
- 6 bits que no se usan. Su valor es "0" y están reservados para usos futuros.
- 6 indicadores de 1 bit con funciones de control:
 - o URG: A "1" indica que el segmento contiene datos urgentes. El Apuntador urgente (16 bits) indica el siguiente byte del campo

de Datos que sigue a los datos urgentes, es decir, indica cuál es el último byte de datos que es urgente.

- o ACK: A “1” indica que el Número de acuse de recibo es válido. Si ACK=0 se ignora el campo de Número de acuse de recibo.
- o PSH: Indica datos “empujados”. Se activa para solicitar al receptor que entregue los datos a la aplicación a su llegada y no los almacene en el buffer hasta la recepción de un buffer completo.
- o RST: Sirve para reestablecer una conexión y para rechazar un segmento no válido o un intento de abrir una conexión.
- o SYN: Campo para la sincronización de los números de secuencia, que se utiliza al establecer la conexión. SYN indica el primer número de secuencia con el que se va a empezar a transmitir. Puede ser distinto de 0.
- o FIN: Se utiliza para liberar conexiones.
- Tamaño de la ventana (16 bits). Indica la cantidad de bytes que pueden enviarse a partir del último byte del que se recibió acuse de recibo. El receptor pone el valor de la ventana a 0 cuando no puede recibir más datos.
- Suma de comprobación (16 bits). Suma de comprobación de la cabecera, los datos y una pseudocabecera conceptual.
- Opciones. Permite agregar características extra no cubiertas en la cabecera normal.
- Para completar el tamaño del segmento TCP hasta que sea múltiplo de 32 bits se usan bits de relleno.

50.1.2.6.2 CONEXIONES TCP

Para establecer una conexión uno de los lados espera pasivamente una conexión entrante y el otro ejecuta una primitiva de conexión, especificando la dirección y el puerto IP con el que se desea conectar, el tamaño máximo de segmento TCP que está dispuesto a aceptar y, opcionalmente, algunos datos de usuario. Esta primitiva genera un

segmento TCP con el bit SYN a 1 y el bit ACK a 0. Al llegar el segmento al destino, la entidad TCP revisa si hay algún proceso escuchando en el puerto indicado en el campo de puerto de destino. Si no lo hay, envía una contestación con el bit RST a 1 para rechazar la conexión. En caso contrario, el proceso recibe el segmento TCP entrante y puede aceptar o rechazar la conexión. Si la acepta, se envía de vuelta un segmento de acuse de recibo.

Cuando se cae un host, por seguridad, no puede reiniciarse durante el tiempo máximo de paquete (120 seg.) para asegurar que no haya paquetes de conexiones previas vagando por Internet.

Para liberar una conexión, cualquiera de las partes puede enviar un segmento TCP con el bit FIN activado, indicando que no tiene más datos que transmitir. Al reconocerse el FIN, ese sentido se apagará. Sin embargo, el flujo de datos en el otro sentido puede continuar. Cuando ambos sentidos se apagan se libera la conexión. En algunas implementaciones de TCP existe un temporizador de seguir con vida (keepalive timer). Cuando una conexión está ociosa durante demasiado tiempo este contador puede agotarse. Si esto ocurre, un lado de la conexión comprueba si el otro aún responde. Si no se recibe respuesta se termina la conexión.

50.1.2.6.3 DETECCIÓN DE ERRORES

Las técnicas más efectivas y usadas son las siguientes:

- Detección de errores. Consiste en añadir uno o más bits de información a cada segmento, de forma que indiquen claramente si se alteró alguno de los bits del mismo en el camino desde emisor al receptor (Paridad, CheckSum, CRC,...).
- Confirmaciones positivas. El receptor devuelve un acuse de recibo positivo por cada uno de los segmentos recibidos correctamente. Se usa para detectar y solicitar el reenvío de segmentos perdidos. Esta es la técnica que se utiliza en el sistema de parada y espera.
- Expiración de intervalos de tiempo. El emisor inicia un contador de tiempo tras enviar un segmento (el temporizador de retransmisión). Si

este contador se agotara sin que se reciba un ACK positivo, el emisor vuelve a transmitir el mismo segmento.

- Confirmación negativa y transmisión. El receptor sólo confirma los segmentos recibidos erróneamente para que el emisor los vuelva a enviar. Por tanto, se utiliza para solicitar el reenvío de segmentos dañados.

50.1.2.6.4 CONTROL DE FLUJO

El control de flujo más simple es lo que se lleva a cabo mediante el sistema de parada y espera. El transmisor guarda un registro de cada segmento que envía, esperando un ACK antes de enviar el siguiente. También arranca un temporizador cuando envía el segmento. Si el temporizador expira antes de recibir el acuse de recibo, retransmite el segmento y reinicia el temporizador. Este mecanismo es el más barato y el más usado cuando se transmiten tramas muy grandes, pero es ineficiente ya que está el canal de transmisión desaprovechado la mayor parte del tiempo.

El control de flujo mediante ventana deslizante permite que el transmisor envíe varios segmentos sin esperar los ACK correspondientes. En este sistema el emisor y el receptor se ponen de acuerdo en el número de segmentos sin procesar que puede guardar este último, dependiendo del tamaño de sus buffers. También se ponen de acuerdo en el número de bits a utilizar para numerar cada segmento. Cuando la ventana tiene un tamaño cero el emisor no puede enviar más segmentos, salvo en dos casos excepcionales: cuando se trata de datos urgentes y cuando el emisor envía un segmento de 1 byte para provocar que el receptor genere un nuevo acuse de recibo con un nuevo tamaño de ventana, evitando así un bloqueo indefinido de la conexión.

Una variedad mejorada del sistema de ventana deslizante es el sistema de control de flujo con adelante-atrás-N, en el que cuando la estación destino encuentra un segmento erróneo devuelve un ACK negativo, rechazando todos los que le lleguen hasta que no reciba otra vez el segmento

incorrecto en buenas condiciones. El emisor, al recibir el ACK negativo, sabe que tiene que volver a transmitir ese segmento y todos los siguientes. Por último, existe otro sistema denominado sistema de control con rechazo selectivo, que se basa en que los únicos segmentos que se vuelven a retransmitir son aquellos rechazados por el receptor o aquellos cuyo temporizador expira sin confirmación. Este método es más eficiente que los anteriores pero precisa que el receptor disponga de un buffer intermedio de gran capacidad en el que guardar todos los segmentos recibidos tras el rechazo de un dado hasta recibir de nuevo el segmento.

50.1.2.6.5 CONTROL DE CONGESTIÓN

Cando la carga ofrecida a la red es mayor que la que puede gestionar se produce congestión. Todos los algoritmos TCP suponen que las terminaciones de temporización son causadas por congestiones y las revisan en busca de problemas.

Cada transmisor mantiene dos ventanas diferentes:

- Ventana negociada con el receptor al establecerse la conexión, cuyo tamaño está basado en el tamaño del buffer de memoria de destino. Esto permite que el transmisor no envíe más datos de los que el receptor puede almacenar evitando así que lo sature.
- Ventana de congestión, determinada por el tamaño de los datos que se pueden enviar sin que se produzca timeout.

El transmisor sólo puede mandar un número de segmentos limitado por el tamaño de la ventana más pequeña. Al establecerse una conexión, el transmisor asigna a la ventana de congestión el tamaño de segmento máximo usado por la conexión. Cada envío reconocido con éxito duplica la ventana de congestión. Este algoritmo se llama arranque lento (slow start) y permite que el tamaño de la ventana de congestión crezca exponencialmente hasta que se produzca una terminación de temporización (timeout) o se alcance el tamaño de la ventana receptora. Este crecimiento exponencial puede producir saturación. Para evitarlo, se introduce otro parámetro, denominado umbral, que toma como valor inicial

64 KBytes. Cuando se produce el timeout se cambia el valor del umbral a la mitad del tamaño de la ventana de congestión, se establece el valor de la ventana al del tamaño de un segmento máximo y se inicializa otra vez el proceso de arranque lento. Ahora, cuando el tamaño de la ventana llega al del umbral esta crece solamente en saltos de un segmento máximo, es decir, con un progreso lineal hasta que se produzca una nueva terminación de temporización.

50.1.2.7 PROTOCOLO UDP

El UDP (User Data Protocol) ofrece a las aplicaciones un mecanismo para enviar datagramas IP en bruto, encapsulados sin tener que establecer una conexión. Es una alternativa a TCP y se usa cuando una entrega rápida es más importante que una entrega garantizada, o cuando la información a enviar cabe en un único datagrama. Sus características son:

- UDP no admite numeración de los datagramas y tampoco utiliza mensajes de confirmación de entrega. Por lo que es posible que los datagramas lleguen duplicados y/o desordenados a su destino.
- Es un protocolo del tipo best-effort (mejor esfuerzo) porque hace lo que puede para transmitir los datagramas hacia el destino, pero no puede garantizar que este los reciba.
- UDP no utiliza mecanismos de control de errores. Cuando se detecta un error en un datagrama, en lugar de entregarlo a la aplicación destino, se descarta.

50.1.2.7.1 DATAGRAMA UDP

El datagrama UDP consiste en una cabecera de 8 bytes sucesiva de los datos. La cabecera presenta el siguiente aspecto.

- Puerto de origen y puerto de destino (16 bits cada uno). Al igual que en TCP, sirven para identificar los puntos terminales de las máquinas de origen y destino.
- Longitud UDP (16 bits). Indica la longitud del datagrama UDP en bytes, incluyendo la cabecera de 8 bytes y los datos.

- Suma de comprobación UDP (16 bits). Esta suma es opcional. Si no se calcula, su valor es 0.

50.1.3 ENCAMINAMIENTO

Para encaminar los paquetes de una red a otra se utilizan unos dispositivos denominados encaminadores o routers. Son los encargados de determinar el camino concreto que seguirá cada paquete en su viaje desde el host origen hasta el host destino.

Cada encaminador posee en su interior una tabla de encaminamiento para alcanzar redes distantes y otra para alcanzar redes locales. En la primera se almacenan direcciones IP de redes y subredes distintas de la actual, así como la máscara e interfaz de salida asociada a cada una de ellas. Y en la segunda tabla las direcciones de los hosts de la subred actual, junto con la dirección de la tarjeta de red de dicho host. De esta forma, cada encaminador sólo tiene que llevar el registro de otras redes/subredes y de los host locales. Las tablas de direccionamiento deben estar ordenadas desde las direcciones más específicas hasta las más generales y recorrerse en ese orden.

Las tablas de encaminamiento pueden ser fijas y contener rutas alternativas que serán utilizadas cuando algún dispositivo de encaminamiento no esté disponible. También pueden ser dinámicas de forma que el router puede ir modificándolas de acuerdo con el estado de la red y de los encaminadores que se comunican con él. Este es el motivo por el que los paquetes pertenecientes a una misma comunicación pueden seguir caminos diferentes.

Los hosts también poseen tablas de encaminamiento (desde simples tablas ARP hasta tablas más complejas). De hecho, cuando un host desea enviar datos a otro lo primero que hace es comprobar si el host destino aparece en sus tablas de encaminamiento. En caso afirmativo los datagramas le son enviados directamente mediante su dirección física (la dirección de su tarjeta de red). En caso contrario envía un mensaje de petición ARP, que será respondido por el host destino enviando su dirección física. A partir de

aquí se procede como en el caso afirmativo. En ambos casos el proceso recibe el nombre de entrega directa. Si ningún host de la red/subred responde al mensaje de petición los datagramas son enviados al router para que este se encargue de su direccionamiento. En este caso se habla de entrega indirecta.

Cuando un paquete IP llega a un encaminador, se extrae la dirección del host destino y se comprueba, pasándole las diferentes máscaras almacenadas en la tabla de encaminamiento, si pertenece a alguna de las redes que dicho router une. En caso afirmativo, el encaminador se comporta como un host más y sigue el proceso de entrega directa explicado en el párrafo anterior. Si el host destino no pertenece a ninguna de las redes que conecta el router, se reenvía al siguiente encaminador por la interfaz dada en la tabla de encaminamiento. De esta forma, el paquete va saltar de un router a otro, hasta llegar a uno que sí esté conectado a la red destino.

50.1.3.1 CIDR

CIDR (Classless Inter-Domain Routing) se lanzó en 1993 para mejorar el sistema de encaminamiento aprovechando mejor las direcciones disponibles. En vez de en las clásicas clases de red, CIDR se basa en VLSM (Variable-Length Subnet Masking) que define la máscara de subred con un número de bits de prefijo, como por ejemplo 10.0.0.0/7 define una máscara de subred donde los 7 primeros bits son 1 y el resto 0. Además CIDR también define la agregación de subredes con prefijos contiguos en redes de mayor tamaño, reduciendo así la tabla de encaminamiento.

CIDR define el concepto de bloque siendo un conjunto de direcciones IP contiguas que siguen un patrón A.B.C.D./N, donde A, B, C y D son números del 0 al 255 representando una dirección IP, y el N es el número de bits (por lo tanto de 0 a 32) que se considera que definen la red. Una determinada dirección IP pertenece a un determinado bloque CIDR cuando los N primeros bits de la misma son idénticos a los N primeros bits de A.B.C.D. Siguiendo el ejemplo anterior 10.0.0.0/7 define una red donde los 7 primeros bits tienen que ser iguales a los 7 primeros bits de la IP

10.0.0.0. De una forma similar la máscara de subred está constituida por N unos sucesivos de 32 – N ceros, que se dividen en 4 bytes y se separan por puntos.

La agregación de subredes, proceso conocido como superneting, permite que, por ejemplo, 128 redes contiguas del tipo 192.168.X.0/24 se agreguen en una sola 192.168.Z.0/20. El proceso requiere que las redes sean del mismo nivel (mismo número N) y contiguas (que la diferencia se produzca en los bits menores a N) y que, si la diferencia se produce en el bit N estén presentes las dos variantes para poder establecer un bloque con N-1, es decir, si hay M bits de diferencias (siempre en los últimos bits distintos de cero de la máscara de subred) se tienen que agregar las 2^M subredes en una “superred” N-M.

50.1.3.2 OSPF

OSPF (Open Shortest Path First) se estandarizó en 1990 desbancando al protocolo de vector de distancia RIP, que sólo funcionaba bien en sistemas pequeños.

Los requisitos que se pretendían cubrir cuándo se diseñó OSPF eran:

- El algoritmo no podía ser propiedad de una compañía sino que tenía que publicarse como literatura abierta.
- El nuevo protocolo tenía que reconocer distintas métricas de distancia, incluidas distancia física y retardo.
- Tenía que ser un algoritmo dinámico que se había adaptado a los cambios de topología de forma rápida y automática.
- El nuevo protocolo tenía que reconocer el encaminamiento basado en el tipo de servicio, diferenciando entre el tráfico de tiempo real y el resto.
- El protocolo tenía que efectuar equilibrio de cargas, dividiéndola entre varias líneas.
- Reconocimiento de sistemas jerárquicos de modo que ningún encaminador había tenido que conocer la topología completa.

- Se requería un mínimo de seguridad para evitar el envío de información de encaminamiento falso a los routers.

OSPF funciona mapeando el conjunto de redes, encaminadores y líneas en un grafo dirigido, en el que la cada arco ha asignado un coste, y calculando la trayectoria más corta desde cada dispositivo de encaminamiento a todos los demás en función de los pesos de los arcos.

OSPF maneja áreas numeradas, donde un área es una generalización de una subred. La topología y detalles de un área no son visibles desde fuera de la misma.

50.1.3.3 BGP

Todo lo que tiene que hacer un protocolo como OSPF, es mover paquetes con la mayor eficiencia posible desde origen al destino sin necesidad de preocuparse por la política. Sin embargo BGP (Border Gateway Protocol), se diseñó para permitir muchos tipos de políticas de encaminamiento.

Las políticas típicas comprenden consideraciones políticas, valga la redundancia, de seguridad o económicas. Se configuran manualmente en cada encaminador BGP y no son parte del protocolo mismo.

BGP tiene especial interés en el tráfico de tránsito. Las redes se agrupan en tres categorías:

- Redes de punta. Sólo tiene una conexión al grafo BGP.
- Redes multiconectadas. Pueden utilizarse para el tráfico de tránsito excepto que se nieguen a hacerlo.
- Redes de tránsito. Están dispuestas a manejar los paquetes de terceros, posiblemente con algunas restricciones.

Dos enrutadores BGP se consideran conectados si comparten una red común. Los pares de routers BGP se comunican entre ellos estableciendo conexiones TCP, proporcionando comunicación fiable y ocultando todos los detalles de la red por la que pasa.

BGP es fundamentalmente un protocolo de vector de distancia, en el que cada dispositivo de encaminamiento mantiene el coste a cada destino y, además, la trayectoria sucesiva. Del mismo modo, en lugar de dar

periódicamente a cada vecino sus costes estimados a todos los destinos posibles, cada enrutador BGP les dice a sus vecinos la trayectoria exacta que está usando. La esencia de BGP es el intercambio de información de encaminamiento entre dispositivos de encaminamiento.

50.1.4 APLICACIONES BÁSICAS: TELNET, FTP (TFTP) Y SMTP

50.1.4.1 TELNET

Este “protocolo” permite a los usuarios conectarse a ordenadores remotos y utilizarlos desde el sistema local mediante la emulación de terminal sobre una conexión TCP. Interconecta el cliente local de una máquina con el servidor con el que se comunica.

Los caracteres que se teclean en un cliente local son enviados por la red y procesados en el ordenador remoto. El resultado de su ejecución se transmite de vuelta y se muestra en la pantalla del ordenador local.

Este protocolo fue uno de los primeros que se definió y fue diseñado para trabajar con terminales en modo texto. Se implementa en dos módulos:

- El módulo cliente, que es un programa que ofrece un entorno no gráfico, es decir, modo carácter y es el encargado de entenderse con el programa servidor.
- El módulo servidor, que permanece escuchando en el puerto adecuado, por defecto el puerto 23 de TCP, a la espera de peticiones por parte de los clientes.

50.1.4.2 FTP

Permite la transferencia de archivos de texto o binarios desde un ordenador a otro sobre una conexión TCP.

FTP (File Transfer Protocol) implementa un sistema estricto de restricciones basadas en propiedades y permisos sobre los archivos. Hay un control de acceso de los usuarios y, cuando un usuario quiere realizar la transferencia de un archivo, el FTP establece una conexión TCP para el intercambio de mensajes de control. De esta manera se puede enviar el nombre de usuario, password, los nombres de los archivos y las acciones que se quieren realizar.

Una vez aceptada la transferencia del archivo, una segunda conexión TCP se establece para la transferencia de datos. El archivo se transfiere sobre la conexión de datos sin la utilización de ninguna cabecera o información de control en la capa de aplicación. Cuando se completa la transferencia, la conexión de control se usa para señalar que la transferencia se completó y para aceptar nuevos comandos de transferencia.

50.1.4.2.1 TFTP

TFTP (Trivial FTP) es un protocolo de transferencia de archivos muy sencillo que podríamos decir es una versión simplificada de FTP. TFTP se utiliza con frecuencia para transferir pequeños archivos entre ordenadores en una red, como cuando un cliente ligero arranca desde un servidor de red (porque no tiene un sistema operativo instalado).

Las principales características de TFTP y las principales diferencias con FTP son:

- Utiliza UDP (en el puerto 69) como protocolo de transporte (a diferencia de FTP que utiliza el puerto 21 TCP).
- No puede listar el contenido de directorios.
- No existen mecanismos de autenticación o cifrado.
- Se utiliza para leer o escribir archivos de un servidor remoto.
- Soporta tres modos diferentes de transferencia, "netascii", "octet" y "mail", de los que los dos primeros corresponden a los modos "ascii" y "binario" del protocolo FTP.

50.1.4.3 SMTP

SMTP (Simple Mail Transfer Protocol) Es el protocolo dedicado a la transmisión de mensajes electrónicos sobre una conexión TCP. Se implementó sobre una sencilla sesión del terminal virtual de red (NVT, Network Virtual Terminal) de Telnet.

El protocolo especifica el formato de los mensajes, definiendo la estructura de la información acerca del remitente, el destinatario, datos adicionales y naturalmente el cuerpo de los mensajes.

Este protocolo no especifica cómo los mensajes deben ser editados. Es necesario tener un editor local o una aplicación nativa de correo electrónico. Una vez el mensaje está creado, el SMTP lo acepta y usa el protocolo TCP para enviarlo a un módulo SMTP de otra máquina. TCP es el encargado de intercomunicar los módulos SMTP de las máquinas implicadas.

Existen extensiones de SMTP, ESMTP, definidas en un conjunto más reciente de normas, que permiten transportar cualquier tipo de información (imágenes, videos, sonidos, etc.).

50.2 BIBLIOGRAFÍA

- Andrew S. Tanenbaum. Redes de computadoras. PRENTICE HALL, 1997

Autor: Matías Villanueva Sampayo

Director de Informática Asociación Provincial de Pensionistas y Jubilados de A Coruña

Colegiado del CPEIG

**51. REDES DE ÁREA LOCAL.
TOPOLOGÍAS. REDES
ETHERNET. REDES
CONMUTADAS Y REDES
VIRTUALES. GESTIÓN DE
REDES. SISTEMAS DE
CABLEADO. ELECTRÓNICA DE
RED: REPETIDORES,
CONCENTRADORES, PUENTES,
CONMUTADORES,
ENCAMINADORES,
PASARELAS.**

Tema 51. Redes de área local. Topologías. Redes Ethernet. Redes conmutadas y redes virtuales. Gestión de redes. Sistemas de cableado. Electrónica de red: repetidores, concentradores, puentes, conmutadores, encaminadores, pasarelas.

51.1 Redes de área local

51.1.1 Funciones de los niveles especificados por el IEEE 802

51.1.1.1 Tramas LLC

51.1.2 Ejemplos de redes locales

51.1.2.1 Técnicas de contienda en bus

51.1.2.2 Técnicas de contienda en anillo

51.2 Topologías

51.2.1 Bus

51.2.2 Anillo

51.2.3 Estrella

51.2.4 Árbol

51.2.5 Malla

51.2.6 Mixta

51.3 Redes Ethernet

51.3.1 Operación de una red Ethernet

51.3.2 Control de acceso al medio

51.3.2.1 Transmisión de una trama

51.3.2.2 Recepción de una trama

51.3.2.3 Algoritmo de BackOff

51.3.2.4 Formato de trama MAC

51.3.2.4.1 Direcciones MAC 802.3

51.3.3 Medio físico

51.3.3.1 10 MBPS

51.3.3.2 100 MBPS

51.3.3.3 1000 MBPS

51.4 Redes conmutadas y redes virtuales

51.4.1 VLAN

51.4.1.1 Tipos de VLAN

51.5 Gestión de redes

51.5.1 Modelo OSI de gestión de red

51.5.2 SNMP

51.5.2.1 Funcionamiento de SNMP

51.5.2.2 Especificaciones técnicas SNMP mínimas requeridas

51.5.2 TMN

51.6 Sistemas de cableado

51.6.1 Estructura del cableado estructurado

51.6.2 Instalaciones comunes de telecomunicaciones

51.6.3 Medios de transmisión

51.6.3.1 Fibra óptica

51.6.3.2 Par trenzado

51.7 Electrónica de red

51.7.1 Repetidores

51.7.2 Concentradores

51.7.3 Puentes

51.7.4 Conmutadores

51.7.5 Encaminadores

51.7.6 Pasarelas

51.8 Bibliografía

51.1 REDES DE ÁREA LOCAL

Una LAN conecta ordenadores y otros dispositivos en un espacio limitado como puede ser una casa, un edificio, una oficina o un conjunto de edificios próximos entre sí.

Normalmente la distancia que abarca una LAN no supera los 100 metros.

La familia de estándares (que lleva el mismo nombre que el comité que los propuso) en el que se basa la mayoría de las tecnologías usadas en LAN y la IEEE 802 que se ocupa de redes de área local y de área metropolitana en las que el tamaño de trama es variable (como oposición a otros tipos de

redes donde se transmiten celdas de tamaño estándar, o flujos continuos,...).

Veremos ahora una introducción a las tecnologías LAN a través de la visión de la estructura que estandariza y de algunos ejemplos de esta familia.

51.1.1 FUNCIONES DE LOS NIVELES ESPECIFICADOS POR EL IEEE 802

En el nivel físico el IEEE 802 define:

- La codificación y señalización (Manchester, 4B/5B, etc.).
- La generación de preámbulos para sincronización.
- Transmisión y recepción de bits.

En el nivel de enlace (subnivel MAC):

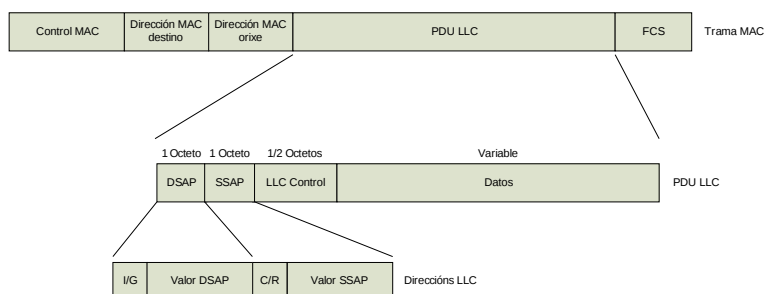
- La capa de control de acceso al medio se encarga de controlar la forma en que las estaciones que comparten el medio físico acceden a él. Este control puede ser centralizado en una estación monitora (lógica de acceso sencilla, se pueden establecer prioridades, etc.) o distribuido entre todas las estaciones (mejora las prestaciones y evita congestiones).
- En cuanto a cómo controlar el acceso al medio, este puede ser síncrono (se dedica una capacidad fija a cada estación) o asíncrono (se asigna la capacidad de transmitir de manera dinámica). Dentro de las técnicas asíncronas podemos nombrar:
 - o Giro circular: A cada estación se le proporciona la posibilidad de transmitir de una manera ordenada y cíclica. Útil cuando muchas estaciones necesitan realizar transmisiones largas.
 - o Reserva: El tiempo se divide en ranuras, las estaciones reservan ranuras para transmitir. Adecuada en tráfico continuo.
 - o Competición: Todas las estaciones compiten dentro de un instante dado por obtener la posibilidad de transmitir. Útil en tráfico a ráfagas.

- Esta capa es la responsable de la detección de errores y rechazar tramas erróneas (el control de errores y retransmisión de tramas corresponde el subnivel LLC).

En el nivel de enlace (subnivel LLC):

- Responsable del interfaz con capas superiores, ofreciendo los mismos servicios con o sin conexión. También se encarga del control de flujo y de errores en la transmisión de tramas. La misma capa LLC puede ofrecer varias opciones MAC.
- Ofrece a los niveles superiores, los siguientes servicios:
 - o En el orientado a conexión sin confirmación: Servicio de tipo datagrama, no incluye mecanismos de control de flujo y de errores, por lo que la recepción de datos no está garantizada. Es lo más frecuente en LANs, y puede encontrarse fácilmente para IP o IPX sobre Token Ring o FDDI.
 - o Modo orientado a conexión: Se establece una conexión lógica entre dos usuarios con control de errores y de flujo. Similar al ofrecido por HDLC. Es empleada por NetBEUI o MS-LAN Manager.
 - o En el orientado a conexión con confirmación: Es una mezcla de los anteriores, los datagramas son confirmados, pero no se establece una conexión lógica.

51.1.1.1 TRAMAS LLC



Significado de los bits I/G y C/R:

- I/G. Bit de dirección individual o grupo de destinos SAP.
- C/R. Bit que indica si se trata de un comando o una respuesta.

Existen los siguientes tipos de tramas:

- No numeradas (U): Formato 11 MM P/F MMM donde MM_MMM indica la función.
 - o 11_101: XID -> Información de intercambio: tamaño venta, etc.
 - o 00_111: TEST -> Test para verificar destino accesible.
 - o 00_000: UI -> Información no numerada (datagrama).
 - o 11_110: SABME -> Establecer modo de conexión balanceada asíncrona.
 - o 11_000: DM -> Modo desconexión.
 - o 00_010: DISC -> Cierre de conexión.
 - o 00_110: UA -> Confirmación no numerada a un SABME o DISC.
 - o 10_001: FRMR: Rechace de una trama incorrecta.
- Información (I): Formato 0 N(S) P/F N(R).
- Supervisión (S): Formato 10 SS 0000 P/F N(R) donde SS indica la función.
 - o 00: RR -> Receptor preparado.
 - o 10 RNR -> Receptor no preparado.
 - o 01 REJ -> Demanda de retransmisión de tramas desde N(R).

51.1.2 EJEMPLOS DE REDES LOCALES

51.1.2.1 TÉCNICAS DE CONTIENDA EN BUS

Más adelante en este mismo tema veremos en detalle cómo funciona Ethernet.

51.1.2.2 TÉCNICAS DE CONTIENDA EN ANILLO

Vamos a ver algún detalle de IEEE 802.5 (Token Ring) para ejemplificar las técnicas de contienda en anillo.

Este tipo de topología, consta de varios repetidores que copian y regeneran cada bit que circula por el anillo, retrasando, en el tiempo de transmisión de un bit, la circulación de la trama.

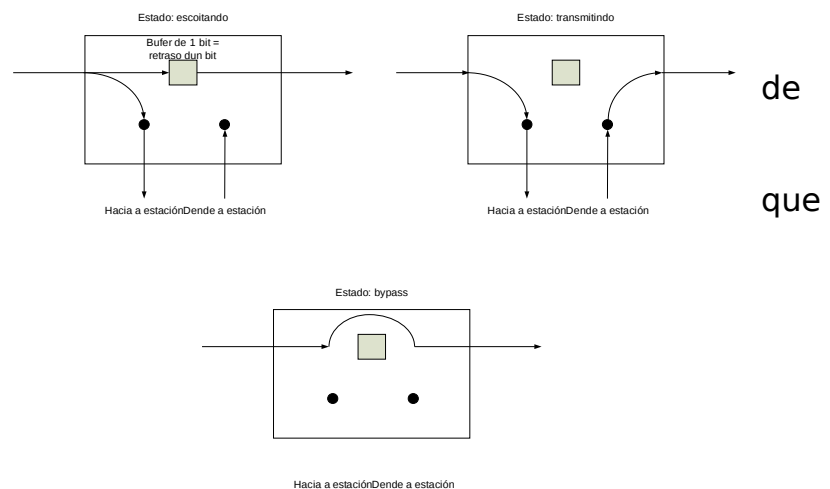
En una topología en anillo, debe controlarse la eliminación de tramas. Esta tarea puede realizarla el destino o más comúnmente, el origen. Siguiendo

este último convenio se facilita el uso de direccionamiento múltiple y confirmaciones automáticas de recepción de la trama.

Esta topología presenta los siguientes problemas:

- Problemas derivados de la pérdida de un enlace o estación.
- Inserción de una nueva estación (necesidad de identificación por parte de sus vecinos).
- Pérdida o duplicidad del testigo.

La topología en estrella-anillo soluciona muchos estos problemas, al existir un nodo central se encarga de monitorizar y aislar fallos.

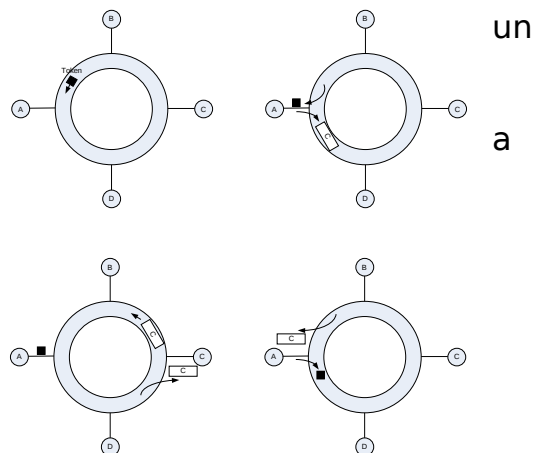


TEXTO: Estado:

escuchando. Estado: transmitiendo. Hacia la estación. Desde la estación.

En la siguiente imagen podemos ver cómo funciona 802.5 con respecto a una estación.

En la siguiente imagen podemos ver ejemplo de funcionamiento de la transmisión de una trama de un nodo otro.

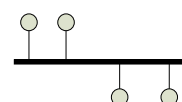


51.2 TOPOLOGÍAS

La topología de red se define como la cadena de comunicación usada por los nodos que conforman una red para comunicarse entre sí.

51.2.1 BUS

En las redes donde se usa una topología en bus cada uno de los nodos se conecta al mismo cable. Una señal enviada desde uno de los ordenadores conectado a la red viaja en ambas direcciones del cable hasta llegar a los extremos alcanzando a todos los nodos en su camino.

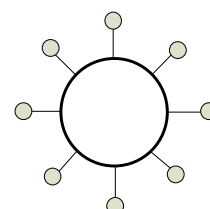


Podemos considerar dos tipos de redes en bus:

- Bus lineal: donde sólo existen dos extremos finales y todos los equipos están conectados al mismo cable.
- Bus distribuido: cuando existen más de dos extremos finales y el bus se configura básicamente conectando más cables al mismo y formando ramas.

51.2.2 ANILLO

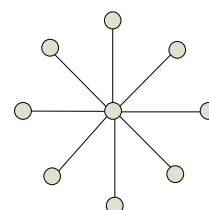
Una topología en anillo se construye en forma circular los datos circulando alrededor del anillo en una sola dirección y cada dispositivo actúa como un repetidor mantener la señal a un nivel adecuado.



con
para

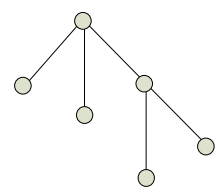
51.2.3 ESTRELLA

En esta topología cada ordenador se conecta a un dispositivo central usando una conexión punto a punto. Todo el tráfico que viaja por la red pasa por el dispositivo central que actúa como un repetidor.



51.2.4 ÁRBOL

En esta topología los nodos se estructuran de forma jerárquica, con un nodo en el nivel superior conectado a uno o varios nodos en el siguiente nivel y así sucesivamente. Puede haber un número fijo de nodos por nodo padre o ser completamente libre. Durante una transmisión, los

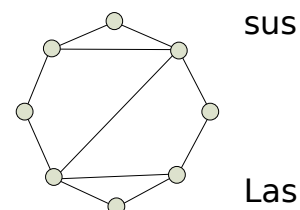


a uno
hijos

datos suben en la jerarquía desde el nodo emisor hasta al primer nodo común entre el emisor y receptor bajando luego hasta el receptor.

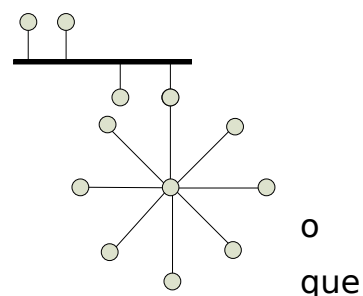
51.2.5 MALLA

Es un tipo de topología donde cada nodo debe enviar propios datos, si tiene un enlace directo al destino, o hacer uso de otros nodos intermedios para que retransmitan los datos de no tener un enlace directo. Las mallas pueden ser total (todos los nodos tienen un enlace directo a los demás nodos) o parcialmente (no todos los nodos tienen un enlace directo a los demás nodos) conectadas.



51.2.6 MIXTA

Las topologías mixtas usan una combinación de dos más de las topologías anteriores adoptando formas pueden tener una elevada complejidad.



51.3 REDES ETHERNET

Ethernet (IEEE 802.3) es la más común de las redes de área local existiendo interfaces (tarjetas,...) para casi cualquier tipo de máquina. A su velocidad original era de 10 Mbps, actualmente existen soluciones comerciales a 100 Mbps (FastEthernet) y 1000 Mbps (Gigabit Ethernet). Ethernet utiliza un método distribuido de acceso al medio para todas las máquinas conectadas. No existe una estación maestra que controle la red. No existen tampoco niveles de prioridad para transmitir. El modo de transmisión es semi-duplex (originalmente Ethernet se montaba usando una topología de bus), aunque los conmutadores actuales permiten full-duplex.

El estándar Ethernet describe las capas física y MAC.

51.3.1 OPERACIÓN EN UNA RED ETHERNET

Ethernet se basa, como comentamos anteriormente, en un acceso distribuido al medio (Carrier Sense Multiple Access with Collision Detection, CSMA/CD por sus siglas en inglés) en el que cualquier equipo puede por sí mismo decidir el inicio de la transmisión y ocupar el medio con sus datos

siempre y cuando no exista otra estación transmitiendo. Pueden ocurrir colisiones debidas al retardo de la propagación (tiempo que tarda la señal en alcanzar todo el medio).

El transporte de datos tiene lugar mediante la emisión de paquetes (tramas) emitidas sobre el medio físico. Estas tramas tendrán una longitud entre 64 y 1518 bytes (con un campo de datos entre 46 y 1500 bytes).

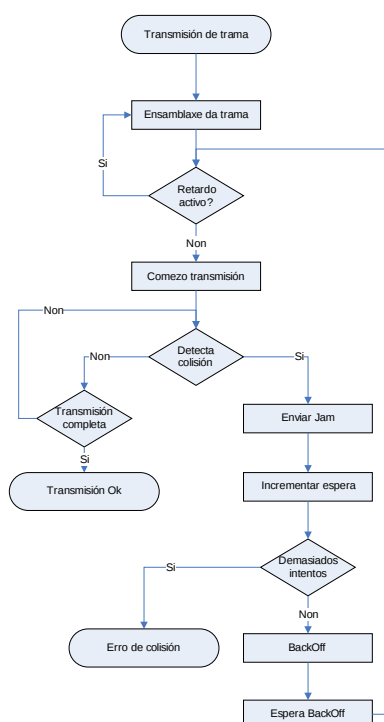
La tarjeta de red del computador gestiona las funciones MAC inherentes a Ethernet y se comunica con la capa LLC superior.

La eficiencia global de Ethernet es generalmente alta, aunque difícil de cuantificar y dependiente del número y tipo de estaciones conectadas. Ethernet tiene una gran eficiencia en redes donde existe un equipo que genera la mayor parte del tráfico y el resto se dedican a recibir y transmitir pequeñas cantidades.

51.3.2 CONTROL DE ACCESO AL MEDIO

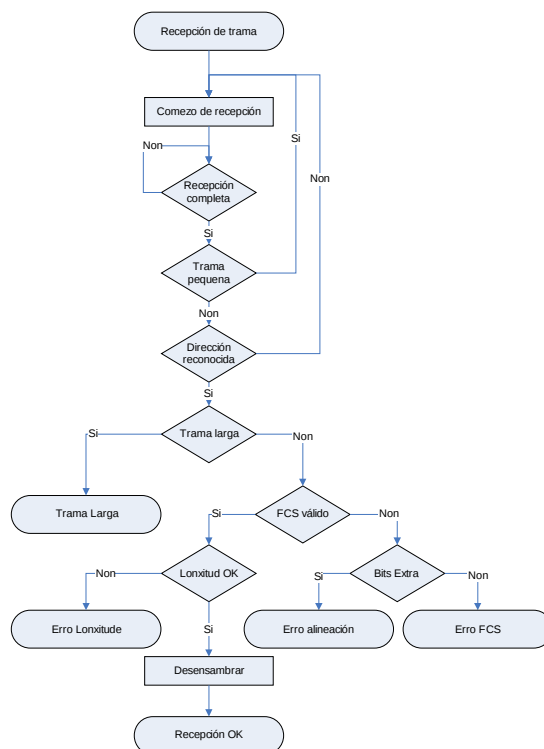
Como ya mencionamos anteriormente, Ethernet usa CSMA/CD para al control de acceso al medio. En las figuras siguientes podemos ver de forma gráfica los principales algoritmos implicados.

51.3.2.1 TRANSMISIÓN DE UNA TRAMA



TEXTO: ENSAMBLAJE DE TRAMA. COMIENZO TRNASMISIÓN. ERROR DE COLISIÓN

51.3.2.2 RECEPCIÓN DE UNA TRAMA



TEXTO: Comienzo de recepción. Trama pequeña. Longitud. Error longitud. Error alineación. Desensamblar

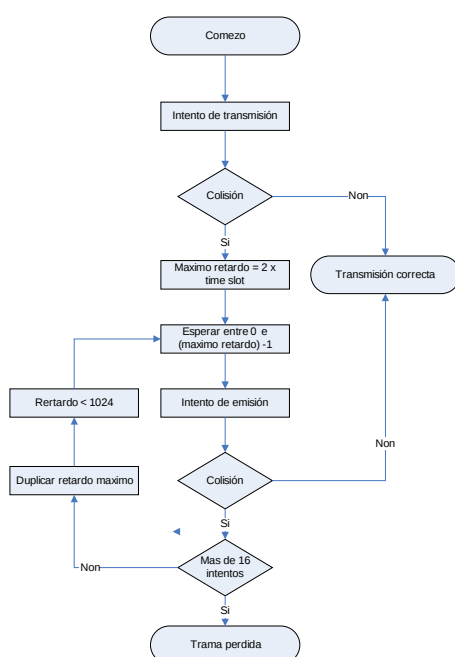
Los posibles errores en la recepción de una trama son:

- Runt (enana): Trama demasiado corta, menor de 64 bytes. Puede haber sido truncada por una colisión. Normalmente será una trama desalineada con un FCS erróneo.
- Jabber: Trama demasiado larga, más de 1518 bytes. Normalmente no existirán tramas de este tipo en la red, a no ser que se trate de:
 - o Una superposición de dos tramas.
 - o Línea sin estructura de frame enviada por un equipo que funciona incorrectamente.

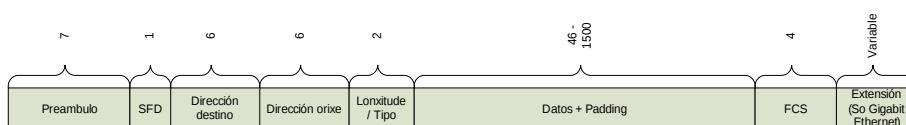
- Trama desalineada: Una trama con un número de bits no divisible entre ocho.
- Trama con FCS erróneo: Trama para la cual el receptor calculó un CRC que no coincide con los últimos 4 bytes.

51.3.2.3 ALGORITMO DE BACKOFF

El algoritmo de backoff define el tiempo que la estación debe esperar para el siguiente intento de emisión de una trama en el caso de una colisión en el anterior intento, habida cuenta los intentos ya realizados.



51.3.2.4 FORMATO DE TRAMA MAC



TEXTO: Dirección origen. Longitud tipo.

El formato MAC para 802.3 consta de los siguientes campos:

- Preámbulo: El receptor utiliza 7 bytes con el patrón 10101010 para sincronización.
- SFD: Delimitador de comienzo de trama 10101011.
- Dirección destino: Indica una estación o estaciones a la que va dirigida la trama. Puede ser individual, de grupo o global.

- Dirección origen de la estación que emite la trama.
- Longitud del campo de datos LLC.
- Datos LLC.
- Relleno (Padding): Octetos añadidos para construir tramas lo suficientemente largas que aseguren un correcto funcionamiento de la técnica CD.
- Secuencia de comprobación de trama (FCS) Código de redundancia cíclica de 32 bits en base a todos los campos excepto los de preámbulo, SFD y el propio FCS.
- A mayores, en el caso de Gigabit Ethernet, se requiere añadir bytes extra a las tramas menores de 512 bytes para garantizar que se detectan las colisiones

51.3.2.4.1 DIRECCIONES MAC 802.3

La dirección MAC es una dirección única (con respecto a todas las tarjetas de red existentes) que posee la tarjeta de red. Pueden ser de 16 o 48 bits. Las de 48 bits son 6 bytes donde:

- Los 3 primeros constituyen el código del vendedor. El primer byte del código de vendedor tiene dos bits especiales:
 - o El bit menos significativo es el que indica si la dirección es individual o de grupo (multicast, bit a uno).
 - o El bit más significativo indica si se trata de una dirección global (visible a través de un puente) o local (bit a uno).
- Los 3 últimos el identificador del dispositivo.

Existe una dirección global (broadcast), representada por los 6 bytes a uno. También existen 247 direcciones diferentes, mantenidas por el IEEE.

Ejemplos:

- 08:00:20:0a:ef:31 (dirección individual)
- 09:00:20:00:00:00 (multicast a todas las máquinas 08:00:20)
- 89:00:20:00:00:00 (multicast local)
- 00:80:C2 (Prefijo usado por el comité IEEE 802)

- 01:80:C2:00:00:00 (multicast para spanning tree en bridges)
- FF:FF:FF:FF:FF:FF (broadcast)

51.3.3 MEDIO FÍSICO

Existen diferentes medios físicos sobre los que podremos montar Ethernet, dependiendo de la velocidad que queremos alcanzar.

51.3.3.1 10 MBPS

	10BASE5	10BASE2	10BASET	10ANCHA36	10BASEFP	10BASEFL
Medios de transmisión	Coaxial 50 Ohms.	Coaxial 50 Ohms.	UTP	Coaxial 75 Ohms.	Par Fibra 850 nm	Par Fibra 850 nm
Topología	Bus	Bus	Estrella	Bus / Árbol	Estrella	Punto a punto
Longitud máxima / segmento	500	185	100	1800	500	2000

51.3.3.2 100 MBPS

	100BASETX	100BASET4	100BASET2	100BASEFX
Medios de transmisión	2 Pares STP / UTP5	4 pares UTP3 / UTP5	2 pares UTP3 / UTP5	Par Fibra 850 nm
Topología	Estrella	Estrella	Estrella	Estrella
Longitud máxima / segmento	100	100	100	100

51.3.3.3 1000 MBPS

	1000BASET	1000BASETX	1000BASECX	1000BASESX	1000BASELX
Medios de transmisión	4 Pares UTP5	2 Pares UTP6	STP	Par Fibra 850 nm	Par Fibra 1300 nm

Topología	Estrella	Estrella	Estrella	Estrella	Punto a punto
Longitud máxima / segmento	100	100	25	275 – 62,5 550 – 50	550 – MMF 5 km – SMF

51.4 REDES CONMUTADAS Y REDES VIRTUALES

Los modelos de red basados en compartir ancho de banda, presentes en las arquitecturas LAN de los primeros noventa, carecen de la potencia suficiente como para proporcionar los cada vez mayores anchos de banda que requieren las aplicaciones multimedia. En este tipo de LANs los usuarios comparten un único canal de comunicaciones, de modo que todo el ancho de banda de la red se asigna al equipo emisor de información quedando el resto de los equipos en situación de espera. Siguiendo la filosofía de compartir el ancho de banda y para aumentar el ancho de banda disponible para cada usuario, se puede optar por la segmentación de los buses y anillos. Sin embargo, estas técnicas no ofrecen buenas prestaciones, debido principalmente a las dificultades que aparecen para gestionar la red. Cada segmento suele contener de 30 a 100 usuarios. La técnica idónea para proporcionar elevados anchos de banda es la conmutación. Mediante esta técnica, cada estación de trabajo y cada servidor poseen una conexión dedicada dentro de la red, con lo que se consigue aumentar considerablemente el ancho de banda a disposición de cada usuario.

Las LANs basadas en compartir ancho de banda se construyen mediante concentradores y encaminadores. En una LAN conmutada, una de las funciones tradicionales del encaminador pasa a ser realizada por el conmutador LAN, quedando el encaminador destinado a funciones relacionadas con el avance de las prestaciones en lo que respecta a la gestión de la red y la conexión con otras redes. Con este nuevo modelo se pueden conectar de 100 a 500 usuarios. El decremento en los precios de

conmutadores Ethernet fue uno de los principales impulsos para que un buen número de empresas se inclinen por una LAN conmutada.

Sin embargo, la continua instalación de conmutadores, dividiendo la red en más y más segmentos (con menos y menos usuarios por segmento) no reduce la necesidad de broadcast. Las VLANs representan una solución alternativa a los encaminadores con función de gestores de la red.

51.4.1 VLAN

Una VLAN (Virtual Local Area Network) es una red lógica creada sobre una red física. Sus principales características son:

- Permite gestionar los segmentos de una LAN como dominios de emisión lógicos. Se restringe de esta forma el tráfico multicast y broadcast.
- No importa la ubicación topológica o física de las estaciones (ya que en caso de ser necesario se produce una comunicación entre conmutadores).
- Si se configura adecuadamente se podrá mover una estación de una VLAN a otra sin necesidad de modificar la dirección IP.
- Los encaminadores sólo se usarán ahora para comunicar VLANs.

51.4.1.1 TIPOS DE VLAN

- Nivel 1: Configuradas usando el puerto del conmutador (incluso entre conmutadores). Es la forma más sencilla de definir VLANs. Si se mueve la estación habrá que reconfigurar manual de la VLAN. Tiene la limitación de que un puerto no puede pertenecer a más de una VLAN.
- Nivel 2: Configuradas usando la dirección MAC de la estación. Estas VLAN se definen en base a un conjunto de direcciones MAC. Un puerto sólo es registrado en una VLAN cuando se constata que un paquete con una determinada MAC origen fue transmitido por ese puerto. Para identificar a qué grupo pertenece una trama debe inspeccionarse la misma por lo que esta técnica es más lenta que la anterior. Esta técnica representa más trabajo al principio ya que se necesita registrar en alguna VLAN todas las MAC.

- Nivel 3: Configuradas por el tipo de protocolo o por subred IP. El particionado por protocolo permite el movimiento sin reconfiguración, y elimina la necesidad de etiquetado de tramas. Pero esta técnica obliga a analizar el paquete de red por completo por lo que tiene un menor rendimiento que las técnicas de nivel 2.
- Técnicas de mayor nivel: Configuradas por los protocolos de nivel superior basándose en aplicaciones y / o servicios. Permite crear una VLAN con todas las máquinas que utilicen el servicio de e-mail, por ejemplo. La mayoría de los fabricantes no la implementan, pues consideran suficiente la técnica de nivel 3.

IEEE 802.1Q sólo define los tipos de nivel 1 y 2. A partir de ese nivel el establecimiento de VLANs no se encuentra estandarizado y cada fabricante lo implementa de manera propietaria resultando algunas implementaciones incompatibles con otras.

51.5 GESTIÓN DE REDES

51.5.1 MODELO OSI DE GESTIÓN DE RED

ISO, siguiendo las directrices del grupo OSI, definió el modelo de gestión de red como la forma más importante para entender las funciones principales de los sistemas de gestión de red.

El modelo OSI de gestión de red categoriza las funciones en 5 áreas que a veces se denominan modelo FCAPS (Fault, Configuration, Accounting, Performance y Security):

- Falla (Fault): Siendo el objetivo de esta área detectar, aislar, corregir y registrar las fallas que se produzcan en la red.
- Configuración (Configuration): Los objetivos de esta área son recoger/fijar/hacer seguimiento de la configuración de los dispositivos. La gestión de la configuración se ocupa de monitorizar información de configuración del sistema y cualquier cambio que se produzca en la misma. La importancia de esta área viene dada por que muchos incidentes en la red son el resultado de cambio sin archivos de configuración, actualización de versiones, etc. Una adecuada gestión de

la configuración obliga a registrar todos los cambios en la configuración software y hardware.

- **Contabilidad (Accounting):** Siendo el objetivo principal recoger estadísticas. La gestión de la contabilidad se preocupa por mantener la información referida a la utilización de la red, de forma que se pueda facturar a usuarios individuales, departamentos, etc.
- **Rendimiento (Performance):** El objetivo de esta área es doble: por un lado preparar la red para el futuro y por otro medir la eficiencia actual de la misma asegurándose que está dentro de los niveles aceptables. La gestión del rendimiento se preocupa de recoger regularmente la información de rendimiento de la red como son los tiempos de respuesta, ratios de pérdida de paquetes, utilización de enlaces de datos, etc.
- **Seguridad (Security):** El objetivo de la gestión de la seguridad es controlar el acceso a los recursos de la red. Esta área no sólo se preocupa de que la red sea segura y no de recabar y analizar la información referida a la seguridad. Las funciones típicas dentro de esta área son la autenticación, autorización, auditoría, de forma que los usuarios (tanto internos como externos) tengan el acceso adecuado a los recursos de la red.

51.5.2 SNMP

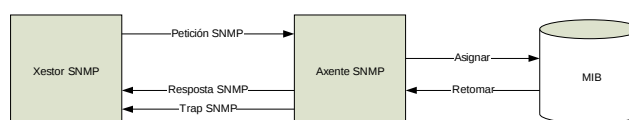
SNMP (Simple Network Management Protocol) es el protocolo definido por los comités técnicos de Internet para ser utilizado como herramienta de administración de los distintos dispositivos en cualquier red. El funcionamiento de SNMP es sencillo, como su propio nombre indica, aunque su implementación puede llegar a ser tremendamente compleja. SNMP utiliza la capa de transporte de TCP/IP mediante el envío de datagramas UDP (los agentes escuchan en el puerto 161 y las estaciones gestoras en el 162). Sin embargo, el hecho de usar UDP hace que el protocolo no sea fiable (en UDP no se garantiza la recepción de los paquetes enviados, como en TCP).

El protocolo SNMP está definido en un gran número de RFCs (Request For Comments), entre ellos el RFC 1157, 1215 (que definen la versión 1), del 1441 al 1452 (que definen la versión 2), del 2271 al 2275 y del 2570 al 2575 (para SNMP v3).

51.5.2.1 FUNCIONAMIENTO DE SNMP

Cada agente (se puede ver a un agente como una máquina en la que queremos monitorizar alguno de sus estados) ofrece una determinada serie de variables, que pueden ser leídas o modificadas. Además, un agente puede enviar “alarmas” (Traps) a otros agentes para avisar de eventos que tienen lugar. Lo normal es que el agente encargado de recibir los eventos se denomine “gestor” (podemos verlo como a la máquina que monitoriza el estado de toda la red). De forma muy resumida podemos ver las capacidades expuestas:

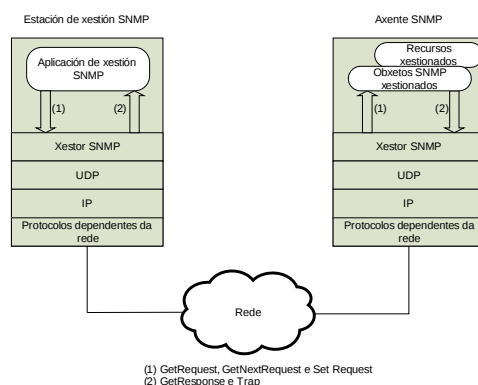
- GET : La estación gestora extrae (lee) el valor de un objeto del agente
- SET : La estación gestora fija (escribe) el valor de un objeto del agente
- TRAP : Permite a un agente notificar a la estación gestora eventos significativos



TEXTO: Gestor. Respuesta. Agente

Las variables ofrecidas para la consulta en los agentes SNMP se definen a través de una MIB (Management Information Base, Base de Información de Gestión). La MIB es una forma de determinar la información que ofrece un dispositivo SNMP y la forma en que se representa. La versión de la MIB actual es MIB-II y está definida en el RFC 1213, aunque hay múltiples extensiones definidas en otros RFCs. La MIB está descrita en ASN.1 para facilitar su transporte transparente por la capa de red.

Cada agente SNMP ofrece información dentro de una MIB, tanto de la estándar (definida en los distintos RFCs) como de aquellas extensiones que desee proporcionar cada uno de los fabricantes.



TEXTO: Estación de gestión. Agente. Aplicación de gestión. Gestor.
Protocolos dependientes de la red. Recursos gestionados. Objetos gestionados

ASN.1 (Abstract Syntax Notation One) es un estándar de nota que describe la representación, la transmisión, la codificación y decodificación de estructuras de datos. Proporciona un conjunto de reglas formales para describir la estructura de objetos que son independientes de las técnicas de codificación de una máquina, aportando una nota formal que elimina a las ambigüedades.

51.5.2.2 ESPECIFICACIONES TÉCNICAS SNMP MÍNIMAS REQUERIDAS

Existen diversas RFCs que definen SNMP. Por ello es importante establecer unos requisitos o especificaciones mínimas. Estas especificaciones mínimas son:

- Versión del protocolo SNMPv2c (Community-based SNMPv2 - RFC 1901)
Utiliza el mismo modelo que la primera versión del protocolo SNMP, y como tal no incluye mecanismos de seguridad. Los únicos avances introducidos en esta versión consisten en una mayor flexibilidad de los mecanismos de control de acceso, ya que se permite la definición de políticas de acceso consistentes en asociar un nombre de comunidad con un perfil de comunidad formado por una vista MIB y unos derechos de acceso a dicha vista (sólo lectura o lectura y escritura).
- La MIB deberá ser compatible con el formato ASN.1. Las implementaciones de otros estándares de la MIB son opcionales. ASN.1

está diseñado para definir información estructurada (mensajes) de tal forma que sea independiente de la máquina utilizada. Para hacer esto ASN.1 define tipos de datos básicos, como enteros y cadenas de texto, y permite construir nuevos tipos de datos a partir de los ya definidos. También utiliza palabras especiales (keywords) para definir sus procedimientos, definir nuevos tipos, asignar valores, definir macros y módulos.

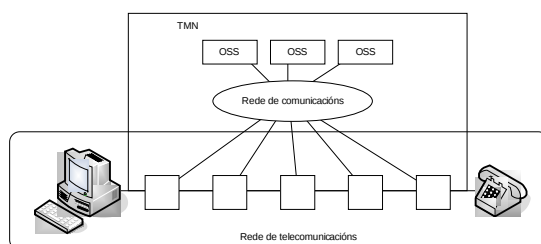
- El acceso múltiple deberá ser permitido, existiendo 3 niveles de acceso con sus correspondientes “login” y “password”.
- El requisito mínimo respecto a la seguridad, es la generación de “Traps” en el caso de una autenticación fallida. La información relevante del infractor que deberá ser enviada en el TRAP, será la dirección IP.

51.5.3 TMN

TMN (Telecommunications Management Network) define un marco de trabajo para alcanzar la interoperabilidad y comunicación entre redes de comunicaciones y sistemas operativos heterogéneos. TMN fue desarrollado por ITU como una infraestructura para soportar la gestión y despliegue de servicios dinámicos de telecomunicaciones.

TMN proporciona un framework flexible, escalable, confiable, barato y fácil de mejorar. TMN permite crear redes más capaces y eficientes definiendo una forma estándar de realizar las tareas de gestión de la red y comunicaciones. El procesamiento en TMN puede ser distribuido para mejorar la escalabilidad.

Una red de telecomunicaciones está compuesta de elementos de conmutación, circuitos, terminales, etc. En terminología TMN todos estos elementos son Elementos de la Red (NE Network Elements). TMN permite la comunicación entre los NEs y OSS (Operations Support Systems).



TMN usa principios de orientación a objetos e interfaces estándar para definir las comunicaciones entre diferentes entidades en la red. El interfaz de gestión estándar se llama Q3. TMN se basa en estándares OSI como CMIP (Common Management Information Protocol), GDMO (Guideline for definition of management objects), ASN.1 y el modelo de referencia OSI. Las funciones de gestión se realizan a través de operaciones compuestas de primitivas CMIS (Common Management Information Service).

La información de gestión de la red, así como las reglas por las que la información se presenta y gestiona, se llaman MIB (Management Information Database). Los procesos que gestionan la información se llaman entidades que pueden ser de dos tipos: gestor o agente.

TMN describe las redes de telecomunicaciones desde distintos puntos de vista:

- Modelo funcional: representado por bloques que aportan una visión general de las funciones y características de TMN.
 - o Los (Operation System): realiza funciones de operación del sistema incluyendo monitorización y control de las funciones de gestión de telecomunicaciones.
 - o MD (Mediation Device): Realiza funciones de mediación entre los interfaces locales TMN y el modelo de información de los OS.
 - o QA (Q-Adapters): Permite a TMN gestionar NEs que no tienen interfaces TMN.
 - o NE (Network Entity): Contiene información gestionable que es monitorizada y controlada polo OS.
 - o WS (Workstations): Traducen la información entre formato TMN y un formato comprensible por el usuario.

- o DCN (Data Communication Network): Representa la red de comunicaciones cubriendo los niveles 1 a 3 de OSI.
- Conjunto de interfaces:
 - o Q: Los interfaces Q existen entre dos bloques funcionales TMN que pertenecen al mismo dominio.
 - Qx: existe entre los NE y los MD, QA y MD y entre los MD y otro MD.
 - Q3: es la interfaz del OS y existe entre los NEs y OS, QA y OS, MD y OS y entre OS y otro OS.
 - o F: Las interfaces F existen entre los WS y OS y entre los WS y MD.
 - o X: Estas interfaces existen entre dos OS TMN de diferentes dominios o entre un OS TMN y otro OS en una red no TMN.
- Modelo lógico o de negocio: Este modelo está basado en capas de distintos niveles jerárquicos:
 - o BML (Business Management Layer): Planificación de alto nivel, presupuestos, BLAs (Business Level Agreements), etc.
 - o SML (Service Management Layer): Usa la información presentada por la capa NML para gestionar los servicios contratados por clientes actuales o potenciales. También es el punto clave de contacto con proveedores de servicio y otras entidades administrativas.
 - o NML (Network Management Layer): La NML tiene visibilidad de toda la red basada en la información de los OSs de la capa EML. NML permite gestionar los NEs de forma individual o como un grupo.
 - o EML (Element Management Layer): Gestiona cada elemento de la red que contiene OSs, cada uno de los cuales gestiona ciertos NEs. También contiene a los MDs.

- o NEL (Network Element Layer): Representa la información gestionable por TMN en un NE. OS QA y los NE están localizados en esta capa.

51.6 SISTEMAS DE CABLEADO

El cableado de una determinada organización o edificio se organiza siguiendo los principios del cableado estructurado. Los sistemas de cableado estructurado son las infraestructuras de cable (ya sea par de cobre, coaxial, fibra óptica, etc. O una combinación de ellos) que transportan las señales de datos desde un emisor hasta un receptor dentro de un edificio, en un campus,...

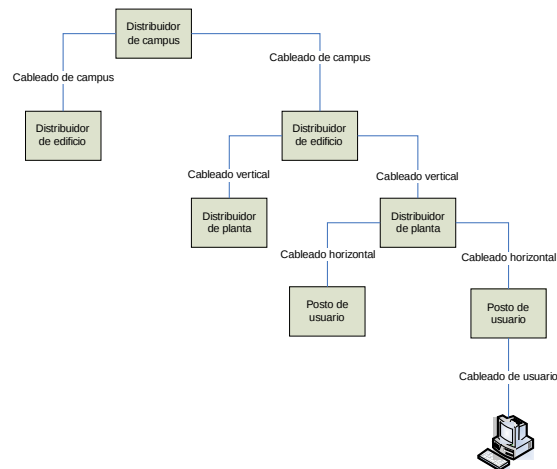
El cableado estructurado facilita enormemente los cambios de ubicaciones en personas y equipos al permitir cambiar las conexiones de un punto a otro sin necesidad de instalar nuevos cables.

También facilita los cambios en el equipamiento de telecomunicaciones ya que está pensado para ser independiente de unos equipos (teléfonos, concentradores,...) concretos.

Existen varias normas que establecen cómo debe ser el cableado, las más importantes son la CENELEC EN 50173 (que define el cableado estructurado) y la legislación vigente en materia de las Instalaciones Comunes de Telecomunicaciones.

51.6.1 ESTRUCTURA DEL CABLEADO ESTRUCTURADO

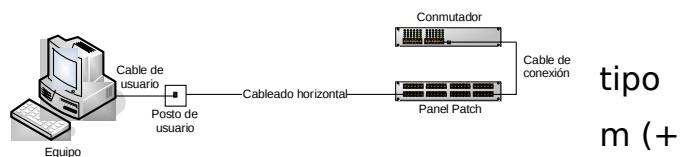
El cableado estructurado se establece de forma jerárquica con cada elemento de orden inferior interconectado con un elemento de nivel superior.



TEXTO: Puesto de usuario.

Los principales componentes del cableado son:

- **Cableado de campus:** Cableado desde todos los distribuidores de edificios al distribuidor de campus. Suele realizarse usando fibra óptica y / o líneas punto a punto (posiblemente sobre una red pública) por las distancias implicadas. Puede incluir repetidores y otros elementos de conexión.
- **Cableado Vertical:** Cableado desde los distribuidores de planta al distribuidor del edificio. Suele componerse si varios cables UTP o fibra óptica que conectan cada distribuidor de planta con el distribuidor del edificio.
- **Cableado Horizontal:** Cableado desde el distribuidor de planta (llegando a unos paneles patch -un conjunto de conectores RJ45 instalados en un bastidor de 19 pulgadas- instalados en dicho distribuidor) a los puestos de usuario. Suele ser un sólo cable UTP en el que no se permiten puentes, derivaciones y empalmes a lo largo de todo el trayecto. La máxima longitud permitida, independientemente del de medio utilizado, es de 90 m (3 m usuario + 7 m cable de conexión al patch panel = 100m).



- Cableado de Usuario: Cableado desde el puesto de usuario a los equipos. Suele consistir en un latiguillo que conecta la toma de la pared con el equipo (ya sea un PC, un teléfono,...).

Los principales puntos de la red de cableado estructurado son:

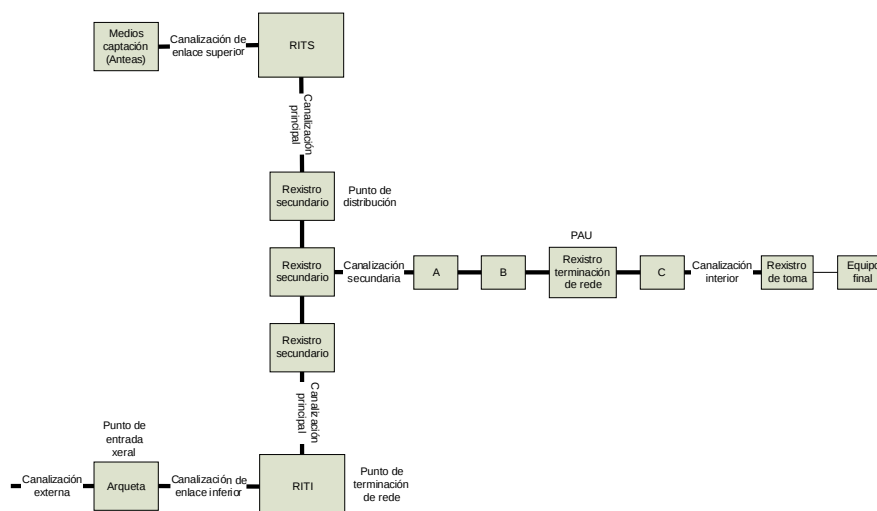
- Distribuidor de campus: Punto central donde llega todo el cableado de campus.
- Distribuidores de edificio: Punto donde se conecta el cableado de campus y donde llega todo el cableado vertical del edificio.
- Distribuidores de planta: Punto donde se conecta el cableado vertical y llega todo el cableado horizontal de la planta.
- Puestos de usuario: Punto donde se conecta el cableado horizontal con el cableado de usuario.

51.6.2 INSTALACIONES COMUNES DE TELECOMUNICACIONES

Un proyecto de ICT describe las instalaciones necesarias para poder dotar a un edificio (normalmente un edificio de viviendas) de una infraestructura común de telecomunicaciones. Este proyecto se debe justificar técnicamente mediante los cálculos y especificaciones correspondientes, con el fin de cumplir mínimamente las siguientes funciones:

- Captación, adaptación y distribución de las señales de radiodifusión sonora y televisión terrestres.
- Captación, adaptación y distribución de las señales de radiodifusión sonora y televisión por satélite.
- Acceso al servicio telefónico disponible al público (RTB).

El proyecto también incorpora la infraestructura necesaria que permite al acceso a los servicios de telecomunicaciones de banda ancha que puedan ofrecer los diferentes proveedores.



TEXTO: Registro secundario. Registro terminación de red. Registro de toma. Registro secundario. Punto de entrada general. Punto de terminación de red.

Canalizaciones en una ICT:

- Canalización de enlace superior: conexión entre los elementos de captación de la señal del TDT y satélite (antenas) incluso el RITS.
- Canalización de enlace inferior: conexión entre la arqueta donde se accede a las redes de telefonía (RTB) y datos hasta el RITI.
- Canalización principal: distribución del cableado desde el RITI y el RITS hasta los registros secundarios en cada planta.
- Canalización secundaria: dispersión del cableado desde el registro secundario de la planta hasta los distintos registros de terminación de la red / PAU de los usuarios.
- Canalización interior: cableado interior de la vivienda desde el PAU hasta las tomas.

Puntos principales de una ICT:

- Recinto de instalaciones de telecomunicaciones superior (RITS): recinto dedicado a las telecomunicaciones en exclusiva y situado en la parte superior del edificio, conteniendo normalmente el equipamiento necesario para la recepción / amplificación de la señal de la TDT o de satélite.

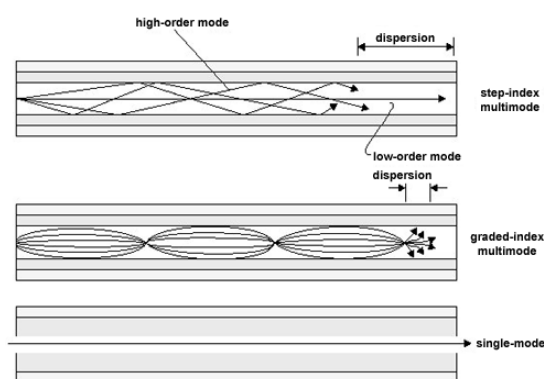
- Recinto de instalaciones de telecomunicaciones inferior (RITI): recinto dedicado a las telecomunicaciones en exclusiva y situado en la parte inferior del edificio, conteniendo normalmente la distribución del cableado para voz y datos hacia las viviendas.
- Registros principales: Registros a los que llegan las distintas canalizaciones de enlace.
- Registros secundarios: Registros existentes en cada planta, a donde llega la canalización principal, y de donde se distribuye la canalización secundaria
- Registro de terminación de red: Registro donde acaba la red de distribución y dispersión del edificio y comienza la del usuario.
- Punto de acceso el usuario (PAU): Punto a donde se conecta la red del usuario.
- Registro de toma: Toma a donde se conectan los equipos finales.

51.6.3 MEDIOS DE TRANSMISIÓN

51.6.3.1 FIBRA ÓPTICA

En general, se distinguen dos tipos de fibras ópticas, multimodo y monomodo, esta clasificación define como la luz viaja en el interior de la fibra:

- Multimodo: En fibras multimodo el núcleo es más grueso (entre 50 y 100 micrómetros) que en las fibras monomodo, haciendo posible que la luz viaje usando varios modos de



propagación (varios caminos). A su vez las fibras multimodo pueden clasificarse en índice escalonado (índice de refracción constante con velocidades de transmisión bajas del orden de 50 Mbps) e índice gradual (índice de refracción no constante con velocidades de

transmisión elevadas del orden de los 1 Gbps). Las fibras multimodo se usan para distancias cortas.

- Monomodo: En este tipo de fibras la luz sólo tiene un camino posible usándose para largas distancias y requiriendo conectores de mejor precisión y dispositivos más caros. El diámetro del núcleo está entre los 7 y los 10 micrómetros. Existen 3 tipos de fibras monomodo: NDSF (No Dispersion-Shifted Fiber), DSF (Dispersion-Shifted Fiber) y NZ-DSF (No Zero-Dispersion-Shifted Fiber).

Algunos de los tipos de fibra óptica son:

- ITU G.651: multimodo índice gradual de 50 micrómetros de núcleo y 125 micrómetros de revestimiento.
- ITU G.652: NDSF con una longitud de onda de 1.130 nm con un alcance de 1000km a 2,5Gbps, 60 Km. a 10Gbps y 3 Km. a 40 Gbps.
- ITU G.653: DSF
- ITU G.655: NZ-DSF. Soportando 2,5Gbps a 6000Km., 10Gbps a 400Km. y 40 Gbps a 25Km.

51.6.3.2 PAR TRENZADO

El tipo de cable más usado para comunicaciones es sin duda el cable de par trenzado, en concreto los cables de 4 pares trenzados con diferentes aislamientos y categorías. Atendiendo a su aislamiento estos cables se dividen en:

- UTP: Unshielded Twisted Pair o par trenzado no blindado. Consiste en 4 pares de hilos en los que cada par está trenzado siguiendo un patrón.
- FTP: Foil/Folded Twisted Pair o par trenzado recubierto. Consiste en un cable UTP que es recubierto con una lámina de aluminio / cobre para mejorar su aislamiento.
- STP: Shielded Twisted Pair o par trenzado blindado. Consiste en 4 pares de hilos en los que cada par aparte de estar trenzado está envuelto en una lámina de cobre o aluminio para mejorar su aislamiento contra interferencias.

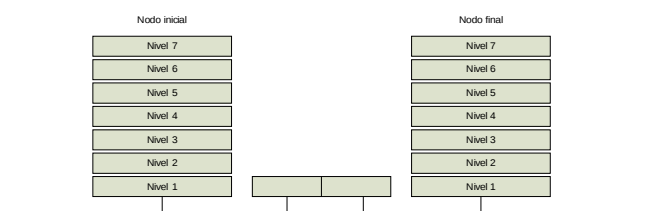
Atendiendo a sus características de transmisión los cables de par trenzado se clasifican en categorías:

Categoría	Frecuencia	Aplicaciones
Cat 1	0,4 MHz	Telefonía
Cat 2	4 MHz	Redes en desuso
Cat 3	16 MHz	Ethernet 10BASE-T y 100BASE-T4
Cat 4	20 MHz	Token Ring 16 Mbit/s
Cat 5	100 MHz	Ethernet 100BASE-TX y 1000BASE-T (no recomendable)
Cat 5e	100 MHz	Ethernet 100BASE-TX y 1000BASE-T
Cat 6	250 MHz	Ethernet 1000BASE-T
Cat 6e	250 MHz	No es un estándar
Cat 6a	500 MHz	Ethernet 10GBASE-T
Cat 7	600 MHz	Ethernet 10GBASE-T (estándar aún por aprobar)
Cat 7a	1000 MHz	Ethernet 10GBASE-T (estándar aún por aprobar)

51.7 ELECTRÓNICA DE RED

51.7.1 REPETIDORES

El repetidor es un elemento que permite la conexión de dos tramos de red y que tiene como función principal regenerar la señal para permitir alcanzar distancias mayores. Normalmente el repetidor recibe la señal desde uno de los segmentos, lo amplifica y lo emite en el otro segmento.

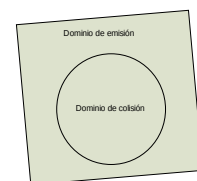


Sus características principales son:

- Es la forma más simple y barata de conectar segmentos de red.
- Se utilizan para superar limitaciones de distancia.
- Sólo valen para conectar topologías de red compatibles.
- No aíslan tráfico ni segmentan la red.

51.7.2 CONCENTRADORES

Un concentrador es un dispositivo que funciona como centro de cableado para una red con topología en estrella. Su función consiste en que el tráfico que llega a cualquiera de sus puertos se propague a través de los demás puertos. Esto crea un medio de red compartido y reúne a las computadoras conectadas a la red en un único dominio de colisión y de difusión, de la misma forma que si estuviesen conectadas a un único cable. Como implicación directa de esto último tenemos que la velocidad de transmisión entre todos los nodos conectados a un concentrador es la misma que entre dos máquinas conectadas por un cable. Los concentradores se pueden apilar o interconectar entre ellos, funcionando como un único concentrador con más puertos, con las mismas ventajas y limitaciones.

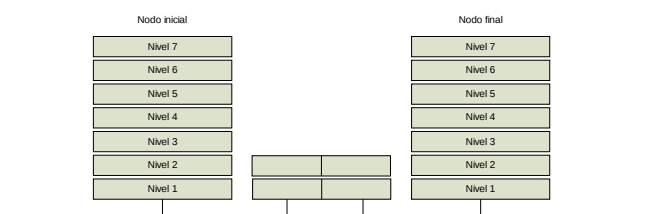


Esto

51.7.3 PUENTES

Un puente es un dispositivo utilizado para conectar segmentos de redes. Opera en el nivel de enlace de datos y es selectivo respecto a los paquetes que pasan a través de él. Frente a los repetidores que trabajan sólo con señales, los puentes trabajan con tramas.

Un puente no transmite datos a los segmentos conectados hasta que llega toda la trama. Por este motivo, dos sistemas que se encuentran en segmentos separados por un puente pueden transmitir a la vez sin que se produzca una colisión. Un puente conecta segmentos de red de tal forma que mantiene en el mismo dominio de difusión pero en distintos dominios de colisión.



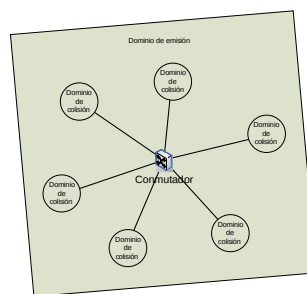
Sus características principales son:

- Pueden aislar el tráfico basándose en la dirección MAC.

- Al igual que los repetidores, los puentes no son direccionables en la red (transparentes para niveles superiores).
- Sólo operan en el nivel MAC de enlace (conectan segmentos de la misma red).
- Extienden la topología de la red (i.e. Anillo-bus)
- Aíslan errores MAC (i.e. Tramas demasiado largas)
- Existen dos tipos:
 - o Transparentes: Conectan topologías de red compatibles (i.e. 10BaseT-10Base2) y no modifican ninguna parte de la trama.
 - o De traslación: Conectan diferentes topologías de red (i.e. 10BaseT-Token Ring) adaptando la trama al protocolo MAC destino.

51.7.4 CONMUTADORES

Un conmutador opera en el nivel de enlace de y es en esencia un puente multipuerto en el cada uno de los puertos es un segmento de independiente. Un conmutador recibe tráfico sus puertos y al contrario que un concentrador, que reenvía el tráfico a través todos los demás puertos, sólo lo reenvía por el puerto necesario para alcanzar su destino.



datos
que
red
por
de

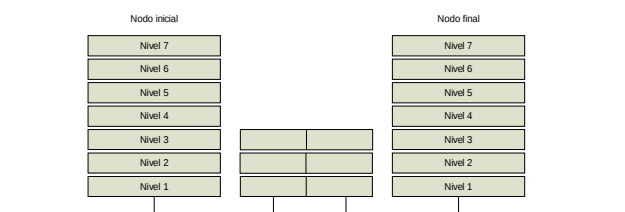
Un sistema conectado a un conmutador posee el equivalente a una conexión dedicada con cada uno de los sistemas restantes conectados al conmutador y con todo el ancho de banda.

Sus principales características son:

- Diseñados para solucionar problemas de rendimiento de LAN (escaseo de ancho de banda, cuellos de botella en la red).
- Alto rendimiento en el envío de paquetes y baja latencia.
- Segmentan un dominio de colisión en otros más pequeños.
- Reduce o casi elimina la contienda por el acceso al medio.

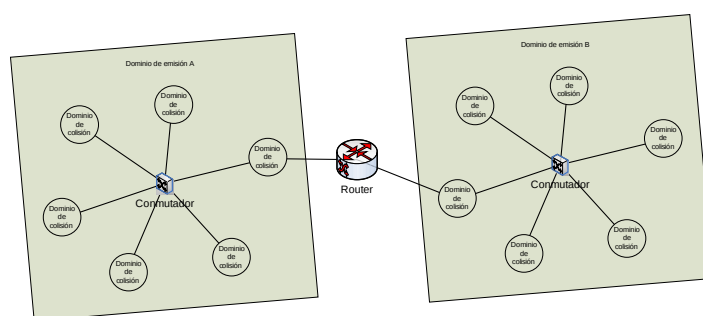
51.7.5 ENCAMINADORES

La labor de un encaminador es la de conectar dos redes completamente independientes en el nivel de red. Los encaminadores son más selectivos que los puentes en el tráfico que pasa entre las redes y son capaces de seleccionar de forma inteligente a ruta más eficiente hacia un destino específico.



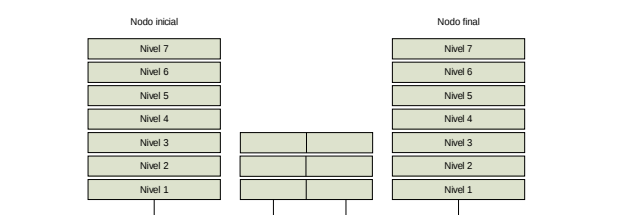
Las funciones básicas de un encaminador son:

- Segmentar la red en dominios individuales de envío (redes aisladas a nivel MAC)
- Proporcionan envío inteligente de paquetes: analizan el tráfico y para cada paquete seleccionan la red que proporciona la mejor ruta hacia el destino. Un paquete puede pasar por varios encaminadores en su camino hacia el destino, cada uno de ellos se conoce como salto. El objetivo suele ser que llegue con el menor número de saltos. Para ello utilizan las llamadas tablas de encaminamiento.
- Proporcionan acceso a las WAN de manera eficiente.
- Soportan caminos redundantes (tolerancia a fallos).
- Proporcionan seguridad / firewall: analizan todo paquete que llega de una de las redes a la que está conectado. Si la dirección de origen y de destino pertenecen a la misma red lo descartan, si no lo reenvían a su destino a través de otra red.



51.7.6 PASARELAS

Una pasarela conecta dos redes distintas que usan protocolos y arquitecturas distintos a todos los niveles. Su función es traducir el protocolo de una red en el protocolo de la otra, pero también pueden conectar redes que usen el mismo protocolo. En este último caso entran las que traducen IP a IP, por ejemplo haciendo NAT (Network Address Translation, que convierte una dirección IP de una red –normalmente una IP personal de una LAN- en otra dirección IP –normalmente en una IP pública- siendo capaz de invertir el proceso).



51.8 BIBLIOGRAFÍA

- Groth, David; Toby Skandier (2005). Network Study Guide
- Andrew S. Tanenbaum. Redes de computadoras. PRENTICE HALL, 1997
- IEEE 802.3™ : ETHERNET
- Real Decreto-ley 1/1998, de 27 de febrero
- La Ley 8/1999, de 6 de abril, de reforma de la Ley 49/1960, de 21 de julio, de Propiedad Horizontal
- El Real Decreto 401/2003, de 4 de abril, que aprueba el Reglamento regulador de las Infraestructuras Comunes de Telecomunicaciones
- La Ley 10/2005, de 14 de junio, de Medidas Urgentes para el Impulso de la Televisión Digital Terrestre, de Liberalización de la Televisión por Cable y de Fomento del Pluralismo

Autor: Matías Villanueva Sampayo

Director de Informática Asociación Provincial de Pensionistas y Jubilados de A Coruña

Colegiado del CPEIG



52. EQUIPAMIENTO HARDWARE. SERVIDORES. PUESTO DE TRABAJO. DISPOSITIVOS PERSONALES.

Tema 52 Equipamiento Hardware. Servidores. Puesto de Trabajo. Dispositivos Personales

ÍNDICE

<i>52.1.1 Arquitecturas hardware.....</i>	<i>2</i>
<i>52.1.2 Componentes básicos hardware de un equipo.....</i>	<i>6</i>
<i>52.1.3 Clases de ordenadores.....</i>	<i>8</i>
<i>52.2.1 Características de un servidor.....</i>	<i>10</i>
<i>52.2.2 Cluster.....</i>	<i>12</i>
52.2.2.1 Clases de clústeres.....	14
52.2.2.2 Componentes de un clúster.....	15
<i>52.2.3 Servidores Blade.....</i>	<i>17</i>
<i>52.4.1 PDA</i>	<i>22</i>
<i>52.4.2 TABLET</i>	<i>24</i>
<i>52.4.3 Smartphones.....</i>	<i>25</i>

52.1.- EQUIPAMIENTO HARDWARE

52.1.1 Arquitecturas hardware

El ordenador se puede ver como un dispositivo electrónico destinado al tratamiento automatizado de la información. Para que un ordenador trate la información es necesario un sistema de información, que ante una entrada, ejecute una serie de instrucciones y devuelva un resultado.

Una arquitectura de ordenador consiste en el diseño, estudio de la estructura, y funcionamiento de un ordenador. Especifica las interrelaciones que deben existir entre los componentes y elementos físicos y lógicos.

Modelos de arquitecturas de ordenadores:

Arquitectura Von Newman:

Consiste en una unidad central de proceso que se comunica a través de un solo bus con un banco de memoria en donde se almacenan tanto las instrucciones del programa, como los datos que serán procesados por éste. Esta arquitectura es la más empleada en la actualidad.

En la memoria se almacenan tanto los datos como las instrucciones que forman el programa, con lo cual el cambio de un programa a otro sólo implica un cambio en el valor de posiciones de memoria.

En la arquitectura de von Newman se produce en la CPU una cierta ralentización debido a que tanto las instrucciones como los datos deben pasar de la memoria a la CPU por un único canal (bus). A este efecto se le conoce como "el cuello de botella de Von Newmann". Esto limita el grado de paralelismo (acciones que se pueden realizar al mismo tiempo), y por lo tanto, el desempeño de la computadora.

En esta arquitectura se asigna un código numérico a cada instrucción. Dichos códigos se almacenan en la misma unidad de memoria que los

datos que van a procesarse para ser ejecutados en el orden en que se encuentran almacenados en memoria. Esto permite cambiar rápidamente la aplicación de la computadora y dio origen a las computadoras de propósito general.

Arquitectura Harvard

Esta arquitectura surgió en la universidad del mismo nombre, poco después de que la arquitectura Von Newman. Al igual que en la arquitectura Von Newman, el programa se almacena como un código numérico en la memoria, pero no en el mismo espacio de memoria ni en el mismo formato que los datos. Por ejemplo, se pueden almacenar las instrucciones en doce bits en la memoria de programa, mientras los datos se almacenan en 8 bits en una memoria aparte.

El hecho de tener un bus separado para el programa y otro para los datos permite que se lea el código de operación de una instrucción, al mismo tiempo que se lee de la memoria de datos los operandos de la instrucción previa. Así se evita el problema del cuello de botella de Von Newman y se obtiene más rendimiento.

La complejidad de esta arquitectura sólo compensa cuando el flujo de instrucciones y de datos es más o menos el mismo. Por eso **no** es ampliamente utilizada en ordenadores de propósito general. Sin embargo, sí se utiliza en algunos casos para construir procesadores de señal (DSP).

Arquitecturas segmentadas

Buscan mejorar el rendimiento realizando paralelamente varias etapas del ciclo de instrucción al mismo tiempo. El procesador se divide en varias unidades funcionales independientes y se dividen entre ellas el procesamiento de las instrucciones.

Si un procesador tiene un ciclo de instrucción sencillo consistente solamente en una etapa de búsqueda del código de instrucción y en otra etapa de ejecución de la instrucción, en un procesador sin segmentación, las dos etapas se realizarían de manera secuencial para cada una de la

instrucciones; por el contrario en un procesador con segmentación, cada una de estas etapas se asigna a una unidad funcional diferente, la búsqueda a la unidad de búsqueda y la ejecución a la unidad de ejecución. Estas unidades pueden trabajar en forma paralela en instrucciones diferentes. Estas unidades se comunican por medio de una cola de instrucciones en la que la unidad de búsqueda coloca los códigos de instrucción que leyó para que la unidad de ejecución los tome de la cola y los ejecute.

La mejora en el rendimiento no es proporcional al número de segmentos debido a que cada etapa no toma el mismo tiempo en realizarse, además de que se puede presentar competencia por el uso de algunos recursos como la memoria principal. Otra razón por la que las ventajas de este esquema se pierden es cuando se encuentra un salto en el programa y todas las instrucciones que ya se buscaron y se encuentran en la cola, deben descartarse y comenzar a buscar las instrucciones desde cero a partir de la dirección a la que se saltó. Esto reduce el desempeño del procesador y aún se investigan maneras de predecir los saltos para evitar este problema.

Arquitectura multiprocesamiento.

Cuando se desea incrementar el rendimiento es necesario utilizar más de un procesador para la ejecución del programa.

Para hacer una clasificación de este tipo de arquitecturas se utiliza la taxonomía de Flynn que se basa en el número de instrucciones concurrentes y en los flujos de datos sobre los que operan:

- *SISD (Simple Instruction Simple Data)*. Computador secuencial que no explota el paralelismo ni en las instrucciones ni en los flujos de datos, por ejemplo, las máquinas con monoprocesador.
- *MISD (Multiple Instruction Simple Data)*. Poco común debido al hecho de que la efectividad de los múltiples flujos de instrucciones suele

precisar de múltiples flujos de datos. Se utilizan en situaciones de paralelismo redundante, como por ejemplo en navegación aérea.

- *SIMD (Simple Instruction Multiple Data)*. Un computador que explota varios flujos de datos dentro de un único flujo de instrucciones para realizar operaciones que pueden ser paralelizadas de forma natural. En esta clasificación entrarían los Procesadores matriciales y los Procesadores vectoriales (aplican un mismo algoritmo numérico a una serie de datos matriciales).
- *MIMD (Multiple Instruction Multiple Data)*. Se tienen múltiples procesadores que de forma sincronizada ejecutan instrucciones sobre diferentes datos. El tipo de memoria que estos sistemas utilizan es distribuida. En esta arquitectura se engloban los sistemas distribuidos, distinguiendo aquellos que explotan un único espacio compartido de memoria (Procesadores superescalares, Multiprocesador simétrico (SMP) y Acceso no uniforme a memoria (NUMA)) de aquellos que trabajan con espacios de memoria distribuida, como los Clusters.
 - o En los sistemas SMP (Simetric Multiprocesesors), varios procesadores comparten la misma memoria principal y periféricos de E/S, normalmente conectados por un bus común. Se conocen como simétricos, ya que ningún procesador toma el papel de maestro y los demás de esclavos, sino que todos tienen derechos similares en cuanto al acceso a la memoria y periféricos y ambos son administrados por el sistema operativo.
 - o Los Clusters son conjuntos de computadoras independientes conectadas en una red de área local o por un bus de interconexión y que trabajan cooperativamente para resolver un problema. Es clave en su funcionamiento contar con un sistema operativo y programas de aplicación capaces de distribuir el trabajo entre las computadoras de la red.

52.1.2 Componentes básicos hardware de un equipo.

Las partes físicas (hardware) que componen un ordenador se pueden esquematizar en las siguientes:

1. **PROCESADOR** también conocido como **CPU** (Central Process Unit). Se encarga de interpretar y ejecutar las instrucciones de los programas, realizando cálculos aritméticos y lógicos con los datos. También es el encargado de comunicarse con las demás partes del sistema.

Internamente está constituida por una colección compleja de circuitos electrónicos. Cuando se incorporan todos estos circuitos en un chip de silicio, a este chip se le denomina microprocesador.

La CPU está compuesta por la unidad aritmética lógica, la unidad de control y los registros del sistema:

- a. Unidad de Control (UC): La función de la unidad de control consiste en leer las instrucciones que residen en la memoria principal, interpretarlas y ejecutarlas dando las oportunas órdenes a la unidad aritmético-lógica y a los restantes elementos del sistema.
- b. Unidad Aritmética Lógica (ALU): Ejecuta las operaciones aritméticas lógicas que le señala la instrucción residente en la unidad de control.
- c. Registros del sistema: Son circuitos que sirven como área interna de trabajo. Almacenan una palabra de bits. Estos circuitos son muy rápidos y forman parte del propio procesador.

Hay que hacer mención especial a los **microprocesadores multinúcleo** que combinan dos o más procesadores independientes en un solo circuito integrado. Un dispositivo de doble núcleo contiene solamente dos microprocesadores independientes. En general, los microprocesadores multinúcleo permiten que un dispositivo computacional exhiba una cierta forma del paralelismo a nivel de

subproceso, también llamado hilo o thread (thread-level parallelism -TLP) sin incluir múltiples microprocesadores en paquetes físicos separados. Esta forma de TLP se conoce a menudo como multiprocesamiento a nivel de chip (chip-level multiprocessing) o CMP.

2. **MEMORIA PRINCIPAL.** Lugar donde se almacenan los datos y las instrucciones de los programas en ejecución, donde se pueden recuperar y grabar en ella datos a través de las dos operaciones básicas definidas sobre ella: lectura o escritura.

Está constituida por celdas o elementos capaces de almacenar 1 bit de información. La memoria se organiza en conjuntos de elementos de un tamaño determinado llamados *palabras de memoria*. A cada palabra le corresponde una dirección única.

Cada palabra es una unidad direccionable en la memoria. El mapa de memoria se corresponde con el espacio de memoria direccionable. Este espacio viene determinado por el tamaño de las direcciones.

3. **BUSES.** Para funcionar el hardware necesita unas conexiones que permitan a los componentes comunicarse entre sí e interaccionar. Estas conexiones se denominan buses o canales. Un bus constituye un sistema común interconectado que coordina y transporta información entre las partes del ordenador.

Un bus se caracteriza por dos propiedades:

- La cantidad de información que puede manipular simultáneamente, llamada “ancho de bus”.
- La rapidez con que puede transferir dichos datos.

Existen tres tipos de buses en un ordenador, en función del tipo de datos que transporten:

- *Bus de Control:* Se encarga de transmitir datos que serán utilizados como órdenes de control.

- *Bus de Direcciones:* Se encarga de transmitir datos que serán utilizados como direcciones de memoria.
- *Bus de Datos:* Se encarga de transportar datos como tales.

El conjunto de estos tres buses forma el **Bus del Sistema**.

4. **PERIFÉRICOS.** Una de las funciones básicas del computador es enviar y recibir datos desde dispositivos externos a la CPU. A estos dispositivos se les conoce con el nombre genérico de periféricos, pudiendo ser de lectura, de escritura y de lectura y escritura.

Los periféricos tienen como hándicap la diferencia entre sus velocidades de transmisión y la velocidad de operación del ordenador. Los periféricos se clasifican según su función en:

- *Dispositivos periféricos de entrada.* Introducen datos e instrucciones en la CPU, por ejemplo: un ratón, un teclado.
- *Dispositivos periféricos de salida.* Permiten ver los resultados, por ejemplo: un monitor, una impresora.
- *Dispositivos periféricos de ENTRADA/SALIDA (E/S).* Tienen comunicación bidireccional con la CPU, por ejemplo, un dispositivo de almacenamiento.

52.1.3 Clases de ordenadores.

A raíz de la evolución de la tecnología, se puede hacer una clasificación no rígida, de los diferentes tipos de ordenadores existentes:

- *Superordenadores:* diseñados especialmente para cálculos que precisen una gran velocidad de proceso. Generalmente están constituidos por un gran número de procesadores que trabajan en paralelo, con lo que consiguen realizar billones de operaciones por segundo.
- *Mainframe:* están diseñados principalmente para dar servicio a grandes organizaciones. Su potencia de cálculo es inferior a los

anteriores, cifrándose la ejecución en millones de operaciones por segundo. Se caracterizan por soportar la conexión de un gran número de terminales. Pueden intervenir en procesos distribuidos en los que se conectan dos o más ordenadores en paralelo.

- *Miniordenadores*: son máquinas de tipo medio, es decir, su capacidad de proceso es inferior a las anteriores y por tanto pueden controlar un número menor de terminales.
- *Microordenadores*: su funcionamiento se basa en el uso de un microprocesador. Proporcionan una serie de prestaciones que, en potencia, manejabilidad, portabilidad, precio, etc., cubren una gama inferior de necesidades informáticas tanto en el ámbito profesional como en el privado. Podemos identificar dos grupos importantes: los ordenadores personales (Personal Computer PC) y las estaciones de trabajo (Workstation).

52.2.- SERVIDORES

Como se observa en el apartado anterior, en la clasificación de los ordenadores no aparece el término servidor. Este término surge originalmente del mundo software debido a la arquitectura cliente/servidor, en la que unos programas denominados *clientes* realizan peticiones a otros programas denominados *servidores* los cuales atienden dichas peticiones realizando las acciones necesarias.

- Un **servidor** se define entonces como un programa que acepta conexiones con objeto de atender peticiones mediante el envío de respuestas.
- Un **cliente** se define como un programa que establece conexiones con el propósito de realizar peticiones.

Este uso dual puede llevar a confusión. Por ejemplo, en el caso de un servidor web, este término podría referirse a la máquina que almacena y maneja los sitios web, y en este sentido es utilizada por las compañías que ofrecen hosting u hospedaje. Alternativamente, el servidor web podría referirse al software, como el servidor de http de Apache, que funciona en la máquina y maneja la entrega de las páginas web como respuesta a peticiones de los navegadores de los clientes.

Debido a la especialización y criticidad de muchos tipos de servidores, el término “Servidor” se utiliza para referirse al ordenador (hardware) donde está instalado el programa que atiende a las peticiones.

Así, un servidor en el ámbito profesional es un ordenador específicamente diseñado para optimizar la ejecución de un determinado programa servidor o un conjunto de ellos.

Lógicamente este hardware específico necesita un sistema operativo (SO) personalizado para ejecutar programas servidores, siendo habitual que las compañías proporcionen SO para usuario final (Windows 7, Ubuntu Desktop) y SO para servidores (Windows 2008 Server R2, Ubuntu Server...).

52.2.1 Características de un servidor

Existen factores como la fiabilidad, el rendimiento o el coste que determinan el tipo de servidor (hardware) que se requiere para albergar un software servidor. Así se puede tener en un mismo servidor hardware varios programas servidores, o bien se puede tener un servidor hardware por cada programa servidor.

Desde este punto de vista, cualquier computador que albergue un determinado software servidor podría ser considerado un servidor. Sin embargo, las máquinas que se diseñan con el propósito de albergar programas servidores tienen una serie de características particulares que hace necesario emplear hardware especializado, orientado a una alta fiabilidad y rendimiento.

- Tienen que procesar numerosas peticiones de clientes en un tiempo corto, por eso necesitan CPUs con velocidades altas de procesamiento. Si por características de la aplicación se requiere una gran cantidad de procesamiento, es más recomendable añadir más CPUs para trabajar en paralelo, en lugar de aumentar la velocidad de una única CPU, por cuestiones de redundancia y fiabilidad.
- Si el servidor recibe peticiones concurrentemente es necesario que cuente con una cantidad de memoria principal o RAM elevada que le permita abrir threads y atender de forma adecuada a los clientes.
- Los buses por los que circula la información dentro del servidor tienen que ser de alto rendimiento para no provocar cuellos de botella.
- Algunos tipos de servidores (ficheros y bases de datos sobre todo) necesitan una tecnología de almacenamiento altamente eficiente siendo normal encontrar dos tipos de tecnologías distintas:
 - o SAN (Storage Area Network). Es una red especializada que permite un acceso rápido y confiable entre servidores y recursos de almacenamiento independientes o externo. De esta forma un dispositivo de almacenamiento no es propiedad exclusiva de un servidor, sino que los dispositivos de almacenamiento son compartidos entre todos los servidores de la red como recursos individuales. Esta arquitectura implica disponer de una infraestructura de red de alta velocidad dedicada sólo para Almacenamiento y Backup, optimizada para mover grandes cantidades de datos, y consistente en múltiples recursos de almacenamiento geográficamente distribuidos.
 - o NAS (Network Attached Storage). Los dispositivos NAS son dispositivos de almacenamiento a los que se accede a través de protocolos de red.

Los dispositivos NAS utilizan usualmente más de un dispositivo de almacenamiento, en la mayoría de los casos están compuestos por RAIDs (Redundant Arrays of Independent Disks) de discos lo que aumenta la capacidad de almacenamiento, la seguridad, y la velocidad de acceso a la información.

- Los servidores están preparados para ofrecer servicios con un grado de disponibilidad de más del 99%. Esto implica:
 - o Que está encendido las 24 horas del día, con lo que es necesario un sistema de refrigeración adecuado. Para ello se ubican en Centros de Procesos de Datos donde existe la temperatura y humedad óptimas de funcionamiento.
 - o Que tienen que contar con Sistemas de Alimentación Ininterrumpida para evitar que un corte eléctrico los deje indisponibles.
 - o Que es necesario utilizar componentes **hot swap**, son componentes que se pueden sustituir “en caliente sin parar el servidor”. Esto tiene especial importancia con servidores críticos que no pueden estar parados por una acción planificada. Los componentes **hot swap** más comunes son:
 - Los discos duros configurados en RAID
 - Las fuentes de alimentación
- Los servidores pueden estar ubicados en armarios RACKs o no. La configuración de servidores en RACKs es modular permitiendo agregar o quitar componentes con más facilidad (añadir una cabina de cintas de backup, una nueva fuente de alimentación o un nuevo servidor).

52.2.2 Cluster

Un clúster es un tipo de computador distribuido o paralelo que consiste en un grupo de computadoras interconectadas que trabajan conjuntamente en

la solución de un problema. Estos sistemas constituyen una solución flexible, de bajo coste y de gran escalabilidad para aplicaciones que requieren una elevada capacidad de cómputo y memoria.

La tecnología de clústeres ha evolucionado en apoyo de actividades que van desde aplicaciones de supercómputo y software de misiones críticas, servidores Web y comercio electrónico, hasta bases de datos de alto rendimiento, entre otros usos.

Los clústeres ofrecen las siguientes características:

- *Alto rendimiento:* diseñados para dar altas prestaciones en cuanto a capacidad de cálculo y velocidad de proceso.
- *Alta disponibilidad:* diseñados para garantizar la total y absoluta disponibilidad del servicio en el tiempo ofreciendo un funcionamiento ininterrumpido. Todas las máquinas de este clúster están sincronizadas y monitorizadas entre sí. Si se produce un fallo en alguna de las máquinas del clúster, se detecta dicho fallo automáticamente y las otras máquinas asumen las funciones y siguen funcionando manteniendo así la disponibilidad del sistema el software. Son tolerantes a fallos.
- *Balanceo de carga:* Un clúster estará compuesto por uno o más nodos que actúan como *frontend* del clúster, y que se ocupan de repartir las peticiones de servicio que reciba el clúster a otros ordenadores del clúster que forman el *backend* de éste, evitando así los cuellos de botella.
- *Escalabilidad:* Es relativamente asequible aumentar un nodo en un sistema cluster.

Un clúster de servidores tiene principalmente dos ventajas considerables sobre las soluciones de servidores estándar:

- Garantizan la alta disponibilidad de servicios y datos.

- Permite aprovechar al 100% la capacidad de los nodos introducidos (no hay nodos en stand-by).

52.2.2.1 Clases de clústeres

La forma en que operará el clúster está determinada por la función que éste deberá desempeñar:

- Clúster de Alto Rendimiento: diseñado para dar altas prestaciones en cuanto a capacidad de cálculo. Existen distintas aplicaciones que se les puede dar a este tipo de clúster, entre las cuales encontramos: cálculos matemáticos, renderizaciones de gráficos, compilación de programas, descifrado de códigos.
- Clúster de Alta Disponibilidad: están diseñados para garantizar el funcionamiento ininterrumpido de ciertas aplicaciones. La idea principal de este tipo de clúster es proporcionar un servicio ininterrumpido las 24 horas del día, los 7 días de la semana.

Están formados por un conjunto de dos o más máquinas que comparten los discos de almacenamiento de datos, y se monitorizan mutuamente. Si se produce un fallo del hardware o de las aplicaciones de alguna de las máquinas del clúster, el software de Alta Disponibilidad es capaz de rearrancar automáticamente los servicios que han fallado en cualquiera de las otras máquinas del clúster. Y cuando la máquina que ha fallado se recupera, los servicios son nuevamente migrados a la máquina original.

- Clúster de Alta Eficiencia: Son clústeres cuyo objetivo de diseño es el ejecutar la mayor cantidad de tareas en el menor tiempo posible. Existe independencia de datos entre las tareas individuales.

Los clúster de alta eficiencia y alta disponibilidad suelen utilizarse para entornos empresariales y esta funcionalidad solamente puede ser efectuada por hardware especializado, mientras que los clúster de alto rendimiento son propios de universidades y centros de cálculo.

52.2.2.2 Componentes de un clúster

Para que un clúster funcione como tal, no basta sólo con conectar entre sí los ordenadores, sino que es necesario proveerlos de un sistema de manejo del clúster, el cual se encargue de interactuar con el usuario y los procesos que corren en él para optimizar el funcionamiento. Es decir que, para poder funcionar, requiere tantos componentes hardware como software.

- **Nodos.** Son los ordenadores en sí mismos, existiendo ordenadores personales, sistemas multi-procesador o estaciones de trabajo (workstations). Pueden ser:
 - o *Dedicados:* su uso está exclusivamente dedicado a realizar tareas relacionadas con el clúster.
 - o *No dedicados:* su uso no está exclusivamente dedicado a realizar tareas relacionadas con el clúster, utilizándose los ciclos de reloj del computador cuando éste no se utiliza.
- **Almacenamiento.** Puede consistir en una NAS, una SAN, o almacenamiento interno en el servidor. El protocolo más comúnmente utilizado es NFS (Network File System), sistema de ficheros compartido entre servidor y los nodos. Sin embargo existen sistemas de ficheros específicos para clústeres como Lustre (CFS) y PVFS2.
- **Red de interconexión.** Se utilizan Redes de Alta Velocidad como solución de alto rendimiento para que las comunicaciones no sean el cuello de botella del rendimiento del sistema.

Las redes de interconexión son un componente fundamental de los clústeres que proporcionan: alto ancho de banda, baja latencia, fiabilidad y escalabilidad.

Las redes de interconexión comunes en clúster son:

- o Ethernet: Estándar de redes de computadoras de área local con acceso al medio por contienda CSMA/CD.

- o Fast Ethernet: Serie de estándares de IEEE de redes Ethernet de 100 Mbps (megabits por segundo).
 - o Gigabit Ethernet: Ampliación del estándar Ethernet que consigue una capacidad de transmisión de 1 gigabit por segundo.
 - o SCI (Scalable Coherent Interface): Estándar de interconexión de redes de alta velocidad utilizado para multi-procesamiento con memoria compartida y paso de mensajes.
 - o ATM (Asynchronous Transfer Mode): Tecnología de telecomunicación desarrollada para hacer frente a la gran demanda de capacidad de transmisión para servicios y aplicaciones.
 - o Myrinet: Red de interconexión de clústeres de altas prestaciones. El procesamiento de las comunicaciones de red se hace a través de chips integrados en las tarjetas de red de Myrinet (Lanai chips), descargando a la CPU de gran parte del procesamiento de las comunicaciones.
 - o HIPPI (High Performance Parallel Interface): Bus para conexiones de alta velocidad para dispositivos de almacenamiento en superordenadores. Ha sido sustituido progresivamente por otras tecnologías más rápidas.
 - o FiberChannel: Tecnología de red utilizada principalmente para redes de almacenamiento, disponible primero a la velocidad de 1 Gbps y posteriormente a 2, 4 y 8 Gbps.
 - o Infiniband: Es una red surgida de un estándar desarrollado específicamente para realizar la comunicación en clústeres. La conexión básica es de 2Gbps efectivos y se podrían alcanzar los 96Gbps.
- **Sistema Operativo.** Tiene que ser multiproceso y multiusuario.

- **Middleware.** Actúa entre el sistema operativo y las aplicaciones, recibiendo los trabajos entrantes al clúster y redistribuyéndolos de manera que el proceso se ejecute más rápido y el sistema no sufra sobrecargas en un servidor determinado. Está compuesto de dos subniveles de software:
 - o *SSI (Single System Image):* ofrece a los usuarios un acceso unificado a todos los recursos del sistema.
 - o *Disponibilidad del sistema:* que permite servicios como puntos de chequeo, recuperación de fallos, soporte para tolerancia a fallos.

52.2.3 Servidores Blade

Blade Server es una arquitectura que ha conseguido integrar en tarjetas todos los elementos típicos de un servidor. Cada servidor blade es una tarjeta (llamada *blades*) que contiene la memoria RAM, el disco duro y la CPU. Los servidores blade en tarjetas se insertan en un chasis que se coloca en un rack estándar ocupando entre 4U y 6U dentro del rack, permitiendo albergar un máximo de 16 servidores blade en un chasis. Este chasis, a su vez integra y permite compartir los elementos comunes como son:

- La ventilación y la refrigeración.
- Los switches de red redundante con el cableado.
- Las fuente de alimentación y el SAI tipo hot swap.
- Interfaces de almacenamiento.

Al estar todo integrado en el chasis se consigue reducir el consumo eléctrico, cableado, sistemas de enfriamiento y el espacio dentro del rack.

Las empresas que requieren de la actualización de sus sistemas se enfrentan al problema de consumo eléctrico, espacio, control de

temperatura y ubicación de los nuevos equipos. Tradicionalmente, hasta la llegada de los servidores Blade, el método para incrementar nuevos requerimientos era agregar más servidores en rack, lo que ocupa más espacio, complica el cableado, hace más compleja la gestión de administración de los sistemas, consume más recursos, etc.

La tecnología blade supone un diseño más eficiente en cuanto a coste y espacio. Para ello se ha reducido el chasis, se ha bajado el consumo, simplificado el cableado y el mantenimiento, mientras se incrementan las funcionalidades.

Estos son los principios básicos en los que se fundamenta la arquitectura blade y que al final proporciona una reducción del coste total.

Diferencias entre un sistema de servidores montados en rack y blade server

La principal diferencia es que en un sistema montado en rack, el servidor es una unidad completa en sí mismo. Esto significa que contiene la CPU, memoria, fuente de alimentación, ventiladores y disipadores. Estos servidores son atornillados en el rack, y cada uno es conectado a la red corporativa usando un cable separado.

Los blade servers son una versión compacta de sistemas montados en rack. El blade incluye una CPU, memoria y dispositivos para almacenar datos. Pero no tiene fuente de alimentación eléctrica ni ventiladores. Los blades son insertados en slots y enlazados entre sí gracias a un bus de alta velocidad dentro del chasis.

Ventajas

- Reduce la gestión gracias a su infraestructura simplificada.
- Comparte fuentes de alimentación y ventiladores y una gestión del sistema centralizada disminuyendo costes porque requieren menos electrónica y consumen menos energía.

- El chasis elimina la mayoría del cableado que se encuentra en los sistemas montados en rack.
- Intercambio en caliente (Hot-Swap): si un blade falla puede ser reemplazado sin ningún impacto en los otros blades.
- Facilitan la gestión y reducen tiempo y coste administrativo al estar todos los servidores en un sólo equipo.
- Se reduce el espacio al integrar en un sólo chasis muchos servidores, sin reducir poder de cómputo.
- Escalabilidad horizontal: porque nos ofrece ampliar el número de servidores fácilmente a medida que va creciendo la demanda.
- Alta disponibilidad, pues la mayoría de los equipos poseen elementos redundantes que garantizan el funcionamiento continuado de los servidores sin interrupciones.

52.3.- PUESTO DE TRABAJO

Lo más habitual en cualquier empresa es que en el puesto de trabajo exista un microcomputador, es decir, o bien un PC o una estación de trabajo (en inglés workstation). El concepto de PC u ordenador personal es ampliamente aceptado.

Una Workstation es un microordenador de altas prestaciones especialmente diseñado para niveles de alto rendimiento en ciertas tareas, como pueden ser, diseño gráfico, edición de video, gestión de redes de Internet, aplicaciones de alto consumo, etc. Estos potentes ordenadores han encontrado su sitio en la ingeniería y desarrollo de software entre otras cosas, debido a su habilidad multitarea.

En la actualidad los PCs son bastantes potentes en cuanto a memoria y capacidad de procesamiento. Sin embargo, el hardware de las estaciones

de trabajo está optimizado para situaciones que requieren un alto rendimiento y fiabilidad, mucha cantidad de memoria, computación de multitarea, etc. donde generalmente se mantienen operativas en situaciones en las cuales cualquier computadora personal tradicional dejaría rápidamente de responder.

Los profesionales cuando escuchan la palabra estación de trabajo, piensan que es una máquina que no necesitan y que tiene un coste muy superior a las expectativas. La realidad es que eso ha cambiado, especialmente en todo lo relativo al factor precio, y ahora, con una inversión mínima, un profesional puede, gracias a una estación de trabajo, obtener hasta un 50 por ciento más de rendimiento en sus tareas diarias.

Existen profesionales que se compran un PC potente, con más de 2 GB de memoria, con una tarjeta gráfica de alto nivel, con alta capacidad de memoria interna, etc. porque necesitan trabajar con aplicaciones de software. Lo hacen porque no conocen la existencia de las estaciones de trabajo pero, sobre todo, porque no saben las diferencias que tienen con un PC y las funcionalidades y ventajas que pueden ofrecerle. Un PC, por ejemplo, en el apartado de memoria, llega hasta donde llega y ahí surgen los problemas. Existen estaciones de trabajo que puede alcanzar los 128 GB de memoria, cinco discos duros, biprocesadores, etc.

Las principales aplicaciones de una Workstation son:

- CAD (Computer Aided Design, Diseño Asistido por Ordenador): destinadas al diseño y análisis de sistemas de ingeniería y arquitectura.
- AEC (Architecture Engineering Construction): aplicables a la edición de planos de construcción y arquitectura, elaboración de presupuestos y seguimientos de obras.

- CAM (Computer Aided Manufacturing): aplicables en el diseño, análisis y prueba de circuitos integrados, tarjetas y otros sistemas electrónicos.
- CASE (Computer Aided Software Engineering): ayuda a la gestión completa de los ciclos de vida de los desarrollos de aplicaciones lógicas.
- GIS (Geographic Information System): para edición, captura y análisis de información sobre determinadas zonas geográficas, con base en referencias de mapas digitalizados.
- Sistemas expertos: basados en técnicas de programación de inteligencia artificial, para aplicaciones tales como detección electrónica de errores, funciones de diagnóstico o configuración de ordenadores.
- Aplicaciones empresariales: investigación cuantitativa, seguridad, simulación de análisis reales...
- Edición electrónica: creación para su posterior publicación de periódicos, revistas, presentaciones y documentación en general.
- Telecomunicaciones: gestión de redes, desarrollo de aplicaciones de telecomunicaciones basadas en inteligencia artificial, aplicaciones de apoyo a la investigación y desarrollo (I+D), edición electrónica y procesado de imágenes.
- Las estaciones de trabajo también pueden ser utilizadas como pasarelas (gateways), para acceder a grandes ordenadores, y para ejecutar remotamente utilizando protocolos de comunicaciones.

52.4.- DISPOSITIVOS PERSONALES

52.4.1 PDA

Una PDA (Personal Digital Assistant) es un ordenador de bolsillo diseñado como una agenda electrónica, pero que actualmente poseen una potencia razonable y son capaces de realizar numerosas funciones más allá de las de mera agenda electrónica constituyéndose como una extensión misma del ordenador personal, que podremos sincronizar con éste.

Otros términos asociados son palmtop y handhelds. Un palmtop es un ordenador pequeño que literalmente coge en la palma de la mano. Un handheld es un ordenador sumamente pequeño que se puede sostener con la mano.

Los términos PDA, palmtop y handhelds surgieron para cubrir necesidades diferentes. Actualmente la división entre ambas es muy difusa; ambos términos se utilizan indistintamente.

Las tecnologías de comunicaciones inalámbricas (Bluetooth, Wi-Fi, IrDA (infrarrojos), GPS...) permiten que con una PDA se pueda consultar el correo electrónico, usarlos como navegador GPS o para temas relativos a la domótica.

Pero más allá de las funciones y software con las que viene equipado la PDA, lo que lo hace verdaderamente potente es la posibilidad de personalización casi ilimitada al permitir cargar las aplicaciones “bajo demanda”.

Características:

- Tienen un tamaño físico muy reducido para que quepa en la mano.
- Son bastantes ligeros para que sea fácil su transporte en un bolsillo.
- La pantalla es táctil ocupando gran parte del dispositivo y dejando poco espacio para ubicar botones hardware. No suelen disponer de

un teclado con botones (salvo algunos dispositivos) por lo que para agregar texto se utiliza un teclado virtual o se le añade un teclado externo por USB.

- Tienen capacidad multimedia, ya que integran altavoz, micrófono y grabadora de voz.
- Disponen de conexión de periféricos: para dispositivos de almacenamiento externo y para módulos de expansión.
- Amplio soporte de conexiones inalámbricas: Bluetooth, infrarrojos, Wi-fi.
- Funcionamiento con baterías de Litio-ion.
- Capacidad de almacenamiento por encima de los 64 MB que se puede ampliar mediante el uso de tarjetas de memoria Flash.
- La sincronización con los ordenadores personales permite la actualización del directorio, haciendo que la información del computador y de la PDA sea la misma. La sincronización también evita la pérdida de la información almacenada en caso de que el accesorio se pierda, sea robado o destruido.
- Utilizan sistemas operativos específicos como son Windows Mobile, HP webOS, Linux.

Limitaciones:

- Potencia de computación reducida, debido a que los microprocesadores tienen que tener en cuenta la duración de las baterías, el sobrecalentamiento, etc.
- Capacidad de almacenamiento, aunque hoy en día con tarjetas de memoria de varios GB es una limitación menor.
- Baja duración de las baterías.
- Comunicaciones.

- Software específico.

52.4.2 TABLET

El Tablet es un ordenador portátil de tamaño reducido, con pantalla sobre la cual el usuario puede escribir usando un lápiz especial (el stylus). El texto manuscrito es digitalizado mediante reconocimiento de escritura. El lápiz también se utiliza para moverse dentro del sistema y utilizar las herramientas y funciones de las Tablet

El Tablet combina la potencia de un ordenador portátil con la comodidad de un PDA.

En función de si disponen o no de teclado se distinguen:

- Tablet “Slate”: no dispone de teclado y es necesario utilizar un lápiz o los dedos para manipularlo.
- Tablet “Convertible”: posee un teclado. Puede ser deslizable para poder deslizarse debajo de la pantalla o de modo que la pantalla pueda girar.

Características:

- Los microprocesadores empleados en estos dispositivos están basados en soluciones para móvil.
- Para el almacenamiento se suelen utilizar discos EIDE convencionales pero de 2,5” (más finos).
- La memoria que suelen utilizar es SODIMM (small online DIMM), especiales para laptop e impresoras.
- Pantalla táctil.
- Nuevas formas de control mediante voz y escritura manual.

52.4.3 Smartphones

Estos dispositivos hacen las funciones de un teléfono móvil convencional, pero están dotados de una mayor versatilidad, ya que también incluyen algunas de las funciones de un ordenador personal. En la actualidad todos ellos tienen en común un conjunto amplio de características, como una pantalla táctil de gran formato, conectividad WiFi, Bluetooth, 3G... No obstante, existen otros importantes parámetros que conviene tener en consideración:

Pantalla

Es un componente de extrema importancia debido a que las pantallas táctiles de los smartphones son la interfaz directa de comunicación entre el usuario y el propio dispositivo.

Existen dos tecnologías aplicables a estas superficies táctiles:

- Las capacitivas: es la más adecuada para facilitar la interacción directa con el dedo en lugar de los habituales stylus, ya que para que respondan al instante basta con deslizarlo, por lo que el usuario no necesita ejercer ningún tipo de presión sobre la superficie. Además, pueden detectar varias pulsaciones de manera simultánea, por lo que la experiencia para el usuario es más atractiva que en el caso de las resistivas.
- Las resistivas: están formadas por varias capas, por lo que cuando las presionamos entran en contacto. Esto produce un cambio de corriente, facilitando, de este modo, la detección de la pulsación. Por esta razón, la experiencia de usuario en este caso parece ser menos atractiva que en el anterior, ya que la respuesta del dispositivo es algo más lenta, o al menos es la sensación que puede brindarnos.

Sistema operativo

El funcionamiento de un S.O. afecta directamente al rendimiento del dispositivo, la usabilidad de su interfaz y las funcionalidades que ponen a disposición de los usuarios.

Actualmente el S.O. que se implanta en un Smartphone ha adoptado tanta trascendencia como el equipo mismo. A tal punto que se habla, de **“Smartphones Android”**, para referirse a los teléfonos que funcionan a través de este desarrollo de **Google**. Por lo tanto, la elección del sistema es casi tan importante como la de un smartphone en sí. Hay que tener en cuenta que además estos S.O. también se utilizan en los tablets, por ejemplo el iOS de Apple se encuentra en su smartphone iPhone y en su tablet iPad, el HP webOS se implanta en los smartphones PalmPre y en su tablet TouchPad, etc. A continuación se exponen los S.O. más relevantes en el mercado:

- **HP webOS** es un sistema operativo multitarea basado en Linux, desarrollado por Palm, Inc., ahora propiedad de Hewlett-Packard Company. Cabe destacar que usa tecnologías web como HTML5, JavaScript y CSS y soporta Flash.

webOS incluye una característica llamada "Synergy" que permite conectar el sistema con numerosos servicios de redes sociales e integrar información de varias fuentes.

webOS hace uso del cloud computing para la sincronización de datos

- **Android**. es un sistema operativo multitarea basado en Linux no sólo en su núcleo, sino también en su concepto: de código abierto y gratuito. Esto significa que cualquier fabricante que desee podrá instalar Android en sus equipos posibilitando que el sistema esté disponible en una amplia gama de smartphones. Fue diseñado originalmente para dispositivos móviles, tales como teléfonos inteligentes, tablets, pero que actualmente se encuentra en desarrollo para usarse en netbooks y PC.

El *Android Market* es un catálogo de aplicaciones que pueden ser descargadas e instaladas en dispositivos Android sin la necesidad de un PC

- **BlackBerry OS** es un sistema operativo móvil desarrollado por Research In Motion para sus dispositivos BlackBerry. Al comienzo de su andadura los BlackBerry estuvieron orientados al público corporativo, pero tras la aparición del iPhone se abrió al uso personal (al igual que muchos smartphones). La interfaz más cómoda para usar un BlackBerry es el teclado físico, que no es sólo un accesorio como en otros smartphones sino que es la llave para acceder a todas las funcionalidades.
- **Windows Phone** es un sistema operativo móvil desarrollado por Microsoft, como sucesor de la plataforma Windows Mobile.[2] Está pensado para el mercado de consumo generalista en lugar del mercado empresarial[3] por lo que carece de muchas funcionalidades que proporciona la versión anterior

El Hub Marketplace es el lugar en el que se pueden comprar y descargar todo tipo de contenido como aplicaciones, música, películas, programas de TV, podcast.

- **iOS** es el sistema operativo móvil de Apple desarrollado originalmente para el iPhone, siendo después usado en el iPod Touch e iPad. Se dice que es un SO que marca tendencias. En la última versión del SO (iOS 4) se soporta la multitarea. Uno de los aspectos más criticados es su falta de soporte para Flash.

La interfaz de usuario de iOS se basa en el concepto de manipulación mediante gestos multitáctil. Los elementos de la interfaz se componen por deslizadores, interruptores y botones. La respuesta es inmediata y se provee de una interfaz fluida. La interacción con el sistema operativo se realiza mediante gestos como deslizar, tocar y pellizca

El App Store de Apple es donde se pueden comprar y descargar contenidos. Fue pionera en ese aspecto.

La carga de las aplicaciones se realiza casi instantáneamente, brindando fluidez al desempeño general del teléfono.

- Otros sistemas operativos: Bada, Meego, Symbian, etc.

52.5.- BIBLIOGRAFÍA

- John L. Hennessy, David A. Patterson Computer architecture : a quantitative approach, Elsevier, Morgan Kaufmann, 2007.
- Carl Hamacher, Zvonko Vranesic and Safwat Zaky. Organización de Computadores, 5ª edición. Ed. Mc Graw Hill, 2002.
- PCWORD Marzo 2010.
- <http://es.wikipedia.com>

Autor: Francisco Javier Rodriguez Martínez

Subdirector de Sistemas Escola Superior Enxeñaría Informática Ourense

Colegiado del CPEIG

53. CONCEPTO, EVOLUCIÓN Y TENDENCIAS DE LOS SISTEMAS OPERATIVOS. SISTEMA OPERATIVO UNIX- LINUX. SISTEMA OPERATIVO WINDOWS.

Tema 53. Concepto, evolución y tendencias de los sistemas operativos. Sistema operativo UNIX-LINUX. Sistema operativo Windows

ÍNDICE

53.1.1 Concepto.....	1
53.1.2 Evolución de los Sistemas Operativos.....	4
53.1.3 Clasificaciones de los Sistemas Operativos.....	7
53.1.4 Estructura de los Sistemas Operativos.....	8
53.1.5 Funciones de un Sistema Operativo.....	10
53.1.6 Tendencias.....	11
53.2.1 Características.....	14
53.2.2 Arquitectura de Unix-Linux.....	16
53.2.3 Gestión de procesos.....	17
53.2.4 Gestión de memoria.....	18
53.2.5 Gestión de E/S.....	20
53.2.6 Gestión de archivos.....	22
53.3.1 Características.....	24
53.3.2 Arquitectura de Windows.....	26
53.3.3 Gestión de procesos.....	27
53.3.4 Gestión de memoria.....	29
53.3.5 Gestión de E/S.....	31
53.3.6 Gestión de archivos.....	32
53.3.7 Seguridad.....	35

53.1.- SISTEMA OPERATIVO.

53.1.1 Concepto

Se puede definir un sistema operativo (S.O.) como un conjunto de programas que controlan directamente los recursos hardware (HW) o físicos de un ordenador (CPU, memoria principal y periféricos) proporcionando una máquina virtual que oculta los detalles físicos de la máquina y ofrece al hombre un entorno más amigable. El sistema operativo es la capa de

software más baja de un ordenador. Cada capa oculta a las capas superiores ciertos detalles de las capas inferiores. De esta forma se construye el software, basándonos en lo que ya existe

El sistema operativo tiene una serie de funciones, que se pueden agrupar en 3:

1. Inicializar la máquina. Prepara la máquina para el funcionamiento. Hay 2 formas de inicialización:

- a) TOTAL: Inicialización de todas las funciones y servicios que la máquina puede ofrecer. Por ejemplo, MS-DOS tiene inicialización total.
- b) PARCIALMENTE: Se va a ser selectivo con los tipos de servicios que se inician. Por ejemplo, Linux y Windows.

La principal ventaja/utilidad de la inicialización parcial es la recuperación de la máquina ante fallos: consiste en que si falla un servicio de la máquina no hace falta apagar toda la máquina, sólo hay que lanzar de nuevo el servicio.

2. Servir de máquina virtual. Se ocultan detalles de hardware proporcionando un entorno más amigable. Esto tiene 2 objetivos:

- a) La SEGURIDAD: En lugar de que el usuario acceda directamente a un recurso HW, lo hace el S.O. para que no se produzcan operaciones no deseadas, también llamadas operaciones peligrosas: operaciones de entrada/salida (E/S), operaciones de acceso a memoria.

El HW tiene dos formas de actuar: modo supervisor y modo usuario.

Todos los programas actuarán en modo usuario hasta el momento en que haya que acceder al HW; será entonces cuando cambia a modo supervisor para evitar las operaciones que puedan causar problemas. Se generará una interrupción al realizarse una de estas operaciones susceptibles de fallo. Esa interrupción la coge el sistema operativo y actúa en consecuencia. El

sistema operativo tomará el control del hardware y realizará la operación que se le indica.

Una interrupción es una señal física que generan los dispositivos del sistema y que la trata el sistema operativo.

Al conjunto de interrupciones se le llama **interface interna** del sistema operativo.

- b) **ABSTRACCIÓN**: Se abstraen las características físicas y reales de la máquina ofreciendo una serie de servicios incluso mayores de los que puede ofrecer la propia máquina. Por ejemplo para trabajar con ficheros se utilizan nombres, pero el ordenador no utiliza esos nombres para referirse a ellos; emplea una dirección.

La E/S: cuando tecleamos un dato lo vemos en pantalla tal como lo hemos imaginado, aunque realmente para la máquina son unos y ceros.

Esto constituye la **interface externa** del S.O., el lenguaje con el que nos vamos a comunicar con él. Se denomina SHELL.

Por tanto, tenemos 2 tipos de interface:

- La externa: forma de comunicación entre nosotros y el ordenador; a través de comandos/órdenes (abstracción).
- La interna: forma de comunicación del sistema operativo con el hardware (modo supervisor).

3. Administrar los recursos para su funcionamiento. Esta administración tiene que cumplir 3 características:

- tiene que ser **CORRECTA**: si hay 2 procesos que quieren acceder a un recurso, hay que darle acceso primero a uno y luego a otro, pero no mezclarlos.
- tiene que ser **JUSTA**: si tenemos 2 procesos hay que darle salida a los dos; un proceso no puede monopolizar.

- tiene que ser EFICIENTE: para mejorar el rendimiento del sistema.

Por último decir que un S.O. tiene que tener estas 2 características:

- DETERMINISMO: si se repite la misma operación con los mismos datos de entrada debemos obtener los mismos resultados.
- INDETERMINISMO: en el sentido de que tiene que responder oportunamente a las interrupciones, es decir, no sabe qué interrupción va a llegar primero, no conoce el orden pero debe saber tratarlas.

53.1.2 Evolución de los Sistemas Operativos

Los sistemas operativos han evolucionado en paralelo al desarrollo del HW. Conforme el HW iba incorporando nuevas capacidades, los S.O. debían adaptarse para permitir gestionar eficientemente esas nuevas capacidades.

La evolución de S.O. puede organizarse en generaciones con algunas características comunes:

Primera Generación

Abarca desde 1945 a 1955. Se caracteriza porque no existía un sistema operativo. Eran los propios diseñadores de las máquinas los que las programaban a través de cableado, y las manejaban.

Segunda Generación

Desde 1955 a 1965. En el campo del hardware aparece el transistor. Se empiezan a utilizar las tarjetas perforadas. Se distinguen 2 tipos de sistema operativo:

- Monitor Residente: el S.O. se limitaba a cargar los programas a memoria, leyéndolos de tarjetas perforadas, y ejecutarlos. El problema era encontrar una forma de optimizar el tiempo entre la retirada de un trabajo y el montaje del siguiente.
- Trabajo por lotes: se utilizan las cintas magnéticas. Como solución para optimizar el tiempo de montaje surgió la idea de agrupar los

trabajos en lotes, en una misma cinta o conjunto de tarjetas, de forma que se ejecutaran uno a continuación de otro sin perder apenas tiempo en la transición. En la memoria del ordenador existen dos ítems: a) el monitor de lotes: indicando qué trabajo se está ejecutando y b) el trabajo actual.

Estos dos tipos de sistema operativo se caracterizan por:

- No existe ningún planificador (el que decide qué trabajo se va a realizar): la razón de su inexistencia es que no es necesario, ya que sólo hay un trabajo en memoria principal
- Tampoco existe un reloj (mide el tiempo que un trabajo está ocupando la CPU): no es necesario porque sólo hay un proceso en memoria ejecutándose.

Tercera Generación

Abarca desde 1965 a 1980. En el campo del hardware tenemos los circuitos integrados con tecnología LSI y VLSI. Antes de ver los distintos S.O., merece la pena dejar claros dos conceptos: Programa: código (algo estático) y Proceso: programa en ejecución (algo dinámico).

- S.O. Multiprogramación. En memoria principal va a haber más de un programa. La CPU ejecuta instrucciones de un programa, cuando el que se encuentra en ejecución realiza una operación de E/S, en lugar de esperar a que termine la operación de E/S, se pasa a ejecutar otro programa. De esta forma es posible, teniendo almacenado un conjunto adecuado de tareas en cada momento, utilizar de manera óptima los recursos disponibles.

Se va a definir el grado de multiprogramación como el número de programas que hay actualmente en memoria

OverHead es un parámetro que mide la diferencia de tiempo que hay entre que el sistema operativo está dedicado a hacer sus tareas y el tiempo dedicado al cambio de contexto entre procesos.

- S.O. Multiproceso. Tiene varios procesos en memoria principal. Hay que distinguir que:
 - o *Multiprogramación IMPLICA Multiproceso.* Multiprogramación: varios programas en memoria principal. Al estar en memoria principal se están ejecutando. Programas en ejecución = procesos.
 - o *Multiproceso NO IMPLICA Multiprogramación* Ahora bien, podemos tener únicamente un programa en memoria y este programa lanzar varios procesos. Un programa puede querer imprimir, leer algo por teclado, ... lanzar procesos. Varios procesos = multiproceso
- S.O. Multiprocesador. Se utilizan donde hay 2 CPU's o más.
- S.O. Interactivos. Sistemas que de alguna forma mantienen un diálogo con el usuario; mediante el SHELL (lenguaje de comandos).

Es muy importante el tiempo de respuesta: tiempo que transcurre entre que el usuario manda hacer algo al sistema hasta que obtiene la respuesta. Siempre se intenta minimizar el tiempo de respuesta.

- S.O. Multiusuario. Aquellos sistemas operativos en los cuales varios usuarios pueden acceder al mismo ordenador simultáneamente.

Por ejemplo: cualquier sistema UNIX o LINUX. Se puede tener una máquina y generar usuarios accediendo a esa máquina (a través de red local, Internet, ...).

- S.O. de Tiempo Compartido. Pretenden dotar a cada persona de una parte de la CPU. El usuario ve el ordenador como suyo propio, aunque no lo es.

- S.O. de Tiempo real. Estos sistemas se usan en entornos donde se deben aceptar y procesar en tiempos muy definidos un gran número de sucesos, en su mayoría externos al ordenador. Si el sistema no respeta las restricciones de tiempo en las que las operaciones deben entregar su resultado se dice que ha fallado.

Cuarta Generación

Abarca desde 1980 hasta nuestros días, está marcada por los ordenadores personales.

Sistema Operativo de Red. El usuario es consciente de que existen otras máquinas. El usuario ya no quiere trabajar solo; quiere trabajar con otros usuarios. Tiene que acceder de forma explícita a esas máquinas.

Sistema Operativo Distribuido. El parámetro clave es la transparencia: el usuario no es consciente de que existen otras máquinas; no sabe en qué máquina está.

53.1.3 Clasificaciones de los Sistemas Operativos

- Según el número de usuarios:
 - o S.O. monousuarios: sólo aceptan un usuario en un momento determinado.
 - o S.O. multiusuarios: aceptan simultáneamente a más de un usuario.
- Según el hardware:
 - o Según el número de CPU'S:
 - S.O. monoprocesador: sólo controla una CPU.
 - S.O. multiprocesador: varios procesadores (más complicado de diseñar).
 - o Según la organización de la memoria principal:

- S.O. centralizados: una memoria principal y los procesadores van a estar intentando acceder a esta memoria principal. Los procesos se comunican a través de la memoria.
- S.O. distribuidos: cada procesador tiene su propia memoria principal. Los procesos tienen otros mecanismos de comunicación.
- Según el modo de trabajo con los sistemas operativos:
 - o Interactivo (on-line): el usuario dialoga con la máquina.
 - o Batch (off-line): no hay comunicación con la máquina cuando está realizando el trabajo.
- Según el objetivo para el que fueron diseñados:
 - o S.O. de propósito general: capaces de realizar cualquier tarea.
 - o S.O. de propósito específico: sólo pueden realizar una tarea específica, se instalan en microprocesadores que controlan el funcionamiento de electrodomésticos, vehículos, equipos de electrónica consumo, etc.
 - o S.O. de Tiempo Real: ofrecen una respuesta en un intervalo de tiempo bien definido.
 - o S.O. Virtuales: corren sobre HW de un ordenador ofreciendo a los niveles superiores copias exactas de la máquina real, de forma que en cada copia se puede ejecutar un sistema operativo distinto.
 - o S.O. de dispositivos móviles: deben adaptarse a las limitaciones que estos dispositivos presentan: procesadores lentos, memoria limitada, pantallas pequeñas y consumo de energía limitado. Ejemplos típicos para estos dispositivos son iOS de Apple, Windows Mobile, Android, etc.

53.1.4 Estructura de los Sistemas Operativos

Sistemas operativos monolíticos

Estos S.O. no tienen una estructura definida. El S.O. se escribe como una colección de procedimientos entrelazados de tal forma que cada uno puede llamar a cualquier otro. Las características de este tipo de estructura son:

- Construcción del S.O. basado en procedimientos compilados separadamente que se unen en un solo fichero objeto a través del enlazador (linker).
- Buena definición de parámetros de enlace entre los distintos procedimientos existentes, lo que genera acoplamiento.
- Carece de protección al entrar a procedimientos que gestionan diferentes aspectos de los recursos del ordenador, como almacenamiento, E/S, etc.
- Son hechos a medida lo que tiene como ventaja que son eficientes y rápidos y como desventaja que carecen de flexibilidad para crecer.

Sistemas operativos con capas

El SO se organiza en una jerarquía de estratos, estando construido cada uno de ellos sobre el otro que tiene menor jerarquía que él. Ejemplos: THE, MULTICS.

Sistemas operativos Cliente-Servidor.

Minimizar el kernel (núcleo) del S.O., desplazando el código de todos sus servicios a estratos lo más superiores posibles. Para ello, la mayoría de sus funciones se implementan como procesos de usuario, denominados procesos servidores, de forma que cuando un proceso de usuario llamado proceso cliente, necesita un servicio del S.O. lo que hace es enviar un mensaje al proceso servidor correspondiente, que realiza el trabajo y devuelve la respuesta.

53.1.5 Funciones de un Sistema Operativo

Las principales funciones que tienen los S.O. son la gestión de procesos, la gestión de la memoria principal, la gestión del almacenamiento secundario y la gestión de los dispositivos de entrada/salida.

Gestión de procesos

La CPU es el recurso principal del ordenador de modo que es necesaria una gestión eficiente de la misma para garantizar su aprovechamiento.

El S.O. ha de cargar los distintos procesos, iniciarlos, supervisar su ejecución llevando a cabo los cambios de contexto necesarios y detectar su terminación normal o anormal. En los entornos multiusuario es fundamental la activación de mecanismos de protección que limiten las posibilidades de acceso de cada proceso a una serie de recursos para los que cuente con la debida autorización.

Gestión de memoria principal

En un sistema multiproceso los procesos tienen que compartir la CPU teniendo que encontrarse en memoria principal para poder pasar a ejecutarse inmediatamente; así, varios procesos tienen que compartir la memoria principal sin que unos puedan acceder a los recursos de otros.

Para ello hay que dividir la memoria en bloques y éstos se les asignaran a distintos procesos. Para hacer la división se utiliza la segmentación, la paginación o la segmentación paginada.

Gestión de los sistemas de archivos

En un sistema de archivos el S.O. tiene que hacerse cargo de: la gestión del espacio libre/ocupado, de los cachés de lectura y escritura, del vínculo entre nombres y archivos, de las asociaciones entre los bloques físicos de los dispositivos y los bloques lógicos, de los permisos para el acceso y modificación a los distintos elementos.

Gestión de entrada/salida (E/S)

La velocidad con que se comunican el procesador y la memoria principal contrasta con la velocidad cuando los programas deben interactuar con algún tipo de dispositivo de E/S; durante este proceso la ejecución del programa se ve interrumpida ya que la comunicación con dichos dispositivos es significativamente más lenta que con la memoria.

Conjuntamente con la multiprogramación surgen dos conceptos: el acceso directo a memoria (DMA) y las interrupciones. El procesador cede el control de la E/S a un módulo que se encarga de ejecutar este tipo de operaciones (el controlador de DMA) y esperar hasta que éstas se completen y cuando esto suceda avisar al procesador (que se encuentra mientras tanto ejecutando otras instrucciones -bien sea del mismo proceso o de algún otro-) que puede continuar con las operaciones subsiguientes que quedaron pendientes cuando se realizó la petición de E/S mediante una interrupción.

53.1.6 Tendencias

Actualmente, la movilidad es lo primordial en nuestra sociedad, y asociado a esta movilidad está la seguridad. Se empieza a hablar de sistemas operativos en la nube (cloud computing) y se consolidan los sistemas operativos de los dispositivos móviles.

Otro aspecto a destacar derivado del momento económico es el ahorro de costes. Fruto de esto se puede ver una tendencia más que clara en la virtualización.

S.O. en dispositivos móviles.

Si existe una carrera hoy en día en el desarrollo de S.O., ésta está en los S.O. para dispositivos móviles. Los nuevos sistemas operativos convierten al teléfono en un completo aparato multimedia. Hasta hace muy poco tiempo la elección de un móvil venía determinada por sus características físicas: recepción de la señal, cámara... pero con la llegada de los smartphone, la elección del S.O. se ha convertido en algo muy importante.

A diferencia del mundo del ordenador personal, y debido quizás a su juventud en el mercado, no existe un dominador claro de S.O. móviles. Hay fabricantes hardware que son los fabricantes de sus propios sistemas operativos como por ejemplo Apple que sólo distribuye el S.O. iOS para iPhones e iPad, lo mismo que RIM que distribuye su S.O. BlackBerry OS en dispositivos BlackBerry, etc. En el otro extremo están los fabricantes que utilizan S.O. de otras compañías como Android, Symbian, Windows Mobile...

Las compañías que fabrican y distribuyen su propio S.O. tienen a favor que las actualizaciones de los dispositivos son muy controladas.

Otra tendencia vendrá de la mano del despegue de los dispositivos tablets (tabletas), teniendo en cuenta los anuncios de lanzamientos de tablets: Apple (iPad 2), RIM (PlayBook), Samsung (Galaxy Tab 2), etc. Esto dará aun más auge a los S.O. móviles.

S.O. en la nube o en red.

Estos S.O. surgen del concepto de Computación en la Nube (Cloud Computing) que es un nuevo paradigma que básicamente permite tener servicios computacionales a través de Internet.

Una de las grandes ventajas que se pueden encontrar a este nuevo paradigma es la baja inversión a realizar en HW ya que toda la infraestructura de la computación en la nube se encuentra en los grandes proveedores de servicios de Internet. Bastaría con un hardware mínimo, un navegador y una buena conexión a Internet.

Otra de las ventajas sería que las aplicaciones no se instalan en el pc, son aplicaciones Web lo que hace que sea compatible con la mayoría de los formatos conocidos.

Permite tener una única copia de un fichero disponible en cualquier lugar y momento.

Sus puntos débiles son la seguridad y la necesidad de una conexión a Internet.

Estos S.O. son una buena opción para los notebook que tienen poco hardware, e incluso podrían hacer que los fabricantes apostasen por modelos más baratos que permitiría difundir mucho más la informática.

Entre los S.O. más importantes destacan: eyeOS, ChromeOS de Google, oOS, iCloud, etc.

53.2.- SISTEMA OPERATIVO UNIX-LINUX

UNIX es un sistema operativo creado en 1969 por un grupo de investigadores de los laboratorios Bell de AT&T, entre ellos Ken Thompson, Dennis Ritchie y Douglas McIlroy, como una versión reducida del proyecto MULTICS; primero fue escrito en ensamblador, pero ello impedía la portabilidad a diferentes ordenadores. Después de que Dennis Ritchie en el 1973 crease el lenguaje C, se reescribe UNIX totalmente en este lenguaje de alto nivel, haciendo por tanto el código casi totalmente independiente del tipo de máquina, permitiendo la instalación de UNIX en diferentes plataformas.

Inicialmente los laboratorios AT&T Bell, consideran que UNIX era más bien un proyecto de investigación y lo llegó a distribuir de forma gratuita entre departamentos informáticos de las universidades, los cuales lo podían modificar y adaptar a sus necesidades. Pero, la gran demanda del sistema operativo hace que los laboratorios Bell iniciara su venta a través de distribuciones oficiales concediendo a los usuarios que lo requerían licencias de uso.

Debido a las múltiples versiones en el mercado de UNIX, el IEEE especifica una familia de estándares para definir una interfaz de programación de aplicaciones (API) para que todas las versiones fuesen 'compatibles'. A esta familia se le conoce como POSIX (Portable Operating System Interface; la X viene de UNIX como señal de identidad de la API)

Linux, se creó en 1991 por Linus Torvalds basándose en otros dos sistemas operativos:

- El sistema abierto UNIX.
- El sistema educativo Minix creado en 1987 por Andrew S. Tanenbaum.

Torvalds crea sólo el Kernel, el núcleo del sistema sin la capa de servicios, gestores, aplicaciones graficas, etc. que serán creadas posteriormente por otros autores. El código del núcleo lo podemos encontrar en la dirección (www.kernel.org).

En la comunidad de programadores se crea el proyecto GNU (Gnu's Not Unix), proyecto para generar software libre, donde se generan editores, compiladores, etc. bajo la licencia pública general GPL (General Public License): usar, copiar, distribuir y modificar siempre que se conserve la firma del autor, pudiendo cobrar por ello.

Linux se crea con esta filosofía de libre distribución y el sistema operativo completo que se construye con este núcleo también. A todo el sistema se le da el nombre de GNU/Linux (distribución completa del sistema operativo con Linux), que contiene el núcleo más las otras capas del sistema operativo y utilidades. Si bien muchas veces se denomina a todo el sistema simplemente LINUX.

53.2.1 Características

Las características más relevantes del sistema UNIX son:

- UNIX ha sido diseñado como un sistema multiusuario en tiempo compartido; ofreciendo protección de los datos privados sobre ficheros y protección del entorno de ejecución.
- Portabilidad: UNIX fue escrito en el lenguaje C, un lenguaje de alto nivel, lo cual hace que sea relativamente fácil de leer, entender, modificar y transportar a otras máquinas con una arquitectura física diferente.
- Código y funcionamiento escrito bajo la familia de estándares POSIX (Portable Operating System Interface).

- Interfaz de usuario simple e interactiva: el intérprete de órdenes (shell) es un programa independiente que el usuario puede sustituir. La sintaxis de utilización es idéntica para todas las órdenes.
- Modularidad: Proporciona primitivas que permiten construir grandes programas a partir de otros más sencillos, así como librerías para linkaje.
- Posee bibliotecas compartidas para facilitar el enlace dinámico.
- Protecciones de memoria.
- Soporta diferentes sistemas de archivos, incluidos los de Microsoft Windows
- Sistema de archivos con estructura de árbol invertido (de múltiples niveles que permite un fácil mantenimiento) y jerárquico (permite la unión de diversos sistemas de ficheros con el sistema principal, y una separación de directorios).
- Todos los archivos de usuario son simples secuencias de bytes (8 bits), no tienen ningún formato predeterminado.
- Independencia de dispositivos: Los discos y los dispositivos de entrada y salida (E/S) se tratan todos de la misma manera: como meros archivos. Las peculiaridades de los dispositivos se mantienen en el núcleo (kernel).
- La arquitectura de la máquina es completamente transparente para el usuario, lo que permite que los programas sean fáciles de escribir y transportables a otras máquinas con hardware diferente
- UNIX no incorpora diseños sofisticados; de hecho, la mayoría de los algoritmos han sido seleccionados por su sencillez y no por su rapidez o complejidad.
- Incorpora todos los servicios de red, TCP/IP, DNS, sendmail, etc.

- Proporciona un completo entorno de programación: los filtros son utilidades simples que se concentran en realizar bien una sola función. Pueden combinarse de forma muy flexible utilizando las pipes (tuberías) y las redirecciones de E/S según las necesidades y preferencias de cada usuario.
- Mantenimiento fácil: consecuencia directa de la modularidad. El sistema sigue evolucionando y se perfecciona y enriquece con nuevas funcionalidades.
- Carácter abierto: permite ampliar fácilmente la funcionalidad con nuevos componentes sin tener que depender de un único fabricante.

53.2.2 Arquitectura de Unix-Linux

La arquitectura está basada en capas o niveles de forma que cada capa únicamente puede comunicarse con las capas que se hallan en los niveles inmediatamente inferior y superior.

En la capa inferior tenemos toda la parte del Hardware que el sistema operativo debe gestionar. Por encima de éste se sitúa el kernel de Unix que es el encargado de la administración de procesos, gestión del sistema de archivos, entradas / salidas, etc. A los procesos que trabajan a ese nivel se les llama procesos en modo kernel.

La biblioteca estándar se ubica por encima del kernel, se encarga, por ejemplo de las operaciones de apertura, cierre, etc. A este nivel se trabaja en modo usuario. La interface entre las dos capas, o el acceso de la capa de biblioteca estándar a la del kernel se realiza a través de la interfaz de llamadas al sistema.

A un nivel superior tenemos los programas y utilidades como el shell, compiladores, etc., que sirven de ayuda a desarrolladores y usuarios que interactúan con el sistema operativo. La interface entre esta capa y la inmediatamente inferior es a través de la interfaz de biblioteca.

Por último, se ubicarían los usuarios que por medio de la interfaz de usuario se comunican con el shell, u otras utilidades del sistema Unix.

El núcleo de UNIX (kernel) es de tipo monolítico, diferenciándose dos partes principales: el núcleo dependiente de la máquina y el núcleo independiente. El núcleo dependiente se encarga de las interrupciones, los dispositivos de bajo nivel y parte de la administración de la memoria. El núcleo independiente es igual en todas las plataformas e incluye la gestión de llamadas del sistema, la planificación de procesos, la paginación e intercambio, la gestión de discos y del sistema de archivos

53.2.3 Gestión de procesos.

La gestión de procesos en UNIX es por prioridad y round robin. En algunas versiones se gestiona también un ajuste dinámico de la prioridad de acuerdo al tiempo que los procesos han esperado y al tiempo que ya han usado la CPU. El sistema provee facilidades para contabilizar el uso de CPU por proceso y una pila común para todos los procesos cuando necesitan estarse ejecutando en modo privilegiado (cuando hicieron una llamada al sistema).

Los procesos trabajan en modo usuario y en modo kernel. El paso de modo usuario a kernel o viceversa se realiza a través de traps que crean una interrupción para acceder a la interfase de llamadas al sistema y al resto de los componentes de nivel kernel. El paso del modo kernel a usuario es un retorno tras la realización de la petición que motivó el paso al modo kernel.

UNIX permite que un proceso haga una copia de sí mismo por medio de la llamada «fork», lo cual es muy útil cuando se realizan trabajos paralelos o concurrentes; también se proveen facilidades para el envío de mensajes entre procesos (pipes, signals).

Los procesos no interactivos se denominan daemons o procesos background. Cuando se inicia un proceso, se le asigna un identificador PID, se guarda el proceso que lo lanzó PPID, el propietario que lo lanzó UID y el grupo de pertenencia GID, lo que definirá el perfil de permisos de acceso a

los que tendrá derecho. Existe la posibilidad de alterar el usuario o grupo efectivo de permisos, durante la ejecución del proceso, mediante la llamada a **setuid** o **setgid**, siempre que se disponga de los permisos apropiados. También existe una bandera de permisos **setuid** asociada al archivo del programa que permite ejecutar éste, con los permisos del propietario del archivo en lugar de los del usuario que lo ejecuta.

LINUX combina multiprogramación y tiempo compartido.

El gestor de procesos en el kernel del sistema UNIX, se encarga de la asignación de CPU, la programación de procesos, y las solicitudes de los procesos. Para realizar estas tareas, el kernel mantiene varias tablas importantes para coordinar la ejecución de estos procesos y la asignación de los dispositivos.

Utilizando una política predefinida, el programador de procesos selecciona un proceso de la cola de procesos listos y comienza su ejecución durante un pedazo de tiempo ya dado.

El algoritmo de programación de procesos selecciona el proceso con la mayor prioridad para ser ejecutado primero. Si varios procesos tienen la misma prioridad, se aplica el algoritmo round-robin.

53.2.4 Gestión de memoria.

Los sistemas UNIX utilizan el manejo de memoria virtual siendo el esquema más usado la paginación por demanda y combinación de segmentos paginados, en ambos casos con páginas de tamaño fijo.

En todos los sistemas UNIX se usa una partición de disco duro para el área de intercambio (swap). Esa área se reserva durante la instalación del sistema operativo.

Una regla muy difundida entre administradores de sistemas es asignar una partición de disco duro que sea al menos el doble de la cantidad de memoria real del ordenador. Con esta regla se permite que se puedan

intercambiar flexiblemente todos los procesos que estén en memoria RAM en un momento dado por otros que estén en el disco.

Si no caben todos los programas en memoria principal se hace uso de la partición de intercambio (swapping)

- **Swap out** Cuando no caben en memoria procesos activos, se “expulsa” un proceso de memoria principal, copiando su imagen a swap, aunque no es necesario copiar todo el mapa. Existen diversos criterios de selección del proceso a intercambiar: dependiendo de la prioridad del proceso; preferencia a los procesos bloqueados; no intercambiar si está activo DMA sobre mapa del proceso.
- **Swap in.** Cuando haya espacio en memoria principal, se intercambia el proceso a memoria copiando la imagen desde swap.

Todos los procesos que forman parte del kernel no pueden ser intercambiados a disco.

Cada proceso dispone de su propio espacio de direcciones, organizado en segmentos según:

- **Text Segment:** que almacena el código
- **Data Segment:** que almacena los datos o variables que utilizan los procesos, éste segmento tiene dos partes: Initialized Data (datos inicializados) y Uninitialized Data (datos no inicializados).
- **Stack Segment:** que almacena la información referente a llamadas a otras funciones.

Es posible compartir código entre procesos mediante el empleo de Shared Text Segments. Dos procesos nunca comparten los segmentos de datos y de pila (salvo los thread), la forma de compartir información se lleva a cabo mediante el empleo de segmentos especiales de memoria compartida Shared Segments.

Linux comparte muchas de las características de los esquemas de gestión de memoria de otras implementaciones UNIX, pero tiene sus características propias.

En lo que respecta a memoria virtual, el direccionamiento de memoria virtual de Linux, hace uso de una estructura de tabla de páginas con tres niveles, formada por los siguientes tipos de tablas (cada tabla individual es del tamaño de una página): Directorio de páginas un proceso activo tiene un solo directorio de páginas que es del tamaño de una página. Cada entrada en el directorio de páginas apunta a una página del directorio intermedio de páginas. Para un proceso activo, el directorio de páginas tiene que estar en la memoria principal; Directorio intermedio de páginas este directorio puede ocupar varias páginas y cada entrada de este directorio apunta a una página de la tabla de páginas; Tabla de páginas esta tabla de páginas también puede ocupar varias páginas, y cada entrada de la tabla de página hace referencia a una tabla virtual del proceso.

Para utilizar esta estructura de la tabla de páginas a tres niveles, una dirección virtual en Linux se ve como un conjunto de cuatro campos. El campo más a la izquierda (más significativo) se utiliza como índice en el directorio de páginas. El siguiente campo sirve como índice en el directorio intermedio de páginas. El tercer campo sirve como índice en la tabla de páginas. Y el cuarto y último campo, indica el desplazamiento dentro de la página seleccionada de la memoria

53.2.5 Gestión de E/S

Los dispositivos de entrada y salida son considerados ficheros especiales: Toda entrada/salida está basada en el principio de que todos los dispositivos se pueden tratar como ficheros simples que se acceden mediante descriptores de archivos cuyos nombres se encuentran generalmente en el directorio «/dev».

Cada proceso en UNIX mantiene una tabla de archivos abiertos (donde el archivo puede ser cualquier dispositivo de entrada/salida). Esa tabla tiene

entradas que corresponden a los descriptores, los cuales son números enteros obtenidos por medio de la llamada del sistema.

Las llamadas al gestor de entrada/salida se hacen de dos formas: síncrona y asíncrona. El modo síncrono es el modo normal de trabajo y consiste en hacer peticiones de lectura o escritura y el proceso espera a que el sistema le responda.

El gestor de entrada/salida utiliza como elementos principales el buffer de cache; el código general de gestión de dispositivos, y drivers de dispositivos de hardware. Existen dos tipos de dispositivos:

Dispositivos de bloques:

- Usan secuencias de bytes (bloques)
- Utilizan buffer-cache
- Están estructurados en bloques de tamaño fijo (512 bytes)
- Permiten optimizar el rendimiento

Dispositivos de carácter:

- Son dispositivos sin estructura (terminales, impresoras, etc)
- No usan buffer
- Las operaciones se realizan carácter a carácter

Interrupciones y excepciones

UNIX permite interrumpir la CPU asíncronamente. Al recibir la interrupción, el kernel almacena el contexto actual, determina la causa y responde a la interrupción. Tras responder a ésta, devuelve el contexto interrumpido y sigue ejecutando. El HW asigna las prioridades a los dispositivos de acuerdo con el orden de actuación en las interrupciones.

Así como las interrupciones están causadas por factores externos a un proceso, las excepciones son sucesos inesperados producidos por procesos, tales como la ejecución de instrucciones reservadas, de forma que el sistema, al encontrarse con una, tiende a reiniciar la instrucción, en lugar de pasar a la siguiente.

No obstante, el kernel debe tener la posibilidad de impedir la aparición de interrupciones en momentos críticos, para evitar la degradación de los datos. El sistema que se utiliza es el de disponer de un conjunto de instrucciones restringidas que colocan el nivel de ejecución del procesador en el estado de palabra (status word). Al asignar un nivel de ejecución del procesado, todas las interrupciones de ese nivel e inferiores quedan suprimidas, permitiendo sólo las superiores.

53.2.6 Gestión de archivos

Un sistema de archivos permite realizar una abstracción de los dispositivos físicos de almacenamiento de la información para que sean tratados a nivel lógico, como una estructura de más alto nivel y más sencilla que la estructura de su arquitectura hardware particular.

El sistema de archivos UNIX se caracteriza porque posee una estructura jerárquica, realiza un tratamiento consistente de los datos de los archivos, protege los datos de los archivos y trata a los dispositivos y periféricos (terminales, unidades de disco, cinta, etc.) como si fuesen archivos.

El sistema de archivos está organizado, a nivel lógico, en forma de árbol invertido, con un nodo principal conocido como nodo raíz ("/"). Cada nodo dentro del árbol es un directorio y puede contener a su vez otros nodos (subdirectorios), archivos normales o archivos de dispositivo.

Los nombres de los archivos (pathname) se especifican mediante la ruta (path), que describe cómo localizar un archivo dentro de la jerarquía del

sistema. La ruta de un archivo puede ser absoluta (referida al nodo raíz) o relativa (referida al directorio de trabajo actual).

Todos los sistemas UNIX pueden manejar múltiples particiones de disco, cada una con un sistema de archivos distinto.

Una partición de disco clásica en UNIX contiene una estructura como la de la figura.

- Bloque de arranque: contiene el código para arrancar el ordenador con esa partición.
- Superbloque: Contiene información crucial acerca de la organización del sistema de archivos, incluido el número de nodos-i (i-nodes), el número de bloques de disco y el principio de la lista de bloques de disco libres. La destrucción del superbloque hace que el sistema de archivos ya no pueda leerse.
- Nodos-i: contiene la representación interna de un fichero que permite entre otras cosas localizar todos los bloques de disco que contienen los datos del archivo
- Bloques de Datos: almacenan la información. Lo normal es que un archivo ocupe más de un bloque de datos no siendo necesario que estén contiguos.

Dentro de la estructura de directorios de UNIX – Linux existen una serie de directorios comunes a todas las instalaciones que es preciso conocer:

- /: Directorio raíz, inicio del sistema de archivos.
- /tmp: Directorio de archivos temporales.
- /dev : Directorio de dispositivos. En él se encuentran todos los dispositivos de E/S, que se tratan como archivos especiales.
- /etc: Directorio para archivos de sistema diversos.

- /bin: Directorio para programas binarios (ejecutables).
- /lib: Directorio de bibliotecas del sistema.
- /usr: Directorio de usuarios.
- /home: Directorio base a partir del cual se ubican los directorios por defecto de las cuentas de usuario.

LINUX comenzó empleando el sistema de archivos de MINIX, pero estaba limitado a nombres de 14 caracteres y a archivos de 64 MB de tamaño. La primera mejora vino de la mano de un sistema de archivos denominado Ext que permitía nombres de archivo de 255 caracteres y 2 GB de tamaño por archivo, pero era muy lento. La evolución vino de la mano del sistema de archivos Ext2, con nombres de archivo largos, archivos grandes y mejor rendimiento. Ext2 evolucionó a Ext3 que trajo principalmente las transacciones (journaling) a Ext2. En ext3 se almacena la información necesaria para restablecer los datos afectados por la transacción en caso de que ésta falle. La evolución de ext3 es **ext4** que soporta un tamaño máximo de sistema de archivos de 1 ExaByte (1 ExaByte = 1024 PetaBytes = 1048576 TeraBytes) y un tamaño máximo por archivo de 16 TB para los archivos y por otro lado, modifica estructuras de datos importantes, como la destinada a almacenar los datos del archivo utilizando “**extent**” que es un conjunto de bloques físicos contiguos, mejorando el rendimiento al trabajar con ficheros de gran tamaño y reduciendo la fragmentación.

53.3.- SISTEMA OPERATIVO WINDOWS

53.3.1 Características

La familia de S.O. Windows es propiedad de Microsoft. Se podría decir que básicamente existen dos versiones distintas de S.O. Windows: aquellos enfocados al mundo empresarial y aquellos enfocados al consumidor final o usuario doméstico.

Dentro de esta simple clasificación podríamos hacer otras clasificaciones. Orientado al usuario domestico existen S.O. para equipos de sobremesa, portátiles, tablets, y dispositivos móviles. Y orientado al mundo empresarial podemos distinguir S.O. para servidores y S.O. para estaciones de trabajo. Aún podríamos dividir más los S.O. para servidores (Standard, Enterprise, Datacenter, Web, Storage, Small Business Server)...

Los últimos S.O. que han visto a luz son Windows 7 con las versiones Starter (sólo para 32 bits), Home Basic, Home Premium, Professional, Ultimate, Enterprise. Y a nivel de S.O. para servidores es Windows Server 2008 R2.

Es destacable el interés de mejora adquirido por Microsoft con los S.O. de servidor, comprometiéndose a un cambio cada 5 años (antes del 2008 estaba el 2003) y a una revisión cada 2 años aprox. (por eso existe Windows Server 2008 R2).

Windows Server 2008 es el último S.O. de servidor que incluye estas mejoras:

- Nuevo proceso de reparación de sistemas NTFS: proceso en segundo plano que repara los archivos dañados.
- Creación de sesiones de usuario en paralelo: reduce tiempos de espera en los Terminal Services y en la creación de sesiones de usuario a gran escala.
- Cierre limpio de Servicios.
- Sistema de archivos SMB2: de 30 a 40 veces más rápido el acceso a los servidores multimedia.
- Address Space Load Randomization (ASLR): protección contra malware en la carga de controladores en memoria.
- Windows Hardware Error Architecture (WHEA): protocolo mejorado y estandarizado de informe de errores.

- Virtualización de Windows Server: mejoras en el rendimiento de la virtualización.
- PowerShell: inclusión de una consola mejorada con soporte GUI para administración.
- Server Core: el núcleo del sistema se ha renovado con muchas y nuevas mejoras.

En los siguientes apartados se verán características de Windows, y si bien la mayoría son comunes para todas las versiones, las explicaciones estarán más centradas en Windows 2008 Server R2.

53.3.2 Arquitectura de Windows

La estructura modular de Windows 2008 aporta una gran flexibilidad. Su diseño le permite ejecutarse en una gran variedad de plataformas hardware. En esta estructura modular se distinguen dos capas principales:

- **Modo usuario**: Cuyos programas y subsistemas están limitados a los recursos del sistema a los que tienen acceso. Está formado por subsistemas que pueden pasar peticiones de E/S a los controladores apropiados del modo núcleo a través del gestor de E/S.
- **Modo núcleo o kernel**: Tiene acceso total al hardware de la máquina, impidiendo a los servicios del modo usuario y a las aplicaciones acceder a al hardware que queda totalmente protegido por el sistema operativo. La arquitectura dentro del modo núcleo se compone de lo siguiente:
 - o El micronúcleo: situado entre la capa de abstracción de hardware y el Executive, proporciona la gestión *multiprocesador*: gestión de procesos, hilos y tratamiento de interrupciones, y de excepciones.
 - o Una capa de abstracción de hardware (en inglés Hardware Abstraction Layer o HAL), se encarga de ocultar las diferencias de hardware y por

tanto proporciona una plataforma única donde pueda ejecutarse el S.O. independientemente del HW.

- o Controladores o también llamados drivers: utilizados para interactuar con los dispositivos hardware.
- o Executive: sobre el cual son implementados todos los servicios de alto nivel. Se relaciona con todos los subsistemas del modo usuario. Se ocupa de la entrada/salida, la gestión de memoria, Plug&Play, la seguridad y la gestión de procesos.

Dado que el enlace estático de los programas de usuario con las bibliotecas de la API Win32 conllevaría un tamaño enorme en los programas y un desperdicio de memoria, pues cada programa en ejecución tendría su copia de estas bibliotecas, todas las versiones de Windows manejan bibliotecas compartidas, llamadas bibliotecas de vínculos dinámicos (DLLs; Dinamic Link Libraries).

53.3.3 Gestión de procesos.

Los procesos se crean como objetos, y un proceso puede tener varios hilos. Dado que el proceso es un objeto, su composición será un conjunto de datos sólo accesibles a través de un conjunto de funciones que los ocultan del resto de aplicaciones o funciones. Estas funciones o servicios se activan por medio de mensajes. El proceso tendrá al menos un hilo, que a su vez puede ejecutar otros hilos, pudiendo hacerlo en paralelo en un sistema multiprocesador.

Windows mantiene dos listas diferentes con la información de todos los procesos e hilos. Cada proceso tiene asociado un bloque o estructura de datos EPROCESS, que apunta al EPROCESS siguiente y al anterior (doble lista enlazada), y la otra estructura es ETHREAD para recoger la información de los hilos.

El algoritmo de planificación está basado en colas de retroalimentación de múltiples niveles con prioridades. Cada cola se gestiona con una política Round Robin.

La planificación se aplica sobre los hilos, no a los procesos (sin tener en cuenta a qué proceso pertenecen los distintos hilos que se ejecutan), y está basada en prioridades, es decir, siempre se ejecutará el hilo de mayor prioridad de la cola de hilos preparados.

Cuando se selecciona un hilo para su ejecución, se le concede un quantum, o intervalo de tiempo durante el cual se permite al hilo ejecutarse antes de que lo haga otro hilo del mismo nivel de prioridad. Los valores de quantum pueden variar.

Aunque se conceda un quantum a un hilo, éste podría no consumirlo completamente porque aparezca en el sistema un nuevo proceso de mayor prioridad, que obligaría al que se está ejecutando a abandonar el procesador.

El sistema trata igual a todos los hilos que tengan la misma prioridad, asignando a cada hilo de mayor prioridad un intervalo de tiempo de procesador con un Round Robin. Si ninguno de estos hilos estuviera preparado para ejecutarse, pasarían a ejecutarse, con la misma política, los de la prioridad inmediatamente inferior.

En cada uno de estos casos, Windows debe determinar qué hilo debe ejecutarse a continuación, y esta decisión es lo que se conoce como dispatcher.

Cada proceso recibe una prioridad base para todos sus hilos. El sistema se basa en 32 prioridades, del 0 (menor prioridad) al 31 (mayor prioridad):

- La prioridad 0 está reservada para el hilo de sistema responsable de poner a cero las páginas libres cuando no las necesiten ningún hilo.

- Las prioridades 1 a 15 son las reservadas para los procesos de usuario (prioridades variables).
- Las prioridades 16 a 31 están reservadas al sistema operativo (prioridades en tiempo real).

El planificador funciona accediendo a la tabla por el proceso de prioridad 31 y viendo si tiene hilos listos para ejecutar. Si los hay toma el primero de la lista y lo ejecuta durante un quantum. Mientras existan procesos preparados de una prioridad superior, el sistema les concederá todo el tiempo que precisen. Este comportamiento se repite para cada una de las entradas de la tabla de prioridades.

En ciertas condiciones un subproceso puede ver incrementada su prioridad base, pero nunca por encima de la prioridad 15 y nunca para subprocesos de prioridad mayor de 15. Si una operación de E/S libera un subproceso, éste ve incrementada su prioridad base de modo que pueda ejecutarse pronto.

También se produce aumento de prioridad si el subproceso estaba esperando por un semáforo, mutex u otro suceso. Estas elevaciones de prioridad van disminuyendo a medida que un subproceso beneficiado va consumiendo por completo su quantum, hasta volver a situarse en su prioridad base.

53.3.4 Gestión de memoria.

La gestión de memoria en Windows es de memoria virtual con paginación.

Las aplicaciones de 32 bits tienen un espacio de dirección del proceso de 4 GB de memoria. Los sistemas operativos de Microsoft Windows proporcionan a las aplicaciones acceso a 2 GB de espacio de dirección del proceso, específicamente conocido como espacio de dirección virtuales del modo de usuario. Todos los subprocesos pertenecientes a una aplicación comparten el mismo espacio de direcciones virtuales del modo de usuario.

Los 2 GB restantes se reservan para el sistema operativo (también conocido como espacio de dirección del modo de kernel).

El espacio de direcciones virtual se pagina por demanda con tamaño fijo de páginas (mínimo 4KB para arquitecturas x86 y x64bits y 8KB para arquitecturas IA64 y máximo de 4MB para arquitectura x86, 2MB para x64 y 16MB para IA64).

Windows utiliza un algoritmo de **paginación por demanda anticipada**, es decir, cada vez que se produce un fallo de página, el sistema copiará en memoria la página correspondiente a la referencia a memoria que ha causado el fallo de página y además un conjunto de páginas próximas a ella, tanto anteriores como posteriores, al suponer que, debido a la localidad de las referencias, es casi seguro que en un futuro próximo también se hará referencia a estas páginas, que cuando se quieran utilizar ya estarán en memoria y, por lo tanto, no producirán fallos de páginas adicionales.

El mecanismo de paginación se apoya mucho en el concepto de **Conjunto de Trabajo (Working Set)** que asegura una cierta cantidad de memoria física para cada proceso.

Windows presta especial atención al momento de arranque de los procesos ya que, como no tienen ninguna página cargada en la memoria, hasta que carguen todas las páginas necesarias se producirán muchos fallos de página. Para optimizar la carga de los procesos, Windows cuenta con lo que se conoce como “Prefetcher” cuya misión es acelerar el proceso de carga.

Si se produce un fallo de página y es necesario sustituir algún marco de página que está en memoria, Windows emplea el algoritmo LRU (aunque algunas versiones utilizan también FIFO).

Permite compartir páginas, al poder proteger contra lectura o escritura las mismas. Igualmente admite que se pueda bloquear una página en memoria

que sea crítica, impidiendo que pueda sustituirse ante una falta de página, facilitando así la implementación de aplicaciones en tiempo real.

53.3.5 Gestión de E/S

El sistema de entrada/salida (E/S) de Windows es el que permite utilizar los dispositivos facilitando el acceso a los mismos e independizando a los programas de los dispositivos, ofreciendo además la seguridad en su uso y la escalabilidad del sistema.

Las entradas y salidas en Windows pueden ser síncronas (el proceso esperará hasta que se haya completado la operación en el dispositivo hardware) o asíncronas (el proceso lanza la operación y sigue con su ejecución y cuando la operación E/S finaliza el S.O. lo avisa).

En Windows se cargan y descargan los drivers en cualquier momento, evitando que consuman recursos si no se van a utilizar.

Esto se hace gracias al Plug and Play (PnP) que permite detectar cualquier dispositivo que se conecte al sistema y cargar el driver correspondiente.

El sistema de E/S se compone de los siguientes módulos:

- El gestor de E/S: define la infraestructura que soporta los drivers de dispositivos. Forma parte del sistema operativo.
- El driver de dispositivo: proporciona un interface de E/S para un determinado tipo de dispositivo. Los drivers reciben peticiones canalizadas a través del gestor de E/S y las dirigen al dispositivo concreto, e informan al gestor de que se ha completado la operación de E/S. Estos módulos los desarrollan los fabricantes.
- El gestor de PnP: detecta los dispositivos hardware al conectarse o desconectarse.

- El gestor de energía: facilita al sistema, así como a los drivers de dispositivo, los cambios de estado de consumo de energía eléctrica de acuerdo con la actividad del dispositivo.

53.3.6 Gestión de archivos

En Windows, la asignación del espacio la realiza el subsistema de ficheros en unidades “cluster”, cuyo tamaño depende de la capacidad del disco, normalmente oscila desde 512 bytes hasta 4 Kbytes. Utiliza 64 bits para direccionar los cluster y permite definir ficheros de 264TB (16.384 petabytes), aunque, lógicamente, el tamaño máximo de los ficheros está limitado por la capacidad de los discos.

Windows gestiona los discos y la información que contienen en base a particiones y volúmenes.

- **Particiones.** Cada disco se puede dividir en particiones primarias y extendidas. Las particiones primarias serán aquellas que puedan contener un S.O. y, por lo tanto, permitan el arranque del S.O. desde las mismas. De aquí podemos deducir, que el sistema requiere como mínimo una partición primaria en algún disco.

Una partición nunca podrá sobrepasar un disco. Sólo puede haber una partición extendida por disco, y como máximo sólo podrá contener 4 particiones en total.

Una vez creada la partición, es necesario darle formato para que pueda contener datos. Un volumen es sinónimo de partición formateada.

En Windows, las particiones las gestiona el gestor de particiones. Este gestor utiliza el gestor de E/S para identificar las particiones y crear los dispositivos que las representen, es decir, las unidades lógicas correspondientes.

Este gestor envía un comando al gestor de volúmenes (descrito más adelante) para saber si la partición tiene un volumen asociado, y si es

así, a partir de ese momento cualquier acción sobre la partición se la notificará al gestor de volúmenes.

- **Volumen.** Un volumen desde el punto de vista del usuario es una partición formateada. Las particiones primarias sólo podrán contener un volumen, mientras que las extendidas podrán albergar varios, teniendo en cuenta que un sistema sólo podrá tener como máximo 24 volúmenes, ya que se identifican por medio de las letras del abecedario, y en inglés sólo tiene 24 letras.

En Windows Server podemos trabajar con dos tipos de discos:

- Discos básicos. Son los que se basan exclusivamente en tablas de particiones MBR (Master Boot Record) o tablas GPT (GUID Partition Table).
- Discos dinámicos. Se basan en *volúmenes dinámicos*, que permiten la creación de volúmenes de particiones múltiples tales como simples, distribuidos, espejos, stripes y RAID-5. Los discos dinámicos se particionan con el Administrador de discos lógicos (LDM – Logical Disk Manager).

Windows trabaja con los siguientes tipos de volúmenes dinámicos:

- Volúmenes distribuidos (spanned). Es un único volumen lógico compuesto por un máximo de 32 particiones libres en uno o más discos. Es una forma de juntar el espacio no asignado en un sistema con varios discos en una única unidad lógica.
- Volúmenes Espejo. En este tipo de volumen, el contenido de la partición se duplica en una partición idéntica en otro disco, aunque se ven como un único volumen y no como dos. Los volúmenes espejo se conocen como RAID de nivel 1 (RAID1) y son tolerantes a fallos.
- Volúmenes divididos (Striped). Similar al volumen distribuido, utiliza el espacio de varios discos y los convierte en una única unidad lógica. Utiliza un tipo especial de formato para escribir en el disco y tiene

más rendimiento que el volumen distribuido. Los fallos de escritura suelen ser mayores que en el caso del volumen distribuido. Se conocen como RAID de nivel 0 (volúmenes RAID-0).

- Volúmenes RAID-5. Como los volúmenes striped, pero con tolerancia a fallos ya que distribuyen la información de paridad entre todos los discos miembros del volumen.

Sistemas de ficheros

Windows soporta los siguientes formatos de sistemas de ficheros:

A) CDFS (sistema de ficheros de CD-ROM): sólo permite la lectura, y soporta los formatos de disco ISO-9660 y Joliet.

B) UDF: es un subconjunto del formato ISO-13346 con extensiones para formatos como CD-R y DVD-R/RW. UDF está incluido en la especificación DVD y es más flexible que el CDFS.

C) FAT12, FAT16, y FAT32: Windows es compatible con el sistema de ficheros FAT por compatibilidad con MS-DOS y otras versiones de Microsoft Windows. El formato FAT (File Allocation Table) incluye un mapa de bits que se utilizan para identificar clusters o bloques en el disco.

FAT32 tiene una capacidad teórica para direccionar volúmenes de 8 terabytes (TB), no obstante limita los volúmenes a un máximo de 32 GB.

D) NTFS (New Technology File System): es el formato nativo de Windows Server para los sistemas de ficheros. NTFS utiliza direcciones de disco de 64 bits con lo que podría gestionar volúmenes de hasta 16 exabytes, sin embargo, Windows limita el tamaño de un volumen NTFS a lo que se pueda direccionar con 32 bits, que es un poco menos de 256 TB (con clústeres de 64 KB). NTFS admite ficheros de máximo 16 TB.

NTFS añade características de seguridad de ficheros y directorios, cuotas de disco, compresión de ficheros, enlaces simbólicos basados en directorios, y cifrado. Una de sus características más significativas es la recuperabilidad: registra los cambios que se realizan en los metadatos

como si fueran transacciones con la finalidad de que se puedan recuperar en el caso de la pérdida de ficheros o de sus datos.

La estructura central de NTFS es la tabla maestra de archivos MFT (Master File Table), que es una sucesión lineal de registros de tamaño fijo (1 KB). Cada registro de MFT describe un archivo o un directorio, contiene los atributos del archivo, como su nombre y marcas de tiempo, y la lista de direcciones de disco donde están sus bloques. Si un archivo es demasiado grande puede ser necesario emplear más de un registro MFT para contener la lista de todos los bloques. En este caso al primer registro se le denomina registro base, y apunta a los demás registros MFT.

53.3.7 Seguridad

El administrador de seguridad, componente del Executive, hace que se respete el complejo mecanismo de seguridad de Windows 2008, que satisface los requisitos C-2 del Libro Naranja del Departamento de Defensa de Estados Unidos.

Cada usuario y grupo de Windows 2008 se identifica con un SID (Security ID) único a nivel mundial. Cada proceso lleva asociado una ficha de acceso que especifica su SID y otras propiedades.

Cada objeto tiene asociado un descriptor de seguridad que indica quién puede realizar qué operaciones con él. Un descriptor de seguridad está formado por un encabezado, seguido de una DACL (discretionary Access Control List) con uno o más elementos de control de acceso (ACE). Los más importantes son Allow y Deny. Además del DACL, el descriptor tiene una SACL (System Access Control List) que no especifica quién puede usar el objeto sino qué operaciones con el objeto se asientan en el registro de sucesos de seguridad del sistema (función de auditoría).

En un sistema autónomo la validación corre por cuenta del proceso winlogon y la configuración de seguridad almacenada en la propia máquina en las claves del registro: SECURITY y SAM. Donde la primera establece las políticas globales de seguridad y la segunda la seguridad específica de cada usuario.

En un sistema en red, la autenticación de los usuarios está centralizada en ciertos servidores denominados controladores del dominio. Los equipos se organizan dentro de Dominios, pudiendo éstos estar gestionados mediante el empleo del Active Directory.

Windows 2008 dispone de administración centralizada de certificados. En las versiones anteriores se confiaba que cada aplicación mantenía su propia lista de claves o CA confiables.

El protocolo KERBEROS (RFC 1510), que es un estándar de Internet para autenticación, es el método nativo que emplean los sistemas Windows 2008. Cualquier servidor del Directorio Activo, automáticamente, tiene el servicio del Centro de distribución de claves de Kerberos (KDC- Kerberos Key Distribution Center).

53.4.- BIBLIOGRAFÍA

- Sistemas Operativos Modernos. Tanenbaum, Andrew. Prentice Hall, 2005
- Linux Bible 2008 Edition. Christopher, N. Wiley Publishing, Inc 2008.
- Windows internals 5th Edition. Mark E. Russinovich, David A. Solomon, Alex Ionescu. Microsoft Press, 2009

Autor: Francisco Javier Rodriguez Martínez

Subdirector de Sistemas Escola Superior Enxeñaría Informática Ourense
Colegiado del CPEIG

54. SERVIDORES DE MENSAJERÍA. SISTEMAS DE CORREO.

Tema 54.- Servidores de Mensajería. Servidores de Correo

ÍNDICE

54.1 Servidores de Mensajería.....	2
54.1.1 Sistema de mensajería Centralizada	3
54.1.2 Sistema de mensajería Distribuido	3
54.2 Servidores de Correo.....	4
54.2.1 Sistemas de correo electrónico: arquitectura	6
54.2.2 SMTP (Simple Mail Transfer Protocol)	10
54.2.3 POP (Post Office Protocol)	14
54.2.4 IMAP - Internet Message Access Protocol	17
54.2.5 Formato de mensajes en internet	21
54.2.6 Extensiones de SMTP	23
54.2.6.1 ESMTP.....	23
54.2.6.2 MIME.....	24
54.3 Bibliografía.....	28

54.1 *SERVIDORES DE MENSAJERÍA*

Un servidor de mensajería es una aplicación que posee la capacidad para manejar mensajes entre dos o más entidades, ya sean aplicaciones de usuario u otros sistemas de gestión de mensajes. Los mensajes de un servidor de mensajería son enviados a través de un middleware, el cual facilita la comunicación entre los distintos elementos del sistema, utilizando generalmente un conjunto de reglas y especificaciones que posibilitan la comunicación entre las distintas partes. Otra de las características de los servidores de mensajería es la capacidad de almacenaje de los mensajes, este almacenamiento se produce generalmente en una cola hasta que es posible el envío del mismo hacia su destinatario, que por lo general resulta ser otra aplicación.

Es muy habitual encontrarse en una empresa u organización un sistema de mensajería funcionando en un servidor y esperando el envío de mensajes a su cola de entrada. Desde allí, el middleware analiza mensaje a mensaje determinando el destino de cada uno. Una vez en el servidor, un mensaje sólo tiene dos posibilidades de entrega, o ser enviado de manera local, o que éste tenga que ser redirigido a otro servidor de mensajería para que sea él el que realice la entrega. Si el mensaje ha de ser entregado a un destino local, entonces es enviado inmediatamente al buzón local. Por el contrario, si el mensaje es determinado como remoto, el servidor de mensajería debe enviar el mensaje a otro servidor de mensajería dentro de su entorno para que sea éste el que realice la entrega del mensaje.

Por lo general, si existen problemas de conexión entre los servidores o no es posible determinar la localización del servidor de mensajería remoto, el usuario el cual realizó el envío del mensaje es informado a través de un mensaje enviado por el servidor de mensajería, informando de la situación. Este tipo de mensaje suelen ser sólo de notificación de que se están teniendo problemas con el envío del mensaje, puesto que el servidor de

mensajería continuará intentando enviar el mensaje hasta que se agoten el número máximo de intentos de envío o hasta que el mensaje caduque, es decir, exceda un límite de tiempo de estancia en el servidor.

Los modelos de los servidores de mensajería suelen adaptarse a una arquitectura centralizada o seguir una solución distribuida.

54.1.1 Sistema de mensajería Centralizada

Un sistema de mensajería centralizada se fundamenta en un núcleo de datos, el cual aloja todos los recursos y servicios de los servidores que conforman el sistema. Este núcleo de datos permite que cualquier usuario del sistema de mensajería se conecte a los servicios de mensajería, ya sea de forma local o remota.

Las características de un sistema de mensajería centralizado son:

- **Datos:** Todos los datos y la información se encuentra albergada y se gestiona desde el núcleo, incluso cuando los usuarios establecen una conexión remota para su utilización. Esta centralización facilita en gran medida la administración de los servicios, puesto que provoca que ésta sea más sencilla.
- **Actualizaciones:** Las actualizaciones se han de realizar únicamente en el núcleo central, en donde se encuentra todo el sistema.
- **Ubicación:** El centro de datos añade al sistema dispositivos de aislamiento de la alimentación o sistemas de alimentación ininterrumpida (SAI). Proporciona además la posibilidad de ofrecer servicios incluso cuando se produce alguna incidencia de carácter grave, ya que posibilita la réplica de todo el sistema de una manera eficaz.

54.1.2 Sistema de mensajería Distribuido

Un sistema de mensajería distribuido está formado por una serie de sucursales repartidas en distintas ubicaciones conectadas entre sí. Cada

sucursal posee un servidor o servidores de mensajería con todos sus servicios de manera independiente del resto de sucursales. Cada uno de los servidores de mensajería realiza el envío de sus mensajes locales y redirige a los otros servidores aquellos mensajes que no son de dominio local y que sí son capaces de resolver alguno de los otros servidores.

- **Datos:** La información se encuentra también distribuida entre cada una de las sucursales y cada una de ellas gestiona y administra esta información y sus servicios, lo que provoca un aumento en la complejidad de estas tareas.
- **Actualizaciones:** Cada vez que se lleva a cabo una tarea de actualización ésta ha de realizarse en cada una de las sucursales, para que tenga efecto en todo el sistema.
- **Ubicación:** Cada sucursal posee su propio centro de datos, los cuales pueden ofrecer los mismos servicios que en una arquitectura centralizada.

54.2 SERVIDORES DE CORREO

Un servidor de correo es una aplicación que nos permite enviar mensajes (correos) de unos usuarios a otros, con independencia de la red que dichos usuarios estén utilizando.

Para lograrlo se definen una serie de protocolos, cada uno con una finalidad concreta:

- **SMTP, Simple Mail Transfer Protocol:** Es el protocolo que se utiliza para que dos servidores de correo intercambien mensajes.
- **POP, Post Office Protocol:** Se utiliza para obtener los mensajes guardados en el servidor y pasárselos al usuario.

- IMAP, Internet Message Access Protocol: Su finalidad es la misma que la de POP, pero el funcionamiento y las funcionalidades que ofrecen son diferentes.

Así pues, un servidor de correo consta en realidad de dos servidores: un servidor SMTP que será el encargado de enviar y recibir mensajes, y un servidor POP/IMAP que será el que permita a los usuarios obtener sus mensajes.

Para obtener los mensajes del servidor, los usuarios se sirven de clientes, es decir, programas que implementan un protocolo POP/IMAP. En algunas ocasiones el cliente se ejecuta en la máquina del usuario, sin embargo existe otra posibilidad: que el cliente de correo no se ejecute en la máquina del usuario; es el caso de los clientes vía web.

El correo electrónico es una de las aplicaciones TCP/IP más utilizadas en estos días. En su forma más sencilla, el correo electrónico, es una manera de enviar mensajes o cartas electrónicas de un computador a otro.

El correo electrónico de Internet se implementó originalmente como una función del protocolo FTP. En 1980 Suzanne Sluizer y Jon Postel realizaron trabajos con un protocolo que posteriormente se denominaría SMTP ("Simple Mail Transfer Protocol"). Hoy en día se sigue utilizando este protocolo, con los avances lógicos que requiere el tipo de transferencia actual.

El protocolo SMTP fue desarrollado pensando en que los sistemas que intercambiarían mensajes, eran grandes computadores, de tiempo compartido y multiusuario conectados permanentemente a la red Internet. Sin embargo, con la aparición de los computadores personales, que tienen una conectividad ocasional, se hizo necesaria una solución para que el correo llegase a estos equipos. Para solventar esta limitación, surgen los protocolos POP e IMAP.

Por lo tanto, podemos discriminar dos tipos de agentes que están involucrados en la transferencia de correo, MUA y MTA:

- Agente de usuario (MUA), interfaz para leer y escribir los mensajes, son los clientes finales.
- Agente de transporte (MTA o estafeta), encargado del transporte de los mensajes (SMTP). A la primera MTA a la que el cliente entrega su correo se la llama MSA (S de sending) y a la última que lo recibe y lo entrega al cliente destinatario se le llama MDA (D de delivering)
- Cuando un MTA no es el destinatario de un correo, se lo debe de entregar a otro y así hasta llegar a su destino. Este comportamiento es conocido como **Relay**.

Es muy importante configurar bien la función Relay de un MTA porque si se configura de forma abierta, se puede terminar siendo una fuente de SPAM.

54.2.1 *Sistemas de correo electrónico: arquitectura*

Los sistemas de correo electrónico se configuran para que trabajen de forma asíncrona en la comunicación, de forma que el cliente envía un mensaje y no tiene que esperar respuesta. De esta forma los buzones de correo y las funciones de transmisión y recepción de mensajes se ubican en un servidor de correo.

El servidor de correo permanece a la “escucha” de conexiones de otros servidores de correo para la recepción de mensajes con destino a sus usuarios, almacena los mensajes de correo recibidos en los buzones y realiza la transmisión de mensajes de los usuarios a otros servidores remotos, es decir, el servidor de correo actúa como un MTA.

Los usuarios de un servidor, interactuarán con él a través de un cliente de correo. Para la recuperación de mensajes se utiliza POP3 o IMAP4. El envío

de mensajes no se realizará directamente a los servidores remotos, sino que en primer lugar se enviará el mensaje al servidor de correo que le da servicio, mediante SMTP y será este servidor el que realice la transmisión definitiva del mensaje al servidor de correo remoto que albergue el buzón destino.

Teniendo en cuenta esto, la arquitectura de un sistema de correo incluye:

- Servidores de correo para el envío, recepción y almacenamiento de la información de los usuarios. Deberán ser correctamente configurados para poder ser alcanzables en el DNS.
- Clientes de correo utilizados por los usuarios para, básicamente, componer y leer correos electrónicos.
- Soporte para plataformas de acceso: hoy en día se puede acceder desde el puesto de trabajo en la intranet de la empresa, desde un equipo portátil en la extranet, hasta smartphones y PDA's.
- Sistema de almacenamiento de los mensajes en los respectivos buzones.
- Sistema de Directorio (Active Directory o LDAP) útiles para acceder a la información de los usuarios de la empresa (nombre, cargo, etc).

Clientes de correo

Los clientes de correo permiten a los usuarios interactuar con el sistema para enviar y recibir mensajes. Desde los inicios del correo electrónico, hasta hoy en día, podemos clasificar los clientes en:

- Clientes en modo texto: es el cliente accesible desde la interfaz de comandos Shell mediante una cuenta en la máquina que alberga el servidor de correo.

- Clientes pesados: software que se instala en el PC del usuario y gestionan todo el ciclo de vida de creación, envío y recepción de mensajes así como la posibilidad de almacenamiento local, por ejemplo Microsoft Outlook, Lotus Notes Thunderbird, etc.
- Clientes ligeros: no hace falta instalar ningún software en el PC, sino que el usuario accede al sistema de correo a través de una interfaz web con un navegador. La seguridad en la comunicación puede implementarse mediante SSL.
- Clientes en smartphones o PDAs: Permiten acceder a los mensajes en cualquier lugar y a cualquier hora. Suelen configurarse con IMAP4 como protocolo de recuperación para permitir que posteriormente, los mensajes procesados sean visibles también desde el PC.

Servidores de correo

Hasta hace pocos años a un servidor de correo se le pedía que gestionase correctamente el servicio del correo. Actualmente, se tiende a proporcionar una solución unificada de mensajería para una organización que integre mensajería móvil, mensajería instantánea, groupware, etc. con lo que la frontera entre servidores puros de correo electrónico y servidores generales de mensajería o entorno colaborativo está poco clara.

Para escoger un servidor u otro deberían de tenerse en cuenta las siguientes consideraciones:

- El cliente que se asocia al servidor, ya que algunos servidores exigen un tipo determinado de cliente, como Lotus Notes.
- Estrechamente relacionado con el anterior punto está la integración de servidor y cliente y, generalmente, se obtendrá una mejor integración cuando el servidor y el cliente son del mismo fabricante, como sucede con Microsoft Outlook y Microsoft Exchange Server o Lotus Notes y Lotus Domino.

- El nivel de gestión requerido, la solución de almacenamiento y la disponibilidad. Para una organización, puede resultar insuficiente en términos de rendimiento, flexibilidad y escalabilidad utilizar los discos de una máquina para almacenar los buzones de correo con lo que es más habitual contar con dispositivos de almacenamiento dedicados como soluciones NAS o SAN con conexiones rápidas de fibra óptica y que además facilitan el uso de clústeres activo/activo al permitir que un servidor asuma los buzones gestionados por otro en caso de caída.
- Es importante utilizar técnicas de benchmarking para evaluar las siguientes características:
 - o La capacidad de tratar correo concurrentemente.
 - o La velocidad de entrega.
 - o La extensibilidad y funciones implementadas.
 - o La estabilidad.
- Al tratarse de una aplicación crítica para una organización, el correo electrónico debe ser configurado como una solución de alta disponibilidad lo cual requiere el establecimiento de políticas de redundancia adecuadas para garantizar el servicio.

Actualmente los programas servidor de correo más extendidos son:

- Microsoft Exchange Server.
- Lotus Domino/Notes.
- Sendmail.

54.2.2 SMTP (Simple Mail Transfer Protocol)

El significado de las siglas de SMTP es Protocolo Simple de Transmisión de Correo. Este protocolo es el estándar de Internet para el intercambio de correo electrónico. SMTP necesita que el sistema de transmisión ponga a su disposición un canal de comunicación fiable y con entrega ordenada de paquetes, con lo cual, el uso del protocolo TCP (puerto 25) en la capa de transporte, es lo adecuado. Para que dos sistemas intercambien correo mediante el protocolo SMTP, no es necesario que exista una conexión interactiva, ya que este protocolo usa métodos de almacenamiento y reenvío de mensajes.

Realmente son tres los estándares que se aplican a un envío de correo de esta clase. El termino SMTP es frecuente y erróneamente usado para referirse a la combinación del grupo de los tres estándares involucrados en el envío de correo electrónico. Ello se debe a que los tres están estrechamente relacionados, pero estrictamente hablando SMTP es uno de los tres estándares. Los tres estándares son:

- Un estándar para el intercambio de correo entre dos computadores, el cual especifica el protocolo usado para enviar correo entre "host" TCP/IP. Este estándar es SMTP y está definido originalmente en el RFC 821, siendo actualizado en los RFC 2821 y RFC 5321 (octubre 2008).
- Un estándar del formato del mensaje de correo, contenido en dos RFC:
 - o RFC 822 describe la sintaxis de las cabeceras del correo electrónico y describe la interpretación del grupo de campos de la cabecera. Este protocolo ha sido actualizado en los RFC 2821 y 5322.
 - o RFC 1049 describe como un conjunto de documentos de tipos diferentes del texto ASCII plano se pueden usar en el cuerpo del correo. Los estándares son PostScript, Scribe, SGML, TEX,

TROFF y DVI. El nombre del protocolo oficial para este estándar es MAIL.

- Un estándar para el encaminamiento de correo usando el DNS (sistema de nombres de dominio), descrito en RFC 974. El nombre oficial del protocolo para este estándar es DNS-MX.

Funcionamiento

El protocolo SMTP es un protocolo cliente/servidor, por lo que siempre es el usuario SMTP el que inicia la sesión y el servidor de correo el que responde.

El protocolo SMTP se basa en la entrega de mensajes extremo a extremo. Cuando un servidor de SMTP, requiere transmitir un mensaje a otro servidor SMTP, el emisor (servidor que inicia la sesión SMTP) establece una conexión con el receptor (servidor que recibe petición de establecer sesión SMTP). Esta conexión es unidireccional, es decir, el emisor puede enviar correo al receptor, pero durante esa conexión, el receptor no puede enviar correo al emisor. Si el receptor tiene que enviar correo al emisor, tiene que esperar a que finalice la conexión establecida y establecer otra en sentido contrario, cambiando los papeles de emisor y receptor. Una vez establecida la conexión, el emisor envía comandos y mensajes.

El protocolo SMTP funciona con comandos y respuestas de texto escritas en ASCII-NVT (estándar USA - 7 bits).

Cada comando se envía al servidor SMTP al puerto 25 de manera predeterminada. A cada comando enviado por el cliente le sigue una respuesta del servidor SMTP compuesta por un código numérico de tres dígitos, seguido de un mensaje descriptivo. El número está pensado para un procesamiento automático de la respuesta, mientras que el texto permite que un humano interprete la respuesta.

En el protocolo SMTP todas las órdenes, respuestas y datos son líneas de texto, delimitadas por el carácter CRLF. Todas las respuestas tienen un código numérico al comienzo de la línea.

Flujo

Los pasos fundamentales para trabajar con el correo electrónico utilizando este protocolo son los siguientes:

- El cliente SMTP se conecta al servidor SMTP, realizando un telnet por el puerto 25 y espera respuesta.
- El servidor SMTP puede responder
 - o “220 Service Ready” junto con el nombre de dominio del servidor, si el servicio de correo está disponible.
 - o “421 Service not available” si el destinatario es temporalmente incapaz de responder.
- Si el servicio está disponible el cliente se tiene que identificar. Para ello envía el comando HELO seguido por el nombre de dominio de su equipo. Desde abril de 2001, las especificaciones para el protocolo SMTP, definidas en RFC 2821, indican que el comando HELO sea remplazado por el comando EHLO.
 - o Un receptor SMTP que no soporte el RFC 2821 responderá con un mensaje "500 Syntax error, command unrecognized". El emisor SMTP debería intentarlo de nuevo con HELO o, si no puede retransmitir el mensaje, enviar un mensaje QUIT.
 - o Si un receptor SMTP soporta las extensiones de servicio, responde con un mensaje “250 OK” que incluye una lista de las extensiones de servicio que soporta.

- El emisor inicia ahora una transacción enviando el comando MAIL FROM: al servidor. Este comando contiene la ruta de vuelta al emisor que se puede emplear para informar de errores. Si se acepta el comando, el receptor responderá con un mensaje "250 OK". Cualquier otro código indica error.
- El segundo paso del intercambio de correo consiste en darle al servidor SMTP el destinatario del mensaje (puede haber más de un receptor). Esto se hace enviando uno o más comandos "RCPT TO: <destinatarios>" (si hay más de un destinatario éstos irán separados por comas. Cada uno de ellos recibirá una respuesta "250 Recipient OK" si el servidor conoce el destino, o un "550 No such user here" si no.
- El siguiente paso es informar al servidor que se va a empezar a introducir el cuerpo del mensaje, para ello se utiliza la orden DATA.
- El servidor contesta con "354 Start mail input, end with <CRLF>. <CRLF>". Donde se indica que el final del mensaje se debe finalizar con un punto en una única línea, seguido de un retorno de carro.
- El cliente envía los datos línea a línea, acabando con la línea <CRLF>. <CRLF> que el servidor reconoce con "250 OK" o el mensaje de error apropiado si cualquier cosa fue mal.
- Una vez que el servidor recibe el mensaje finalizado con un punto puede almacenarlo si es para un destinatario que pertenece a su dominio, o bien retransmitirlo a otro servidor para que finalmente llegue a un servidor del dominio del receptor.
- Ahora hay varias acciones posibles:

- o El emisor no tiene más mensajes que enviar; cerrará la conexión con un comando *QUIT*, que será respondido con "221 Service closing transmission channel".
- o El emisor no tiene más mensajes que enviar, pero está preparado para recibir mensajes (si los hay) del otro extremo. Mandará el comando TURN. Los dos SMTPs intercambian sus papeles y el emisor que era antes receptor puede enviar ahora mensajes.

Si se requiere autenticación TLS/SSL la conexión se realiza a los puertos 465 o 587, en vez del puerto 25.

54.2.3 POP (Post Office Protocol)

El protocolo de oficina de correo, POP, es un protocolo cuya misión es la de entrega final del correo al destinatario, no sirve para enviar correos ni para enviarlos. Su objetivo principal es poder gestionar los correos sin tener que estar conectado a Internet, es decir, permite a los usuarios con conexiones intermitentes ó muy lentas (p.ej. módem), descargar el correo electrónico mientras tienen conexión y revisarlo posteriormente incluso estando desconectados.

Modelo de comunicaciones POP

La descripción del protocolo POP la podemos encontrar en el RFC 1939. La última versión del POP es la 3, por eso se suele referir a este protocolo como POP3.

El protocolo POP3 es un protocolo cliente/servidor, por lo que siempre es el usuario POP3 el que inicia la sesión y el servidor de correo el que responde.

El protocolo POP3 funciona con comandos y respuestas de texto escritas en ASCII.

El cliente POP se conecta con el servidor a través del puerto TCP, 110. Para conectarse al servidor, es necesario una cuenta de identificación en dicha

máquina (lo que le permite tener un espacio reservado para sus correos). A continuación es necesario verificar que es dueño de la cuenta a través de una clave. Una vez conectado al sistema, el cliente POP puede dialogar con el servidor para saber, entre otros, si existen mensajes en la casilla, cuántos mensajes son o para solicitar la descarga de alguno de ellos.

Cuando la conexión TCP está establecida, POP3 continúa con tres fases:

- **Autorización:** Se envía el login y password para identificar al usuario que quiere leer el correo. Cuando se verifica que el nombre y la clave son correctos, el servidor pasa a un estado de transacción. Antes de pasar a este estado, el servidor POP bloquea el buzón para impedir que los usuarios modifiquen o borren el correo antes de pasar al estado siguiente.
- **Transacción:** Se produce la manipulación del contenido del buzón del usuario.
- **Actualización:** Todas las modificaciones se realizan cuando el cliente finaliza el servicio (con el comando QUIT).

Por lo tanto, el protocolo POP3 administra la autenticación utilizando el nombre de usuario y la contraseña. Sin embargo, esto no es seguro, ya que las contraseñas, al igual que los correos electrónicos, circulan por la red como texto plano, sin cifrar. En realidad, según RFC 1939, es posible cifrar la contraseña utilizando un algoritmo MD5 y beneficiarse de una autenticación segura. Sin embargo, debido a que este comando es opcional, pocos servidores lo implementan. Además, el protocolo POP3 bloquea las bandejas de entrada durante el acceso, lo que significa que es imposible que dos usuarios accedan de manera simultánea a la misma bandeja de entrada.

Flujo

Los pasos fundamentales para trabajar con el correo electrónico utilizando este protocolo son los siguientes:

- El cliente establece una conexión TCP en el puerto 110 del servidor POP.
- El servidor POP responderá con un indicador de estado y una palabra clave. Si el servicio está disponible responderá con el indicador de estado +OK, en caso contrario responderá con -ERR.
- Si el servicio está disponible se pasa a la fase de autorización y el cliente se identificará con los comandos USER y PASS.
- Si la información es correcta, el servidor responderá con +OK y da acceso exclusivo al buzón.
- El cliente puede interactuar con el buzón, para ello utiliza los siguientes comandos
 - o LIST muestra los correos que hay en el buzón y su tamaño.
 - o STAT da el número de correos no borrados en el buzón y su longitud total.
 - o TOP <nº_mens> <num_líneas> muestra n líneas del correo, cuyo número se da en el argumento. En el caso de una respuesta positiva del servidor, éste enviará de vuelta los encabezados del correo, después una línea en blanco y finalmente las primeras n líneas del correo.
 - o RETR < nº_mens > recoge un correo especificado por su número
 - o DELE <nº_mens> borra un correo especificado por su número.
 - o RSET recupera los correos borrados (en la conexión actual).

- o UIDL obtiene el listado con todos los identificadores únicos de mensajes. El servidor asigna un identificador único a cada mensaje, de modo que no cambie su identificador entre sesiones. Este identificador es el UID.
- Para terminar la sesión POP se utiliza el comando QUIT. Se eliminan aquellos mensajes que han sido marcados con el comando DELE. Hasta que no se invoca a la orden QUIT los mensajes marcados no son borrados del buzón.

Si se requiere autenticación TLS/SSL la conexión se realiza al puerto 995, no al puerto 110.

54.2.4 *IMAP - Internet Message Access Protocol*

El protocolo IMAP (Protocolo de acceso a mensajes de Internet) es un método utilizado por las aplicaciones cliente de correo electrónico para obtener acceso a los mensajes almacenados remotamente. En este caso, los mensajes no son recuperados por el gestor de correo, sino que se trabaja con ellos directamente sobre el servidor.

Es un protocolo más complejo que POP3. Algunas ventajas sobre el anterior son:

- Las transacciones IMAP pueden durar mucho más tiempo.
- El servidor guarda información del estado de los mails (si fueron leídos o no, si fueron guardados en una carpeta, etc).
- Se pueden definir distintas carpetas para acceder a distintos buzones.
- Se pueden devolver partes del mensaje al cliente, ahorrando ancho de banda.
- Se puede conectar más de un cliente al mismo buzón.

- Posee buscadores que se ejecutan en el servidor.
- A diferencia de POP (donde el Cliente debe estar conectado al Servidor para que se realicen los cambios), IMAP permite a los Clientes realizar cambios tanto estando estos conectados como desconectados.
- Es totalmente compatible con diferentes estándares de mensajes de Internet, como MIME.

Sin embargo posee ciertas desventajas:

- Es más complejo de implementar que POP3.
- El servidor debe ser más potente para atender a todos los usuarios. Consume más recursos de CPU, memoria, etc.

El protocolo IMAP es un protocolo cliente/servidor, por lo que siempre es el usuario IMAP el que inicia la sesión y el servidor de correo el que responde.

Los clientes IMAP pueden acceder siguiendo uno de estos tres modos de conexión:

- **Modo offline.** Periódicamente se conecta al servidor para descargar mensajes nuevos y sincronizar cualquier cambio que haya podido suceder en las diferentes carpetas. Existe la posibilidad de borrar los mensajes a medida que los descargamos, siguiendo un funcionamiento muy parecido a POP3.
- **Modo online.** Se accede directamente a la copia de los mensajes del servidor exactamente cuando hace falta, sincronizando los cambios prácticamente al vuelo.
- **Modo desconectado.** En este caso el cliente trabaja con una copia local mientras que no tiene acceso a internet, creando/borrando/leyendo sus emails. La próxima vez que se conecte

a Internet estos cambios se sincronizarán con la copia maestra del servidor.

El protocolo IMAP funciona con comandos y respuestas de texto escritas en ASCII. Actualmente la versión operativa es la 4 por eso a este protocolo también se le conoce como IMAP4.

Dado que se parte de un modelo en el que los mensajes se guardan normalmente en el servidor después de ser leídos, IMAP define una manera sencilla de administrarlos: con buzones de correo, es decir, con carpetas. Éstas siguen una jerarquía de tipo árbol. Siguiendo el estándar siempre existirá un buzón de entrada que será el principal, pero podremos crear otras carpetas con diferentes atributos. Por ejemplo, existen atributos para especificar que una carpeta contiene sólo correos (*\NoInferiors*) o sólo carpetas (*\NoSelect*), pero también pueden tener otros atributos que indiquen si existen o no mensajes nuevos desde la última vez que la abrimos (*\Marked* y *\Unmarked*).

Una clase parecida de etiquetas pueden tener los correos que se reciban y/o envíen. Uno de los más usados será el que indica si está leído o no (*\Seen*), pero también existen otros que indican que el mensaje ha sido contestado (*\Answered*), que el mensaje ha sido destacado (*\Flagged*), que es un borrador (*\Draft*), etc... Toda esta información se guarda directamente en el servidor y no en el cliente, lo que permite sincronizar perfectamente estos metadatos entre varios clientes.

En la RFC 2060 (actualmente la RFC 3501) se definen las instrucciones para poder interactuar con el servidor de correo y sus buzones.

Fases de una Sesión IMAP. Al igual que en el POP3, en una sesión IMAP existen las siguientes fases:

- Non-authenticated state: En este estado el Cliente aún no se ha autenticado con el Servidor.

- **Authenticated state:** El Cliente ha sido autenticado por el Servidor y debe seleccionar un buzón para interactuar.
- **Selected state:** El cliente ha seleccionado un buzón y se pueden realizar acciones sobre los correos contenidos en él.
- **Logout state:** La conexión ha sido finalizada.

Flujo

Los pasos fundamentales para trabajar con el correo electrónico utilizando este protocolo son los siguientes:

- El cliente establece una comunicación TCP con el servidor IMAP por el puerto 143.
- El servidor responde con OK si el servicio está disponible; en caso contrario el servidor responderá con BAD.
- A continuación el cliente tiene que identificarse mediante el comando `LOGIN <usuario> <password>`, para poder acceder a los buzones. Esta es una forma no segura porque la password no va cifrada. Se puede utilizar el comando `AUTHENTICATE` para autenticar al usuario de forma segura.
- Si los datos son correctos el servidor responde OK. Si se produce un fallo de autenticación devolverá un NO. Si los argumentos no son válidos devolverá un BAD.
- Ahora el cliente puede interactuar con sus mensajes. Para ello usa los comandos:
 - o `LIST` para ver los buzones existentes.
 - o `SELECT <nombre_buzón>` para ver el contenido de un buzón determinado.

- o CREATE <nom_buzón_nuevo> para crear buzones.
 - o DELETE <nombre_buzón> para borrar buzones.
 - o RENAME <nombre_buzón_old> <nombre_buzon_new> para renombrar buzones.
 - o FETCH <num_mens> <parte_mens> para ver las diferentes partes de los mensajes del buzón que se haya seleccionado.
 - o CLOSE cierra el buzón y borra los mensajes marcados para borrar.
 - o EXPUNGE borra todos los mensajes marcados para borrar.
 - o SEARCH busca mensajes según algún criterio de búsqueda.
 - o COPY copia los mensajes de una carpeta a otra.
- Con el comando LOGOUT se termina la sesión.

Si se requiere autenticación TLS/SSL la conexión se realiza al puerto 993, no al puerto 143.

54.2.5 *Formato de mensajes en internet*

La RFC 2822 define el estándar del formato de mensaje de Internet. El correo electrónico se divide en dos partes separadas por una línea en blanco.

- La cabecera del mensaje.
- El cuerpo del mensaje.

Cuerpo del mensaje. Contiene la información que se intercambian el emisor y el receptor. La forma en que está codificada viene determinada por el RFC 2231.

Encabezados del mensaje. Es la metainformación colocada antes del cuerpo del mensaje. En general, el software de transporte de correo no revisa ni altera los encabezados del correo, a excepción de la cabecera Received. Están formadas por la tupla Palabra_clave: valor. Las cabeceras más importantes son:

- From: Dirección del emisor del mensaje.
- Reply-to: Cuenta de correo a donde se dirigirán las respuestas al correo. En ausencia de este campo las respuestas se dirigirán a la/s dirección/es indicadas en el campo From.
- To: Este campo contiene la/s direcciones del/de los principal/es destinatario/s del mensaje.
- Cc: Copia a destinatarios. Campo que indica la/s dirección/es a las que se les hará llegar una copia del correo, aunque el contenido del mensaje puede que no vaya dirigido expresamente a ellos.
- Bcc: Copia oculta. Se manda una copia a los destinatarios aquí indicados sin que el resto de destinatarios tengan conocimiento de ello.
- Message-ID: Es un identificador único de cada mensaje. Este código es asignado por el servidor de donde sale el mensaje. Este identificador no se puede cambiar ni modificar.
- Reference: Contiene todos los Message-ID de los mensajes a los que éste hace referencia. Este campo es generado por la aplicación cliente.
- Keywords: Palabras clave que identifican el contenido del mensaje.
- Return-Path: Contiene la trayectoria de regreso al remitente.

- Received: Es la información que se utiliza para comprobar los problemas que hayan aparecido en el reparto de un mensaje. En ella se muestran las direcciones de las máquinas por las que pasó el mensaje en dirección a su destino, junto con la fecha y hora en que lo hizo.
- Date: Fecha y hora en la que el mensaje es entregado a la cola del servidor SMTP para su envío. Este campo lo establece el servidor origen.
- Subject: Este campo contiene un pequeño texto con la descripción del asunto del mensaje.
- X- : Son campos definidos por el usuario. Siempre tienen que empezar por X-, seguidos del nombre que se le quiera asignar al campo. Por ejemplo X-mailer: “Mi gestor de correo”. Se está utilizando una cabecera X-SPAM para marcar correos como presuntos correos basura.

Sólo las cabezas subrayadas son obligatorias según el estándar.

54.2.6 *Extensiones de SMTP*

54.2.6.1 ESMTP

El protocolo ESMTP es una extensión del protocolo SMTP, definido en la RFC 4954.

Se trata de un mecanismo para autenticar la identidad del cliente que se conecta al servidor, y además permite la negociación de una capa de seguridad para hacer más segura la comunicación. El protocolo SMTP permanece inalterado, lo que se hace es agregar los siguientes comandos:

- EHLO dominio: Hace que el servidor realice una consulta al DNS del reverso del dominio indicado para verificar que el mismo exista.

- ETRN dominio (Extended Turn). Este comando permite que el cliente le pida al servidor que le envíe todos los mensajes que posee destinados al cliente. Si hay mensajes para la máquina cliente, el servidor debe iniciar una nueva sesión SMTP para enviarle los mensajes.
- AUTH: Comando que sirve para negociar un protocolo de seguridad para el intercambio de datos. Los posibles protocolos, para la capa de seguridad, que se pueden negociar los da como respuesta el servidor al comando EHLO.

54.2.6.2 MIME

El protocolo SMTP impone determinadas restricciones sobre el contenido de los mensajes:

- El contenido sólo debe estar compuesto de caracteres ASCII, no se puede enviar ficheros binarios como audio, video, documentos, etc.
- Las líneas no pueden exceder los 100 caracteres.
- El tamaño total del contenido no puede exceder una determinada dimensión.
- Además, también existen problemas a la hora de enviar mensajes en lenguajes distintos del inglés:
 - o Lenguajes sin alfabetos “occidentales” (chino, japonés)
 - o Lenguajes con alfabetos no latinos (ruso, árabe)
 - o Lenguajes con acentos (alemán, castellano)

Para solventar estas limitaciones se han definido las especificaciones MIME (Multipurpose Internet Mail Extensions) que son unas extensiones del correo electrónico utilizadas también en otros protocolos como el HTTP que permiten la transmisión de datos no ASCII, a través de e-mail, en el cuerpo del mensaje.

MIME no cambia a SMTP ni lo reemplaza, por lo que los mensajes a enviar con MIME también cumplirán este protocolo. Dado que SMTP utiliza para comandos y respuestas el ASCII de 7 bits, el camino seguido para transmitir cualquier fichero es transformar (codificar) el fichero no ASCII en ASCII de 7 bits (haciéndolo compatible con SMTP), transmitirlo en este formato y reconvertirlo en destino al formato original (decodificarlo).

MIME incorpora las siguientes características al servicio de correo electrónico:

- Capacidad de enviar múltiples adjuntos en un solo mensaje.
- Longitud ilimitada del mensaje.
- Uso de conjuntos de caracteres no pertenecientes al código ASCII.
- Uso de texto enriquecido (diseños, fuentes, colores, etc.).
- Adjuntos binarios (ejecutables, imágenes, archivos de audio o video, etc.), que se pueden dividir de ser necesario.

Las cabeceras descritas en la RFC 2822 son suficientes para enviar correo codificado en texto ASCII, pero no son adecuadas para mensajes multimedia. Para ello MIME añade unas cabeceras que describen el tipo de contenido del mensaje y el tipo de código. Estas son:

- **MIME-Version:** Contiene la versión de las extensiones MIME empleadas en el mensaje.

- **Content-Transfer-Encoding:** Señala como ha sido codificado el mensaje para su transmisión por e-mail, de forma que pueda viajar sin problemas de que sea corrompido desde el destinatario al receptor a través de los agentes de correo (MUAs). Para transferir datos binarios, MIME ofrece cinco formatos de codificación:

- o 7bit: Significa que el fichero es SÓLO texto ASCII (caracteres no acentuados). Las líneas deben ser "cortas", de 100 caracteres o menos, terminando con CRLF.
- o Quoted-Printable: Utilizado por texto que es mayoritariamente US-ASCII (7 bit) pero con un pequeño porcentaje de caracteres "extraños" (8 bit). Este es el caso del castellano.

En esta codificación, cada carácter de 8-bits es codificado en tres caracteres de 7 bits, el primero el signo igual (=) y el valor hexadecimal del carácter. Por ejemplo, la "ñ", "F1" en hexadecimal, se codifica como "=F1".

- o base64: usado para codificar secuencias arbitrarias de octetos de forma que satisfaga las reglas de 7bit. Se utiliza para enviar binarios.
 - o 8bit: formato de texto de 8 bits.
 - o binary: envío de binarios.
- **Content-Type:** indica que tipos de datos contiene el mensaje. Un tipo de MIME está compuesto de la siguiente manera: tipo_mime_principal/subtipo_mime Pueden encontrarse los siguientes tipos:
- o text: texto con o sin formato.
 - o image: imágenes estáticas.

- o video: imágenes dinámicas, puede incluir audio.
- o audio: sonido.
- o message: significa que el contenido está configurado según el estándar RFC 822; esto puede ser usado para reexpedir mensajes.
- o application: se emplea para señalar que el contenido es para ser enviado a un programa externo, por ejemplo, texto para una impresora PostScript.
- o multipart: un mensaje también puede tener varias partes con varios contenidos separados, incluso de tipos diferentes (texto, audio e imágenes). Incluso cada parte puede tener subpartes (ser a su vez multiparte), puesto que el formato MIME puede ser recursivo.

Aparte del tipo, también se puede especificar un subtipo, ambos separados por una barra inclinada /. Por ejemplo image/gif es una imagen en formato GIF; el tipo es image y el subtipo gif; text/html, text/plain, etc.

Si el tipo es multipart, los subtipos admitidos son:

- o mixed: permite que en un solo mensaje contenga varios submensajes independientes, cada uno con su tipo y codificación. De esta forma se puede incluir en un mensaje imágenes, audio, video....
- o parallel: permite incluir en un mensaje subpartes que se pueden ver simultáneamente, por ejemplo reproducir audio y video.
- o digest: permite incluir en un mensaje varios mensajes.

- o **alternative:** permite que en un mismo mensaje se pueda incluir una única información pero en diversos formatos. Esto es útil cuando los destinatarios tienen distinto hardware y/o sistema operativo.

Finalmente, puede tener parámetros opcionales empezando por un punto y coma ;. Por ejemplo, el parámetro `charset=` en `Content-type: text/plain; charset=iso-8859-1`, indica que el cuerpo del mensaje utiliza el juego de caracteres ISO-8859-1.

54.3 **BIBLIOGRAFÍA**

- Internet y Correo electrónico. Silva Salinas, Sonia; López Sanjurjo, Catherin, (aut.) Ideaspropias Editorial. 2007
- Correo electrónico. Romero Dueñas, Carlos u Gonzalez Hermonso, Alfredo. Edelsa, 2001

Autor: Francisco Javier Rodriguez Martínez

Subdirector de Sistemas Escola Superior Enxeñaría Informática Ourense

Colegiado del CPEIG

55. SERVIDORES DE APLICACIONES Y SERVIDORES WEB.

Tema 55.- Servidores Web y Servidores de Aplicaciones

Tema 55.- Servidores Web y Servidores de Aplicaciones

55.1 Servidores Web

- 55.1.1 Introducción Cliente/Servidor*
- 55.1.2 Servidores Web*
- 55.1.3 Características de los servidores web*
- 55.1.4 Arquitectura*
- 55.1.5 Apache*
- 55.1.6 Microsoft IIS*
- 55.1.7 Lighttpd*

55.2 Servidores de Aplicaciones

- 55.2.1 Servicios proporcionados por un servidor de aplicaciones*
- 55.2.2 Estándar J2EE*
- 55.2.3 Estructura de un servidor de Aplicaciones*
- 55.2.4 Oracle Weblogic (Antes BEA WebLogic)*

55.3 Servidores de Aplicaciones y Servidores Web

55.4 Bibliografía

55.1 Servidores Web

55.1.1 Introducción Cliente/Servidor

La tecnología Cliente/Servidor consiste en el procesamiento cooperativo de la información mediante un conjunto de procesadores, en el cual múltiples clientes, geográficamente dispersos, pueden realizar peticiones a uno o más servidores centrales.

Desde una perspectiva funcional, podemos definir cliente-servidor como una arquitectura distribuida que permite a los usuarios obtener acceso de forma transparente a la información. Este tipo de arquitectura es la más extendida en los sistemas distribuidos.

Un sistema cliente servidor se basa en las siguientes características:

- *Servicio*: el servidor los proporciona y el cliente los utiliza.
- *Recursos compartidos*: son muchos los clientes que emplean los mismos servidores mediante los cuales comparten recursos no sólo lógicos sino también físicos.
- *Protocolos asimétricos*: los clientes son los encargados de iniciar la comunicación con el servidor, los cuales esperan el establecimiento de la conexión de forma pasiva.
- *Transparencia de localización*: los clientes no saben donde se localizan físicamente los recursos que desean utilizar.
- *Independencia de la plataforma*.
- *Sistemas débilmente acoplados*: Interacción basada en envío de mensajes.

- *Encapsulamiento de servicios*: la implementación que los servidores realizan de los servicios son transparentes para los clientes.
- *Escalabilidad horizontal*: incorporar nuevos clientes.
- *Escalabilidad vertical*: aumentar la potencia de los servidores.
- *Integridad*: tanto los datos como los programas están centralizados en servidores que facilitan su integridad y mantenimiento.

55.1.2 Servidores Web

Un servidor http o servidor web es un programa que permite procesar las peticiones de los distintos navegadores, sirviendo los recursos que estos soliciten mediante los protocolos HTTP o HTTPS. De forma general, un servidor web funciona de manera muy simple, ejecutando constantemente las siguientes acciones:

1. Esperar peticiones en el puerto TCP indicado.
 - a. Por defecto se empleará el puerto 80.
2. Recibir una petición.
3. Procesar la solicitud.
4. Enviar al cliente la respuesta obtenida, empleando la misma conexión por la que se recibió la petición.
5. Volver a esperar nuevas peticiones.

Si un servidor web se ciñe al patrón anterior, cumplirá todos los requisitos básicos de los servidores HTTP, aunque se verá limitado a servir ficheros estáticos. Los servidores web existentes actualmente se han diseñado e implementado a partir del patrón anterior, donde la variación entre ellos

sólo radica en el tipo de peticiones que van a atender, si son o no multiproceso, etc.

55.1.3 Características de los servidores web

- *Servir ficheros estáticos:* un servidor web debe ser capaz de servir ficheros estáticos que se localicen en algún lugar del disco (Requisito imprescindible).
 - o Debe ser posible especificar qué parte del disco se servirá.
 - o Aunque un servidor pueda especificar un directorio por defecto, no debe obligar a emplear uno concreto.
 - o En muchos servidores es posible especificar otros subdirectorios o directorios, indicando en qué punto del sistema de ficheros virtual del servidor irán localizados los recursos.
- *Seguridad:* un servidor web debe poder especificar directivas de seguridad, esto es, establecer quién puede acceder a qué recursos.
 - o Algunos servidores permiten especificar los ficheros que se considerarán como índice del directorio.
- *Contenido dinámico:* es una de las características fundamentales. Indica la capacidad del servidor para ofrecer contenido dinámico.
 - o La gran mayoría del contenido web que se sirve es dinámico.
 - o Punto fundamental a la hora de elegir un servidor.
- *Soporte para distintos lenguajes:* la mayor parte de los servidores ofrece soporte para algunos lenguajes de programación como:
 - o PHP

- o JSP: para que un servidor atienda peticiones JSP requerirá algún tipo de software para funcionar, como un contenedor de Servlets.
- o ASP
- o CGI (sistema más antiguo y sencillo para generar contenido dinámico.)

Antes de seleccionar un lenguaje de programación de servidor, es necesario considerar, si se desea un lenguaje más estándar que pueda ser atendido por cualquier servidor genérico o bien, si se prefiere una arquitectura concreta, etc.

55.1.4 *Arquitectura*

La arquitectura de un servidor web se divide en:

1. Capa servidor
2. Capa soporte

Capa servidor: contiene 5 subsistemas, cuya función es la de implementar las funcionalidades del servidor.

- *Subsistema de recepción:* es el encargado de esperar las peticiones del cliente a través de la red.
 - o Tiene la capacidad de manejar peticiones simultáneas, pudiendo analizarlas para determinar si son o no compatibles con el navegador.
- *Analizador de peticiones:* asocia al recurso de red un archivo local.
- *Control de acceso:* se encarga de validar y permitir el acceso.
- *Controlador de recursos:* fija el tipo de recurso que se ha solicitado, lo ejecuta y obtiene la respuesta.

- *Registro de transacción:* su función es registrar las peticiones junto con sus respuestas.

Capa soporte: conforma la interfaz entre el servidor web y el sistema operativo, y maneja los siguientes subsistemas.

- *Útil:* contiene las funciones que utilizan los otros subsistemas.
- *Capa abstracta del sistema operativo:* encapsula el funcionamiento del sistema operativo para facilitar la portabilidad del servidor entre las diferentes plataformas.

55.1.4.1 Funcionamiento del servidor web

Un servidor web se ejecuta esperando peticiones por parte de un navegador web (cliente) y atendiendo a dichas peticiones de forma adecuada, respondiendo mediante un mensaje de error o una página web con la respuesta a la petición formulada.

Por ejemplo, si tecleamos www.xunta.es en un navegador, el proceso que se desencadena es el siguiente:

- El navegador realiza una petición HTTP al servidor de la dirección solicitada.
- El servidor responde enviando el código HTML de la página solicitada.
- El cliente recibe el código de la página, lo interpreta y lo muestra en pantalla.

Es el cliente el encargado de interpretar el código HTML, mostrar los textos y objetos de la página, sus colores, fuentes, etc. El servidor por su parte se limita a transmitir el código de la página sin realizar ningún tipo de interpretación de dicha página.

Un servidor web, además de transmitir código HTML, también puede

entregar aplicaciones web, que son segmentos de código que se ejecutan cuando se producen ciertas peticiones o respuestas HTTP.

Es necesario distinguir entre:

1. *Aplicaciones en el lado del cliente:* es el navegador web el encargado de ejecutar estas aplicaciones en el equipo del usuario (scripts). En esta categoría encontramos aplicaciones como Applets de Java o Javascript.
 - El servidor proporciona el código de estas aplicaciones al cliente y es el navegador de éste, el que las ejecuta.
 - Es necesario que el navegador del cliente disponga de la capacidad para ejecutar estas aplicaciones.
 - Por defecto, la mayoría de los navegadores permite ejecutar scripts de java y javascript, aunque mediante plugins pueden añadirse más lenguajes.
2. *Aplicaciones en el lado del servidor:* es el servidor el encargado de ejecutar la aplicación, la cual, una vez ejecutada genera un código HTML que el servidor toma y lo envía al navegador del cliente mediante HTTP.

Generalmente la opción que se escoge es la de las aplicaciones en el lado del servidor, ya que al ejecutarse en el servidor y no en el equipo del cliente, éste no requiera de ningún tipo de software o funcionalidad añadida, mientras que en el caso de las aplicaciones en el lado del cliente, sí que es necesario.

55.1.5 Apache

El servidor Apache es un servidor web de código abierto, que se desarrolla dentro del proyecto HTTP Server de la Apache Software Foundation, y que puede ser instalado en plataformas Windows, Unix, Mac y otras. Este servidor viene instalado en la mayoría de distribuciones de Linux y en Mac OS X, Apache viene integrado como parte de su propio servidor web.

Se trata del servidor web más empleado, y si bien presenta algunas vulnerabilidades de seguridad, la gran mayoría de estas sólo podrían ser explotadas de forma local y no remotamente.

55.1.5.1 httpd.conf

Apache puede ser configurado mediante el fichero *httpd.conf*. Cada vez que se introduzca una modificación en este fichero, será necesario reiniciar el servicio apache. Se trata de un servidor altamente configurable, si bien su interfaz gráfica no es demasiado intuitiva.

El fichero de configuración *httpd.conf* puede dividirse en varias secciones:

- *Sección 1:* Entorno global. Sección del fichero donde se localizan las rutas a otros ficheros de configuración y se describe el funcionamiento general del servidor.
- *Sección 2:* Entorno servidor principal. Sección del fichero donde se describe la configuración que no atiende a las peticiones de los servidores virtuales. Se trata del comportamiento predeterminado del servidor.
- *Sección 3:* Entorno de servidores virtuales. Sección del fichero donde se pueden configurar servidores virtuales para trabajar con el mismo programa.

55.1.5.1.1 Directivas de entorno global

La configuración se realiza mediante directivas, variables almacenadas en un archivo de texto, que permiten alterar y controlar el funcionamiento de Apache en función de los valores que estas tomen.

- *ServerType*: permite indicar cómo será la respuesta del servidor.
 - o *Inetd*: se ejecuta cuando hay una petición.
 - o *Standalone*: siempre existe un proceso httpd en ejecución y este crea nuevos hijos para las conexiones con los diferentes clientes.
- *ServerRoot*: permite detallar el directorio que actuará como raíz del servidor.
- *Timeout*: permite especificar el número de segundos que se mantiene a la espera un servidor, desde que se recibe la petición hasta que se entiende la conexión como inactiva.
- *MaxClients*: limita el número máximo de clientes que se pueden conectar de forma simultánea. Si este número se supera, los clientes son bloqueados.
- *Listen*: permite a Apache atender peticiones en otra dirección y/o puertos además de los establecidos por defecto.
- *BindAddress*: se emplea para especificar qué direcciones o IPs deben atenderse en el servidor. Permite dar soporte a servidores virtuales.
- *LoadModule*: permite cargar un nuevo módulo para aportar mayor funcionalidad al servidor.

55.1.5.1.2 Directivas de configuración del servidor principal

- *Port*: permite especificar el puerto en que escuchará el servidor. Sólo

puede existir una directiva *Port*, mientras que se pueden especificar varias *Listen*.

- *User y Group*: permite indicar el usuario o grupo que puede iniciar la ejecución de httpd.
- *ServerAdmin*: establece la dirección de correo electrónico a la que enviar los problemas que puedan surgir. Esta dirección se mostrará en las páginas de error que genera el servidor.
- *ServerName*: permite asignar el nombre del servidor, que será mostrado a los clientes. No es aconsejable emplear el nombre real de la máquina.
- *ServerSignature on/off/email*: se emplea para que en caso de acceso a una página inexistente, el servidor devuelva una página de error indicando la versión de Apache y el nombre de la máquina.
- *DocumentRoot*: especifica el directorio en que se emplazan los documentos web que el servidor podrá a disposición de los clientes.

55.1.5.2 Módulos de Apache

Apache es un servidor estructurado en módulos cuya configuración se realiza mediante la modificación de las directivas presentes en cada módulo.

Los módulos de Apache pueden ser clasificados en los siguientes grupos:

- Módulos base: módulos que engloban las funciones básicas de Apache.
- Módulos multiproceso: módulos que se encargan de la interconexión

con los puertos del ordenador, aceptando las peticiones y enviando a los distintos hilos a atender las peticiones. Módulos adicionales: cualquier módulo que incorpore una funcionalidad al servidor.

55.1.6 Microsoft IIS

IIS (Internet Information Services) es un servidor web específico para el sistema operativo Microsoft Windows. IIS convierte un ordenador en un servidor Web, que permite publicar páginas web y hacerlas accesibles localmente, hacia una intranet o hacia Internet, además proporciona las funciones y herramientas necesarias para realizar de forma sencilla la administración de un servidor web seguro.

IIS se basa en diversos módulos que le proporcionan la capacidad de servir varios tipos de páginas, como ASP (Active Server Pages), ASP.NET, PHP o Perl.

55.1.6.1 Administración de IIS

La última versión de IIS es la 7, aplicable a Windows 7, Windows Server 2008, Windows Server 2008 R2 y Windows Vista.

En IIS7 hay varias herramientas para realizar su administración y configuración. Entre las cuales se incluyen:

- Administrador de IIS.

- Herramienta de línea de comandos denominada Appcmd.exe.
- Almacén de configuración de IIS que consta de archivos ApplicationHost.config y Web.config.
- Espacio de nombres de Instrumental de administración de Windows (WMI).

55.1.7 *Lighttpd*

lighttpd es un servidor web libre, distribuido bajo la licencia BSD, diseñado para ser rápido, seguro, flexible, y respetuoso con los estándares. Está diseñado para entornos donde la velocidad es muy importante y se requieren respuestas rápidas y de alta escalabilidad. Consume menos memoria y procesador que otros servidores.

Algunas características de lighttpd son:

- Permite la comunicación con programas externos mediante SCGI o FastCGI.
- Tiene un módulo de reescritura y de redirección de URLs.
- Se han hecho mejoras específicas para su integración con PHP y Ruby on Rails.
- Permite módulos externos.
- Permite VirtualHosting.
- Puede servir tanto HTTP como HTTPS.
- Autenticación con LDAP, htpasswd o MySQL.

- Acepta Webdav.

Lighttpd puede usarse solo o combinado con otros, de hecho, es habitual emplearlo para liberar de carga a otros servidores más lentos, especialmente cuando hay que realizar el envío de ficheros grandes que suele ser mucho más rápido que en el resto de servidores. Es común encontrar Lighttpd en combinación con instalaciones de Apache, para hacerlo más escalable y rápido en situaciones de carga.

55.2 Servidores de Aplicaciones

Por servidor de aplicaciones entendemos a aquel que permite la ejecución de una serie de aplicaciones. Habitualmente se trata de un programa software que gestiona casi por completo las funciones de lógica de negocio y de acceso a los datos de la aplicación. Su propósito es gestionar centralizadamente la forma en que los clientes se conectan a la base de datos o a los servicios con los que éstos deben interactuar.

Los servidores de aplicaciones comienzan a surgir cuando se hace patente que las aplicaciones cliente/servidor iban a presentar problemas de escalabilidad cuando se tratase de servir a un gran número de usuarios. Además era necesario trasladar las reglas de negocio a un lugar intermedio entre los clientes y la base de datos.

El concepto de servidor de aplicaciones está muy ligado con el de sistema distribuido, los cuales permiten mejorar 3 aspectos fundamentales en una aplicación:

- *La alta disponibilidad:* se refiere a la necesidad de que un sistema funcione 24 horas al día, todos los días. Para poder cumplir con esta característica son necesarias técnicas de balanceo de carga y de recuperación ante fallos.
- *La escalabilidad:* consiste en la capacidad de hacer crecer un sistema cuando aumentan el número de peticiones. Cada sistema puede atender a un número limitado de peticiones, puesto que sus recursos son finitos, al añadir nuevos equipos la cantidad de recursos se multiplica y con ello el número de peticiones que pueden ser

atendidas.

- *El mantenimiento:* tiene que ver con la facilidad para realizar actualizaciones, depurar fallos y mantener el sistema.

55.2.1 *Servicios proporcionados por un servidor de aplicaciones*

- *Gestión de la sesión:* el servidor debe conservar la información entre peticiones de un usuario mientras dure dicha sesión.
 - Esta es una característica fundamental para las aplicaciones de comercio electrónico, que requieren establecer al usuario a través de su navegación por el sitio web, sin embargo, el protocolo http es un protocolo sin sesión, por lo que no permite mantener una conexión abierta entre cliente y servidor más allá de lo que dura la transferencia de información. Por ello son los servidores de aplicaciones los que se encargan de todo lo relacionado con la gestión de la sesión.
- *Balanceo de carga:* un servidor de aplicaciones debe proporcionar técnicas para equilibrar su propia carga, es decir, debe ser capaz de repartir el procesamiento entre diversos servidores, lo cual es fundamental para su escalabilidad.
 - Las peticiones que realizan los clientes se transmiten a la máquina que esté menos ocupada en cada momento, lo cual mejorará el rendimiento global de la aplicación.
 - Con un buen balanceo de carga, además de conseguir un sistema más escalable, se consigue una mayor tolerancia a fallos.
- *Acceso a los datos:* un servidor de aplicaciones proporciona un acceso sencillo para realizar la administración de las conexiones a bases de datos relacionales.
 - Es habitual que también permitan realizar acceso a otros tipos de fuentes de datos como:
 - ERP

- Repositorios XML
 - Sistemas heredados
-
- *Pooling de conexiones*: es habitual que los servidores de aplicaciones mantengan de forma permanente conexiones con las bases de datos. Estas conexiones se distribuyen entre los procesos de forma transparente, ya que sería muy costoso, además de influir negativamente en el rendimiento de la aplicación, el abrir una conexión por cada consulta que se quiera realizar.
 - *Gestión de transacciones*: las transacciones son fundamentales en cualquier software y más aun en los de tipo comercial, puesto que evitan la aparición de información inconsistente.
 - Los servidores de aplicaciones suelen contar con esta característica, de forma que con indicar en qué momento se inicia una transacción y en cual se finaliza, el propio sistema se encargaría de deshacer los pasos intermedios en caso de que se produzca un error en la aplicación.

55.2.2 **Estándar J2EE**

Las plataformas más comunes en las que se asientan los servidores de aplicaciones son J2EE y .NET. J2EE está más extendida y hasta hace relativamente poco, era impensable implementar un servidor de aplicaciones que no siguiese este modelo.

El estándar J2EE permite desarrollar aplicaciones empresariales de forma eficiente y sencilla. El hecho de desarrollar una aplicación con tecnologías J2EE permite que esta sea desplegada en cualquier servidor de aplicaciones que cumpla con dicho estándar. Un servidor de aplicaciones es una implementación de la especificación J2EE que se compone de:

1. Cliente Web o contenedor de applets: es un navegador web que interactúa con el contenedor web mediante HTTP.
 - a. Puede ejecutar applets y código javascript.
 - b. Recibe páginas HTML o XML.
2. Aplicación Cliente: se trata de clientes que no se ejecutan dentro de un navegador.
 - a. Pueden utilizar distintas tecnologías para comunicarse con el contenedor web.
 - b. Pueden comunicarse directamente con la base de datos.
3. Contenedor Web o servidor web: se corresponde con la parte visible de un servidor de aplicaciones.
 - a. Emplea los protocolos HTTP y SSL
4. Servidor de aplicaciones: proporciona servicios que dan soporte a la ejecución y disponibilidad de las aplicaciones desplegadas.

Existen distintas implementaciones partiendo de este estándar, cada una con sus propias peculiaridades que las pueden hacer más adecuadas para un determinado sistema. Algunas de las más destacadas son:

- Oracle Weblogic (BEA WebLogic)
- IBM WebSphere
- Sun-Netscape IPlanet
- Sun One
- Oracle IAS
- Borland AppServer
- HP Bluestone

55.2.3 Estructura de un servidor de Aplicaciones

Un servidor de aplicaciones se asienta en una estructura en 3 capas que permite realizar una estructuración más eficiente del sistema.

- *Capa Cliente*: contiene los programas que ejecutan los usuarios, como navegadores Web. Estos programas pueden estar implementados en cualquier lenguaje de programación.
- *Capa Media*: contiene el servidor de aplicaciones y otros que pueden ser direccionados por los clientes, como servidores proxy o servidores web existentes.
- *Capa Datos*: contiene los recursos, como sistemas de bases de datos, ERP, etc.

55.2.4 Oracle Weblogic (Antes BEA WebLogic)

OracleWebLogic Server es un servidor de aplicaciones completo y basado en estándares, que proporciona el fundamento sobre el cual una empresa puede construir sus aplicaciones. Presenta un completo conjunto de características, como son, el cumplimiento de los estándares abiertos, la arquitectura de varios niveles, y el apoyo para desarrollo basado en componentes, etc.

Oracle WebLogic Server proporciona todas las funciones básicas esenciales de un servidor de aplicaciones y servicios, tales como:

- Equilibrio de carga
- Tolerancia a fallos
- Servicios Web
- Transparencia en la red
- Integración de sistemas heredados
- Gestión de transacciones
- Seguridad
- Multi-threading
- Persistencia
- Conectividad con bases de datos
- Agrupación de recursos

Estas funcionalidades agilizan el desarrollo de aplicaciones y alivian los esfuerzos de los desarrolladores.

Además de J2EE, Oracle WebLogic Server implementa todos los estándares importantes de programación, integración y trabajo en red que son la base para la construcción de una infraestructura de aplicaciones, incluyendo:

- XML: Oracle WebLogic Server implementa la última versión del Api de Java API para el procesamiento de XML (JAXP), e incluye un analizador integrado Apache Xerces y un analizador XML de alto

rendimiento diseñado específicamente para pequeñas y medianas empresas.

- **SOAP:** SOAP es el nuevo estándar para el intercambio de información en un entorno distribuido. Es el protocolo de comunicación para definir el formato de los datos para los servicios Web que se entregan a través de HTTP.
- **WSDL:** WSDL es un lenguaje basado en XML utilizado para describir un servicio Web publicado. BEA WebLogic Server tiene soporte incorporado para WSDL y genera un guión WSDL de forma automática cuando un servicio Web se implementa en el servidor WebLogic.
- **UDDI:** Un registro UDDI es un directorio de servicios web, distribuido y basada en Web, muy similar a una libreta de teléfonos. Oracle WebLogic Server incluye incrustado un registro UDDI y una API para la búsqueda y la actualización de este, o cualquier otro registro UDDI.
- **JMX y SNMP:** La infraestructura del servidor WebLogic se basa en el estándar abierto y extensible JMX. Además, el agente SNMP está disponible para la compatibilidad con sistemas que se basen en SNMP.
- Los administradores de sistemas pueden configurar sus políticas de seguridad de basadas en roles de acceso.

55.3 Servidores de Aplicaciones y Servidores Web

La diferencia básica entre el servidor web y un servidor de aplicaciones es que el servidor web sirve para ver las páginas en un navegador web, mientras que un servidor de aplicaciones proporciona los métodos necesarios, que pueden ser llamados por las aplicaciones cliente. En otras palabras, las peticiones HTTP son manejados por los servidores web y la lógica de negocio se sirve a los programas de aplicación, a través de una serie de protocolos en el servidor de aplicaciones. En un servidor de aplicaciones, un cliente puede utilizar la GUI y los servidores web, mientras que en los servidores web el cliente puede usar HTML y HTTP.

	<i>Servidor Web</i>	<i>Servidor de Aplicaciones</i>
<i>¿Qué es?</i>	Un servidor que gestiona conexiones HTTP.	Un servidor que expone la lógica del negocio al cliente mediante una serie de protocolos, pero no exclusivamente HTTP
<i>¿Añade Funcionalidad?</i>	Un servidor Web no añade funcionalidad simplemente recibe una petición y envía la respuesta al cliente.	Añade funcionalidad, puesto que implementa una lógica de negocio intermedia.

<i>¿Qué tipo de aplicaciones sirve?</i>	Sólo basadas en web	Aplicaciones basadas en web, pero también otras que no lo son, lo cual es posible ya que un servidor de aplicaciones incluye internamente un servidor web.
<i>¿Qué tipo de clientes permite?</i>	Navegadores.	Navegadores e interfaces pesadas.
<i>¿Cuáles son sus funciones?</i>	Almacenar ficheros escritos en HTML, PHP, etc., de tal forma que sean accesibles para los navegadores web cuando los sitios web necesiten acceder a ellos.	Ofrecer aplicaciones a otro sistema.

55.4 Bibliografía

- Apache: The Definitive Guide, Third Edition. Ben Laurie, Peter Laurie
- Apache : soluciones y ejemplos para administradores de Apache. Ken Coar and Rich Bowen
- Web Server Technology. Nancy J. Yeager, Robert E. McGrath
- Linux Apache web server administration. Charles Aulds
- Managing Internet information services, Cricket Liu
- Client-server computing: architecture, applications and distributed systems management. Bruce R. Elbert and Bobby Martya

Autor: Francisco Javier Rodríguez Martínez

Subdirector de Sistemas Escola Superior Enxeñaría Informática Ourense
Colegiado del CPEIG



**56. DISEÑO DE CENTRO DE
PROCESOS DE DATOS.
INSTALACIONES
(ELECTRICIDAD, CONTROL DE
ACCESO, CONTROL DE
PRESENCIA, SISTEMA ANTI-
INCENDIOS, CLIMATIZACIÓN,
SISTEMAS DE ALIMENTACIÓN
ININTERRUMPIDA).**

Tema 56: Diseño de centro de procesos de datos. Instalaciones (electricidad, control de acceso, control de presencia, sistema anti-incendios, climatización, sistemas de alimentación ininterrumpida).

ÍNDICE

ÍNDICE.....	1
56.1 Centro de proceso de datos.....	1
56.2 Diseño de centro de procesos de datos.....	1
56.3 Instalaciones.....	19
56.4 Clasificación de los CPD.....	29
56.5 Bibliografía.....	31

56.1 CENTRO DE PROCESO DE DATOS

Un Centro de proceso de datos es el conjunto de recursos físicos, lógicos y humanos necesarios para la organización y control de las actividades informáticas de una empresa u organización. Se considerará que es aquella ubicación donde se encuentran los equipos informáticos principales que dan soporte al conjunto de información de una organización. Se puede decir que los Centros de Proceso de Datos (CPD) son los depositarios, los "guardianes", de la información utilizada por todas las áreas de una organización.

56.2 DISEÑO DE CENTRO DE PROCESOS DE DATOS

Un CPD puede ocupar una habitación de un edificio, uno o varios pisos, o un edificio entero. La mayoría del equipamiento se suele presentar en forma de servidores montados en armarios rack (también llamados bastidores, cabinets o armarios) de 50 cm de ancho. Pueden alojar distintos dispositivos:

- Servidores cuya carcasa ha sido diseñada para adaptarse al bastidor. Existen servidores de 1U, 2U y 4U, y recientemente, se han popularizado los servidores blade que permiten compactar más compartiendo fuentes de alimentación y cableado.
- Conmutadores y enrutadores de comunicaciones.
- Paneles de parcheo, que centralizan todo el cableado de la planta.
- Cortafuegos.
- Sistemas de audio y vídeo.

Los armarios rack suelen estar dispuestos en filas formando pasillos entre ellos. Esto permite a las personas acceder al frontal y a la parte posterior de cada armario. Ciertos equipamientos del CDP como los mainframes y los dispositivos de almacenamiento pueden llegar a ser tan grandes como los propios racks y se sitúan a lo largo de estos.

Para llevar a cabo el diseño de un CPD se deben tener en cuenta muchas consideraciones que van desde la ubicación geográfica, análisis de riesgos, las infraestructuras interiores... hasta las medidas de seguridad, tanto físicas como lógicas.

56.2.1 *Requisitos a cumplir por el Centro de proceso de datos*

En primer lugar se deben establecer los requisitos a intentar cumplir por el CPD:

- Instalación de alto riesgo. Se considera a un CPD como una instalación de alto riesgo. Una instalación de alto riesgo es aquella que tiene las siguientes características:
- Datos o programas que contienen información confidencial de interés nacional o que poseen un valor competitivo alto en el mercado.

- Pérdida potencial considerable para la institución y, en consecuencia, una amenaza potencial alta para su subsistencia.
- Disponibilidad y monitorización “24x 7x 365”. Un centro de datos diseñado apropiadamente proporcionará disponibilidad, accesibilidad y confianza 24 horas al día, 7 días a la semana, 365 días al año.
- Fiabilidad Infalible (5 ‘nueves’). Es decir, con un 99,999% de disponibilidad, lo que traduce en una única hora de no disponibilidad al año. Los centros de datos deben tener redes y equipos altamente robustos y comprobados.
- Seguridad, Redundancia y Diversificación. Almacenaje exterior de datos, tomas de alimentación eléctrica totalmente independientes y de servicios de telecomunicaciones para la misma configuración, equilibrio de cargas, SAIs o Sistemas de Alimentación Ininterrumpida), control de acceso, etc.
- Control ambiental / Prevención de Incendios. El control del ambiente trata de la calidad del aire, temperatura, humedad, electricidad, control de fuego, y por supuesto, acceso físico.
- Acceso Internet y conectividad WAN. Los centros de datos deben ser capaces de hacer frente a las mejoras y avances en los equipos, estándares y anchos de banda requeridos, pero sin dejar de ser manejables y fiables. Las comunicaciones dentro y fuera del centro de datos se proveen por enlaces WAN, CAN/MAN y LAN en una variedad de configuraciones dependiendo de las necesidades particulares de cada centro.
- Rápido despliegue y reconfiguración. Otros aspectos tratan de las previsiones para hacer frente a situaciones críticas, con el objetivo de superarlas y volver rápidamente a la normalidad en caso de catástrofe.

- Gestión continúa del negocio. El funcionamiento de muchas compañías que constantemente realizan miles de transacciones por minuto gira en torno a la información almacenada. Para garantizar la fiabilidad existen los sistemas inteligentes de control de asignaciones y monitorización.
- Cableado flexible, robusto y de altas prestaciones. La infraestructura física de los centros debe soportar sistemas de comunicación de alta velocidad altas prestaciones capaces de atender al tráfico de SANs (Storage Area Networks), NAS (Network Attached Storage), granjas de servidores de archivos/aplicación/web, servidores blade y otros dispositivos de almacenaje (Fibre channel, SCSI o NAS) así como Sistemas de Automatización del Edificio, sistemas de voz, video y CCTV.

56.2.2 *Análisis de riesgos y planes de contingencia*

Para realizar un buen diseño también debemos establecer un compromiso entre la necesaria operatividad del sistema frente a los diversos riesgos potenciales, los mecanismos y técnicas que permiten minimizar sus efectos y costes directos e indirectos del empleo de dichas técnicas.

Del estudio pormenorizado de los riesgos y de la criticidad se determina el nivel aceptable de seguridad y se eligen las medidas a adoptar. Estas medidas se traducen en la Seguridad Preventiva y el Plan de Contingencia.

56.2.2.1 Análisis de riesgos

Deberemos determinar cuantitativa y cualitativamente los riesgos a que esté sometida la organización. Una vez tipificados procederemos a estimar la probabilidad de ocurrencia de cada uno. Esta probabilidad no depende tanto del riesgo en si como de las características concretas de cada CPD. Para ello se puede confeccionar una escala con unos niveles subjetivos o bien se puede recurrir a las estadísticas propias de la instalación (caso de existir) o a las editadas por empresas de consultoría o seguros.

Se debe establecer un listado priorizado de elementos críticos (aplicaciones, bases de datos, software de base, equipos centrales, periféricos, comunicaciones) según el impacto que su carencia o malfuncionamiento causaría en la operatividad del sistema.

Para ello podemos utilizar una escala que marque el tiempo que se podría tolerar un fallo de funcionamiento de cada elemento: 24 horas, 2-3 días, 1 semana, 15 días, más de un mes. También podemos tener en cuenta la diferente criticidad según la época del año, del mes o de la semana.

56.2.2.2 Elección de medidas a adoptar

Consiste en seleccionar las medidas de seguridad que permitan prevenir los daños en lo posible y corregirlos o minimizarlos una vez acaecidos, determinando los recursos necesarios para su implantación.

56.2.2.3 Plan de contingencia

Las medidas de corrección se plasman en un plan con unos objetivos concretos:

- Minimizar las interrupciones en la operación normal.
- Limitar la extensión de las interrupciones y de los daños.
- Posibilitar una vuelta rápida y sencilla al servicio.
- Ofrecer a los empleados unas normas de actuación frente a contingencias.
- Proveer los medios alternativos de proceso en caso de catástrofe.

Para garantizar su validez y que no quede obsoleto con el tiempo, deberá estar en continua revisión. Además el personal debe estar entrenado mediante pruebas simuladas periódicas. En la elaboración del plan debe intervenir la dirección, los técnicos de explotación, los técnicos de desarrollo, el personal de mantenimiento, los usuarios y los proveedores.

El plan debe recoger, en forma de planes unitarios, las respuestas a los diferentes problemas que puedan surgir, y se desglosa en:

- **Plan de emergencia:** Guía de actuación "paso a paso" en cada fallo o daño. Determina una serie de acciones inmediatas (parada de equipos, aviso a responsables, activar o desactivar alarmas, uso de extintores u otros elementos auxiliares, llamada a mantenimiento lanzar salvaguardas o listados, etc.), una serie de acciones posteriores como salvamento, valoración de daños, elaboración de informes, relanzar procesos, relanzar el sistema operativo, recuperar copias de seguridad, saltar procesos, etc. así como una asignación de responsabilidades, tanto para las acciones inmediatas como para las posteriores.
- **Plan de Recuperación:** Desarrolla las normas de actuación para reiniciar todas las actividades normales de la organización, bien en el propio CPD, bien en otro centro de respaldo. Si se recupera en el propio centro, se deberán activar los equipos duplicados o auxiliares (si no es automático), se utilizarán los soportes de procesamiento alternativos, se iniciarán las actuaciones de mantenimiento o sustitución de equipos dañados y se utilizarán si es preciso las copias de seguridad. Si se utiliza un centro de respaldo, se deben definir los procedimientos a emplear según la causa que originó el problema, se debe realizar una política de traslados (y vuelta posterior al centro original), se debe recuperar el sistema operativo, el software de base y las aplicaciones), se deben relanzar las operaciones (recuperando desde la última salvaguarda en caso de necesidad) y se debe revisar la operación mediante la introducción de pruebas que aseguren el correcto funcionamiento.
- **Plan de Respaldo:** Especifica todos los elementos y procedimientos necesarios para operar en el centro de respaldo (si existe) y mantener en el mismo información sobre la configuración del equipo

y de las comunicaciones, del sistema operativo, del software de base, de las aplicaciones, del soporte humano y técnico, suministros de documentación y formularios, modo de regenerar el software para su operativa normal, reglas de explotación y operación, política de accesos y confidencialidad, identificación de usuarios, terminales, etc.

56.2.3 *Ubicación geográfica*

Los edificios o instalaciones de los CPD's requieren unas características adicionales de protección física que deben ser consideradas antes de seleccionar su ubicación, teniendo en cuenta aspectos tales como la posibilidad de daños por fuego, inundación, explosión, disturbios civiles, cercanía de instalaciones peligrosas (depósitos de combustible, aeropuertos, acuartelamientos, etc.) o cualquier otra forma de desastre natural o provocado.

Se deberán analizar de forma integral las características dominantes de los distintos entornos, evaluando las ventajas y los riesgos potenciales que pudieran afectar al buen funcionamiento del CPD y planteando las respuestas adecuadas en relación con el entorno natural, artificial y urbanístico.

56.2.3.1 Entorno natural

Tendremos en cuenta:

- Climatología: tormentas, precipitaciones de agua y nieve, temperaturas extremas, huracanes, ventisca y vientos dominantes.
- Geotecnia: mecánica de los suelos (corrimientos de tierra, hundimientos, estructura físico-química, humedad, existencia de minerales magnéticos, sismicidad, etc.).
- Hidrología: proximidad de ríos, proximidad del mar, embalses cercanos y posibles avenidas, etc.

56.2.3.2 Entorno artificial

Podemos considerar:

- Acceso a medios de emergencia: bomberos, policía, servicios sanitarios, etc.
- Centrales de gas o depósitos de gas, centrales nucleares.
- Redes de telecomunicaciones.
- Suministro eléctrico, redes de suministro accesibles.
- Plantas petroquímicas, fábricas de cemento, betunes, derivados del vidrio, etc.
- Conducciones o depósitos de líquidos (agua potable, aguas residuales, combustibles, etc.).
- Contaminación atmosférica: polvo, vapores corrosivos o tóxicos, etc.
- Perturbaciones locales: ruidos, vibraciones, radiaciones parásitas (radares, balizas de navegación, emisoras de radio y televisión, torres de telecomunicaciones, líneas de alta tensión cercanas, grandes transformadores o motores, centrales eléctricas, repetidores, centrales nucleares, aeropuertos).

56.2.3.3 Entorno urbanístico

Tenemos entre otras:

- Dotaciones urbanas: metro, autobuses, intercambiadores ferroviarios, autopistas, aeropuertos, puertos marítimos, hospitales, universidades, supermercados, etc.
- Zonas urbanas: parcelas abiertas, edificaciones colindantes, zonas de oficinas y negocios, parques empresariales, recintos feriales.

- Ambiente de trabajo y salud laboral (microclima de trabajo, contaminación ambiental, sobrecargas físicas y psíquicas influyentes, etc.).

Actualmente se ha acuñado el término "AMENITIES" para abarcar todos los servicios complementarios que no son estrictamente necesarios para el desempeño de la actividad de proceso de datos, pero que pueden ofrecerse en el conjunto de la oferta inmobiliaria sobre todo en los parques empresariales o zonas singulares.

Entre ellos están

- Áreas de descanso, ocio y servicios terciarios.
- Guardería.
- Aparcamiento.
- Clubes, gimnasios e instalaciones deportivas.
- Cajeros automáticos.
- Restaurantes y cafeterías.
- Hoteles.
- Centros comerciales.

56.2.4 *Infraestructuras interiores*

Una vez seleccionada la ubicación física del edificio que albergará el CPD, habrá que analizar las características específicas de las instalaciones, haciendo hincapié en algunos aspectos:

- Deben estar diseñadas de forma que no se faciliten indicaciones de su propósito ni se pueda identificar la localización de los recursos informáticos.

- Incluir zonas destinadas a carga y descarga de suministros y su inspección de seguridad.
- Cumplir, en los elementos constructivos internos (puertas, paredes, suelos, etc.), el máximo nivel de protección exigido por la Norma Básica de Edificación (NBE/CPI-91).
- Disponer de canalizaciones protegidas de cableado de comunicaciones y de electricidad, para evitar ataques (sabotajes, fuego, roedores, insectos), interceptación o perturbaciones por fuentes de emisión próximas (radio, electricidad magnetismo, calor).

56.2.4.1 Habitabilidad

La mayoría de construcciones de edificios públicos, de oficinas o de negocios no empezaron a cubrir las necesidades de preinstalaciones e instalaciones informáticas hasta bien entrados los años ochenta.

Actualmente, el diseño arquitectónico de un CPD debe estar lo más cercano posible a la arquitectura inteligente. Este hecho ha dado cabida a la domótica.

La domótica comprende todos aquellos desarrollos tecnológicos enfocados al diseño de soluciones rentables que pueda tener el inmueble en el marco de la propia génesis del proyecto arquitectónico. Es la automatización del edificio más la disponibilidad de los recursos de las telecomunicaciones y la ofimática.

Los requerimientos de habitabilidad tienen en cuenta la arquitectura informática del momento. Prevén no sólo el crecimiento del equipamiento informático, sino también el cambio total a otro entorno informático y mantienen rentable las infraestructuras y las dotaciones inteligentes o servicios avanzados del inmueble:

- Habitabilidad en horizontal, es el edificio informático óptimo, el de pocas plantas

- Habitabilidad en torre, las torres pierden en diafanidad, dificultan la extensión horizontal de la sala de ordenadores y complican la evacuación de emergencia, etc.

56.2.4.2 Requerimientos de las edificaciones e instalaciones

Se aplicarán las normas generales de obligado cumplimiento:

- Norma Básica de la Edificación.
- Normas tecnológicas de la Edificación.
- Ordenanzas Municipales.
- Reglamentos electrotécnicos.
- Verificación de los Productos y Suministros Industriales en el marco de la construcción.
- Normas de Preinstalación de las Firmas Informáticas.

Además de la aplicación de las normas generales, el estudio para la elección del edificio deberá comprender todo lo que compete a la arquitectura tradicional y muy especialmente a:

- La estructura y sobrecargas de uso.
- Las fachadas del inmueble.
- Accesos a los almacenes.
- Instalaciones para las salas de informática.
- Muelles de carga y descarga, elevadores, montacargas, etc.
- Acceso al edificio de mercancías pesadas (montacargas industrial).
- Acceso a la Sala de Informática (siempre puertas doble hoja).

- Existencia de salidas de Seguridad al CPD.
- Falso suelo y techo tecnológicos.
- Protección contra las infiltraciones de agua y humedad.
- Suministros de energía eléctrica y agua.
- Iluminación de día y de emergencia.
- Resistencia al Fuego en minutos de la estructura, forjados y muros de carga.
- Muros cortafuegos.
- Puertas contra incendios.
- Situación de las puertas de acceso y evacuación.
- Túneles de seguridad y escaleras de emergencia.
- Particiones interiores o mamparas dobles.
- Que no crucen las salas de informática conducciones de aguas tanto pluviales como de desagües excepto las propias de la climatización.
- Tratamientos referentes a resistencias eléctricas, acústicas y mecánicas.
- Protección contra la energía eléctrica de reacción: Toma de tierra del edificio, pararrayos.

56.2.5 Seguridad física

La seguridad física consiste en el conjunto de mecanismos y normas encaminados a proteger las personas, instalaciones, equipos centrales y periféricos y los elementos de comunicaciones contra daños eventuales. Está relacionada con los controles que protegen de los desastres naturales

como incendios, inundaciones o terremotos, de los intrusos o vándalos, de los peligros medioambientales y de los accidentes.

Los controles de seguridad física regulan además de la sala donde se alberga el equipo del ordenador, la entrada de datos, el entorno (bibliotecas, registros cronológicos, medios magnéticos, áreas de almacenamiento de copias de seguridad y salas de instalaciones de servicios) y todos los detalles o requerimientos tanto arquitectónicos como de preinstalación y mantenimiento de todos los servicios e infraestructuras, incluso la previsión de disponer de una seguridad física integral del entorno, de conformidad con el Artículo 9 de la LOPD (Ley Orgánica de Protección de datos de Carácter Personal).

Se deberá contemplar y analizar la seguridad física independientemente de los sistemas de gestión y control implementados en el CPD.

Se instalará un sistema informatizado para la gestión y el control integral de todas las alarmas procedentes del equipamiento informático, de las infraestructuras y de las instalaciones específicas de seguridad del CPD.

Dicho sistema, recibirá las señales de alarma, dispondrá de la gestión de las mismas y de la posibilidad de realizar desde el mismo la modificación de ciertos parámetros u operaciones de parada, arranque o maniobra del equipamiento de las salas de informática o del recinto del CPD:

- Red de incendios (Sala del CPD, áreas de servicios y despachos, zonas del SAI y del grupo electrógeno).
- Alarmas en general.
- Arranque, paro o maniobra del entorno industrial del CPD.
- Control de accesos y movimientos.
- Control de ahorro de energía.

- Control en el bloque de multicasilleros de reparto.
- Control de la expedición de la producción.
- Control de los stocks de almacenes.
- Estado de las baterías de los SAIs y control de los grupos electrógenos.
- Control de climatización, sobrepresión y renovación ambiental.
- Red de sondas ambientales en falso suelo, techo y sala de ordenador.
- Red de detección de humedad.

El objetivo de las áreas controladas es permitir un conocimiento inmediato y preciso del hecho y su localización, por lo que su actuación debe ser absolutamente fiable dentro de unos parámetros previamente establecidos. Ello exige unas revisiones de funcionamiento y un riguroso mantenimiento preventivo cuya periodicidad dependerá del sistema de detección y del tipo de área controlada al que se aplique.

La detección de un hecho anómalo requiere la información necesaria para una reacción proporcionada. Dependiendo de la información suministrada por el medio de detección y los parámetros previamente establecidos, antes de llegar a un estado de alarma se puede pasar por un estado de alerta.

Así los medios de reacción se van organizando en previsión de su posible actuación. Todos los medios de detección deben integrarse en el Sistema de Gestión de la Seguridad para que los gestione y:

- Avise de la anomalía y su gravedad.
- Inicie acciones de corrección automáticas o proponga acciones manuales a realizar por el personal entrenado para ello.

- Controle las actuaciones (qué, quién, cómo, dónde y cuándo).

Este sistema debe estar bajo vigilancia permanente y combinado con los servicios de mantenimiento, para los casos de mal funcionamiento de cualquier medio de detección. Hay que subrayar que los sistemas de detección deben funcionar incluso con el suministro eléctrico de emergencia.

56.2.5.1 Control de acceso y movimientos

Se refiere a las medidas que podemos establecer para evitar un acceso indebido al conjunto del CPD. Han sido ya referenciadas en la seguridad física. El establecer un área segura es importante para el buen funcionamiento del centro, puesto que la información almacenada y los procedimientos que se realizan en el CPD son vitales para la organización.

Por ello se deben adoptar todas las medidas cuyo coste esté justificado. Entre ellas:

- Servicio de seguridad: que no sólo controle los accesos al recinto, sino que también realice inspecciones periódicas de las dependencias, sobre todo de las que no tengan personal en cada momento. Su importancia se hace evidente en horas nocturnas o días festivos.
- Barreras, puertas de seguridad, ausencia de ventanas. Son medidas que tienden a dificultar el acceso de personal no autorizado.
- Vídeo vigilancia y alarmas volumétricas: controladas por una centralita en la cabina de seguridad.

56.2.5.1.1 Planificación del acceso

Los responsables de las áreas controladas deben mantener unos controles de acceso efectivos y proporcionales al valor de los activos a proteger para que puedan cumplir con unos requisitos de auditabilidad mínimos. Los objetivos son:

- Permitir el acceso únicamente a las personas autorizadas por el responsable del área.
- Registrar las entradas y/o salidas (quién, por dónde y cuándo).

Para facilitar el control de los accesos a estas áreas, es recomendable la existencia de un único punto o puerta de acceso habitual para entrada y salida, sin perjuicio de que existan otras salidas para emergencias que se puedan abrir desde el interior mediante el empuje de una barra.

La entrada en las Áreas de Acceso Limitado (AAL) tiene que efectuarse desde un área interna, nunca desde un área pública. Cada área de acceso limitado debe tener identificado formalmente un responsable o propietario cuyas responsabilidades son:

- Aprobar y mantener actualizada la relación de personas con autorización de acceso permanente. Las personas que tengan su autorización cancelada, por petición de su dirección o por haber causado baja en la empresa, deben ser eliminadas de la relación de acceso en un tiempo razonable.
- Aprobar accesos temporales a estas áreas. En este caso la persona autorizada debe saber que la autorización es para una sola vez.

Las Áreas de Acceso Restringido (AAR) no deben tener ventanas al exterior y la entrada en las mismas tiene que efectuarse desde un área interna o un Área de acceso limitado, nunca desde un Área pública. Tienen que tener barreras de aislamiento de suelo y techo, incluyendo el falso suelo y el falso techo, o bien detectores volumétricos de intrusos.

Cada área de acceso restringido debe tener identificado formalmente un responsable o propietario cuyas responsabilidades son:

- Aprobar y mantener actualizada la relación de las personas con autorización de acceso permanente, generalmente, porque el trabajo

a realizar requiere su presencia dentro del área. La lista de acceso debe ser actualizada siempre que haya cambios que así lo aconsejen y revisada formalmente, al menos, cada seis meses. Las personas que tengan su autorización cancelada por petición de su dirección o por haber causado baja en la empresa tienen que ser eliminados de la lista de acceso inmediatamente.

- Aprobar los accesos temporales a estas áreas, incluyendo los accesos del personal que, estando destinado en el área, accede fuera de su jornada laboral. En este caso, la persona autorizada debe saber que la autorización es para una sola vez. Las autorizaciones temporales deben contener:
 - o Nombre de quien autoriza si no es el propietario.
 - o El nombre de la persona autorizada.
 - o Razón social (si corresponde) o motivo.
 - o Fecha y hora de acceso y la firma.
 - o Fecha y hora de salida y la firma.

56.2.6 *Seguridad lógica*

Este tipo de seguridad debe estar completamente coordinada con la seguridad física ya que ambas están estrechamente relacionadas y comparten objetivos y presupuestos.

La seguridad lógica consiste en el conjunto de operaciones y técnicas orientadas a la protección de la información contra la destrucción, modificación indebida, divulgación no autorizada o retraso en su gestación.

Es conveniente que el proveedor ofrezca diferentes niveles de acceso según la función deseada: desde la combinación de usuario y clave, que puede ser suficiente para la publicación de páginas HTML con datos no críticos, pasando por la transferencia de datos mediante conexiones HTTPS,

(por ejemplo, para las aplicaciones de control a disposición del usuario o para la consulta de sus estadísticas), hasta llegar a las conexiones completamente cifradas, ya sea empleando HTTPS o tecnología VPN, complementadas con autenticación de cliente mediante certificación digital.

Además es necesario un servicio de log, reporting y detección de intrusos. En un proveedor de servicios es normal que haya cientos de intentos de acceso no autorizado a la semana, desde los típicos barridos de puertos, los intentos de exploits del “bug del día”, hasta algunos intentos más elaborados y peligrosos. Una cuestión adecuada en este punto es saber cuántos intentos de acceso se detectan regularmente. Si la respuesta es pocos o ninguno, debemos preocuparnos, puesto que se pone en duda la capacidad de detección de las herramientas y técnicas que se emplean, o peor aún, los procedimientos de seguimiento y resolución de dichos incidentes.

Para realizar el seguimiento de cualquier incidente es necesario disponer de los ficheros de registro de las diferentes aplicaciones, sean estándar o programadas a medida para los distintos servicios. Siempre es conveniente que el proveedor proporcione informes de acceso a las diferentes aplicaciones, incluyendo aquellos que reflejan las direcciones IP desde las que se producen los accesos y los fallos de autenticación.

La combinación de todo lo comentado anteriormente debería cubrir las necesidades que se buscan en lo referente a seguridad lógica, siempre que se realice de forma coherente y con conocimiento de los aspectos críticos para el cliente.

La infraestructura del CPD debe incluir medidas de seguridad que protejan frente a ataques a través de las redes a las que ésta esté conectado. Puesto que el núcleo de la electrónica de red suele –y debe– estar situado en el CPD, es necesario contemplar estas necesidades a la hora de implantar un nuevo CPD.

Es común que el acceso a internet sea un recurso crítico para la Organización, por lo que se recomienda contratar dos proveedores de acceso distintos y establecer una configuración en alta disponibilidad de todos los elementos de red que se encuentren en la ruta hacia Internet (cortafuegos, routers, switches, etc.). Esto es especialmente crítico si la organización proporciona servicios on-line, tales como comercio electrónico o hosting web.

Si es necesario implementar medidas adicionales de seguridad perimetral como IDS/IPS, filtrado de contenidos o antivirus de correo electrónico y/o navegación web, así como mecanismos de acceso remoto (VPN), el cortafuegos corporativo –o incluso el proxy, si se dispone de él– es el lugar idóneo para ello. De este modo se centraliza la administración de estas medidas y se reducen los posibles puntos de fallo. Actualmente, existe gran cantidad de dispositivos que implementan todas estas funcionalidades en un único equipo.

Además de los evidentes mecanismos de control que es necesario establecer desde y hacia Internet, es muy conveniente realizar una segregación de redes. Es decir, conviene realizar una división de la red interna de la Organización en distintas subredes, interconectadas entre sí por cortafuegos que establezcan los flujos de información permitidos entre cada una. Cada servidor, en función de las necesidades de control de acceso de las aplicaciones que ejecute, se conectará finalmente a una de estas subredes.

56.3 INSTALACIONES

56.3.1.1 Instalaciones eléctricas

Los cuadros de mandos se instalarán en lugares fácilmente accesibles, con espacio holgado (previendo las posibles ampliaciones), correcta y claramente etiquetados y por supuesto con el más estricto rigor en materia

de calidad de aparatos y montaje (deberán cumplir con las normas habituales de protección y seccionamiento).

Se evitarán las perturbaciones electromagnéticas, aislando adecuadamente aquellas máquinas generadoras de campos inductivos y armónicos.

Se evitará la electricidad estática empleando los revestimientos más adecuados, instalando las tomas de tierra convenientes y manteniendo la humedad en el rango adecuado (al menos del 55%).

Los recursos informáticos son sensibles a las variaciones de tensión y de frecuencia de la corriente eléctrica. Los requerimientos básicos para el suministro de energía eléctrica son dos: Calidad y Continuidad.

Relacionado con la Calidad se puede destacar que:

- Las variaciones de frecuencia deben corregirse con equipos estabilizadores que la mantengan dentro de los rangos establecidos por los fabricantes de los recursos informáticos a alimentar, aunque algunos recursos informáticos de nueva tecnología los llevan incluidos.
- Las variaciones de tensión deben ser manejadas por un Sistema de Alimentación Ininterrumpida (SAI en inglés UPS), de modo que se puedan prevenir los efectos de posibles micro cortes.

En relación con la continuidad del suministro eléctrico debe tenerse en cuenta que las caídas de tensión pueden ser manejadas por un SAI (UPS), pero sólo por tiempo limitado, ya que el desgaste de sus acumuladores es muy rápido y su recarga muy lenta para utilizarlo en cortes sucesivos y nunca como única alternativa.

Las soluciones habituales se basan en una de las siguientes o en la combinación de varias de ellas:

- Conexión conmutada a dos compañías suministradoras.

- Conexión conmutada a dos estaciones transformadoras de la misma compañía pero situadas en rutas de suministro diferentes.
- Capacidad de transformación de corriente asegurada mediante equipos redundantes.
- Equipos electrógenos de combustión.

Siempre que el volumen de las instalaciones informáticas así lo aconseje, el suministro eléctrico y las tomas de tierra deben ser independientes de las generales del edificio y a suficiente distancia de ellas, correctamente instaladas y rigurosamente mantenidas.

56.3.1.2 Control de acceso

Este control se basa en medidas de identificación unívoca de las personas que acceden al CPD. El servicio de seguridad debe llevar un registro de las entradas y salidas al centro. Las visitas autorizadas deben llevar obligatoriamente una tarjeta identificativa o etiqueta en lugar visible que indique claramente que es una visita a las áreas a las que puede acceder y el tiempo de validez (suele ser diaria).

El personal propio debe portar una tarjeta identificativa con fotografía. Se pueden utilizar colores para identificar las áreas a las que puede acceder.

En centros de alta seguridad pueden requerirse medidas auxiliares de identificación:

- Huellas dactilares.
- Fondo de ojo (retina).
- Introducción de códigos de acceso para abrir las puertas.

56.3.1.2.1 Niveles de seguridad de acceso

Las instalaciones de la empresa deben clasificarse en varias áreas o zonas que, dependiendo de su utilización y los bienes contenidos, estarán

sometidas a unos u otros controles de acceso. Las instalaciones pueden clasificarse de acuerdo con los criterios y denominaciones siguientes:

- Áreas Públicas: espacios en los que no hay- ningún tipo de restricción de acceso a empleados o personas ajenas a la empresa.
- Áreas Privadas: espacios reservados habitualmente a los empleados y personas ajenas a la empresa con autorización por motivos de negocio. En ellos puede haber recursos informáticos con un valor bajo.
- Áreas de Acceso Limitado (AAL): espacios cuyo acceso está reservado a un grupo reducido de empleados y personas ajenas a la empresa autorizadas por un acuerdo escrito. Pueden concentrarse en ellos recursos informáticos que, en su conjunto, tiene un valor medio.
- Áreas de Acceso Restringido (AAR): espacios cuyo acceso está reservado a un grupo muy reducido de empleados y personas ajenas de la empresa autorizadas por un acuerdo escrito, que tengan necesidad de acceder por razones de negocio. En ellos se encuentran recursos informáticos que, en conjunto, tienen un alto valor o contienen activos de información críticos para las actividades del negocio.

A las dos últimas se les denomina Áreas Controladas. Tienen que permanecer cerradas, incluso cuando estén atendidas, y sus accesos controlados. En las áreas controladas, todos los empleados y las personas ajenas a la empresa con autorización para acceder por razones de negocio tienen que llevar permanentemente y en lugar visible un identificador:

- Los empleados, al menos, con fotografía y nombre.
- Las restantes personas, al menos el nombre (legible) y distintivo de la función que cumplen (ej.: visita, contratado, suministrador, etc.).

- Los identificadores de los empleados con acceso a áreas controladas pueden tener la posibilidad de lectura por banda magnética o por cualquier otro medio, para facilitar el control de accesos y su registro.

Todo identificador, especialmente los que permiten el acceso a áreas controladas, es personal y debe ser considerado como una contraseña de acceso físico y no compartirlo con nadie, para evitar verse envuelto en algún incidente de seguridad no deseado.

En las áreas controladas tiene que estar prohibido comer, fumar, consumir bebidas alcohólicas y cualquier tipo de drogas. Las dos últimas están consideradas de alto riesgo potencial para la instalación, por lo que adicionalmente debe impedirse la entrada a cualquier área controlada a las personas de quién se sospeche el consumo.

Los suministros informáticos que sean peligrosos o combustibles tienen que ser almacenados a una distancia prudencial y no trasladarlos al área donde se encuentran el resto de recursos informáticos hasta el momento de su utilización. De igual forma, hay que retirarlos de la zona inmediatamente después de finalizar su uso.

56.3.1.3 Sistemas anti-incendios

El fuego causa el mayor número de accidentes en los CPDs. Por ello es imprescindible controlar puntos zonales y además realizar un estudio en función de los agentes extintores (tener en cuenta la prohibición del uso del HALÖN, Protocolo de Montreal sobre CFCs).

Se procederá a estudiar como medidas:

- El acceso de los bomberos a cualquier zona del edificio previendo las tomas de agua a presión convenientes.
- La resistencia al fuego de los materiales de construcción carpintería, revestimiento, etc. Se evitarán aquellos materiales que generen productos tóxicos o gran cantidad de humo al ser sometidos al fuego

(NBE-CPI-91). También hay que evitar que se acumulen listados de control y otros papeles en el CPD.

- El mecanismo más adecuado para cortar la alimentación eléctrica en caso de incendio.
- Los mecanismos idóneos para evitar que los conductos de refrigeración y ventilación actúen como chimeneas y contribuyan a propagar el incendio, parándose automáticamente el aire acondicionado en caso de incendio.
- La compartimentación del edificio, aislando aquellas zonas que contengan materiales fácilmente combustibles, que se limitarán al máximo.
- Tabicados de hormigón con mamparas y puertas ignífugas.
- La instalación de puertas contra fuegos dotadas de los mecanismos que aseguren su cierre de forma automática.
- La prohibición de fumar, colocando carteles claramente visibles, en las zonas de mayor riesgo.
- El mobiliario, fabricado con materiales resistentes al fuego.
- Los contenedores de papel, materiales plásticos, etc., deberán tener una tapa metálica, que permanecerá cerrada de forma automática.
- La construcción de recintos de protección combinada o la disposición de armarios ignífugos.
- La instalación de un sistema de alarmas cruzadas y centralizadas en el Sistema Integral de Gestión de la Seguridad, para la detección o extinción de incendios en el CPD.

La mayoría de los armarios que se utilizan en las salas de informática no son ignífugos sino refractarios o simples cajas fuertes. No corresponden al grado de vulnerabilidad exigido en la CEE.

En caso de incendio, su extinción puede realizarse con medios manuales o automáticos. Los medios manuales se basan en extintores portátiles, mangueras, etc. Es importante resaltar que:

- Existen diferentes tipos de fuego (de sólidos, líquidos, gases eléctricos) y hay extintores apropiados para cada tipo.
- El elemento extintor localizado en un área debe ser el apropiado para el que previsiblemente puede declararse en ella. Cualquier medio de extinción puede ser excelente utilizado en un área o más dañino que el propio fuego, si es usado en otra.
- Nunca debe emplearse un medio de extinción manual basado en agua donde pueda haber fuego eléctrico por peligro de electrocución.
- No es aconsejable la intervención de personal no entrenado para ello.
- Siempre que se disponga de tiempo, hay que avisar a la brigada interior de incendios (si la hubiera) o al Servicio de Bomberos.

Los medios automáticos se basan en la inundación del área mediante agua, CO₂ u otros agentes extintores. El más recomendable es el basado en agua, por su bajo coste y su nulo impacto en el entorno. Los sistemas automáticos basados en el agua deben tener un mecanismo de preacción que, en caso de llegar a un estado de alerta o alarma, sustituye el aire de la conducción por agua.

La actuación de estos sistemas de extinción debe ser combinada con la previa desconexión del suministro de energía eléctrica del área afectada.

El agente extintor más usado actualmente es el HFC 227ea es un hidrofluorocarburo (o heptafluoropropano). Desde el punto de vista

medioambiental el agente extintor HFC 227ea ha sido aceptado por la EPA (Agencia de protección medioambiental americana) en el marco del programa de nuevas alternativas significativas (Significant New Alternative Program o SNAP). Este gas puede intervenir en las mayores clases de incendio y es seguro, limpio y no es conductor eléctrico.

56.3.1.4 Climatización

Con la evolución tecnológica ya existen en el mercado recursos informáticos que reducen (prácticamente eliminan) los tradicionales requerimientos de aire acondicionado. Sin embargo, debido al parque existente en España y a su antigüedad media, se deben tener en cuenta las siguientes consideraciones:

- Para mantener el ambiente con la temperatura y la humedad adecuadas, especialmente los de las grandes instalaciones, hay que disipar el calor que generan a través del aire acondicionado.
- La suficiente potencia y redundancia de estos equipos permitirá que trabajen desahogadamente y que las operaciones de mantenimiento sean sencillas y frecuentes.
- Un elemento fundamental del sistema acondicionador de aire es el mecanismo de corte automático tras producirse una detección de incendio.

Se recomiendan equipos de climatización específicos para salas informáticas con control microprocesador de temperatura y humedad. Estos equipos deben ser del tipo servicios total y capaz de producir frío, calor y humectar o deshumectar de forma automática, dentro de unos márgenes de $\pm 1^{\circ}\text{C}$ y $\pm 2\%\text{HR}$ para valores de funcionamiento previstos de 21°C y $60\%\text{HR}$.

Las unidades de climatización se deberán calcular para un funcionamiento continuo 24h/días y los 365 días del año. La potencia frigorífica para una

temperatura de bulbo seco interior de 24°C debería bastar para mantener las características de las salas para las variaciones de temperatura ambiente medias actuales y para el 120% de la carga total de los locales (carga eléctrica + aportaciones de los locales + iluminación + presencia no continua de personas en sala).

56.3.1.5 Sistemas de alimentación ininterrumpida

También denominados SAI (UPS, “Uninterruptible Power Supply”), es un dispositivo que gracias a sus baterías, puede proporcionar energía eléctrica tras un apagón a todos los dispositivos que tenga conectados. Otra de las funciones de los SAI es la de mejorar la calidad de la energía eléctrica que llega a las cargas, filtrando subidas y bajadas de tensión y eliminando armónicos de la red en el caso de usar corriente alterna.

Existen dos tipos de de SAI:

- SAI de corriente continua (activo). Las cargas conectadas a los SAI requieren una alimentación de corriente continua, por lo tanto éstos transformarán la corriente alterna de la red comercial a corriente continua y la usarán para alimentar a la carga y almacenarla en sus baterías. Por lo tanto no necesitan convertidores entre las baterías y las cargas.
- SAI de corriente alterna (pasivo). Estos SAI generan como salida una señal alterna, por lo que necesitan un inversor para transformar la señal continua obtenida de las baterías en una señal alterna.

56.3.1.6 Otras características a tener en cuenta

56.3.1.6.1 Recinto de protección combinada

Son recintos de protección combinada aquellos compartimentos dentro de los CPD capaces de garantizar una custodia segura de los soportes magnéticos de respaldo ante los agentes más peligrosos que puedan atacarlos. Estarán dotados al menos con:

- Apantallamiento electromagnético y jaulas de Faraday.
- Protección contra reacciones químicas que produzcan HCL y gases de combustión corrosivos dentro de la cámara.
- Protección contra la intrusión y el robo (puerta de seguridad).
- Protección contra el vandalismo y explosiones.
- Protección contra incendios y sus efectos derivados (humos y vapores).
- Protección contra las inundaciones interiores del CPD.
- Protección contra el impulso electromagnético nuclear (NEMP).
- Sellado de las instalaciones y de la cámara contra altas frecuencias e incendios.

56.3.1.6.2 Instalaciones de agua

Se evitará, en lo posible las canalizaciones de agua en la sala de ordenadores (sobre todo por falso techo, falso suelo o visibles). En todo caso se preverán los mecanismos de detección de fugas y la instalación de válvulas que puedan cerrar las conducciones afectadas. Los detectores de agua se basarán en sensores puntuales o de banda que cubran áreas completas.

El cableado debe estar impermeabilizado cuando discorra por zonas con riesgo de humedad o inundación. Si no es posible separar los conductos de agua del resto de instalaciones, se preverá dotar al techo o solera del forjado, por donde discurren las tuberías, de la inclinación oportuna para evacuar el agua hacia los puntos de drenaje establecidos, evitando su acumulación.

Si existen en el edificio o adosados a él depósitos de agua u otro tipo de líquido, se asegurará la estanqueidad de los mismos y se instalarán de

forma que su rotura no afecte a los servicios esenciales ni por supuesto a las personas.

En el caso de salas de informática situadas en sótanos se reforzará la estanqueidad de paredes, pisos, techos, puertas y ventanas. Se preverá la instalación de bombas automáticas para evacuar eventuales inundaciones, que deben alimentarse con un sistema eléctrico aislado del resto de la sala para permitir su funcionamiento independiente.

Si las CPU precisan agua fría para la refrigeración, se preverá la red de tuberías con sus válvulas de corte y retención, sondas detectoras y sistema auxiliar de emergencia desde el contador del canal con filtrado del líquido.

56.4 CLASIFICACIÓN DE LOS CPD

El estándar TIA-942 describe los requisitos que debe cumplir la infraestructura de un centro de proceso de datos. Se establecen cuatro niveles de disponibilidad:

- **Tier I:** Centro de proceso de datos (CPD) Básico. La tasa de disponibilidad máxima del CPD es del 99.671% del tiempo, es decir, el nivel Tier I del estándar TIA-942 consigue reducir el tiempo de parada del CPD a lo largo de un año a 29 horas como máximo.

Un CPD Tier I puede admitir interrupciones tanto planeadas como no planeadas. Cuenta con sistemas de aire acondicionado y distribución de energía, pero puede no tener piso técnico, SAI o generador eléctrico. Si los posee pueden tener varios puntos únicos de fallo. La carga máxima de los sistemas en situaciones críticas es del 100%. La infraestructura del CPD deberá estar fuera de servicio al menos una vez al año por razones de mantenimiento y/o reparaciones. Los errores de operación o fallas en los componentes de su infraestructura causarán la interrupción del CPD.

- **Tier II:** Componentes Redundantes. La tasa de disponibilidad máxima del CPD es del 99.749% del tiempo, es decir, el nivel Tier II del

estándar TIA - 942 consigue reducir el tiempo de parada del CPD a lo largo de un año a 22 horas como máximo. Un CPD con componentes redundantes son ligeramente menos susceptibles a interrupciones, tanto planeadas como las no planeadas. Estos CPD cuentan con suelo técnico, SAI y generadores eléctricos, pero está conectado a una sola línea de distribución eléctrica. Su diseño es (N+1), lo que significa que existe al menos un duplicado de cada componente de la infraestructura. La carga máxima de los sistemas en situaciones críticas es del 100%. El mantenimiento en la línea de distribución eléctrica o en otros componentes de la infraestructura, pueden causar una interrupción del servicio.

- **Tier III:** Mantenimiento Concurrente. La tasa de disponibilidad máxima del CPD es del 99.982% del tiempo, es decir, el nivel Tier III del estándar TIA -942 consigue reducir el tiempo de parada del CPD a lo largo de un año a 1,5 horas como máximo. Las capacidades de un CPD de este nivel le permiten realizar cualquier actividad planeada sobre cualquier componente de la infraestructura sin interrupciones en la operación. Las actividades planeadas incluyen mantenimiento preventivo, reparaciones o reemplazo de componentes, agregar o eliminar componentes, realizar pruebas de sistemas o subsistemas, entre otros. Para infraestructuras que utilizan sistemas de enfriamiento por agua, significa doble conjunto de tuberías. Debe existir suficiente capacidad y doble línea de distribución de los componentes, de forma tal que sea posible realizar mantenimiento o pruebas en una línea y mientras que la otra atienda la totalidad de la carga. En este nivel, actividades no planeadas como errores de operación o fallos espontáneos en la infraestructura pueden todavía causar una interrupción del CPD. La carga máxima en los sistemas en situaciones críticas es de 90%.

Muchos CPD Tier III son diseñados para actualizarse a Tier IV, cuando los requerimientos del negocio justifiquen el costo.

- **Tier IV:** Tolerante a Fallos. La tasa de disponibilidad máxima del CPD es del 99.995% del tiempo, es decir, el nivel Tier IV del estándar TIA-942 consigue reducir el tiempo de parada del CPD a lo largo de un año a 26 minutos como máximo.

Un CPD de este nivel provee capacidad para realizar cualquier actividad planeada sin interrupciones en el servicio, pero además la funcionalidad tolerante a fallos le permite a la infraestructura continuar operando aún ante un evento crítico no planeado. Esto requiere dos líneas de distribución simultáneamente activas, típico en una configuración System+System. Eléctricamente esto significa dos sistemas de SAI independientes, cada sistema con un nivel de redundancia N+1. La carga máxima de los sistemas en situaciones críticas es de 90%. Persiste un nivel de exposición a fallos, por el inicio una alarma de incendio o porque una persona inicie un procedimiento de apagado de emergencia (EPO), los cuales deben existir para cumplir con los códigos de seguridad contra incendios o eléctricos.

56.5 BIBLIOGRAFÍA

Centro de procesamiento de datos en Wikipedia:

http://es.wikipedia.org/wiki/Centro_de_procesamiento_de_datos.

TIA-942: Data Center Standars Overview:

<http://www.adc.com/Attachment/1270711929361/102264AE.pdf>

Eduardo Leyton Guerrero: Auditoría al CPD.

Autor: Francisco Javier Rodriguez Martínez

Subdirector de Sistemas Escola Superior Enxeñaría Informática Ourense

Colegiado del CPEIG

**57. VIRTUALIZACIÓN DE
SERVIDORES. VIRTUALIZACIÓN
DEL ALMACENAMIENTO.
VIRTUALIZACIÓN DEL PUESTO
CLIENTE. COMPUTACIÓN
BASADA EN SERVIDOR (SBC).
GRID COMPUTING. CLOUD
COMPUTING. GREEN IT Y
EFICIENCIA ENERGÉTICA.**

Tema 57: Virtualización de servidores. Virtualización del almacenamiento. Virtualización del puesto cliente. Computación basada en servidor (SBC). Grid Computing. Cloud computing. Green IT y eficiencia energética.

57.1 Virtualización de servidores.....	1
57.2 Virtualización del almacenamiento.....	5
57.3 Virtualización del puesto cliente.....	10
57.4 Computación basada en servidor.....	12
57.5 Grid Computing.....	15
57.6 Cloud computing.....	19
57.7 Green IT e eficiencia energética.....	21
57.8 Bibliografía.....	29

57.1 VIRTUALIZACIÓN DE SERVIDORES

Podemos definir virtualización como la técnica que consiste básicamente en agrupar diferentes aplicaciones y servicios de sistemas heterogéneos dentro de un mismo hardware, de forma que los usuarios y el propio sistema los vean como máquinas independientes dedicadas. Para ello, el sistema operativo virtualizado debe ver el hardware de la máquina real como un conjunto normalizado de recursos independientemente de los componentes reales que lo formen.

De esta forma, para virtualizar un sistema de servidores, los administradores deben, básicamente, optimizar los recursos disponibles, incluyendo el número y la identidad de los servidores físicos individuales, procesadores, y sistemas operativos, con el objetivo de producir una mejora tanto en la gestión como en el manejo de sistemas informáticos complejos. El administrador del sistema virtual utilizará un software para la

división del servidor físico en entornos virtuales aislados. Estos entornos son lo que se conoce técnicamente como servidores privados virtuales, pero también se pueden encontrar referencias como particiones, instancias, contenedores o emulaciones de sistemas.

En concreto, podemos decir que un servidor privado virtual es un término de marketing utilizado por los servicios de hosting para referirse a una máquina virtual para el uso exclusivo de un cliente individual del servicio. El término se utiliza para enfatizar que la máquina virtual, a pesar de ejecutarse en el mismo equipo físico que las máquinas virtuales de otros clientes, es funcionalmente equivalente a un equipo físico independiente, está dedicado a las necesidades individuales del cliente y puede ser configurado para ejecutarse como un servidor de internet (es decir, para ejecutar software de servidor). El término VDS o Virtual Dedicated Server (Servidor Virtual Dedicado) para el mismo concepto.

Cada servidor virtual puede ejecutar su propio sistema operativo y ser reiniciado de modo independiente.

57.1.1 Funcionamiento

El servidor físico realiza una abstracción de los recursos que se denomina Hypervisor o VMM (Virtual Machine Monitor), elemento software que se instala en la máquina donde se va a llevar a cabo la virtualización y sobre la que se configuran las máquinas virtuales que es donde van a residir las aplicaciones. Es el encargado de gestionar los recursos de los sistemas operativos “alojados” (guest) o máquinas virtuales.

Desde un punto de vista lógico, el usuario percibe que son máquinas independientes y aisladas entre sí, pero desde una perspectiva física, todas las máquinas virtuales residen en un único servidor. A estas máquinas virtuales se les asigna un porcentaje de los recursos del servidor físico, que serán los únicos que el cliente conozca.

Se pueden encontrar tres modelos de virtualización: el modelo de máquina virtual o virtualización completa, el modelo paravirtual o virtualización parcial; y la virtualización a nivel de sistema operativo.

57.1.1.1 Virtualización completa

El modelo de máquina virtual está basado en la arquitectura cliente/servidor, donde cada cliente funciona como una imagen virtual de la capa hardware. Este modelo permite que el sistema operativo cliente funcione sin modificaciones. Además permite al administrador crear diferentes sistemas cliente con sistemas operativos independientes entre sí. La ventaja principal de este modelo radica en el desconocimiento por parte de los sistemas huésped del sistema hardware real sobre el que está instalado. Sin embargo, realmente todos los sistemas virtuales hacen uso de recursos hardware físicos. Estos recursos son administrados por un el hypervisor que coordina las instrucciones CPU, convirtiendo las peticiones del sistema invitado en las solicitudes de recursos apropiados en el host, lo que implica una sobrecarga considerable. Casi todos los sistemas pueden ser virtualizados utilizando este método, ya que no requiere ninguna modificación del sistema operativo. A pesar de esto, es necesaria una virtualización de la CPU como apoyo para la mayoría de los hypervisores que llevan a cabo la virtualización completa.

Ejemplos típicos de sistemas de servidores virtuales son VMware Workstation, VMware Server, VirtualBox, Parallels Desktop, Virtual Iron, Adeos, Mac-on-Linux, Win4BSD, Win4Lin Pro, y z/VM, openvz, Oracle VM, XenServer, Microsoft Virtual, PC 2007 y Hyper-V.

57.1.1.2 Paravirtualización

El modelo de máquina paravirtual (PVM) o virtualización parcial se basa, como el modelo anterior, en la arquitectura cliente/servidor, incluyendo también la necesidad de contar con un sistema monitor. Sin embargo, en este caso, el VMM accede y modifica el código del sistema operativo del sistema huésped. Esta modificación se conoce como porting. El porting

sirve de soporte al VMM para que pueda realizar llamadas al sistema directamente. Al igual que las máquinas virtuales, los sistemas paravirtuales son capaces de soportar diferentes sistemas operativos instalados en el hardware real. Esta técnica se utiliza con intención de reducir la porción de tiempo de ejecución empleada por el huésped empleado en realizar las operaciones que son mucho más difíciles de ejecutar en un entorno virtual en comparación con un entorno no virtualizado. Así se permite que el invitado(s) y el huésped soliciten y reconozcan estas tareas, que de otro modo serían ejecutados en el dominio virtual (donde el rendimiento de ejecución es peor). Una plataforma paravirtualizada exitosamente puede permitir que el VMM sea menos complejo (por la reubicación de la ejecución de las tareas críticas del dominio virtual en el dominio del servidor), y/o reducir la degradación del rendimiento global de la máquina virtual durante la ejecución de invitado.

UML, XEN, Xen, Virtuozzo , Vserver y OpenVZ (que es el código abierto y la versión de desarrollo de Parallels Virtuozzo Containers) son modelos de máquinas paravirtuales.

57.1.1.3 Virtualización por S.O.

La virtualización a nivel de sistema operativo se diferencia de las anteriores en que, en este caso, no existe un sistema cliente/servidor propiamente dicho. En este modelo el sistema principal exporta la funcionalidad del sistema operativo desde su propio núcleo. Por esta razón, los sistemas virtuales usan el mismo sistema operativo que el nativo (aunque en la mayoría de los casos pueden instalar distintas distribuciones). Esta arquitectura elimina las llamadas del sistema entre capas, lo que favorece una reducción importante en el uso de CPU. Además, al compartir los ficheros binarios y librerías comunes del sistema en la misma máquina, la posibilidad de escalado es mucho mayor, permitiendo que un mismo servidor virtual sea capaz de dar servicio a un gran número de clientes al mismo tiempo.

La Virtualización de SO mejora el rendimiento, gestión y eficiencia. Podemos entenderlo como un sistema en capas. En la base reside un sistema operativo huésped estándar. A continuación encontramos la capa de virtualización, con un sistema de archivos propietario y una capa de abstracción de servicio de kernel que garantiza el aislamiento y seguridad de los recursos entre distintos contenedores. La capa de virtualización hace que cada uno de los contenedores aparezca como servidor autónomo. Finalmente, el contenedor aloja la aplicación o carga de trabajo.

Ejemplos de sistemas que usan virtualización a nivel de sistema operativo son Virtuozzo y Solaris.

57.2 VIRTUALIZACIÓN DEL ALMACENAMIENTO

Este tipo de virtualización permite una mayor funcionalidad y características avanzadas en el sistema de almacenamiento. Consiste en abstraer el almacenamiento lógico del almacenamiento físico y suele usarse en SANs (Storage Area Network, Red de área de almacenamiento).

Este sistema de almacenamiento también se conoce como “storage pool”, matriz de almacenamiento, matriz de disco o servidor de archivos. Estos sistemas suelen usar hardware y software especializado, junto con unidades de disco con el fin de proporcionar un almacenamiento muy rápido y fiable para el acceso a datos. Son sistemas complejos, y pueden ser considerados como un ordenador de propósito especial diseñado para proporcionar capacidad de almacenamiento junto con funciones avanzadas de protección de datos. Las unidades de disco son sólo un elemento dentro del sistema de almacenamiento, junto con el hardware y el software de propósito especial incorporado en el sistema.

Los sistemas de almacenamiento pueden ser de acceso a nivel de bloque, o acceso a nivel de ficheros. El acceso por bloques suele llevarse a cabo por medio de Fibre Channel , iSCSI , SAS , FICON u otros protocolos. Para el acceso a nivel de archivo se usan los protocolos NFS o CIFS.

Dentro de este contexto nos podemos encontrar con dos tipos principales de virtualización: la virtualización por bloques y la virtualización por archivos.

57.2.1 Virtualización por bloques

Este tipo de virtualización se basa en la abstracción (diferenciación) entre el almacenamiento lógico y el almacenamiento físico, consiguiendo que el acceso no tenga en cuenta el almacenamiento físico o estructura heterogénea.

Existen tres tipos de virtualización por bloques: basada en host, basada en dispositivos de almacenamiento, basada en red.

57.2.1.1 Virtualización basada en host

Esta virtualización requiere software adicional que se ejecuta en el host. En algunos casos la administración de volúmenes está integrada en el sistema operativo, y en otros casos se ofrece como un producto separado. Los volúmenes (LUN) disponibles en el sistema son manejados por un controlador de dispositivos físicos tradicional. Por encima de este controlador se encuentra una capa software (el gestor de volúmenes) que intercepta las peticiones de E / S, y proporciona la búsqueda de meta-datos y mapeos de E / S.

Los sistemas operativos más modernos tienen algún tipo de gestor de volúmenes lógicos integrado (MVI en UNIX / Linux, o Administrador de discos lógicos o LDM en Windows), que realiza tareas de virtualización.

Existen varias tecnologías que implementan este tipo de virtualización, como pueden ser la gestión de volúmenes lógicos (Logical Volume Management, LVM), los sistemas de archivos (CIFS, NFS) o el montaje automático (autofs)

57.2.1.2 Virtualización basada en dispositivos de almacenamiento

Se puede llevar a cabo la virtualización basada en medios de almacenamiento masivo utilizando un controlador de almacenamiento primario que proporcione los servicios de virtualización y permita conexión directa de los controladores de almacenamiento. En función de la implementación es posible usar modelos de distintos fabricantes.

El controlador primario proporcionará la puesta en común y los meta-datos de servicio de gestión. También puede ofrecer servicios de replicación y migración a través de los controladores que se virtualizan.

Una nueva generación de controladores de serie del disco permite la inserción posterior de los dispositivos de almacenamiento.

Los sistemas RAID pueden ser un ejemplo de esta técnica. Estos sistemas combinan varios discos en una sola matriz.

Las matrices avanzadas de disco, cuentan a menudo con clonación, instantáneas y replicación remota. En general, estos dispositivos no ofrecen los beneficios de la migración de datos o de replicación a través de almacenamiento heterogéneo, ya que cada fabricante tiende a utilizar sus propios protocolos propietarios.

57.2.1.3 Virtualización basada en red

Esta es una virtualización de almacenamiento operando en un dispositivo basado en red (por lo general un servidor estándar o un smart switch) y el uso de redes iSCSI o FC de Fibre Channel para conectar como SAN (Storage Area Network). Este es el tipo de virtualización de almacenamiento más común.

El dispositivo de virtualización se encuentra en la SAN y proporciona la capa de abstracción entre los host, que permiten la entrada/salida, y los controladores de almacenamiento, que proporcionan capacidad de almacenamiento.

Hoy en día existen dos implementaciones distintas, la basada en el **dispositivo** y la basada en **conmutación**. Ambos modelos proporcionan los mismos servicios: gestión de discos, búsqueda de meta-datos, migración y replicación de datos. Igualmente, ambos modelos necesitan de un hardware específico que permita ofrecer dichos servicios.

La basada en dispositivos consiste en establecer el hardware especializado entre los hosts y la parte de almacenamiento. Las solicitudes de entrada/salida se redirigen al dispositivo, que realiza la asignación de meta-datos, mediante el envío de sus propias órdenes de E/S a la solicitud de almacenamiento subyacente. El hardware usado también puede proporcionar almacenamiento de datos en caché, y la mayoría de las implementaciones proporcionan algún tipo de agrupación de cada uno de los dispositivos para mantener un punto de vista atómico tanto de los meta-datos como de los datos de la caché.

Este tipo de almacenamiento también puede clasificarse en in-band (simétrica) o out-of-band (asimétrica).

57.2.1.3.1 In-band (simétrica)

En este caso los dispositivos de virtualización se asientan entre el host y el almacenamiento. Todas las peticiones de E/S y datos pasan a través del dispositivo. Los host nunca interactúan con el dispositivo de almacenamiento sino con el dispositivo de virtualización.

57.2.1.3.2 Out-of-band (asimétrica)

Los dispositivos usados en este tipo de virtualización también son llamados servidores de meta-datos. La única finalidad de estos dispositivos es proporcionar la asignación de meta-datos. Esto implica el uso de software adicional en el host, que es conocedor de la ubicación real de los datos. De este modo, se intercepta la petición antes de que salga del host, se solicita una búsqueda de meta-datos en el servidor (puede ser a través de una interfaz que no sea SAN) y se devuelve la ubicación real de los datos solicitados por el host. Finalmente se recupera la información a través de

una solicitud de E/S común al dispositivo de almacenamiento. No se puede dar un almacenamiento en caché ya que los datos nunca pasan a través del dispositivo de virtualización.

57.2.2 *Virtualización a nivel de archivo*

Con este tipo de virtualización se pretende eliminar las dependencias entre el acceso a datos a nivel de archivo y la ubicación física de los mismos. Esta técnica, conocida como NAS (Network-Attached Storage) o almacenamiento conectado a red, suele ser un equipo especializado pensado exclusivamente para almacenar y servir ficheros. Los equipos que funcionan como dispositivo NAS suelen incluir un sistema operativo específico para el propósito, como puede ser FreeNAS o FreeBSD.

Estos sistemas pueden contener uno o más discos duros, dispuestos a menudo en contenedores lógicos redundantes o arrays RAID.

NAS utiliza protocolos basados en archivos como NFS (sistemas UNIX), SMB / CIFS (Server Message Block/Common Internet File System) (sistemas MS Windows), o AFP (Apple Filing Protocol, sistemas Apple Macintosh). Las unidades NAS no suelen limitar a los clientes a un único protocolo. FTP, SFTP, HTTP, UPnP, rsync y AFS (Andrew File System) también lo soportan.

De este modo se consigue optimizar la utilización del almacenamiento y las migraciones de archivos sin interrupciones.

57.2.3 *Diferencias entre NAS y SAN*

NAS proporciona almacenamiento y un sistema de archivos, lo que suele contrastar con SAN, que solamente proporciona almacenamiento basado en bloques y deja del lado del cliente la gestión del sistema de archivos.

NAS aparece en el sistema cliente como un servidor de archivos (se pueden asignar unidades de red a las acciones del servidor) mientras que un disco a través de una SAN se presenta al cliente como un disco más del sistema operativo, que podemos montar, desmontar, formatear...

	NAS	SAN
Tipo de datos	Archivos compartidos	Datos a nivel de bloque, por ejemplo, bases de datos.
Cableado utilizado	Ethernet LAN	Fibre Channel dedicado
Cientes principales	Usuarios finales	Servidores de aplicaciones
Acceso a disco	A través del dispositivo NAS (IP propia)	Acceso directo
NAS		
SAN		

57.3 VIRTUALIZACIÓN DEL PUESTO CLIENTE

Esta técnica consiste en la separación del entorno de usuario de un ordenador personal de la máquina física con el modelo cliente-servidor. El modelo que sigue un servidor para implementar dicha característica se

denomina VDI (Virtual Desktop Infrastructure, NAS Infraestructura de Escritorio SAN Virtual), también llamada Interfaz de Escritorio Virtual.

La mayoría de implementaciones comerciales de esta tecnología usan un servidor central remoto para llevar a cabo la “virtualización” del escritorio del cliente, en lugar de usar el almacenamiento local del cliente remoto. Esto implica que todas las aplicaciones, procesos, configuraciones y datos del cliente están almacenadas en el servidor y se ejecutan de forma centralizada.

El sistema cliente puede utilizar una arquitectura de hardware completamente diferente de la utilizada por el entorno de escritorio

proyectado, y también puede estar basada en un sistema operativo completamente diferente.

El modelo de virtualización del puesto cliente permite el uso de máquinas virtuales para que múltiples suscriptores de red puedan mantener escritorios individuales en un solo ordenador, el servidor central. Este servidor central puede operar en una residencia, negocio o centro de datos. Los usuarios pueden estar geográficamente dispersos, pero todos están conectados a la máquina central por una red de área local, una red de área amplia, o Internet.

57.3.1 *Modos de Operación de VDI*

Básicamente existen cuatro modelos de operación VDI:

- Alojado (como servicio). Suelen contratarse a proveedores comerciales y normalmente proporciona una configuración del sistema operativo del puesto cliente administrado. Los principales suministradores son CITRIX, VMware y Microsoft.
- Centralizado. En este caso todas las instancias VDI están alojadas en uno o más servidores centralizados, los datos están en sistemas de almacenamiento conectados a estos. Este modelo a su vez puede distinguir dos tipos:
 - o VDI estático o persistente. Existe una única imagen de escritorio asignado por cliente y estos deben ser gestionados y mantenidos.
 - o VDI dinámico o no persistente. Existe una imagen maestra común para todos los clientes que se clona y personaliza en el momento de la petición con los datos y aplicaciones particulares de cada cliente.
- Remoto (o sin ataduras). Tiene como base el concepto de VDI centralizado pero permite trabajar sin la conexión a un servidor

central o a Internet. Se copia una imagen al sistema local y se ejecuta sin necesidad de más conexión. Las imágenes tienen un cierto periodo de vida y se actualizan periódicamente. Esta imagen se ejecuta en el sistema local que necesita un sistema operativo y un hipervisor (que ejecuta la instancia VDI). Esto implica que el dispositivo cliente tenga mayores necesidades de memoria, espacio en disco, CPU... La ventaja es la menor dependencia de conexión.

Los modelos alojado y centralizado necesitan de una red que conecte con el servidor donde se ejecuta la instancia VDI. El concepto base de este modelo es similar al de clientes ligeros debido a que el cliente sólo tiene que mostrar el escritorio virtual.

En el caso del modelo remoto, se permite a los usuarios copiar la instancia VDI en el sistema y luego se ejecutará el escritorio virtual sin necesidad de ningún tipo de conexión.

57.4 COMPUTACIÓN BASADA EN SERVIDOR

También conocida como SBC del inglés Server Based Computing, consiste en la separación del procesamiento de ciertas tareas como la gestión de datos que será realizado en un servidor central y otras tareas de procesamiento, como la presentación de aplicaciones de usuario e impresión de datos en el cliente. Lo único transmitido entre servidor y cliente son las pantallas de información. Esta arquitectura puede dar solución a los principales problemas que aparecen cuando se ejecutan aplicaciones en los clientes. Además simplifica procesos como pueden ser los entornos hardware, actualizaciones de software, despliegue de aplicaciones, soporte técnico, almacenamiento y respaldo de datos. Se centraliza la gestión de todos estos procesos en un único servidor.

Los clientes que actúan en esta arquitectura suelen llamarse thin clients, o clientes ligeros, este es un término general para dispositivos que se basan en un servidor para operar. El thin client proporciona pantalla, teclado,

ratón y un procesador básico que interactúa con el servidor. Los thin client no almacenan ningún dato localmente y requiere de pocos recursos de procesamiento. La característica más destacada de estos terminales es la reducción de costes asociados con el mantenimiento, administración, soporte, seguridad e instalación de aplicaciones comparándolo con un PC tradicional.

Esta tecnología está compuesta por tres componentes principales:

- Sistemas operativos multi-usuario que permiten el acceso y ejecución de modo concurrente, usando aplicaciones diferentes y con sesiones de usuario protegidas. Ejemplos de algunas terminales de servicio son: 2x Terminal Server para Linux, Microsoft Windows Terminal Server (Windows NT/2000), Microsoft Windows Terminal Services (Windows 2003), Citrix Presentation Server, Citrix XenApp Server, AppliDis Fusion, 2X Application Server, HOblink, Propalms TSE (antes Tarantella), Jethro cabina, GraphOn GO-Global, VMware View..
- El thin client se puede ejecutar con una cantidad mínima de software pero necesita al menos un programa de conexión a servicios de terminal. El thin client y el programa de servicios de terminal pueden ser ejecutados en sistemas operativos completamente diferentes.
- Un protocolo que permita al programa de servicios de terminal y al thin client comunicarse y enviar las pulsaciones de teclado, de ratón y las actualizaciones de pantalla a través de la red. Los protocolos más populares son RDP3 (Remote Desktop protocol), ICA y NX.

Entre las ventajas de la computación basada en servidor se puede nombrar:

- Reducción de los costes de administración. La gestión de clientes ligeros está casi en su totalidad centralizada en el servidor.

- Reducción de costes de hardware. El hardware en los clientes ligeros es generalmente más barato porque no es necesario tener memoria para las aplicaciones o un procesador de gran alcance.
- Seguridad. Puede ser controlada centralmente.
- Menor consumo de energía. El hardware especializado en el cliente ligero tiene un consumo mucho menor de energía que los tradicionales.
- Reducción de la carga de red. El tráfico de red que generan los terminales ligeros sólo es el de los movimientos del ratón, teclado e información de pantalla desde / hacia el usuario. En el caso de que un cliente pesado abriese y guardase un documento ya implicaría el paso de este dos veces por la red. Usando protocolos eficientes de red tales como ICA y NX ya es posible usar esta tecnología en un ancho de banda de 28,8 Kbps.
- Actualización de hardware simple. Si el uso está por encima de un límite predefinido, es relativamente sencillo solucionar el problema, bastaría con un disco nuevo en un rack de servidores, aumentando así el número de recursos, exactamente la cantidad necesaria. Si ocurriese esto con clientes pesados habría que reemplazar un PC completo, lo que acarrearía tanto costes económicos como de recursos humanos.

A pesar de lo anterior, esta tecnología también presenta ciertos inconvenientes:

- Altos requerimientos de servidor. Al centrarse la carga de trabajo en el servidor, el sistema de clientes ligeros implica mayor consumo de recursos en los servidores, incluso es habitual que se use un gran número de servidores, lo que se denomina “granja de servidores”.

- Pobre rendimiento multimedia. El envío de datos de audio y video requieren mucho ancho de banda, por lo que estos sistemas son menos útiles para aplicaciones multimedia.
- Menos flexibilidad. No todos los productos software del mercado pueden funcionar correctamente en un cliente ligero.

57.5 GRID COMPUTING

Arquitectura distribuida y paralela, de ámbito extenso geográficamente, en la que se premia la distribución, y a continuación la paralelización. Sus creadores fueron Ian Foster y Carl Kesselman. Su nombre proviene del paradigma de la red eléctrica (power grid).

Se basa en la compartición, selección y agregación de forma dinámica y en tiempo de ejecución de recursos autónomos, distribuidos geográficamente, dependiendo de criterios como la disponibilidad del hardware, la capacidad transaccional, el rendimiento que se pueda aportar a la solución final, el coste y los criterios de calidad del servicio que el demandante pueda proporcionar y exigir.

La red está formada por un conjunto de ordenadores independientes e interconectados que ponen a disposición del grid los excedentes de su procesamiento individual, es decir, los ciclos de reloj de sus CPUs no aprovechados por ellos mismos, sin poder superar un determinado porcentaje de dedicación configurado individualmente en cada nodo. A partir del porcentaje proporcionado por cada nodo, se virtualiza un recurso computacional único.

Los sistemas basados en grid computing están indicados para atender productividades sostenidas y sostenibles, sin poder nunca superar un determinado umbral. En estos sistemas se garantiza la escalabilidad como un criterio parametrizable. Es posible definir con qué criterio añadimos cada nuevo nodo a la solución final.

Actualmente, el único criterio que se tiene en cuenta es la capacidad de procesamiento (transaccionalidad), pero en el futuro, será posible tener en cuenta criterios más finos, referidos a la calidad del servicio.

Además, estos sistemas están dotados de un comportamiento dinámico, según el cual, un determinado programa en ejecución en el sistema, puede modificar en tiempo real el dimensionamiento de la grid para adaptarlo a sus necesidades.

57.5.1 *Características:*

- Podemos conseguir un máximo aprovechamiento de los nodos (100% de utilización de la CPU).
- Los nodos no tienen que estar dedicados. Además, al contrario que en el caso del cluster, nos aseguramos que la aportación al Grid no va a sobrepasar un determinado porcentaje de tiempo de procesamiento en cada nodo.
- Son sistemas heterogéneos, en los que podemos encontrar diversos HW y SW.
- La escalabilidad parametrizable es la característica más potente de esta arquitectura.

57.5.2 *Funcionalidades:*

- Localización dinámica de recursos (máquinas con excedente).
- Optimización del acceso a datos, mapeando las estructuras de datos en cachés temporales locales (directorios).
- Autenticación del usuario (usr/pwd, certificados...).
- Monitorización de tareas y procesos desde cualquier nodo de la red, siempre que el usuario tenga permisos.
- Las máquinas se encuentran en situación paritaria.

- Si es posible, se paraleliza. Lo fundamental es la distribución de procesos débilmente acoplados.

57.5.3 *Arquitectura Grid*

Habitualmente se describe la arquitectura del Grid en términos de "capas", ejecutando cada una de ellas una determinada función. Como es habitual en este tipo de enfoque, las capas más altas están más cerca del usuario, en tanto que las capas inferiores lo están de las redes de comunicación.

Empezando por los cimientos, nos encontramos con la capa de red, responsable de asegurar la conexión entre los recursos que forman el Grid.

En la parte más alta está la capa de recursos, constituida por los dispositivos que forman parte del Grid: ordenadores, sistemas de almacenamiento, catálogos electrónicos de datos e incluso sensores que se conecten directamente a la red.

En la zona intermedia está la capa "middleware", encargada de proporcionar las herramientas que permiten que los distintos elementos (servidores, almacenes de datos, redes, etc.) participen de forma coordinada en un entorno Grid unificado. Esta capa es la encargada de las siguientes funciones:

Encontrar el lugar conveniente para ejecutar la tarea solicitada por el usuario.

- Optimiza el uso de recursos, que pueden estar muy dispersos.
- Organiza el acceso eficiente a los datos.
- Se encarga de la autenticación de los diferentes elementos.
- Se ocupa de las políticas de asignación de recursos.
- Ejecuta las tareas.
- Monitoriza el progreso de los trabajos en ejecución.

- Gestiona la recuperación frente a fallos.
- Avisa cuando se haya terminado la tarea y devuelve los resultados.

El ingrediente fundamental del middleware son los metadatos (datos sobre los datos), que contienen, entre otras cosas, toda la información sobre el formato de los datos y dónde se almacenan (a veces en varios sitios distintos).

El middleware está formado por muchos programas software. Algunos de esos programas actúan como agentes y otros como intermediarios, negociando entre sí, de forma automática, en representación de los usuarios del Grid y de los proveedores de recursos. Los agentes individuales presentan los metadatos referidos a los usuarios, datos y recursos. Los intermediarios se encargan de las negociaciones entre máquinas (M2M) para la autenticación y autorización de los usuarios y se encargan de definir los acuerdos de acceso a los datos y recursos y, en su caso, el pago por los mismos. Cuando queda establecido el acuerdo, un intermediario planifica las tareas de cómputo y supervisa las transferencias de datos necesarias para acometer cada trabajo concreto. Al mismo tiempo, una serie de agentes supervisores especiales optimizan las rutas a través de la red y monitorizan la calidad del servicio.

En la capa superior de este esquema está la capa de aplicación donde se incluyen todas las aplicaciones de los usuarios, portales y herramientas de desarrollo que soportan esas aplicaciones. Esta es la capa que ve el usuario.

Además, en las arquitecturas más comunes del Grid, la capa de aplicación proporciona el llamado "serviceware", que recoge las funciones generales de gestión tales como la contabilidad del uso del Grid que hace cada usuario.

Para poder hacer todo lo anterior, las aplicaciones que se desarrollen para ser ejecutadas en un PC concreto, tendrán que adaptarse para poder invocar los servicios adecuados y utilizar los protocolos correctos. Igual que las aplicaciones que inicialmente se crearon para funcionar aisladamente se adaptan para poder ser ejecutadas en un navegador Web, el Grid requerirá que los usuarios dediquen cierto esfuerzo a "GRIDizar" sus aplicaciones.

Sin embargo, una vez adaptadas al Grid, miles de usuarios podrán usar las mismas aplicaciones, utilizando las capas de middleware para adaptarse a los posibles cambios en el tejido del Grid.

57.6 CLOUD COMPUTING

Modelo que permite acceso a un conjunto compartido de recursos informáticos configurables a través de la red (por ejemplo, redes, servidores, almacenamiento, aplicaciones y servicios) que pueden ser desarrollados y desplegados rápidamente con mínimo esfuerzo de gestión o interacción con el proveedor de servicios.

Este término se refiere a la utilización y el acceso de múltiples recursos basados en servidores a través de una red. Los usuarios de la "nube" pueden acceder a los recursos del servidor utilizando un ordenador, netbook, pad computer, smart phone u otro dispositivo. En el cloud computing, el servidor presenta y gestiona las aplicaciones; los datos también se almacenan de forma remota en la configuración de la nube. Los usuarios no descargan ni instalan aplicaciones en su sistema, todo el procesamiento y almacenamiento se mantiene por el servidor. Los servicios on-line pueden ser ofrecidos a partir de un "proveedor de la nube" o por una organización privada.

57.6.1 Arquitectura

Normalmente la arquitectura de los sistemas software implicados en el desarrollo de cloud computing incluyen múltiples componentes

denominados “componentes cloud” que se comunican mediante mecanismos de bajo acoplamiento, tales como las colas de mensajes.

Los dos componentes más significativos de la arquitectura cloud computing se conocen como el front-end y el back-end. El front-end es la parte vista por el cliente, es decir, el usuario del PC. Esto incluye la red del cliente y las aplicaciones utilizadas para acceder a la nube a través de una interfaz de usuario, como un navegador web. El back-end de la arquitectura es la propia nube, que comprende varios ordenadores, servidores y dispositivos de almacenamiento de datos.

Dentro de esta arquitectura se pueden distinguir las siguientes capas:

- Proveedor: Empresa responsable de proporcionar el servicio en la “nube”.
- Cliente: Serán el hardware y software diseñados para cloud computing, que permiten interactuar con los servicios remotos.
- Aplicación: Son los servicios en la “nube” o “Software as a Service” (SaaS), el software se proporciona a través de internet como si de un servicio se tratase. De este modo se evita la necesidad de instalar y ejecutar en el equipo del cliente la aplicación. Se reducen así el mantenimiento y el apoyo.
- Plataforma: Son los servicios de plataforma en la “nube”, también conocidos como “Platform as Service” (PaaS), proporcionan una plataforma de procesamiento y una pila de soluciones como un servicio, constituyen la base e infraestructura de las aplicaciones de la nube. Facilita el desarrollo de aplicaciones evitando el coste y la complejidad de comprar y mantener el hardware y las capas de software de base.
- Infraestructura. Servicios de infraestructura, también conocidos como “Infrastructure as a Service” (IaaS), proporciona la infraestructura

como un servicio, suele ser una plataforma virtualizada. En lugar de comprar servidores, software, centro de datos especiales o equipos de red, los clientes adquieren dichos recursos de servicios externos. La IaaS ha evolucionado a partir de las ofertas de servidores virtuales privados.

57.6.2 Modelos de implementación

- Nube pública o external cloud: Es el concepto tradicional donde los recursos se presentan a través de internet en función de la demanda, a través de aplicaciones o servicios web.
- Nube de la comunidad: Se da cuando varias organizaciones con las mismas necesidades comparten recursos. En este caso existen menos usuarios que en la nube pública y se ofrece mayor privacidad y seguridad. Un ejemplo puede ser el Google's "Gov Cloud".
- Nube híbrida. Es común que una empresa use tanto la nube pública como desarrollos privados para satisfacer sus necesidades con respecto a las TI. Existen varias empresas como HP, IBM, Oracle and VMware que ofrecen tecnologías para manejar la complejidad de mantenimiento, seguridad y privacidad consecuencia del uso del conjunto de estos servicios.
- Nube combinada. Se denomina al conjunto formado varios servicios cloud de distintos proveedores.
- Nube privada. Es trasladar el concepto de nube pública a una red de uso privado. Es decir, el uso de la nube única y exclusivamente dentro de la red de una empresa.

57.7 GREEN IT E EFICIENCIA ENERGÉTICA

El término Green Computing se acuñó posiblemente por primera vez tras el inicio del programa Energy Star en 1992, promocionado por el gobierno estadounidense.

Tenía por objetivo etiquetar monitores y equipamiento electrónico caracterizados por su eficiencia energética. El término quedó registrado ya en 1992 en un grupo de noticias. Hoy en día el programa Energy Star es el motor de la eficiencia energética en los sistemas electrónicos (no sólo de procesamiento de la información, sino también del equipamiento electrónico doméstico).

La adopción de productos y aproximaciones más eficientes pueden permitir más equipamiento dentro del mismo gasto energético, lo que se denomina huella energética, o energy footprint. Las regulaciones se están multiplicando y podrían limitar seriamente a las empresas a la hora de construir centros de procesamiento de datos, ya que el efecto de las redes de suministro eléctrico, las emisiones de carbono por el incremento de uso y otros impactos medioambientales están siendo investigadas. Por tanto, las organizaciones deben considerar las regulaciones y tener planes alternativos para el crecimiento de sus centros de procesamiento de datos y de su capacidad.

Con el paso de los años, el número de servidores existentes en todo el mundo crece de forma casi exponencial. Consecuencia de esto es el creciente gasto energético para la refrigeración y gestión de los equipos. Hoy en día ya se están empezando a plantear soluciones que optimicen este gasto energético.

Este consumo energético no es el único problema ambiental relacionado con las TI. La etapa de fabricación de equipos presenta serios problemas relacionados con el medio ambiente: materiales de desecho tóxicos, producción de gases contaminantes, etc. La tendencia actual es la de minimizar el impacto contaminante (carbon footprint) presente en las tecnologías de fabricación de los sistemas electrónicos.

Finalmente, también tiene un impacto inmediato la eliminación de equipos para las TI, caracterizados por un tiempo de vida increíblemente breve de unos dos o tres años. Si no se reciclan de forma eficiente, terminan tirados

en vertederos, y debido a la presencia de componentes tóxicos, son una fuente de contaminación terrestre y de las aguas. Todos estos aspectos deben ser considerados de manera global por los fabricantes y usuarios de equipos TI. La concienciación de la existencia de este problema ha llevado a la elaboración de numerosas y rígidas normativas a todos los niveles, lo que empieza a obtener algunos resultados.

GreenPeace Internacional realiza un ranking con los 18 principales fabricantes del sector electrónico (ordenadores personales, teléfonos móviles etc.) de acuerdo con sus políticas de reducción de emisiones tóxicas, reciclado o minimización de impacto en el cambio climático, y lo publica en su Guía para la Electrónica Verde (Guide to Greener Electronics), de publicación trimestral. Como se puede ver en los resultados de Diciembre de 2010, las empresas del sector obtienen unas calificaciones realmente bajas, siendo la mejor Nokia con un 7,5 sobre 10.

La mitad de estas 18 empresas suspenden un estudio que busca que las empresas analizadas:

- Limpian sus productos al eliminar sustancias peligrosas. Los productos químicos peligrosos con riesgo impiden el posterior reciclado de los equipos.
- Reciclen de equipos/productos bajo su responsabilidad una vez quedan obsoletos.
- Reduzcan el impacto climático debido a sus operaciones y productos.

Por todo lo expuesto, la resolución efectiva del impacto ambiental de las tecnologías TI requiere un enfoque holístico del problema que englobe las cuatro vías:

- Utilización ecológica: principalmente a través de la reducción del consumo energético. La producción de energía eléctrica es la principal fuente de generación de gases de efecto invernadero.
- Diseño ecológico o eco-diseño: incluye diseño de equipos más eficientes energéticamente y respetuosos con el medio ambiente.
- Fabricación ecológica: eliminando completamente o minimizando el impacto del proceso de fabricación en el medio ambiente (emisiones, materiales de desecho, etc.).
- Eliminación ecológica: una vez finalizado el período de utilización de un equipo se deben poner en marcha las estrategias denominadas tres R: reutilización y renovación de equipos y, si no son aprovechables, reciclado.

La idea principal del enfoque holístico es que se cierre el ciclo de vida de los equipos TI de forma que no se perjudique el medio ambiente, lo que permitiría conseguir una mejora sustancial de cara al desarrollo sostenible.

57.7.1 *Tecnologías verdes*

Hoy en día existen distintos enfoques tecnológicos que se acercan a un desarrollo sostenible de las TI.

- Monitores LCD. Con el paso de los años los monitores pasaron de ser CRT a LCD, este cambio no es sólo estético o de tamaño, sino que los niveles de consumo han disminuido notablemente. Un monitor CRT medio requiere 85W si está activo, frente a los 15W de uno LCD, 5W en modo bajo consumo para un CRT mientras que un LCD consumiría 1,5W. Apagados ambos consumirían 0,5W. En los últimos años se ha revolucionado el mercado de las pantallas de ordenador con la aparición de la tecnología OLED (Organic Light Emitting Diode), basadas en la utilización de diodos LED cuya capa electro-luminiscente se hace con un compuesto orgánico (un polímero que se

ilumina al aplicarle un voltaje). La ventaja principal de este tipo de pantallas frente a las tradicionales de cristal líquido (LCD) es que los diodos OLED no necesitan retro-iluminación, por lo que el consumo de energía que requieren es muy inferior.

- **Discos duros.** El consumo de los discos duros no es para nada despreciable, sobre todo en el arranque del sistema. Por ejemplo, el disco Seagate Barracuda 7200.8 requiere hasta 2,5 A de la línea de alimentación de 12 V. Si a esto le sumamos 3W que extrae desde la línea de +5 V se puede llegar a un consumo de pico en el arranque de 33 W. Si en lugar de sólo un disco duro hablamos de un equipo con dos o más empezamos a hablar de cifras muy comprometidas. Esto ha hecho que los fabricantes de discos duros comiencen a tener en cuenta el consumo en sus productos, creando casi todos una nueva gama denominada “verde” o “ecológica”. Por ejemplo Así, Western Digital con “Caviar Green”, Samsung con Eco Green, o Hitachi con eco-friendly Deskstar y Travelstar. Como alternativa a los discos tradicionales aparecen los discos en estado sólido (SSD), que presentan menores consumos de energía y es la tecnología a la que se espera evolucionen los sistemas de almacenamiento.
- **CPDs.** Aquí es donde se aloja toda la infraestructura de soporte a los diversos servicios computacionales, y una estructura adecuada permitirá buenos ahorros de energía, de espacio y de costos a mediano y/o largo plazo. Buscando la reducción de energía se puede empezar por la acción más simple que es apagar el equipo que no se esté utilizando, la reducción del hardware estudiando necesidades reales, o actuaciones específicas en función de la actividad de la empresa.
- **Virtualización.** La virtualización de servidores permite el funcionamiento de múltiples servidores en un único servidor físico. Esto ayuda a reducir la huella de carbono del centro de datos al

disminuir el número de servidores físicos y consolidar múltiples aplicaciones en un único servidor con lo cual se consume menos energía y se requiere menos enfriamiento. Además se logra un mayor índice de utilización de recursos y ahorro de espacio.

- Cliente/Servidor. Estos sistemas mantienen el software, las aplicaciones y los datos en el servidor. Se puede tener acceso a la información desde cualquier ubicación y el cliente no requiere mucha memoria o almacenamiento. Este ambiente consume menos energía y enfriamiento.
- Cloud computing. Esto proporciona a sus usuarios la posibilidad de utilizar una amplia gama de recursos en red para completar su trabajo. Al utilizar computación en nube las empresas se vuelven más ecológicas porque disminuyen su consumo de energía al incrementar su capacidad sin necesidad de invertir en más infraestructura.
- Tele trabajo. Definido por Merrian-Webster como el trabajo en casa con el uso de un enlace electrónico con la oficina central. Al no desplazarse el empleado la contaminación es menor.

57.7.2 *Actividades relacionadas con Green IT*

Existen varias actividades que promocionan e intentan solventar las cuestiones expuestas anteriormente. Estas actividades están patrocinadas bien desde administraciones públicas, bien desde empresas, que están entendiendo que Green IT, además de una necesidad, puede ser un negocio, desde el punto de vista de consultoría y servicios, o bien por consorcios de empresas.

The Green Grid (<http://www.thegreengrid.org>) es un consorcio global dedicado a avanzar en la eficiencia energética de los centros de procesamiento de datos y en ecosistemas de computación de negocio. En cumplimiento de su misión, The Green Grid se centra en:

- Definir métricas y modelos significativos y centrados en el usuario.
- Desarrollar estándares, métodos de medida, procesos y nuevas tecnologías para mejorar el rendimiento de los centros de procesamiento de datos frente a las métricas definidas.
- Promocionar la adopción de estándares, procesos, medidas y tecnologías energéticamente eficientes.

El comité de directores de The Green Grid está compuesto por las siguientes compañías miembros: AMD, APC, Dell, HP, IBM, Intel, Microsoft, Rackable Systems, Sun Microsystems y VMware.

Climate Savers. Iniciada por Google e Intel en 2007, Climate Savers Computing Initiative (www.climatesaverscomputing.org) es un grupo sin ánimo de lucro de consumidores y negocios con conciencia ecológica y organizaciones conservacionistas. La iniciativa se inició bajo el espíritu del programa Climate Savers de WWF (<http://www.worldwildlife.org/climate/projects/climateSavers.cfm>), que ha movilizado a una docena de compañías desde 1999 a recortar las emisiones de dióxido de carbono, demostrando que reducir las emisiones es bueno para el negocio. Su objetivo es promover el desarrollo, despliegue y adopción de tecnologías inteligentes que puedan mejorar la eficiencia de uso de la energía del computador y reducir su consumo cuando el computador se encuentra inactivo.

SNIA (Storage Networking Industry Association, <http://www.snia.org>) es una organización global sin ánimo de lucro compuesta por unas compañías de la industria del almacenamiento. SNIA Green Storage Initiative (<http://www.snia.org/green>) está llevando a cabo una iniciativa para avanzar en el desarrollo de soluciones energéticamente eficientes para el almacenamiento en red, incluyendo la promoción de métricas estándares, la formación y el desarrollo de buenas prácticas energéticas o el establecimiento de alianzas con organizaciones como The Green Grid.

Energy Star. En 1992 la Agencia de Protección Medioambiental de EEUU (U.S. Environmental Protection Agency) lanzó el programa Energy Star, que se planificó para promocionar y reconocer eficiencia energética en monitores, equipos de climatización y otras tecnologías. Aunque de carácter voluntario inicialmente, resultó pronto de amplia aceptación, pasando a ser un hecho la presencia de un modo de descanso (sleep mode) en la electrónica de consumo.

Directiva Europea de Eco-Diseño. Siguiendo la misma línea que la iniciativa Energy Star de EEUU, la Unión Europea aprobó la directiva 2005/32/EC para el eco-diseño, nuevo concepto creado para reducir el consumo de energía de productos que la requieren, tales como los dispositivos eléctricos y electrónicos o electrodomésticos. La información relacionada con las prestaciones medioambientales de un producto debe ser visible de forma que el consumidor pueda comparar antes de comprar, lo cual está regulado por la Directiva de Etiquetado de la Energía (Energy Labelling Directive). Los productos a los que se conceda la Eco-etiqueta serán considerados como cumplidores con la implementación de las medidas, de forma muy similar a la etiqueta de Energy Star.

El Código de Conducta de la Unión Europea para Centros de Datos está siendo creado como respuesta al creciente consumo de energía en centros de datos y a la necesidad de reducir el impacto ambiental, económico y de seguridad de abastecimiento energético relacionado. El objetivo es informar y estimular a los operadores o propietarios de los centros de datos a que reduzcan el consumo de energía de una forma rentable sin dificultar su funcionamiento. Este código de conducta quiere conseguir esto mediante la mejora de la comprensión de la demanda de energía dentro del centro de datos, aumentando la concienciación, y mediante la recomendación de prácticas y objetivos energéticamente eficientes.

Grupo de trabajo sobre Green IT de la plataforma INES (Iniciativa Española de Software y Servicios, <http://www.ines.org.es>) es la Plataforma

Tecnológica Española en el área de los Sistemas y Servicios Software y constituye una red de cooperación científico-tecnológica integrada por los agentes tecnológicos relevantes de este ámbito (empresas, universidades, centros tecnológicos, etc.).

Según la Agenda Estratégica de Investigación de INES, el plan de dinamización para el Grupo de Trabajo de Green IT consiste en las siguientes acciones:

- Análisis de la influencia e importancia de las soluciones de Green IT.
- Difusión de las informaciones, noticias y existencia de este grupo de trabajo por Internet.
- Fomentar el interés y apoyar el desarrollo bajo Green IT.

Big Green Innovations (<http://www.ibm.com/technology/greeninnovations/>), programa de IBM. Dentro de este programa, y con fines educativos, IBM ha presentado un centro de datos virtual ecológico denominado Virtual Green Data Center.

La lista Green500 (<http://www.green500.org>) proporciona una clasificación de los supercomputadores más eficientes energéticamente del mundo, sirviendo como una visión complementaria a la lista Top500 (<http://www.top500.org>).

Otras empresas, como Google, Dell o Symantec, están desarrollando programas de eficiencia energética, tanto para sus propios procesos de TI como para los de sus clientes.

57.8 BIBLIOGRAFÍA

- Windows Server 2008 Hyper-V : kit de recursos. Larson, Robert. Anaya, D.L. 2009

- Grid computing : experiment management, tool integration, and scientific workflows. Prodan, Radu Berlin: Springer, cop. 2007
- Virtualización na Wikipedia: <http://es.wikipedia.org/wiki/Virtualizaci%C3%B3n>
- Green IT: Tecnologías para la Eficiencia Energética en Sistemas TI. Marisa López-Vallejo, Eduardo Huedo Cuesta y Juan Garbajosa Sopeña.
- Dot-cloud : the 21st century business platform built on cloud computing. Fingar, Peter Tampa (FL) : Meghan-Kiffer Press, cop. 2009

Autor: Francisco Javier Rodriguez Martínez

Subdirector de Sistemas Escola Superior Enxeñaría Informática Ourense

Colegiado del CPEIG

**58. REDES SAN Y ELEMENTOS
DE UN SAN. REDES DE
ALMACENAMIENTO:
TOPOLOGÍAS, PROTOCOLOS,
ELEMENTOS DE CONEXIÓN.
SISTEMAS DE
ALMACENAMIENTO:
ARQUITECTURAS Y
COMPONENTES. SERVIDORES:
HBA Y SOFTWARE
MULTI-PATH.**

Tema 58: Redes SAN y elementos de un SAN. Redes de almacenamiento: topologías, protocolos, elementos de conexión. Sistemas de almacenamiento: arquitecturas y componentes. Servidores: HBA y Software MultiPath.

ÍNDICE

58.1. Redes de almacenamiento: topologías, protocolos, elementos de conexión.	2
58.1.1 Estructura de las SAN.....	5
58.1.2 Protocolos.....	5
58.1.3 Topologías.....	8
58.1.3.1 Topologías en AoE.....	8
58.1.3.2 Topologías en Fibre Channel.....	9
58.1.3.3 Topologías en iSCSI.....	12
58.2. Sistemas de Almacenamiento: Arquitecturas y componentes	13
58.2.1 Arrays de discos.....	13
58.2.2.1 Estrategias (Niveles) de RAID.....	14
2.2 Copias de seguridad.....	23
58.3. Servidores: HBA y Software Multipath.....	25
58.3.1 Protocolos de SAN y HBAs.....	26
58.3.2 Software multipath.....	27
58.4 Bibliografía.....	28

58.1. REDES DE ALMACENAMIENTO: TOPOLOGÍAS, PROTOCOLOS, ELEMENTOS DE CONEXIÓN.

Como resumen una SAN es una red donde se realiza el almacenamiento y se gestiona la seguridad de los datos. Las SAN (*Storage Area Network*, Redes de Almacenamiento) son redes en las que se conectan servidores de almacenamiento (especialmente arrays de discos). También hay que considerar como parte de las SAN las librerías necesarias para el uso de los arrays y los accesos a las redes. De forma contraria a las redes tradicionales, en las SAN se emplean protocolos orientados a la recuperación de la información de los arrays de disco e inspirados en los propios estándares de comunicación con discos tradicionales (SCSI y SATA).

Normalmente, el equipamiento diseñado para participar en estas redes suele ser especialmente caro aunque su precio depende, en una gran medida, de las tecnologías y protocolos empleados para la transmisión de los datos. Entre las tecnologías disponibles en la actualidad se encuentran: iSCSI (Internet Small Computer Storage Interconnect), Fibre Channel y AOE (ATA Over Ethernet, Advanced Technology Attachment Over Ethernet).

Entre las ventajas de la interconexión de redes de almacenamiento se resaltan las siguientes:

- ✓ Elimina los límites de distancia de discos introducidos por SCSI o ATA
- ✓ Consigue mayor caudal de datos ya que los protocolos están específicamente diseñados para la transferencia de datos de dispositivos de almacenamiento.
- ✓ Permite un aprovechamiento mayor de los discos permitiendo que más de un servidor acceda al mismo disco.
- ✓ Capacidad para el uso de múltiples discos de forma transparente desde uno o varios servidores.

- ✓ Adquisición de discos diferida debido al mayor aprovechamiento
- ✓ Capacidades de recuperación ante desastres. Los arrays de discos empleados en las SAN suelen disponer de discos de reserva (para fallos de otros discos) y permitir distintos esquemas de RAID.
- ✓ Recuperación en caliente ante desastres
- ✓ Mejor capacidad de administrador. La administración es más sencilla y está más centralizada.
- ✓ Reducción de los costes de administración y de almacenamiento de datos
- ✓ Avance de disponibilidad global ya que las SAN tienen menos fallos que los discos internos de los equipos.
- ✓ Reducción de servidores eliminando servidores de archivos antiguos (NFS, SMB, etc.).
- ✓ Reducción del caudal de las redes convencionales pues las copias de seguridad se pueden hacer desde las SAN
- ✓ Incremento de la rapidez de las operaciones de Entrada/Salida
- ✓ Reducción de los costes de administración de backups
- ✓ Protección de datos críticos
- ✓ Incremento de la capacidad de forma transparente
- ✓ Desarrollo y prueba de aplicaciones de forma más eficiente mediante el uso de copias de los datos de producción realizadas en la SAN.
- ✓ Facilita el empleo de clusters de servidores que tienen que disponer de un almacenamiento común.
- ✓ Permiten el almacenamiento bajo demanda de forma que cualquier servidor puede solicitar espacio de almacenamiento según sus necesidades.

Dentro de una organización, se debería incluir en una SAN la siguiente información:

- ✓ La información almacenada por SGBDs (Sistemas Gestores de Bases de Datos). De hecho, algunos sistemas gestores como Oracle, Sybase, SQLServer, DB2, Informix o Adabase recomiendan esta alternativa
- ✓ La información almacenada por servidores de archivos. Los servidores de archivos funcionarán mejor y con menos recursos si los archivos están almacenados en una SAN.
- ✓ Servidores de backup. Si los servidores de backup están conectados a una SAN se conseguirá reducir los tiempos de copia de seguridad con respecto a hacerlos en una LAN (Local Area Network, Red de Área Local) y reducir el tráfico de la LAN.
- ✓ Archivos de servidores de voz y video para streaming. Debido a que este tipo de servicios requiere grandes cantidades de disco, una SAN puede reducir los costes asociados al almacenamiento, desplazando el máximo posible el coste (incluir nuevos discos en los arrays cuando sean necesarios).
- ✓ Buzones de usuario (mailboxes) de servidores de correo permitiendo que los servidores de correo funcionen más rápido y que se pueda realizar una restauración rápida en caso de que algún archivo se corrompa.
- ✓ Servidores de aplicaciones de alto rendimiento. Las SAN pueden mejorar el rendimiento de cualquier aplicación incluyendo gestores documentales, aplicaciones científicas, aplicaciones de datawarehouse y cuadros de mando integrales, aplicaciones para gestionar las relaciones con los clientes (CRM), etc.
- ✓ Soluciones de Virtualización.

Asimismo no es conveniente usar una SAN para:

- ✓ Servidores web que no requieran grandes necesidades de almacenamiento (la mayoría)
- ✓ Servidores con servicios de red básicos como DNS, DHCP, WINS (Windows Internet Name Servers) y controladores de dominio de

Windows (DC). Este tipo de servidores no requieren de las capacidades de almacenamiento permitidas por las SAN.

- ✓ PCs de escritorio
- ✓ Servidores que necesitan menos de 10Gb de almacenamiento
- ✓ Servidores que no necesitan un acceso rápido a la información
- ✓ Servidores que no comparten archivos

58.1.1 Estructura de las SAN

Habitualmente las SAN se conciben y estructuran en tres capas:

1. La capa de hosts: Constituida en su mayoría por los servidores, los drivers y software necesarios para la conexión a la red y los HBAs (Host Bus Adapters) que son dispositivos (tarjetas) que se conectan a cada servidor para acceder al almacenamiento (en algunas soluciones concretas son adaptadores Ethernet simples y en el caso Fibre Channel llevan un conector GBIC-Gigabit Interface Connector).
2. La capa de estructura (fabric layer): Constituida por HUBs, Switches, Gateways y Routers si fuera necesario. Si se utiliza la tecnología Fibre Channel, todos estos dispositivos emplean GBICs (Gigabit Interface Connectors) para la interconexión de los dispositivos de las capas superiores e inferiores.
3. La capa de almacenamiento (storage layer): Constituida por todo tipo de dispositivos de almacenamiento.

Un conjunto de discos situados en el mismo sitio y sin funcionalidades adicionales se conoce como JBOD (Just a Bunch Of Disks). Dentro de la capa de almacenamiento, los arrays no son simplemente JBODs, sino que incluyen ciertas funcionalidades interesantes implementadas en el firmware de la controladora como el RAID.

58.1.2 Protocolos

En la actualidad existen distintos protocolos que permiten las comunicaciones en la capa de infraestructura entre los distintos equipos

que participan en una SAN: (i) AoE (ATA over Ethernet) (ii) FCP (Fibre Channel Protocol) (iii) FCoE (Fibre Channel over Ethernet) (iv) FICON (Fibre Connection), (v) HyperSCSI, (vi) iFCP (Internet Fibre Channel Protocol), (vii) iSCSI (Internet Small Computer Interface) y (viii) iSER (iSCSI Extensions for RDMA).

AoE permite hacer disponible discos SATA a través de una red Ethernet interconectada con hilos de par trenzado (Gigabit Ethernet) o fibra óptica (10 Gigabit Ethernet). Este tipo de soluciones es muy popular por su bajo coste y alto rendimiento. Coraid Inc. fabrica este tipo de soluciones.

FCP es la solución más destacada y permite mapear el protocolo SCSI sobre Fibre Channel. Fibre Channel es una tecnología Gigabit y diseñado específicamente para redes SAN. Fibre Channel es un protocolo inspirado en el modelo OSI y diseñado en 5 capas (FC0, FC1, FC2, FC3 y FC4) y, a pesar de su nombre, puede ser empleado sobre cables de fibra o pares trenzados.

FcoE es una encapsulación del protocolo Fibre Channel sobre redes Ethernet. De este modo las capas FC0 y FC1 son reemplazadas por las capas físicas y de Enlace utilizadas en el protocolo Ethernet. Empleando esta tecnología se pueden combinar en la SAN tecnologías basadas en el uso del protocolo IP con Fibre Channel o emplear el mismo hardware para la red LAN y la SAN reduciendo el coste del hardware.

ESCON (Enterprise System Connnection) sobre Fibre Channel (FICON) es un protocolo empleado para interconectar mainframes de IBM con dispositivos de almacenamiento ESCON (también diseñados por IBM).

HyperSCSI permite el mapeo de SCSI sobre redes Ethernet. No llegó a ser comercializado porque ya FCP estaba totalmente establecido. Es una solución de bajo coste semejante a AoE que usa directamente el protocolo

Ethernet para transmitir comandos SCSI (CDBs, Command Descriptor Blocks).

iFCP o SANoIP: Son soluciones para mapear FCP sobre el protocolo IP.

iSCSI (Internet Small Computer Interface) es un protocolo de la capa de aplicación de TCP/IP para el almacenamiento de datos que se usa para transmitir comandos SCSI (CDBs). Funciona habitualmente en los puertos 860 y 3260 TCP. Este tipo de soluciones pueden ser empleadas para almacenamiento utilizando redes de área extensa (incluso Internet). Los clientes de almacenamiento se llaman iniciadores (initiators) y pueden realizar operaciones de almacenamiento sin necesidad de emplear cables de propósito específico como en el caso de FCP.

iSCSI Extensions for RDMA (Remote Direct Memory Access) (iSER). Es una tecnología que permite extender el protocolo iSCSI implementando el Acceso Directo a Memoria. Este acceso directo a memoria es normalmente implementado sobre TCP mediante el protocolo iWARP (Internet Wide Area RDMA Protocol) o sobre la tecnología InfiniBand que es un estándar que proporciona conectividad de alta velocidad y baja latencia para el almacenamiento de datos.

Debido a que los protocolos más empleados para desarrollo de SAN son FCP, iSCSI y AoE, el documento se centrará en mayor medida en ellos. La figura 1 muestra una comparativa entre las capas que componen los protocolos más empleados para el desarrollo de SAN.

	SCSI	SCSI	
	iSCSI	FC4 - Capa de mapeo	
ATA	Capa de transporte - TCP	FC3 - Capa de servicios comunes	
AoE	Capa de red - IP	FC2 - Capa de Red	FC-PH
Capa de Enlace - Ethernet	Capa de enlace - Ethernet	FC1 - Capa de Enlace	
Capa física	Capa física	FC0 - Capa física	
<i>AOE</i>	<i>iSCSI</i>	<i>Fibre Channel</i>	

Figura 1: Estructura de los protocolos de SAN más extendidos

Como se puede ver en la Figura 1, la Tecnología AOE es mucho más sencilla que las tecnologías iSCSI o Fibre Channel. De ahí deriva su bajo coste y su rapidez.

58.1.3 Topologías

Las topologías disponibles para el desarrollo de SAN dependen de forma importante de las tecnologías empleadas. Por lo tanto, este subapartado se dividirá en distintas secciones para estudiar las topologías posibles según cada uno de los protocolos estudiados.

58.1.3.1 Topologías en AoE

AoE depende exclusivamente del protocolo Ethernet (capa física y de enlace del modelo TCP-IP) obviando la estructura y funcionamiento de las capas superiores (IP, TCP, UDP). AoE no permite el routing (por funcionar sobre la capa de enlace) y representa una alternativa de bajo coste para iSCSI y Fibre Channel. Además de existir hardware específico (Coraid Inc.), existen distribuciones de Linux que implementan el protocolo del lado del servidor permitiendo compartir discos según este paradigma (Lanart Bussiness Server).

Dado su particular concepción, las topologías típicas de AoE son equivalentes a las distintas posibilidades de interconexión que ofrece Ethernet a nivel de capa 2. Por lo tanto, AOE permite dos topologías básicas:

- ✓ Punto a punto en la que el equipo host se interconecta directamente con el dispositivo de almacenamiento mediante un cable par trenzado.
- ✓ Infraestructura conmutada. Todos los dispositivos se interconectan con un switch Ethernet. Según las interfaces de red de los arrays (Gigabit / 10 Gigabit) habrá que emplear un switch adecuado y un dispositivo adecuado para el computador (con hilos de par trenzado o fibra).

58.1.3.2 Topologías en Fibre Channel

Un enlace Fibre Channel está constituido por dos fibras ópticas empleadas para transmitir TX y recibir RX. Para la comunicación, empleando las fibras ópticas se utiliza un protocolo específico diseñado especialmente para la comunicación con dispositivos de almacenamiento.

Con esta tecnología se pueden desplegar tres tipos de topologías:

1. Punto a punto (FC-P2P, Point to Point): implica que sólo existen dos dispositivos participando en la SAN que son el servidor y el array de disco. Estos dispositivos se interconectan directamente.
2. Anillo arbitrado (FC-AL, Arbitrated loop): implica que los dispositivos están en una disposición en forma de anillo (Token Ring). En el anillo participan tanto servidores como arrays de disco. El principal problema de esta topología consiste en que cuando falla una conexión se interrumpe el funcionamiento del anillo entero. Este es el método más barato para crear una SAN.
3. Infraestructura conmutada (FC-SF, Switched Fabric). Todos los dispositivos se conectan a conmutadores (switches) de FC. La forma de funcionar es muy similar al funcionamiento de Ethernet en el

sentido en que cuando un servidor quiere realizar una operación de almacenamiento en un array, se realiza una interconexión de las bocas del switch donde están el servidor y el array.

En el caso de contar con anillos arbitrados, se suelen usar hubs (concentradores) que realizan internamente las conexiones que implementan el anillo. En la Figura 2 se muestra esquemáticamente el funcionamiento de un hub.

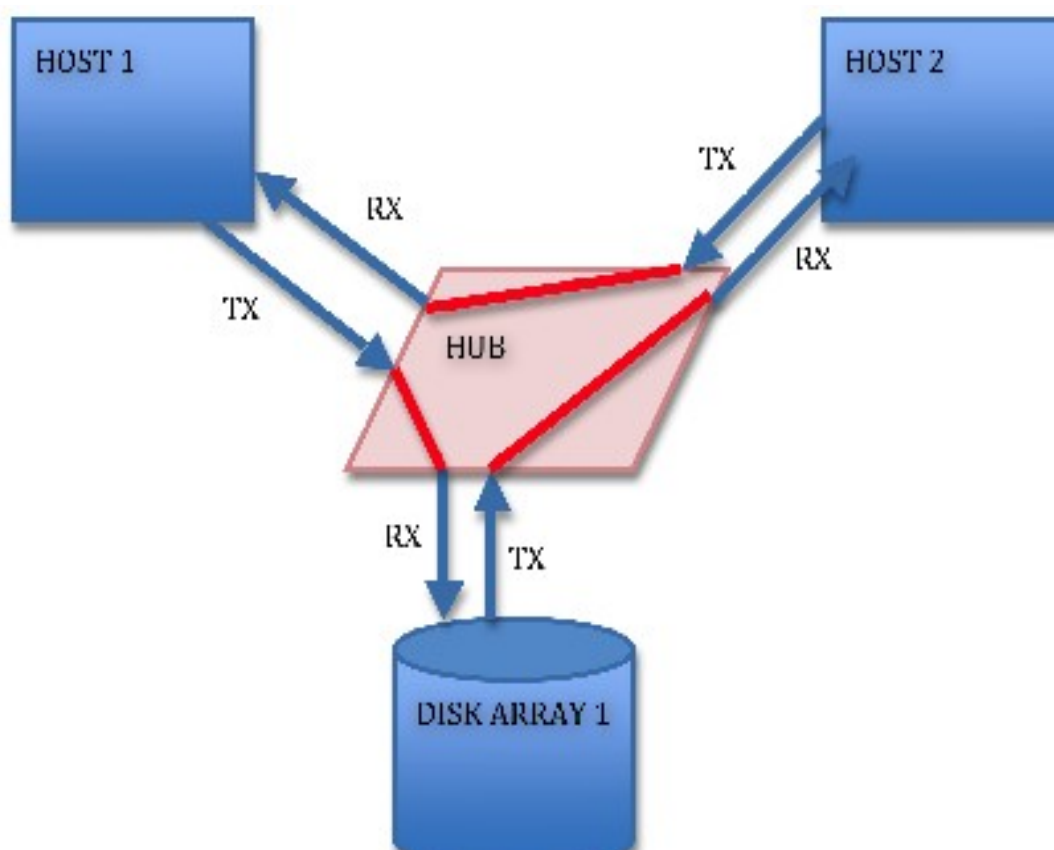


Figura 2: Esquema de funcionamiento de un hub

Dado el funcionamiento interno de un hub, el despliegue de topologías en anillo resulta muy sencillo. Además, este tipo de topologías admite infinidad de arquitecturas de red entre las que se incluyen la colocación de hubs en cascada (Figura 3) o en bucle.

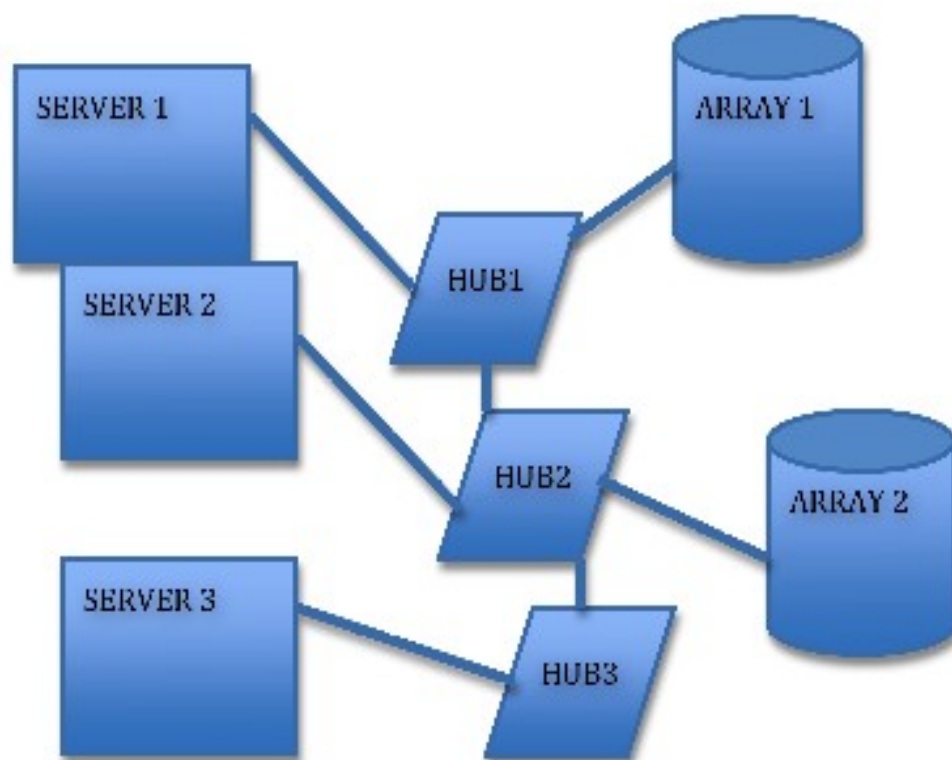
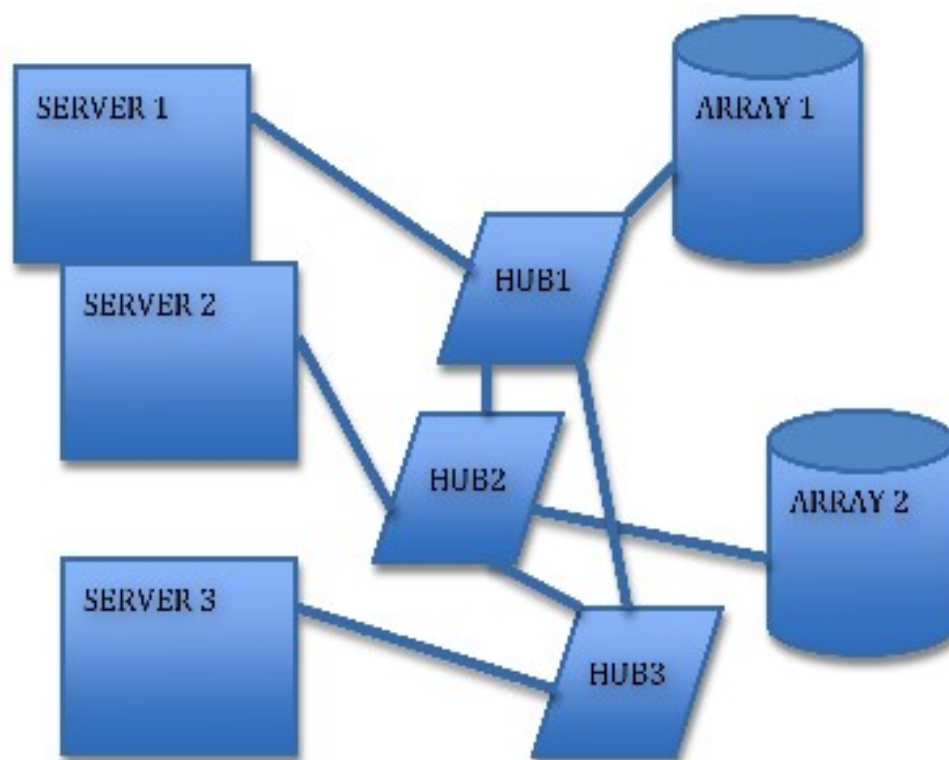


Figura 3: Topología en anillo usando hubs en cascada

En el caso de las topologías de anillo uniando los hubs en forma de bucle se obtiene una mejor redundancia para las conexiones. Aunque parezca extraño, este tipo de configuraciones puede tolerar fallos en un determinado hub así como la posibilidad de usar distintas rutas para las conexiones que pueden ser empleadas para mejorar la velocidad de transferencia de datos como se verá en el apartado 3.



Figura

4: Topología en anillo usando hubs en forma de bucle

De forma semejante a como se puede refinar la topología en anillo, la topología de infraestructura conmutada puede implementar bucles de switches u otras combinaciones que permiten eliminar la posibilidad de fallos y multiplicar las rutas disponibles para el acceso a los equipos participantes en la SAN para aumentar la velocidad de acceso e implementar la tolerancia a fallos.

58.1.3.3 Topologías en iSCSI

iSCSI es una arquitectura de SAN considerablemente distinta a la ofrecida por Fiber Channel. En vez de diseñar por completo un protocolo, iSCSI es un protocolo que en la capa de aplicación de TCP/IP aprovechando por completo toda la arquitectura de capas de TCP/IP y permitiendo el salto entre distintas redes (routing). En la práctica, no tener una conectividad con una velocidad superior a 1 Gbps no permite alcanzar velocidades adecuadas en el almacenamiento.

Dado que iSCSI y FCP son protocolos muy extendidos, es posible comprar arrays que soportan conexiones iSCSI de forma nativa e implementan al mismo tiempo un gateway para FCP. De hecho, una de las mayores ventajas introducidas por iSCSI es la posibilidad de administrar este tipo de equipos sin un conocimiento profundo de FCP aunque con conocimientos avanzados de TCP/IP.

Debida a toda esta casuística, la topología en iSCSI puede ser cualquiera empleada en una red TCP/IP convencional desplegada sobre una capa de enlace cualquiera (Ethernet, 802.11x, Token Ring, etc.).

58.2. SISTEMAS DE ALMACENAMIENTO: ARQUITECTURAS Y COMPONENTES

Los sistemas de almacenamiento que se pueden conectar a una SAN son arrays de discos y sistemas de backup. En los siguientes subapartados se hará una descripción detallada de estas tecnologías.

58.2.1 Arrays de discos

Un array de discos es un sistema de almacenamiento que contiene múltiples discos. La principal diferencia con un JBOD es que disponen de memoria caché y funcionalidades avanzadas como el RAID y la virtualización. Un array de discos se compone de:

- ✓ Una controladora de disco
- ✓ Memoria caché
- ✓ Carcasa de los discos
- ✓ Fuente de alimentación

Normalmente los arrays de discos suelen contar con mayor disponibilidad, resistencia y facilidad de mantenimiento. Para implementar estas características emplean redundancia de hardware. Además, normalmente los discos pueden ser intercambiados sin realizar un apagado del equipo.

Dentro de los arrays de discos es común emplear distintos esquemas de RAID (Redundant Array of Independent Disks) para gestionar el espacio en los discos. A nivel lógico, la tecnología RAID permite combinar varios discos físicos en una sola unidad de disco lógica a la que se le asigna un identificador único llamado LUN (Logical Unit Number).

Otra característica habitual de los arrays de disco es la existencia de discos de reserva (spare disks) que sirven para el reemplazo automático de discos que fallan en un volumen RAID (sólo tiene sentido en algunos tipos de RAID). El siguiente apartado presenta las estrategias de RAID y sus características. Los discos de reserva pueden ser hot spare (en caliente) o (standby spare) en frío. A diferencia de los standby, los hot están físicamente conectados a la SAN e inicializados de forma que el proceso de uso es más eficiente.

58.2.2.1 Estrategias (Niveles) de RAID

Existen distintos niveles de RAID que tienen que ver con los esquemas de seguridad y redundancia implementados. Los esquemas de RAID más empleados son el 0, 1 y el 5. No obstante, existen multitud de esquemas algunos de los cuales son propietarios.

Un RAID 0 (o volumen dividido) distribuye los datos equitativamente entre dos o más discos sin información de paridad ni redundancia alguna. RAID 0 permite aumentar el rendimiento y crear grandes volúmenes virtuales mediante la combinación de discos de pequeña capacidad. Un RAID 0 creado a partir de discos de distinto tamaño tendrá una capacidad igual al número de discos multiplicado por el tamaño del disco con menor capacidad. La fiabilidad de una unidad lógica RAID 0 será igual a la fiabilidad media de los discos que lo componen. No es posible la utilización

de discos de reserva cuando se produce un fallo de un disco. La Figura 5 muestra una configuración RAID 0.

B1	B2
B3	B4
B5	B6
B7	B8

disco 1

disco 2

Figura 5: Esquema de uso de los discos en RAID 0

Un RAID L distribuye los datos en dos o más discos de forma no equitativa y sin paridad ni redundancia alguna. Los discos funcionan como extensiones permitiendo aumentar el espacio disponible pero sin sacar beneficio del hecho de existir varios discos. Cuando existen discos de distintos tamaños, una unidad lógica RAID L permite que la capacidad global sea igual a la suma de las capacidades de los discos que lo conforman. La figura 6 muestra un esquema del funcionamiento de RAID L.

B6	
B5	
B4	
B3	
B2	B8
B1	B7

disco 1

disco 2

Figura 6: Esquema de uso de los discos en RAID L

Un RAID 1 (o espejo) crea una copia exacta de los datos almacenados en dos o más discos según se puede apreciar en la figura 7. Un volumen lógico RAID 1 tendrá tanto espacio como el más pequeño de los discos que lo conforman. La fiabilidad de emplear un RAID 1 es igual al producto de las

probabilidades de fallo de los discos que conforman el RAID 1. Además, pese a lo que parece más probable, el tiempo de acceso al disco puede reducirse ya que es posible emplear las distintas copias para leer más rápido. En el caso de escritura, los discos se escriben al mismo tiempo sin empeorar ni mejorar el rendimiento. Cuando un disco falla en este esquema de RAID, es posible su sustitución automática por un disco de reserva (spare disk).

B4	B4
B3	B3
B2	B2
B1	B1

disco 1 *disco 2*

Figura 7: Esquema de uso de los discos en RAID 1

Un RAID 2 divide los datos a nivel de bits (en lugar de a nivel de bloques como se hace en los anteriores esquemas) y usa un código de Hamming para la corrección de errores. Además, los discos se sincronizan con la controladora para funcionar con una alta tasa de transferencia. A pesar de esto, actualmente no se emplea este tipo de RAID ya que teóricamente serían necesarios 39 discos en un sistema informático moderno de los que 32 se emplearían para almacenar los bits individuales y 7 para la corrección de errores. La figura 8 muestra un esquema del almacenamiento de los bits en los distintos discos en RAID 2.

d1	d2	d3	d4	d _{p1}	d _{p2}	d _{p3}
c1	c2	c3	c4	c _{p1}	c _{p2}	c _{p3}
b1	b2	b3	b4	b _{p1}	b _{p2}	b _{p3}
a1	a2	a3	a4	la p1	la p2	la p3
<i>disco 1</i>	<i>disco 2</i>	<i>disco 3</i>	<i>disco 4</i>	<i>disco 5</i>	<i>disco 6</i>	<i>disco 7</i>

Figura 8: Esquema de uso de los discos en RAID 2

Un RAID 3 usa una división a nivel de bytes con un disco de paridad dedicado. No se suele usar en la práctica ya que no es posible atender varias peticiones simultáneas puesto que cada bloque de disco (habitualmente de 512bytes) estará dividido en varios discos en la misma dirección en cada uno de ellos. La figura 9 muestra el funcionamiento de un RAID 3.

b10	b11	b12	b _{p(10-12)}
b7	b8	b9	b _{p(7-9)}
b4	b5	b6	b _{p(4-6)}
b1	b2	b3	b _{p(1-3)}
<i>disco 1</i>	<i>disco 2</i>	<i>disco 3</i>	<i>disco 4</i>

Figura 9: Esquema de uso de los discos en RAID 3

Un RAID 4 (IDA, Independent Data Access) disponen de acceso independiente a los discos y discos de paridad. Usa una división a nivel de bloques con un disco de paridad dedicado. Necesita un mínimo de 3 discos físicos permitiendo que funcionen de forma independiente cuando se pide un único bloque. Además, este esquema permite resolver peticiones de escritura y lectura de forma simultánea siendo el único cuello de botella el disco que almacena las paridades. La figura 10 muestra un esquema del funcionamiento de este nivel de RAID.

B10	B11	B12	$B_{p(10-12)}$
B7	B8	B9	$B_{p(7-9)}$
B4	B5	B6	$B_{p(4-6)}$
B1	B2	B3	$B_{p(1-3)}$
<i>disco 1</i>	<i>disco 2</i>	<i>disco 3</i>	<i>disco 4</i>

Figura 10: Esquema de uso de los discos en RAID 4

Un RAID 5 usa una división de los datos a nivel de bloques distribuyendo la información de paridad entre todos los miembros del conjunto. Este esquema de RAID es muy popular gracias a su bajo coste en la implementación de la redundancia. En la práctica el cálculo de la paridad suele ser implementado por hardware. Funciona de un modo parecido a la RAID 4 pero evitando que el disco de paridad sea un cuello de botella mediante la distribución de toda la información de paridad por todos los discos. Además, permite la lectura y escritura de datos de forma simultánea siempre y cuando los bloques que hay que leer simultáneamente estén en distintos discos. Este esquema permite el uso de discos de reserva de forma automática siempre y cuando el fallo no se produzca en más de un disco aunque, en este caso, a veces se hace uso de la referencia RAID 5E. El número de discos que admite RAID 5 es teóricamente ilimitado permitiendo reducir la probabilidad de fallos y aumentar el rendimiento con cada disco adicional. La figura 11 muestra un esquema del funcionamiento de este tipo de RAID.

B13	B14	B15	B _{p(13-15)}
B _{p(10-12)}	B10	B11	B12
B7	B _{p(7-9)}	B8	B9
B4	B5	B _{p(4-6)}	B6
B1	B2	B3	B _{p(1-3)}
disco 1	disco 2	disco 3	disco 4

Figura 11: Esquema de uso de los discos en RAID 5

Una unidad lógica RAID 6 amplía las funcionalidades de un volumen RAID 5 añadiendo un bloque de paridad adicional calculado a partir de otro polinomio diferente. Al añadir códigos adicionales es posible alcanzar cualquier número de discos y recuperarse ante un fallo que se produzca en 1 bloque por cada uno de los discos. El RAID 6 es ineficiente cuando se emplea un número reducido de discos pero aumenta la eficiencia a medida que se incrementa el número de discos. En este sentido, las operaciones de lectura no se ven castigadas en exceso mientras que las operaciones de escritura requieren de un mayor tiempo para el almacenamiento de los dos códigos de paridad. La capacidad total de almacenamiento de un volumen RAID 6 es igual al producto de la capacidad de los discos multiplicado por el número de discos menos 2 [*capacidad* * (*n*-2)]. De forma paralela a RAID 5, se permite el uso automático de discos de reserva aunque esta variante es conocida a veces como RAID 6E. La figura 12 muestra un esquema del funcionamiento de este nivel de RAID.

B _{q(13-15)}	B13	B14	B15	B _{p(13-15)}
B _{p(10-12)}	B _{q(10-12)}	B10	B11	B12
B7	B _{p(7-9)}	B _{q(7-9)}	B8	B9
B4	B5	B _{p(4-6)}	B _{q(4-6)}	B6
B1	B2	B3	B _{p(1-3)}	B _{q(1-3)}
disco 1	disco 2	disco 3	disco 4	disco 5

Figura 12: Esquema de uso de los discos en RAID 6

RAID 5E y 6E hace referencia, como bien se ha mencionado anteriormente, al uso de discos de reserva con los esquemas de RAID correspondientes. Hay que tener en cuenta, no obstante, que los discos de reserva no pertenecen en las soluciones SAN a una unidad lógica concreta sino que están disponibles para los posibles fallos que puedan producirse en todas las unidades lógicas del array de discos.

Una unidad lógica RAID 0+1 (o RAID 01) es un RAID usado para compartir datos entre varios discos haciendo un espejo de cada copia según muestra la figura 13.

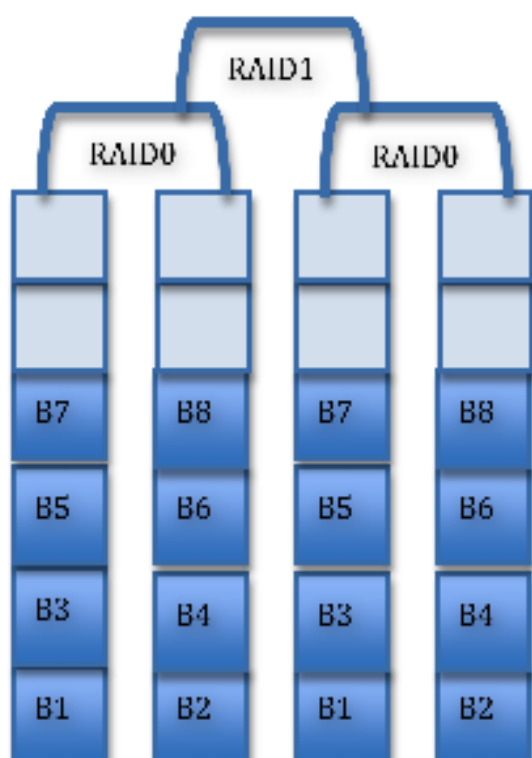


Figura 13: Esquema de uso de los discos en RAID 0+1

El esquema RAID 1+0 (a veces denominado RAID 10) es semejante al RAID 0+1 con la excepción de que invierte los niveles de RAID que lo forman según el esquema que se muestra en la figura 14. Este esquema es mucho

más fuerte que el raid 0+1 y está empezando a ser adoptado en muchos entornos empresariales debido al incremento de la probabilidad de fallos en los nuevos discos.

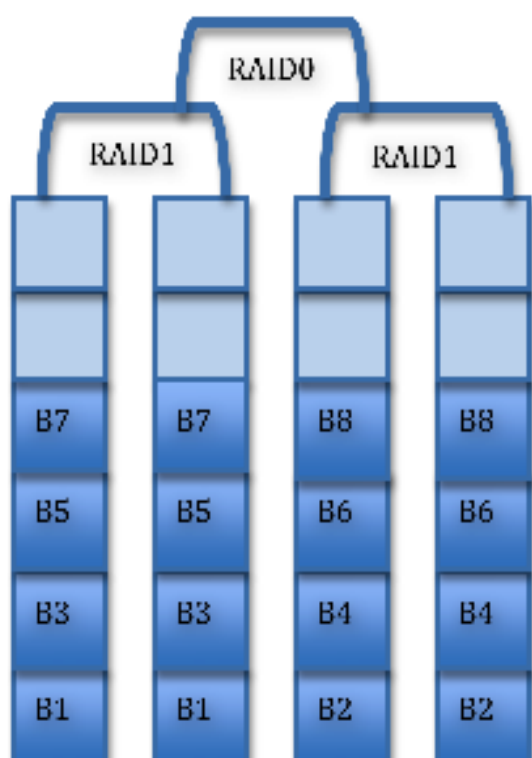


Figura 14: Esquema de uso de los discos en RAID 1+0

De forma paralela a cómo se crearon o RAID 1+0 y 0+1 se crearon respectivamente los raid 3+0 y 0+3. De estos dos es popular el RAID 30 que está diseñado para obtener una tasa de transferencia alta con gran fiabilidad. El principal problema que plantea es su coste de implantación debido a la necesidad de emplear gran cantidad de discos.

Un RAID 100 (o también llamado RAID 10 + 0) es una división de conjuntos RAID 10. La principal ventaja de este esquema es el mayor rendimiento manteniendo un nivel de seguridad muy alto. Esta elección suele ser habitual para el almacenamiento de bases de datos extremadamente grandes. La figura 15 muestra el funcionamiento de este esquema de RAID.

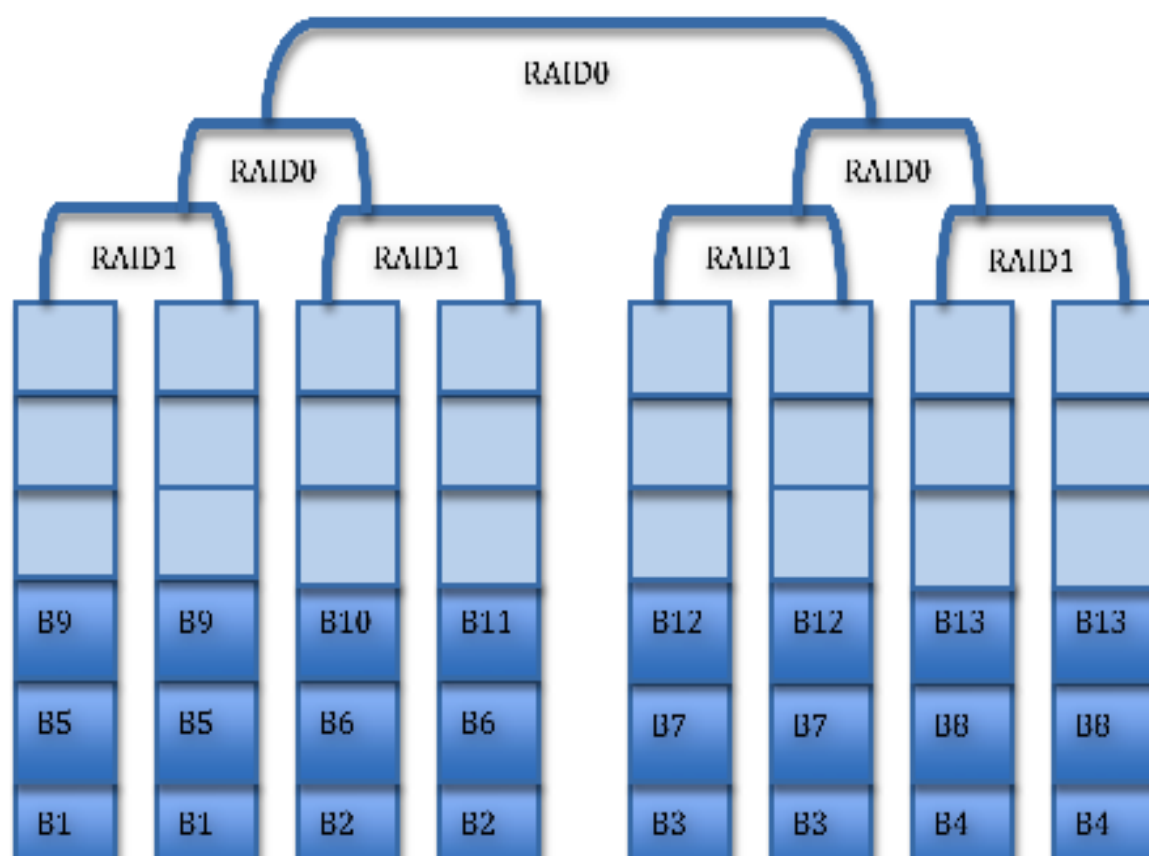


Figura 14: Esquema de uso de los discos en RAID 100

Un RAID 50 (RAID 5+0) combina la división en bloques de un RAID 0 con la paridad distribuida de un RAID 5 tal como se muestra en la figura 15.

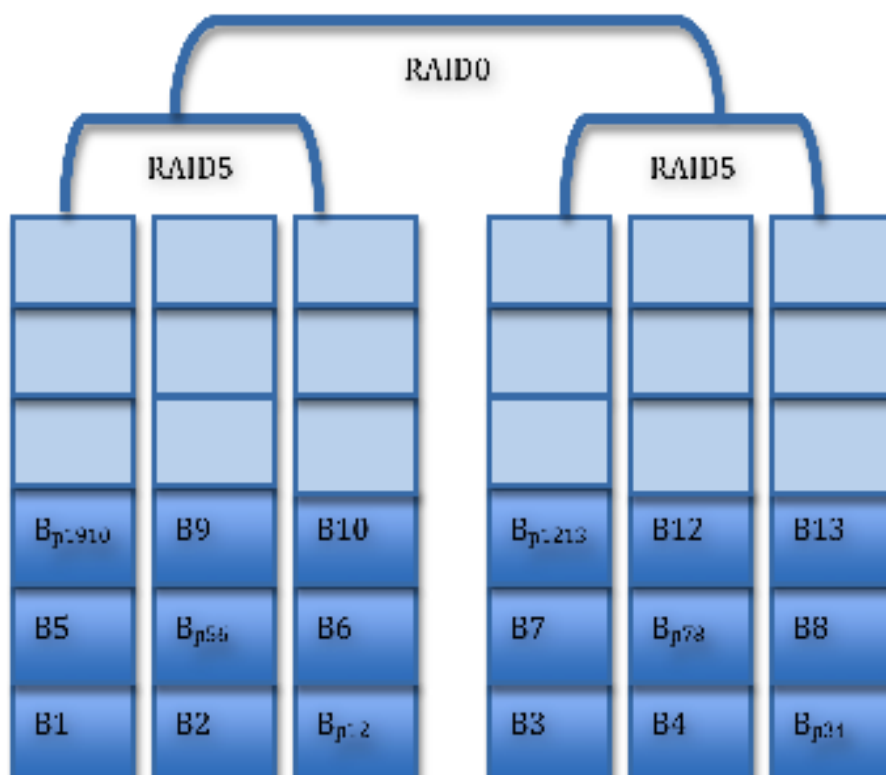


Figura 15: Esquema de uso de los discos en RAID 50

Existen otras combinaciones de RAID como el RAID 5+3, el RAID 0+5, el RAID 5+1 o el RAID 6+0 que son factibles de ser implementados en las SAN. Sin embargo, la combinación de RAIDs no es una estrategia comúnmente empleada.

También se destaca la existencia de distintos esquemas de RAID propietarios como son: RAID de Paridad Doble, RAID 1.5 (RAID 15 es incorrecto), RAID 7, RAID S (o RAID de paridad), MATRIX RAID, IBM SERVER RAID 1E y RAID Z.

2.2 Copias de seguridad

Las copias de seguridad pueden hacerse sobre la red LAN o sobre la SAN. Sin embargo, el principal objetivo de las SAN es eliminar tráfico de almacenamiento de las redes LAN. En este sentido resulta más adecuado hacer el backup dentro de la propia SAN.

Existen dos opciones para hacer copias de seguridad sobre una LAN: (i) Usar una unidad de cinta en cada computador o (ii) usar software de backup en un servidor para volcar la información sobre la LAN y hacer el backup en el servidor. La primera de las opciones es una opción cara porque hay que comprar una unidad de cinta y las cintas correspondientes para cada servidor, mientras que la segunda opción resulta más lenta y ocupa la mayor parte del ancho de banda de la red LAN. La opción de hacer el backup en la SAN resulta más atractiva porque combina la ventaja de realizar el backup en la LAN con la posibilidad de eliminar el tráfico en la red LAN.

Cuando se habla de backup es habitual manejar el término de ventana de backup. La ventana de backup es simplemente un espacio de tiempo en el que se puede realizar la copia de seguridad y en el cual, normalmente, las aplicaciones no se están ejecutando o están en modo de offline. Este último concepto es habitual en los servidores de bases de datos (por ejemplo el quiescent mode de los servidores IDS2K de Informix o el offline mode de las bases de datos de Oracle). La ventana de backup es cada vez más pequeña por necesidades propias de las empresas (como la necesidad de globalizarse e internacionalizarse) y por eso es cada vez más importante reducir el tiempo de backup. Por esa razón es necesario contar con una solución que sea realmente rápida siendo capaz de mover los datos de una manera verdaderamente eficiente. El backup en la SAN resulta mucho más rápido reduciendo así la ventana de backup necesaria.

Para realizar el backup se pueden usar unidades de cinta colocadas en los propios servidores aunque realizando las comunicaciones únicamente sobre la SAN. Existen distintos tipos de unidades de backup con distintos tipos de medios de almacenamiento incluyendo los siguientes: (i) DAT con una capacidad desde 1.3 hasta 80GB y una velocidad entre 0,5 y 6 MBps., (ii) DLT con una capacidad de 40 hasta 80GB y una velocidad de entre 6 y 60 MBps, (iii) SDLT con una capacidad de 100 a 300GB y una velocidad de

entre 11 y 36 MBps, (iv) AIT con una capacidad de 50 a 400GB y una velocidad de entre 6 y 24 MBps, (v) LTO1-5 con una capacidad entre 100GB y 1,6 TB y una velocidad de entre 15 y 180 MBps. Según el dispositivo concreto será posible determinar el tiempo necesario para almacenar los datos así como las unidades de cinta necesarias.

Otra posibilidad para realizar el backup en una SAN consiste en emplear bibliotecas de cintas (a menudo conocidos informalmente cómo robots de backup). Las bibliotecas de cintas son conjuntos de cintas colocados en determinadas disposiciones junto con un brazo robotizado que permite el intercambio de forma automática de la cinta que se está grabando. Existen distintos tamaños de librerías de cintas logrando con algunos esquemas conseguir capacidades de backup importantes.

Además de los backups sobre cintas, resulta interesante mencionar la posibilidad de hacer imágenes e instantáneas (snapshots) de los contenidos de los discos. Mientras que las imágenes son copias bit a bit de los discos, las instantáneas son solamente copias de los metadatos de los discos (punteros que apuntan a donde está almacenada la información en los discos físicos). Este tipo de funcionalidades suele estar directamente implementada en los arrays de disco conectados a las redes SAN.

58.3. SERVIDORES: HBA Y SOFTWARE MULTIPATH

Para que los servidores de la capa Host se puedan conectar a la SAN necesitan emplear un HBA (Host Bus Adapter). Se trata de un dispositivo (tarjeta) que permite el acceso a la SAN. Este mismo término también se usa para dispositivos que permiten la conexión dentro del PC de dispositivos de almacenamiento SCSI, SAS o incluso SATA. Dependiendo de la tecnología, el HBA puede ser diferente. El subapartado 3.1 hace un estudio de los distintos HBA empleados según el protocolo de la red SAN.

Por otro lado, además del hardware es necesario disponer de un software a modo de controlador de dispositivo que implemente el acceso a los arrays que se encuentran en la SAN. Este software puede implementar multitud de características interesantes:

- ✓ Target: Permite que el equipo que ha instalado el software pueda funcionar como dispositivo de almacenamiento en la red SAN
- ✓ Multipath: Permite que el equipo pueda acceder a un dispositivo de la SAN empleando distintas rutas físicas (hilos). Este acceso multiruta puede ser aprovechado para incrementar el ancho de banda, hacer balanceos de carga sobre los paths o bien para implementar redundancia de conexiones ante fallos. Este apartado será específicamente tratado en el apartado 3.2.
- ✓ iSCSI initiator: Combina una red SAN iSCSI con el soporte nativo SCSI de forma que los discos remotos de los arrays actúan como discos locales SCSI.

58.3.1 Protocolos de SAN y HBAs

Debido a la existencia de gran variedad de protocolos para implementar a las SAN, existe una amplia variedad de HBAs. De este modo, según el protocolo y tecnología empleados, será necesario conocer algunas características básicas de los HBA necesarios.

Para conectar los hosts con las SAN que empleen Fibre Channel es necesario contar con una tarjeta adaptadora. En el caso de este protocolo, los HBA disponen de conectores GBICs (GigaBit Interface Connectors) para interconectar todos los elementos que conforman la SAN. Cada HBA dispone de un único WWN (World Wide Name) así como cada dispositivo Ethernet tiene una dirección MAC. Existen distintos modelos de HBA para FC con distintas velocidades: 1 Gbps, 2 Gbps, 4 Gbps, 8 Gbps, 10 Gbps y 20 Gbps. En el caso de Fibre Channel el mismo concepto HBA es abreviatura de High Bandwidth Adapter con el mismo sentido semántico.

Los HBA iSCSI además de incluir una interfaz 10GB Ethernet o GB Ethernet, implementa normalmente un iniciador hardware de iSCSI. Este iniciador es hardware dedicado que permite rebajar la sobrecarga introducida por el procesamiento necesario para los protocolos TCP e iSCSI y las interrupciones Ethernet y mejorar por lo tanto, el rendimiento del servidor.

Con la tecnología de Infiniband (iSER) HBA es abreviatura de Host Channel Adapter con el mismo sentido semántico.

Con la tecnología AoE, el HBA es una tarjeta Ethernet que permita la interconexión con hilos de par trenzado (en Gigabit Ethernet) o fibra óptica (en 10 Gigabit Ethernet). Una de las ventajas de AoE radica en que los HBA son excepcionalmente baratos.

58.3.2 Software multipath

Una característica importante de las redes SAN son sus capacidades multipath. Un path o ruta es un camino posible entre un HBA de un host hasta la controladora de un array de discos. Un software multipath sería capaz de aprovechar las distintas rutas para balancear la carga con la finalidad de maximizar la velocidad de acceso o conseguir una mayor tolerancia a fallos.

En este sentido, a veces los arrays de disco disponen de dos conexiones con la intención de hacer disponibles múltiples paths entre un HBA de un host y una unidad lógica (LU) que pueden ser aprovechados para una mayor velocidad de acceso. Esta característica es muy empleada en AoE, iSCSI y FC.

En la Wikipedia (http://en.wikipedia.org/wiki/Multipath_I/O) se puede obtener un listado relativamente completo de software multipath para SAN.

58.4 BIBLIOGRAFÍA

1. Redes de área de Almacenamiento en la Wikipedia.
http://es.wikipedia.org/wiki/Red_de_area_de_almacenamiento
2. Cristopher Poelker y Alex Nikitin. Storage Arena Networks for Dummies.
3. RAID en la Wikipedia. <http://es.wikipedia.org/wiki/RAID>

Autor: José Ramón Méndez Reboredo

Profesor Escuela Superior ingeniería Informática Ourense

Colegiado del CPEIG



**59. SISTEMAS DE BACKUP:
HARDWARE Y SOFTWARE DE
BACKUP. ESTRATEGIAS DE
BACKUP A DISCO.
DISPONIBILIDAD DE LA
INFORMACIÓN RPO, RTO.
REPLICACIÓN LOCAL Y
REMOTA, ESTRATEGIAS DE
RECUPERACIÓN.**

Tema 59.- Sistemas de backup: hardware y software de backup. Estrategias de backup a disco. Disponibilidad de la información RPO, RTO. Replicación local y remota, estrategias de recuperación.

59.1 Sistemas de Backup: hardware y software de backup.....	3
<i>59.1.1 Hardware de Backup.....</i>	<i>4</i>
59.1.1.1 Cintas.....	4
59.1.1.1.1 Digital Linear Tape (DLT).....	5
59.1.1.1.2 Linear Tape Open (LTO).....	5
59.1.1.1.3 Sun StorageTek T10000 (T10k).....	6
59.1.1.1.4 Características de almacenamiento en cinta.....	6
59.1.1.2 Disco.....	7
59.1.1.3 Medios Virtuales.....	8
59.1.1.4 Medios Ópticos.....	9
59.1.1.4.1 CD.....	9
59.1.1.4.2 DVD.....	10
<i>59.1.2 Software de Backup.....</i>	<i>11</i>
59.1.2.1 Herramientas de código abierto – AMANDA.....	11
59.1.2.2 Herramientas de código abierto – BackupPC.....	12
59.1.2.3 Herramientas de código abierto – Bacula.....	16
59.1.2.4 Software Propietario CommVault Simpana.....	18
59.1.2.5 Software Propietario Symantec NetBackup.....	20
59.2 Estrategias de Backup a Disco	23

59.3 Disponibilidade de la información RPO, RTO.....	27
59.3.1.1 Obxectivo de Punto de Recuperación.....	28
59.3.1.2 Obxectivo Tempo de Recuperación.....	29
59.4 Replicación local y remota, estrategias de recuperación.....	29
59.4.1 <i>Replicación Local</i>	31
59.4.1.1 Tecnoloxías de replicación local.....	31
59.4.1.1.1 Basada en replicación en host local.....	31
59.4.1.1.2 Basada en arrays de discos.....	32
59.4.2 <i>La replicación remota</i>	33
59.4.2.1 Tecnoloxías de replicación remota.....	33
59.4.2.1.1 Replicación remota baseada en LVM.....	33
59.4.2.1.2 Basada en trasvase de registros.....	34
59.5 Bibliografía.....	34

59.1 SISTEMAS DE BACKUP: HARDWARE Y SOFTWARE DE BACKUP

Un factor importante en todo sistema de backup es la elección de los sistemas hardware y software que lo componen.

59.1.1 Hardware de Backup

En la categoría de elementos hardware de backup tenemos:

59.1.1.1 Cintas

Tradicionalmente, los cartuchos de cinta magnética son los medios de comunicación más habituales en los sistemas de backup. Como soporte de almacenamiento de los respaldos de datos, la cinta magnética tiene una larga historia de uso y es el medio de copia de seguridad con mayor nivel de madurez. La cinta magnética, o de una forma más abreviada, la cinta, es un componente basado en cartuchos que se hace típicamente de algún tipo de plástico rígido. Contiene uno o más bobinas de plástico flexible que se han impregnado con un material con comportamiento magnético.

Los cartuchos de cinta están fabricados en varios formatos. Cada formato tiene unas características diferentes que responden a las diferentes necesidades de almacenamiento físico y de tiempo de preservación de la copia de seguridad, tanto en términos de la cantidad de datos almacenados, como de vida útil de los medios de almacenamiento o su coste. Los formatos de cinta de uso común son los siguientes:

- DLT/ SDLT
- LTO
- AIT
- STK 9840/9940/T10000

Según el tipo de cada cartucho este posee distintas capacidades o características como la velocidad de funcionamiento. El mercado está renovando continuamente este tipo de dispositivos con el fin de mejorar ambos aspectos. Sin embargo, existen tres formatos que podemos considerar de los más comunes y tienen características particulares que se describen aquí como ejemplos de elementos arquitectónicos de diseño: *DLT, LTO, T10000 y STK*.

El resto de formatos, aunque sean formatos comunes, se utilizan normalmente para entornos especializados, como el archivado y almacenamiento intermedio (nearline storage) empleado entre el almacenamiento online y el almacenamiento de backups.

59.1.1.1.1 *Digital Linear Tape (DLT)*

Digital Linear Tape (DLT) es el formato de cinta más antiguo y por lo tanto uno de los productos más maduros del mercado. Originalmente fue diseñado e implementado por DEC en 1984, para posteriormente ser adquirida por Quantum y redistribuido en 1994.

DLT es el primer cartucho de cinta compacta para copias de seguridad de sistemas abiertos en la empresa. Mientras que otros tipos de medios se encontraban en uso (como la cinta media pulgada, 4mm/8mm, y otros), DLT proporciona el mejor compromiso entre todos los factores debido a su tamaño, la fiabilidad de su almacenamiento, la capacidad, y disponibilidad relativa.

La conectividad de DLT, se limita a los tradicionales de SCSI, y está limitado a 300 GB de capacidad nativa de almacenamiento y 160 MB /seg velocidad de transferencia (SDLT600). Existían otras variantes disponibles, pero nunca llegaron a popularizarse con carácter general. Hoy en día, DLT se encuentra normalmente como copia de seguridad de larga duración en entornos pequeños que no requieren mayor capacidad.

59.1.1.1.2 *Linear Tape Open (LTO)*

Linear Tape Open (LTO) fue diseñado y concebido como una evolución y alternativa a los formatos DLT y otros ya existentes, y estaba destinado a proporcionar una plataforma común para los backups en cinta.

Seagate, HP e IBM fueron los iniciadores originales del consorcio LTO, encargado de realizar el desarrollo inicial y el cuál mantiene la licencia de la tecnología y la certificación del proceso. En teoría, se debería de haber

producido un formato estándar de cinta, con el cual los fabricantes podrían seguir trabajando con el estándar en el mercado e incorporando sus propias características y funciones adicionales.

Sin embargo, entre el original LTO-1 y los formatos de LTO-2 hubo problemas de compatibilidad. Estos problemas abarcaban desde bloqueos en las cintas cuando se utilizan medios adquiridos a dos proveedores distintos hasta la incapacidad de una unidad LTO de un fabricante a leer los datos escritos en un cartucho de otra.

El LTO-1 inicial proporcionaba 100 GB de almacenamiento nativo y 15 MB /seg; con los actuales sistemas de LTO-4 se proporcionan 400 GB de almacenamiento nativo de 160 MB / seg. Por su parte, el LTO-5 proporciona 800 GB de capacidad de almacenamiento nativo a 160 MB / seg.

59.1.1.1.3 *Sun StorageTek T10000 (T10k)*

El T10000 / StorageTek (T10k) de Sun representa uno de las tecnologías de almacenamiento en cinta que mejor se ha comportado en términos de capacidad. El T10k es un formato propietario producido únicamente por StorageTek y se encuentra normalmente en entornos en los que se empleaban las tecnologías anteriores de Sun como el STK (9840/9940). También se han utilizado en sistemas abiertos de servidores o mainframe. El T10k está diseñado para 500 GB de almacenamiento nativo de 120 MB / seg.

59.1.1.1.4 *Características de almacenamiento en cinta*

Aunque todos los datos anteriores indican un valor interesante en cuanto al rendimiento, todos los dispositivos de cinta con características similares de rendimiento deben tenerse en cuenta a la hora de diseñar entornos de backup.

La primera y más importante de ellas es el hecho de que todas las unidades de cinta son entornos serie. A diferencia de los dispositivos de disco, los dispositivos de cinta escriben los bloques de datos de forma lineal, uno tras otro. Las unidades de cinta sólo tienen una cabeza de escritura que escribe un bloque de datos de cada vez en la cinta, a medida que ésta se mueve por ella. Los dispositivos de disco tienen una serie de dispositivos de escritura, o cabezas, que se mueven a varios puntos del disco giratorio para situar los datos de una manera óptima. Esto permite que los dispositivos de disco puedan leer cualquier trozo de información solicitada. Dado que los discos tienen varias cabezas para obtener bloques de datos en paralelo, varios sistemas pueden acceder al disco al mismo tiempo.

La lectura de los datos de una cinta, se realiza mediante el proceso inverso: La cinta debe rebobinarse hasta el principio, hacia adelante hasta bloque que se necesita, y leer así el bloque de datos. Al poder devolverse únicamente un segmento de datos con cada lectura, los dispositivos de cinta no se pueden compartir de forma paralela entre sistemas sin un mecanismo para transferir el control entre los sistemas que usan dicho dispositivo.

El tipo de conectividad también tiene influencia sobre la utilización de dispositivos de cinta. Las unidades de cinta dependen de una conexión directa con el host para el transporte de los datos. Una vez más, esto se debe al hecho de que las unidades de cinta son dispositivos de serie que sólo aceptan una sola conexión a la vez.

59.1.1.2

Disco

La cinta proporciona un método muy maduro, muy conocido, y de bajo coste para almacenar copias de seguridad. Sin embargo, las debilidades, tales como la naturaleza secuencial de la cinta, la complejidad mecánica, y la gran variabilidad del rendimiento de los dispositivos de cinta están rápidamente relegando a la cinta a medio de almacenamiento secundario o terciario en muchos entornos.

Con todos los problemas con la cinta, los administradores buscaban un medio que permitiera un rápido acceso a las copias de seguridad y que

proporcionase una forma de tener un almacenamiento rápido y fiable: el *disco*.

Los backup a disco son simples sistemas de archivos que han sido situados aparte para que el software de backup los use. Aunque esto parece sencillo, la implementación y gestión de las soluciones basadas en disco pueden ser muy complejas.

El almacenamiento en disco supera algunas de las desventajas propias de las cintas. Por la capacidad de recibir datos de forma rápida, tiene múltiples flujos para almacenar copias de seguridad al mismo tiempo, y tiene la capacidad de presentar el almacenamiento de un número de maneras diferentes, dependiendo de la necesidad del sistema, por eso, el disco es muy empleado como un medio de almacenamiento de copia de seguridad primario.

Pero el disco también tiene sus debilidades, el coste de los medios de comunicación, la falta de portabilidad, y la dificultad de asegurar la plena utilización de los medios de comunicación hacen que el disco no sea tan satisfactorio como parece a priori.

59.1.1.3

Medios Virtuales

Los medios virtuales emulan el hardware físico de cinta con el objetivo de reducir o eliminar los problemas de gestión asociados a los medios físicos. Mediante la eliminación del hardware con una alta complejidad mecánica y de gestión y la eliminación de sus sistemas asociados y reemplazándolos por unidades de disco, los medios virtuales también tiene la ventaja de aumentar la fiabilidad general del entorno de backup. Los medios virtuales ofrecen estas ventajas sin cambiar los procedimientos operativos o exigir modificaciones del software de copia de seguridad. Además, en algunos casos, el rendimiento puede aumentarse a través de un mejor uso del ancho de banda en los medios de comunicación utilizados para conectar los medios virtualizados con los servidores de backup.

Los Medios virtuales de copia de seguridad se asocian tradicionalmente de forma exclusiva con bibliotecas de cintas virtuales (VTL) pero recientemente se han realizado nuevas implementaciones a través de protocolos que permiten la virtualización de otros tipos de sistemas de almacenamiento.

59.1.1.4

Medios Ópticos

Los medios ópticos se sitúan entre las ventajas de las cintas y las del disco. Sobresalen en las áreas de fiabilidad, flexibilidad, ciclo de trabajo e inamovilidad, mientras que sus retos los encontramos en las áreas de rendimiento, capacidad y coste.

59.1.1.4.1

CD

CD, o compact disk, es un soporte digital óptico que se utiliza para el almacenamiento de prácticamente cualquier tipo de datos. En la actualidad el uso del CD está decayendo a favor del aumento del uso de un nuevo medio de similares características como el DVD.

El CD ha servido y sigue sirviendo como medio de almacenamiento de copias de seguridad gracias a su fiabilidad e inamovilidad. Proporciona en comparación con otros medios como la cinta magnética, mayor seguridad y protección de los datos, dado que el propio medio es mucho más robusto frente a interacciones físicas externas (por ejemplo los campos magnéticos).

Además de ser un medio habitual para el almacenamiento de pistas de audio, los CDs se utilizan habitualmente para la generación de copias de seguridad relacionadas con la recuperación de los sistemas.

Los sistemas de CD utilizan un dispositivo hardware específico para grabar información, conocido como grabadora/regrabadora de CD. Existen también dispositivos hardware similares que solamente permiten la lectura de este medio.

Las capacidades habituales de los CD estándar abarcan desde los 650MB hasta los 900MB.

59.1.1.4.2**DVD**

Los DVDs vienen a ser la evolución de la tecnología digital óptica de los CDs.

Al igual que los CDs, existen dos tipos de dispositivos para el uso de los DVDs que son las grabadoras y los lectores. Existen diferentes tipos de DVDs y diferentes categorizaciones, siendo la más importante la relativa al número de capas, factor que determina la capacidad final del dispositivo.

Las capacidades actuales abarcan desde los 4,3Gb hasta los 17Gb. Los DVD utilizan dos tipos de sistemas de ficheros que reemplazan el antiguo ISO 9660 de los CDs, y que son el UDF y el Joliet.

59.1.2

Software de Backup

En la categoría de elementos software de backup tenemos herramientas de código abierto o software libre y software privativo o comercial. Las herramientas más comunes a nivel de software son:

59.1.2.1 **Herramientas de código abierto - AMANDA**

Amanda (Advanced Maryland Automated Network Disk Archiver), es el software de código abierto de copia de seguridad más conocido. Amanda se desarrolló inicialmente en la Universidad de Maryland en 1991 con el objetivo de proteger los archivos de un gran número de estaciones de trabajo cliente con un servidor de copia de seguridad único. James da Silva fue uno de sus desarrolladores originales.

El proyecto Amanda se registró en SourceForge.net en 1999. Jean-Louis Martineau, de la Universidad de Montreal ha sido el líder del desarrollo de Amanda en los últimos años. Durante años, más de 250 desarrolladores han contribuido al código fuente de Amanda, y miles de usuarios aportan pruebas y comentarios, lo que lo convierte en un paquete robusto y estable. Amanda se incluye con la mayor parte de las distribuciones Linux.

En un principio, Amanda fue utilizado mayoritariamente en las universidades, laboratorios técnicos, y departamentos de investigación. Hoy, con la amplia adopción de Linux en los departamentos de informática, Amanda se encuentra en muchos otros lugares, sobre todo cuando la atención se centra en aplicaciones LAMP (Linux+Apache+MySQL+PHP). Con los años, Amanda ha recibido múltiples premios de los usuarios.

Amanda permite configurar un único servidor backup maestro para realizar múltiples copias de seguridad de equipos Linux, Unix, Mac OS X, y Windows en una amplia variedad de dispositivos: cintas, discos, dispositivos ópticos, bibliotecas de cintas, sistemas RAID, dispositivos NAS, y muchos otros.

Las principales razones para la adopción generalizada de Amanda son:

- Se puede configurar un único servidor de copia de seguridad de varios clientes en red con cualquier dispositivo de almacenamiento: una cinta, disco o sistema de almacenamiento óptico.
- Está optimizado para el backup en disco y cinta, permitiendo escribir simultáneamente backup a cinta y disco.
- No utiliza drivers propietarios, cualquier dispositivo soportado por un sistema operativo también podrá funcionar en Amanda.
- Utiliza herramientas estándar, como dump y tar. Puesto que no son formatos propietarios, los datos se pueden recuperar con esas mismas herramientas.
- Se utiliza un planificador que optimiza niveles de seguridad para los diferentes clientes, de tal manera que el tiempo total del backup es aproximadamente el mismo para cada ejecución.
- Existe una amplia y activa comunidad de usuarios que crece día a día.
- El coste total de propiedad (TCO) de una solución de backup basada en Amanda es significativamente menor que el TCO de cualquier solución que utilice software privativo.

59.1.2.2 Herramientas de código abierto - BackupPC

BackupPC es un sistema de alto rendimiento que permite realizar copias de seguridad de sistemas Unix, Linux, Windows y MacOS en un disco. Es por tanto una herramienta basada totalmente en disco.

Ofrece una serie de ventajas como son:

- **Soporta cualquier sistema operativo cliente.** Esto se debe a que se utilizan herramientas estándar que o vienen con el SO o se pueden añadir al SO, sin necesidad de instalar cliente. Así resulta más fácil integrar un nuevo cliente.
- **Interfaz Web** con control de usuario para acceder a copias de seguridad. La mayoría de los SO trae un navegador web, así que usar

una interfaz web es otra manera de acelerar el proceso de incorporación de nuevos clientes con diferentes sistemas operativos. La interfaz web está diseñada para dar el máximo control posible al cliente de forma segura. El usuario puede solicitar restauraciones, y navegar fácilmente y restaurar archivos individuales. Sin embargo, el usuario no podrá ver las máquinas de otro usuario.

- **Soporte de clientes DHCP.** Mediante el uso de servicios estándar, BackupPC soporta clientes DHCP, siempre y cuando el cliente esté registrado con un servicio de nombres como DNS, Active Directory o LDAP.

Funcionamiento de BackupPC

El modelo de BackupPC tiene un usuario por cliente. Esto es así porque BackupPC fue específicamente diseñado para realizar copias de seguridad de PCs de varios usuarios (de ahí el nombre).

Normalmente, el usuario es el propietario de los datos de la máquina. Si se trabaja con un servidor de ficheros, el usuario deberá ser un administrador.

BackupPC envía mensajes de correo electrónico al propietario si no puede realizar la copia de seguridad después de un tiempo configurable; el propietario puede gestionar las restauraciones de las copias a través de una interfaz web.

En los siguientes puntos se describen algunas de las características proporcionadas por BackupPC:

- **Directo al disco.** BackupPC almacena todas sus copias de seguridad directamente en el disco. Los archivos idénticos en cualquier directorio o cliente se guardan sólo una vez, lo que reduce drásticamente los requisitos de almacenamiento del servidor. Estos archivos se almacenan en un conjunto de discos. Además del conjunto de discos, las copias de seguridad están en un árbol de directorios organizados por host.

BackupPC también tiene un proceso (que se lanza por las noches) que recupera espacio del conjunto de discos que no está referenciado por

ningún backup, lo que evita un uso inadecuado del espacio en disco. Este es un proceso automático que el administrador no tiene que configurar.

- **Sistema operativo del servidor** La parte del servidor de BackupPC está diseñada para ejecutarse en un sistema tipo Unix con Perl y mod_perl. Ofrece el mejor rendimiento con Apache, pero se puede ejecutar en cualquier servidor web que soporte Perl (se requiere mod_perl o Perl setuid.) El servidor debe tener un disco con gran capacidad o RAID para almacenar los backups.

- **Sistema operativo del cliente.** Como se comentó anteriormente, soporta cualquier SO. Las versiones más modernas de las variantes comerciales de Unix (Solaris, AIX, IRIX, HP-UX) traen en la propia distribución las herramientas tar, compress, gzip, rsync, y rsh y / o ssh. Otros sistemas operativos tipo Unix (Linux, FreeBSD, OpenBSD, NetBSD, Mac OS X) también cuentan con estas herramientas.

Los clientes de Windows pueden hacer copias de seguridad de diferentes formas dependiendo de si las políticas locales permiten o no la instalación de software. Si no se permite, BackupPC utiliza parte de la suite Samba (<http://www.samba.org>) para hacer backup de la información compartida mediante SMB o CIFS. Si se permite instalar software, se utiliza rsync junto con el conjunto de herramientas Cygwin (<http://www.cygwin.com>).

- **Soporte para herramientas nativas.** BackupPC utiliza las herramientas estándar de Unix para su funcionamiento interno. Esto incluye programas como Perl, tar, rsync, compress, gzip, bzip2, zip, apache y samba.

BackupPC no utiliza una base de datos o catálogo para almacenar la información de respaldo. En su lugar, utiliza el árbol de directorios para almacenar esta información. Esto simplifica las actualizaciones del sistema operativo del servidor de BackupPC o de la propia aplicación BackupPC.

- **Control de los backups y restauraciones a través de interfaz web.** La Web es la interfaz principal de BackupPC. Tras la configuración inicial, no es necesario acceder al servidor mediante línea de comandos para administrar BackupPC. La interfaz web está escrita en

Perl y fue diseñada para funcionar tanto con mod_perl como con CGI o con Perl setuid.

La interfaz permite a los usuarios identificarse, acceder y controlar los respaldos y las restauraciones.

El usuario puede solicitar copias de seguridad de tipo one-time, de tipo completa, o de tipo incremental.

Se pueden utilizar varias opciones para recuperar ficheros:

- o Los archivos individuales se recuperan mediante selección.
- o Los grupos de archivos o directorios se pueden restaurar a su ubicación original.
- o El usuario puede descargar los archivos como un archivo tar o zip.

El usuario tiene control absoluto sobre qué archivos o directorios se restauran y donde hay que restaurarlos. Un histórico muestra que archivos se han modificado durante cada copia de seguridad en cada directorio.

- **Soporte para clientes DHCP.** Los clientes BackupPC se referencian por nombre de host. Si la red de la copia de seguridad utiliza DHCP y se permite la resolución de nombres dinámica, no hay que hacer nada más para que el servidor BackupPC respalde a los clientes DHCP. Si este no es el caso, y los clientes son máquinas Windows, BackupPC se puede configurar para buscar un conjunto de direcciones de los clientes, localizándolos mediante SMB.

Si el cliente no está en línea durante el período de copia de seguridad normal, el servidor BackupPC no genera un error a menos que haya transcurrido un período de tiempo establecido desde la última copia de seguridad. En este punto, el servidor envía un email al propietario del cliente y le recuerda que se asegure que la máquina está en la red para hacer una copia de seguridad. (El servidor también puede enviar cualquier error al administrador.)

Los clientes que residen en otra LAN pueden ser gestionados a nivel local asumiendo que hay conectividad de entre las redes. Esto significa

que se puede hacer backup de los clientes conectados a través de una red privada virtual (VPN).

Si el usuario no desea realizar copias de seguridad en un momento dado, se conectaría a través de la interfaz web para cancelar la copia de seguridad.

- **Pool de Backups.** Cuando los clientes utilizan el mismo sistema operativo se duplican los archivos respaldados. Si se quiere mantener múltiples copias de seguridad completas aumenta el número de archivos duplicados, lo que aumenta los requisitos de capacidad de almacenamiento para el servidor. BackupPC almacena un árbol de directorios por cliente respaldado, pero comprueba si los archivos se han almacenado antes. Si es así, BackupPC utiliza un enlace que apunta al fichero existente en el conjunto de discos común, ahorrando una gran cantidad de espacio. Además, BackupPC puede comprimir opcionalmente para ahorrar más espacio.

- **Fácil configuración por cliente.** Una vez que el administrador haya definido cuáles deberían de ser las políticas de backup del sitio, es muy fácil anular cualquier opción de configuración en base a un cliente. Esto permite una gran flexibilidad sobre qué, cuándo, y cómo hacer copia de seguridad de un cliente. No hay clases de clientes por sí mismo.

59.1.2.3 Herramientas de código abierto - Bacula

Bacula es un conjunto de programas Open Source, listos para ser utilizados en un entorno doméstico y profesional, que permiten administrar los backups, restauración y verificación de datos en una red heterogénea. Bacula es relativamente fácil de usar y eficiente, a la vez que ofrece muchas funcionalidades avanzadas para la administración de los datos almacenados, lo cual facilita hallar y recuperar archivos perdidos o dañados. En términos técnicos, Bacula es un sistema de backups Open Source, orientado a la red y listo para la empresa.

Es capaz de realizar copias de seguridad en disco, cinta o medios ópticos. Bacula fue escrita originalmente por John Walker y Kern Sibbald en el año 2000. John dejó el proyecto no mucho tiempo después de su creación, y Kern, trabajó en él desde mediados del 2000 hasta el primer lanzamiento público de Bacula en abril de 2002. Desde entonces, otros desarrolladores han contribuido a su desarrollo.

Bacula está disponible bajo licencia AGPL versión 3. La página web del proyecto se encuentra en <http://www.bacula.org>, y los archivos descargables y un repositorio CVS se alojan en SourceForge.

Bacula Arquitectura

Bacula es una solución distribuida de backups. Esto significa que Bacula está compuesto por varios elementos, que pueden o no residir en el mismo host. Por ejemplo, se puede tener un host con el catálogo y en otro el storage.

Se basa en una arquitectura Cliente-servidor que resulta eficaz y fácil de manejar, dada la amplia gama de funciones y características que brinda: copiar y restaurar ficheros dañados o perdidos. Además, debido a su desarrollo y estructura modular, Bacula se adapta tanto al uso personal como profesional.

Se puede utilizar TLS (Transport Layer Security) para proteger los datos durante la transmisión.

Los componentes principales de esta arquitectura son:

- **Director (DIR)** es el encargado de gestionar de forma centralizada la lógica de los procesos de backup y los demás servicios. Trabaja en base a una unidad básica denominada JOB (un cliente, un conjunto de archivos, ...) de tal forma que el Director planifica, inicia y supervisa todos los jobs.

También es el encargado de mantener el catálogo, por lo que el servidor de la base de datos debe estar accesible desde la máquina que ejecuta el Director.

- **Storage** es el encargado de gestionar los dispositivos de almacenamiento; esto exige que esté instalado en la máquina que posea la conexión física a los dispositivos de almacenamiento, tales como: discos locales, grabadoras, unidades de cinta, volúmenes NAS o SAN, autocargadores o librerías de cinta.
- **File Daemon** es el agente que corre del lado del cliente, es decir, en la máquina cuyos datos se van a respaldar, y que tiene como objetivo empaquetar los datos y enviarlos al Storage, donde serán almacenados.
- **Consola** es la herramienta que permite al usuario o administrador controlar Bacula. Se comunica con el director vía red, iniciando los jobs, revisando la salida del job, haciendo consultas y modificaciones en el catálogo.

Existen consolas en modo texto, modo GUI para Windows y Linux/UNIX e interfaces web.

- **Catálogo** es una base de datos donde se guarda información sobre los jobs y sobre los datos respaldados. El catalogo permite dos cosas:
 - o Por un lado, como guarda información de los jobs, pools y volúmenes, Bacula lo usa para saber si hay un backup completo para un job, y si no lo hay, realizará para ese backup una copia completa.
 - o Por otro lado, el catálogo tiene todos los nombres de archivo (y sus atributos, como fecha de última modificación, etc.) que se respaldaron, y eso es lo que permite hacer una recuperación selectiva, es decir, seleccionar (marcar, en la jerga de Bacula) individualmente qué archivos y/o directorios restaurar.

59.1.2.4 Software Propietario CommVault Simpana

Simpana comenzó como un proyecto dentro de AT & T Labs en 1987 y posteriormente fue adquirido por la empresa CommVault.

Simpania es un software de backup que realiza copias de seguridad de entornos Unix, Windows, Linux, servidores de correo Exchange, Lotus Notes, bases de datos Oracle, MySQL, SQLServer y máquinas virtuales

VMware. Además permite funciones avanzadas como puede ser el archivado, la deduplicación y la replicación de ficheros.

El funcionamiento de la aplicación se basa en el uso de los bloques de disco, por lo que todos los módulos no utilizan la información del archivo, si no que trabaja a más bajo nivel. Con ello consigue mejores ratios de compresión y una importante reducción de la ventana de backup, al utilizar únicamente los bloques modificados y no el fichero entero para realizar estas operativas.

Otra característica que incide en el uso de almacenamiento de bajo coste es la capacidad de generar políticas como las de archivado, mediante las que automáticamente permite mover ficheros de un almacenamiento a otro con mayor capacidad a menor coste. De esta forma, por ejemplo se podrían pasar los datos de una cabina de fibra a otra con discos SATA, pudiendo llegar a un tercer nivel a cinta, en base a unos requisitos (fecha del archivo, último acceso al archivo, etc.). Todos los movimientos se realizan de forma transparente para el usuario, tanto en el archivado como en su recuperación (si fuese necesario).

A estas funcionalidades hay que sumar la capacidad de deduplicación, que realiza una compresión de los datos aprovechando las duplicidades de los datos a nivel de bloque, consiguiendo alcanzar ratios de hasta el 50% de ahorro en el uso de almacenamientos en datos de segundo nivel y hasta el 90% en los de tercer nivel.

Para terminar el repaso a las principales funcionalidades, la replicación, permite la utilización de snapshots a nivel de cabina permitiendo volver el almacenamiento replicado a un estado anterior o montar la imagen snapshot como un recurso compartido.

Todo se administra desde una única consola centralizada, que simplifica toda la administración de la plataforma. Adicionalmente el motor de búsqueda ofrece la opción de buscar rápidamente y recuperar datos sin necesidad de saber donde se ubican.

59.1.2.5 Software Propietario Symantec NetBackup

Symantec NetBackup es actualmente el titular de la mayor cuota de mercado del entorno de software de copia de seguridad.

Netbackup 7 es la nueva versión de la solución de copia de seguridad y recuperación de datos orientada a grandes corporaciones. Esta herramienta trata de simplificar la gestión de la información reduciendo el volumen de almacenamiento de datos con técnicas de deduplicación en los ordenadores cliente de la red además del propio servidor, ofreciendo protección para entornos virtualizados. Todo ello con el único propósito de agilizar los procesos de backup y recuperación de datos.

La nueva herramienta incluye eliminación de datos duplicados nativos dentro del cliente NetBackup y permite a los clientes multiplicar por diez la velocidad de las copias de seguridad en oficinas remotas, el propio centro de datos y los entornos virtuales. Esta eliminación de datos duplicados en el cliente y en el destino ofrece una mayor cobertura con menos herramientas.

El proceso de deduplicación se contempla para todos los sistemas físicos y virtuales, independientemente del método de copia de seguridad. De este modo se integra una mayor protección para los cada vez más extendidos entornos virtualizados bajo las plataformas Hyper-V y VMware. Es en el caso de esta última en la que se ha podido observar un incremento de velocidad de hasta el 50% a la vez que disminuye el volumen de almacenamiento necesario en un 40%.

Otro de los aspectos notablemente mejorados en Netbackup 7 es la velocidad de recuperación de datos ante desastres. Permitiendo la restauración de grandes volúmenes de información en pocos segundos desde cualquier lugar y punto en el tiempo. Esta gestión se facilita al administrador de TI mediante un sistema centralizado de supervisión y alerta, que integra la administración de varios dominios de archivos con sus respectivas políticas de salvaguarda de datos.

La tecnología incluida en NetBackup acelerará la transición a un entorno virtual para las organizaciones empresariales que instalen un gran número

de máquinas virtuales o que decidan crear una infraestructura de nube privada.

La solución NetBackup también ofrece una elaboración de informes simplificada y un mayor soporte a las aplicaciones de bases de datos de Oracle y MySQL.

Algunas de las prestaciones y beneficios incluidos en la última versión de la herramienta son:

- La tecnología Virtual Machine Intelligent Policy incorpora la automatización a la localización y la protección de máquinas virtuales y minimiza los esfuerzos de administración necesarios para realizar copias de seguridad de máquinas virtuales VMware de alto rendimiento.
- Un 50% más de rapidez en copias de seguridad de máquinas virtuales gracias a que la tecnología Granular Recovery Technology (GRT) se encuentra ahora disponible para sistemas Linux en entornos VMware. Esto permite a los clientes reducir los tiempos comparables de copias de seguridad de máquinas virtuales en un 50%, además de simplificar la administración y mejorar la velocidad de recuperación de archivos individuales.
- Recuperación “a la carta” desde cualquier lugar con la nueva tecnología de replicación de imagen que permite a los clientes que replican datos entre múltiples sitios o dominios de NetBackup realizar backup de datos en un sitio alternativo.
- Recuperación acelerada: NetBackup RealTime ofrece soporte a entornos VMware para eliminar el espacio de tiempo entre copias de seguridad, además de reducir el impacto para grandes hosts de VMware y permitir la recuperación casi instantánea de sistemas completos.
- Satisfacer los requisitos normativos y de cumplimiento para seguimiento de auditorías.
- Incorpora informes mejorados de las políticas del ciclo de vida del almacenamiento, del seguimiento de las auditorías y del estado de las licencias.

- Deduplicación para Oracle mejorando el rendimiento de las copias de seguridad.
- Se añade un nuevo agente que presta soporte a MySQL para centralizar y automatizar las copias de seguridad y la recuperación de datos de las bases de datos de MySQL.
- Actualización simplificada de clientes con LiveUpdate que permite mejoras en equipos cliente para UNIX, Linux y Windows respecto a la versión NetBackup 6.5 y posterior desde una política única controlada por el administrador de NetBackup.

59.2 *ESTRATEGIAS DE BACKUP A DISCO*

Las estrategias de backup definen el plan que se ha de seguir para garantizar la integridad de la información. Los motivos por los que se debe establecer una correcta estrategia antes de comenzar a realizar las copias de seguridad pueden ser muy diversos, pero en esencia se trata de determinar la mejor manera para asegurar la información teniendo en cuenta las posibles dificultades de recuperación de parte de los datos, el coste de los medios que se emplearan y el tiempo que se necesitara.

Como no todos los sistemas son iguales, no todas las estrategias de backup son adecuadas para todos los sistemas. Partiendo de unas características comunes, algunas de las propiedades básicas de una estrategia backup son:

Tiempo de almacenamiento. Define el tiempo máximo que una copia permanece almacenada en un dispositivo. Al finalizar este tiempo la copia puede cambiar de dispositivo o ser borrada para liberar espacio en el medio de almacenamiento y poder hacer uso del mismo.

Almacenamiento alternativo. Posibilita realizar una o varias copias de seguridad en una ubicación externa al sistema y a la localización geográfica del mismo, manteniéndola durante un elevado período de tiempo, aumentando la seguridad ante cualquier catástrofe, ya sea a nivel de software o de hardware.

Protección ante fallo de los dispositivos. Establece el número de medios que se emplean. Cuanto mayor es el número de medios utilizados, mayor es la seguridad contra posibles pérdidas de información producidas por un fallo en el dispositivo de almacenamiento.

Tiempo de restauración. Esta característica especifica el tiempo de regeneración del sistema en caso de producirse algún fallo.

El coste. Suele ser un factor determinante a la hora de seleccionar la estrategia a realizar.

Las estrategias para la realización de copias de seguridad pueden ser muy distintas, dependiendo del sistema en cuestión sobre el cual se realizan.

En algunos casos, solamente se efectúa un backup de todo el contenido. Esto se produce cuando por algún motivo especial y muy específico o por algún motivo técnico, cuestiones de tiempo o por que existe un elevado riesgo para los datos. Alguno de estos casos especiales pueden ser:

No disponer del software original.

Desconocimiento de la ubicación de los ficheros de configuración.

Cambiar un disco de almacenamiento rígido.

Realizar cambios en las particiones de uno o más discos de almacenamiento rígidos.

Es habitual que este tipo de situaciones concretas se produzcan a la hora de llevar a cabo tareas de reparación o actualización sobre sistemas no controlados.

Cuando se trata de cubrir alguno de estos casos la estrategia de backup a seguir es sencilla, realizar un resguardo o copia de seguridad de todo el contenido de las unidades involucradas para así garantizar que no se perderá ninguna información y que será posible realizar la restauración completa del sistema.

Por otro lado, cuando realmente se ha de diseñar un plan estratégico para la realización de las copias de seguridad de un sistema propio o de una organización externa, se deben tener en cuenta una serie de pautas que ayudan a que el plan estratégico de backups sea el más conveniente y conseguir la mejor relación coste/beneficio posible.

Estas pautas aportan una reducción en el tiempo de respuesta a la hora de realizar una recuperación en caso de que se producirse cualquier tipo de contingencia.

Al intentar definir un plan de backups, surgen una serie de dudas:

¿Qué datos se deberían resguardar en cada backup? Datos a resguardar.

Es un factor determinante para una estrategia de backup que se determine el grado o grados de importancia de la información, es decir, establecer que información resulta de mayor valor para la organización. No tienen la misma transcendencia un documento de trabajo que una copia de respaldo de la configuración de una aplicación.

¿Cada cuánto se debería efectuar un backup de los datos? Frecuencia del backup.

Para determinar la periodicidad con la que se deben realizar las copias de seguridad no existe un criterio claramente definido. Sin embargo si se tienen en cuenta factores como:

Tiempo empleado en la creación de la información.

Coste invertido en la creación de la información.

Posibles consecuencias derivadas de su pérdida.

¿Cuánto tiempo deberían permanecer guardadas las copias de seguridad? Tiempo de Almacenamiento.

El período máximo de tiempo de estancia de una copia de seguridad en un dispositivo, es decir, el tiempo de retención, está directamente relacionado con los medios de almacenamiento disponibles, y por consiguiente por el presupuesto de la estrategia de backup.

Otra de las decisiones importantes a tomar durante la elaboración de una estrategia para la realización de copias de seguridad es la de seleccionar y planificar los distintos tipos de copias de seguridad.

Los backups son copias exactas de la información. Se pueden definir como instantáneas de los datos en un momento determinado, almacenados en un formato estándar, se puede realizar un seguimiento a lo largo de su periodo de utilidad y con cada nueva copia se mantiene la independencia con copia inicial. Se pueden crear múltiples niveles de backups, siendo los principales:

Copias de seguridad completas (Full backups): representan una copia exacta en un momento dado, de los datos que se pretende proteger. Proporcionan la base para todos los demás niveles de backup.

Por otro lado, están dos niveles de backup que capturan únicamente los cambios realizados sobre una copia de seguridad completa.

1. **Copia de seguridad diferencial**, también conocida como la *copia de seguridad incremental acumulativa*, captura copias de seguridad que se han producido desde el último backup completo y suele utilizarse en entornos en los que no se produce un elevado número de cambios. La copia de seguridad diferencial se debe utilizar con cuidado debido a que puede crecer con rapidez e igualar e incluso superar el tamaño de la copia de seguridad completa.

La ventaja de utilizar las copias de seguridad diferenciales viene dada en el momento de la restauración puesto que en el momento de restaurar una copia de seguridad diferencial sólo se necesita el backup completo y la última copia diferencial realizada. Debido a que únicamente se precisan dos imágenes para la restauración, la probabilidad de que ambas imágenes sufran algún percance, pérdida, corrupción, etc., se reduce significativamente.

2. **Copia de seguridad incremental**, es capaz de capturar los cambios que se han producido desde la última copia de seguridad realizada, independientemente del tipo que sea. Es la forma más utilizada para la realización de copias de seguridad, evidentemente combinada con una copia de seguridad completa.

Este tipo de copia de seguridad contiene la menor cantidad de datos necesarios durante cada ciclo de backup, reduciendo la cantidad de datos que se transfieren y el tiempo que se necesita para la creación de una copia de seguridad.

Sin embargo las copias de seguridad incrementales tienen aspectos negativos. Si se está recuperando un grupo de archivos de un conjunto de copias de seguridad completas e incrementales, es probable que se requieran más de dos imágenes de copias de seguridad diferentes para completar la restauración, lo que aumenta la probabilidad de que alguna de estas partes sufra algún tipo de problema y no se pueda completar la restauración.

59.3 DISPONIBILIDAD DE LA INFORMACIÓN RPO, RTO

La información representa uno de los activos más importantes en el contexto actual, y como tal, debe existir siempre un plan estratégico y de contingencia que proporcione los mecanismos necesarios para garantizar la seguridad y disponibilidad de la misma.

Existen en el mercado una gran cantidad de soluciones tecnológicas y metodologías que nos permiten aplicar o instaurar protocolos específicos de protección y garantía de disponibilidad de la información corporativa, independientemente de la entidad en la que nos encontremos. Para establecer un criterio de selección entre toda esta gran cantidad de soluciones, existen un conjunto de indicadores técnicos que nos proporcionan un mecanismo estándar para poder establecer comparativas objetivas sobre cuál de las diferentes soluciones es la más conveniente. Estos dos indicadores son el Objetivo de Punto de Recuperación (RPO) y el Objetivo de Tiempo de Recuperación (RTO).

A grandes rasgos, podemos definir ambos conceptos de la siguiente manera:

Objetivo de Punto de Recuperación o RPO: Es la cantidad máxima de información que puede ser perdida cuando el Servicio es restaurado tras una interrupción.

Objetivo de Tiempo de Recuperación o RTO: Es el tiempo máximo permitido para la recuperación de un servicio de TI tras una interrupción.

Dentro de los planes de contingencia desarrollados para prevenir y paliar los casos de caída de servicio o pérdida de información en una organización, pueden existir diferentes alternativas aplicables en función de determinados criterios relacionados con el flujo y la cantidad de información con la que se trabaja. Para evaluar cuales son las técnicas más apropiadas, los conceptos anteriores marcan un punto inicial que se debe tomar como referencia para la implantación de las políticas adecuadas en el tratamiento de los datos.

59.3.1.1 Objetivo de Punto de Recuperación

El indicador RPO es una manera objetiva para comparar diferentes productos, sistemas o metodologías de recuperación de información cuando lo que interesa controlar es la cantidad de información que podría llegar a perderse en caso de contingencia. Como se ha definido con anterioridad, RPO establece un indicador que evalúa la cantidad de información que puede llegar a perderse sin graves consecuencias, es decir, es un indicador de riesgo.

Este indicador debe tomarse con cautela dado que es altamente dependiente del contexto en el que se encuentre la organización, así como de su volumen de generación de datos.

Para ilustrar el ejemplo, se plantea la situación de una organización en la que se realiza una copia de seguridad incremental cada noche. En este escenario, la pérdida máxima de datos que podrían llegar a perderse en caso de contingencia (fallo de los servidores, etc...) sería como máximo un día hábil, dado que asumimos que cada noche se realiza la copia de seguridad incremental.

Esta medida puede ser válida para determinados modelos de negocio en los cuáles el volumen de datos con el que se trabaja a lo largo de un día hábil no es demasiado elevado. Sin embargo, el mismo modelo aplicado a

una entidad bancaria en la cual se realizan millones de transacciones diarias, la pérdida máxima de un día hábil no es aceptable.

59.3.1.2 Objetivo Tiempo de Recuperación

El RTO determina el tiempo de recuperación frente a una contingencia, es decir, el tiempo que se puede estar sin el servicio operativo. Para ello es necesario identificar al inicio todas las funciones críticas del negocio y su apoyo a los componentes de Tecnologías de la información. Una vez identificadas, podemos establecer el tiempo necesario en caso de fallo para poder reanudar las operaciones normales.

El RTO es un indicador íntimamente relacionado con el BIA (Business Impact Analysis) y se suele expresar en términos de tiempo (horas, minutos,...). De hecho, en muchas organizaciones ya se establecen por norma primas sobre la disponibilidad de los sistemas y acceso a datos corporativos.

RTO y RPO están también enteramente vinculados. A la hora de diseñar un plan de contingencia, es necesario saber qué estrategia RPO se implantará dado que el volumen de datos a recuperar en caso de fallo, que está ligado a la estrategia RPO, influye directamente en el indicador RTO, es decir, en el tiempo que se tardará en recuperar el sistema.

59.4 REPLICACIÓN LOCAL Y REMOTA, ESTRATEGIAS DE RECUPERACIÓN

La replicación es el proceso de creación de una copia exacta de los datos. La creación de una o varias réplicas de los datos de producción es una de las maneras de proporcionar continuidad al del negocio (BC).

Estos modelos pueden ser utilizados para operaciones de recuperación y reinicia de los sistemas en caso de que se produzca una pérdida de datos.

Una réplica ha de proporcionar:

La capacidad de recuperación: permite la restauración de los datos de los volúmenes de producción en caso de que se produzca una pérdida

de los datos. Se ha de proporcionar un mínimo de y RTO y un RPO concreto que nos garanticen la reanudación de las operaciones comerciales en los volúmenes de producción.

La capacidad de reinicio: garantiza la coherencia de los datos de la réplica, posibilitando la reanudación de las operaciones de negocio utilizando para ello la información contenida en las réplicas.

La replicación se pueden clasificar en dos grandes categorías: ***locales y remotos***

59.4.1 *Replicación Local*

La replicación local hace referencia al proceso creación de réplicas dentro del mismo array de discos o el mismo centro de datos.

59.4.1.1 *Tecnologías de replicación local*

Las replicaciones Host-based (basadas en replicación en host local) y Storage-based (basadas en almacenamiento) son las dos principales tecnologías adoptadas para la replicación local. La replicación de archivos del sistema y la replicación basada en LVM son ejemplos de la tecnología Host-based de replicación local. La replicación de almacenamiento basada en matrices de disco puede llevarse a cabo con soluciones distintas, la duplicación de todo el volumen, la replicación pointer-based de todo el volumen, y la replicación basadas en punteros y virtual.

59.4.1.1.1 *Basada en replicación en host local*

En este tipo de replicación, los administradores del sistema llevan a cabo el proceso de copia y restauración en la propia máquina, pudiendo basarse la recuperación en una replicación integral del volumen mediante LVM (Logical Volume Manager), o bien mediante instantáneas del sistema de ficheros.

Replicación del volumen mediante LVM: El LVM se encarga de crear y controlar el volumen de host a nivel lógico y está formado por tres componentes: los discos físicos, los volúmenes lógicos y los grupos de volúmenes. En la replicación de volúmenes basado en LVM, cada partición lógica en un volumen se asigna a dos particiones físicas en dos discos diferentes. De esa forma se consigue un espejo que permite redundancia y recuperación directa en caso de necesitar replicar.

Instantánea de archivos del sistema: Consiste en crear una réplica a base de instantáneas del sistema de ficheros mediante la utilización de metadatos almacenados en un mapa de bits. Estos metadatos van reflejando el cambio que se va produciendo en el sistema de ficheros y van almacenando un registro de las direcciones accedidas mediante operaciones de lectura/escritura. Este sistema requiere de una fracción del espacio utilizado por el sistema de ficheros original.

59.4.1.1.2***Basada en arrays de discos***

En este tipo de replicación se hace uso de matrices de discos que pueden estar distribuidas dentro del CPD. El entorno operativo es el que lleva a cabo el proceso de replicación de un determinado sistema de ficheros, sin necesidad de que los recursos de acogida (CPU y memoria) del anfitrión intervengan en el proceso de replicación.

59.4.2 ***La replicación remota***

La replicación remota consiste en el proceso de creación de réplicas del conjunto de datos en lugares con otra ubicación física. Las réplicas remotas ayudan a las organizaciones a mitigar los riesgos asociados a las interrupciones regionales del servicio, que pueden estar provocadas por diferentes causas, por ejemplo, desastres naturales. La infraestructura en la que los datos se almacenan inicialmente se llama fuente. La réplica, o infraestructura remota en la que se almacena la copia se le llama blanco.

59.4.2.1 ***Tecnologías de replicación remota***

La más habitual es la tecnología de replicación basada en host remoto, que utiliza uno o más componentes de la máquina para realizar y gestionar la operación de replicación. Existen dos enfoques fundamentales para la replicación basada en host remoto: Replicación remota basada en LVM y replicación de bases de datos a través de trasvase de registros.

59.4.2.1.1 ***Replicación remota basada en LVM***

En este modelo, la replicación se efectúa y gestiona a nivel de grupo de volúmenes. El LVM de la máquina origen es el encargado de gestionar y transmitir la información del volumen al LVM de la máquina remota. El LVM de la máquina remota se encarga de recibir los datos y realiza la operación de réplica del volumen.

Antes del inicio de la replicación, se deben configurar los sistemas fuente y remoto para que los sistemas de archivos, los volúmenes y la agrupación de volúmenes sea idéntica en ambos. El punto de partida, o sincronización inicial, se puede realizar de diferentes formas, siendo la más frecuente la restauración en el punto remoto de una copia de seguridad de los datos de origen.

En la replicación remota basada en LVM se soportan dos modos de transferencia de datos, que son el sincrónico y el asincrónico. En el modo asíncrono, las operaciones de escritura se van almacenando en una cola de registros gestionada por el LVM y se van enviando al host remoto en el orden en el que son recibidas. En caso de fallo de la red, las operaciones siguen acumulándose en la cola de registros.

En la replicación síncrona, las operaciones de escritura deben estar comprometidas tanto en origen como en destino. Las operaciones de escritura consecutivas no pueden ocurrir en fuente ni destino hasta que las operaciones previas hayan finalizado. Esto garantiza que los datos de la fuente y destino son exactamente los mismos en todo momento. Esto hace posible que el RPO en caso de fallo sea cero o cercano a cero. Sin embargo, como contraprestación al nivel de seguridad, el tiempo de respuesta es mucho mayor. El grado de impacto en el tiempo de respuesta depende de la distancia entre ambos sitios (fuente y destino), del ancho de banda disponible y de la infraestructura de conectividad de red.

59.4.2.1.2 *Basada en trasvase de registros*

La replicación de bases de datos a través de trasvase de registros consiste en la captura de las transacciones realizadas en la base de datos fuente, que son almacenadas en registros que se transmiten periódicamente de un host fuente a un host destino. El host destino recibe el conjunto de registros y realiza las operaciones oportunas en la base de datos replicada. El proceso inicial de producción y reproducción requiere que todos los componentes importantes de la base de datos se repliquen en el sitio remoto.

Los sistemas gestores de bases de datos permiten definir un intervalo de tiempo para el envío de los ficheros de registro, o bien configurar un tamaño predeterminado de los mismos. Cuando un registro supera el intervalo de tiempo establecido o alcanza su tamaño máximo, se cierra, y se abre un nuevo fichero para registrar las transacciones. Los registros cerrados van siendo enviados desde la fuente al destino garantizando que la base de datos replicada en destino sea consecuente con la fuente hasta el último registro cerrado. El RPO en el sitio remoto dependerá del tamaño del fichero de registro y de la frecuencia de cambio de registro en la fuente.

59.5 *BIBLIOGRAFÍA*

- System & Disaster Recovery Planning. Richard Dolewski

- Information Storage and Management: Storing, Managing, and Protecting Digital Information. G. Somasundaram y Alok Shrivastava.
- Backup & Recovery. W. Curtis Preston y O'Reilly Media.

Autor: Francisco Javier Rodriguez Martínez

Subdirector de Sistemas Escola Superior Enxeñaría Informática Ourense

Colegiado del CPEIG

60. ADMINISTRACIÓN Y GESTIÓN DE REDES Y SISTEMAS DE ALMACENAMIENTO. VIRTUALIZACIÓN DEL ALMACENAMIENTO. GESTIÓN DEL CICLO DE VIDA DE LA INFORMACIÓN (ILM).



Tema 60.- Administración e xestión de redes e sistemas de almacenamento. Virtualización do almacenamento. Xestión do ciclo de vida da información (ILM).

60.1 ADMINISTRACIÓN Y GESTIÓN DE REDES Y SISTEMAS DE ALMACENAMIENTO.

60.1.1 Administrador de red

Un administrador de red como su nombre indica "administra" una red, es decir, se encarga de:

- Instalación y configuración de la red.
- Hardware de red, conexiones físicas, hubs, switches, routers, servidores y clientes.
- Software de red, como los sistemas operativos de red, servidores de correo electrónico, software para la realización de copias de seguridad, base de datos servidores y software de aplicación.

Lo más importante, el administrador tiene cuidado de los usuarios de la red, respondiendo a sus preguntas, escuchar sus problemas, y resolver sus problemas.

Cuando las tareas de administración se realizan en una red grande y compleja, este conjunto de tareas han de abarcarse de manera dedicada, es decir, poseer una o varias personas realizando únicamente las tareas de administración de la red. Esto debe ser así debido a que las redes tiende a ser volátiles en el sentido de:

- Los usuarios de la red cambian constantemente.
- Los equipos fallan.

- Se producen conflictos entre las distintas aplicaciones.
- En general, una red compleja sufre continuos estados de crisis.

Por el contrario, las redes de menor tamaño y por ello menos complejas son generalmente mucho más estables. Suele ser habitual que una vez puesta en funcionamiento una red sencilla no tenga que sufrir continuas y complejas tareas de administración ya sean de hardware o software.

En este tipo de redes pequeñas los problemas también aparecen, pero como intervienen un reducido número de equipos es normal que sean sencillos, pocos y distantes entre sí.

Independientemente del tamaño de una red, un administrador debe cubrir las siguientes tareas que son comunes a cualquier tipo de red:

- Involucrarse y formar parte en la toma de decisiones para la adquisición de nuevo equipamiento, servidores, equipos, impresoras, etc.
- Establecer las acciones necesarias para el correcto funcionamiento cada vez que se añada un nuevo equipo, es decir, un administrador de red cuando se integra un nuevo elemento a la red se encarga de introducir cambios en la configuración del cableado, de asignar un nombre de red al nuevo equipo, integrar a un nuevo usuario en el sistema de seguridad garantizando además sus privilegios.
- Estar al corriente de las actualizaciones de software que publiquen los proveedores y considerar si sus nuevas características son suficientes para justificar una posible actualización.

En la mayoría de los casos, la parte más difícil de un proceso de actualización de software es la determinación del camino a seguir, como llevar a cabo la actualización de toda la red afectando lo menos posible al funcionamiento de los usuarios. Esto suele ser aún más crucial si el software a actualizar es el sistema operativo de red, puesto que cualquier cambio en el puede afectar a toda la red.

Dentro de este procesos de actualización también intervienen afectando en menor medida a la estabilidad del sistema los parches y Service Packs que publican los proveedores para actualizar sus soluciones y que solventan problemas menores.

- Realizar tareas rutinarias como la realización de copias de seguridad de los servidores, la administración del historial de datos o la liberación de espacio en los discos duros. Gran parte de la tareas de administración de una red consisten en asegurarse de que todo funcione correctamente, buscando y corrigiendo los problemas que puedan tener los usuarios.
- Recopilar, organizar y controlar el inventariado de toda la red, para poder solventar en el menor tiempo posible cualquier imprevisto.

60.1.2 *Administración y gestión de redes*

El concepto de administración tiene asociado muchos significados. Desde un punto de vista informal, la gestión de redes se refiere a las actividades relacionadas con el funcionamiento de una red, junto con la tecnología necesaria para apoyar estas actividades. Otro aspecto de importancia en la gestión de una red es la monitorización de la misma, es decir, entender en todo momento que es lo que está sucediendo en la red.

Desde un enfoque software, la gestión de redes hace referencia al conjunto de actividades, métodos, procedimientos y herramientas que

intervienen en las operaciones de administración, mantenimiento y aprovisionamiento de los sistemas existentes dentro de la red.

Supone además garantizar toda la oferta operativa de servicios manteniendo la red en marcha y funcionando sin problemas. Para conseguir esto se hace imprescindible la utilización de herramientas para la monitorización de la red, que ofrezcan la detección de problemas tan pronto como sea posible, incluso antes de que algún usuario se vea afectado.

La administración abarca a su vez las tareas de seguimiento de los recursos en la red y de cómo estos se asignan, haciendo uso de todos los procesos o acciones de limpieza de la red que sean necesarias para mantener todo bajo el control del administrador o administradores.

El proceso de *mantenimiento*, que se ocupa de realizar las operaciones de reparación y mejora, ha de llevar a cabo tareas como el reemplazo de una tarjeta de red, actualización del sistema operativo de un router, añadir un nuevo switch al entramado de red. El mantenimiento también implica medidas para la corrección y prevención, como por ejemplo, el ajuste de los parámetros necesarios de un dispositivo en función de las necesidades que se soliciten o intervenir cuando sea necesario para mejorar el rendimiento de la red en momentos puntuales.

Otro aspecto de la administración de una red es el *aprovisionamiento*, tarea que concierne a la configuración y adaptación de los recursos de red para dar soporte a los servicios ofertados. Un ejemplo de aprovisionamiento es el hecho de añadir las configuraciones necesarias en los sistemas para proporcionar el servicio de voz a un nuevo usuario.

60.1.2.1 Tareas de la gestión de red

Las tareas de gestión de una red se pueden caracterizar de la siguiente manera:



- QoS y Gestión del Rendimiento: un administrador de red debe supervisar y analizar periódicamente los routers, hosts y el funcionamiento de los enlaces y luego en función de los resultados obtenidos realizar una redirección del flujo de datos para evitar la sobrecarga de ciertos puntos de la red. Para realizar esta tarea de seguimiento de la red, existen herramientas que detectan rápidamente los cambios que se producen en el tráfico de una red.
- Gestión de fallos por la red: cualquier fallo en la red, enlaces, nodos, routers, fallos de hardware o software, debe ser detectado, localizado y respondido por la propia red, es decir, la propia red debe poseer mecanismos para intentar solventar por sí sola el mayor número de contingencias que se puedan producir.
- Gestión de la configuración: esta tarea implica el seguimiento de todos los dispositivos bajo gestión y la confirmación de que todos los dispositivos están conectados y funcionan correctamente. Si se produce un cambio inesperado en las tablas de enrutamiento, el administrador ha de descubrir el problema de configuración y solucionarlo lo antes posible para que ningún servicio ni usuario se vea afectado.
- Gestión de la seguridad: el administrador de red es el responsable de la seguridad de la red. Para poder manejar esta tarea se utilizan principalmente los firewalls, puesto que un firewall puede monitorizar y controlar los puntos de acceso a la red informando sobre cualquier intento de intrusión.
- Gestión de facturación y contabilidad: el administrador especifica a los usuarios de la red los accesos o restricciones sobre los recursos y se encarga de la facturación y de los cargos a los usuarios por el uso de los mismos.

60.1.2.2 Elementos de la gestión de red

La gestión de red está compuesta por tres componentes principales:

- **Centro de gestión:** compuesto por el administrador de red y sus oficinas o centros de trabajo. Normalmente el centro de gestión está compuesto por un grupo humano importante.
- **Dispositivos a gestionar:** conformado por el equipamiento de la red, incluido su software, que es controlado mediante el centro de gestión. Cualquier hub, bridge, router, servidor, impresora o módem es considerado un dispositivo que ha de ser gestionado.
- **Protocolo de gestión de la red:** es el conjunto de políticas que adopta el centro de gestión para controlar y manejar todos los dispositivos que conforman la red. El protocolo de gestión de red permite al centro de gestión conocer el estado de los dispositivos.

60.1.2.2.1 Estructura de Gestión de la Información (SMI, Structure of Management Information):

Define las reglas para nombrar los objetos y para codificarlos en un centro de gestión de una red, es decir, es un lenguaje mediante el cual se definen las instancias dentro de un centro de gestión de red.

El lenguaje SMI también ofrece construcciones del lenguaje de mayor nivel que, habitualmente, especifican los tipo de datos, el estado y la semántica de los objetos que contienen la información necesaria para realizar las tareas de gestión. Por ejemplo, la cláusula STATUS especifica si la definición del objeto es actual o está obsoleta.

Trabaja bajo el protocolo SNMP (Simple Network Management Protocol) definiendo los conjuntos de objetos dentro la gestión de información base (MIB).

60.1.2.2.2 La Gestión de la Información Base (MIB, Management Information Base)

Es un medio de almacenamiento de información que contiene los objetos que muestran el estado actual de una red. Debido a que los objetos tienen asociado información que se almacena en el MIB, este forma colecciones de objeto, en las que incluye las relaciones entre ellos, en el centro de gestión.

Los objetos se organizan de una forma jerárquica y se identifican por la notación abstracta ASN.1, lenguaje de definición de objetos. La jerarquía, conocida como ASN.1, es un árbol de identificadores de objeto en el cual cada rama tiene un nombre y un número, permitiendo así a la gestión de red identificar objetos por una secuencia de nombres o números desde la raíz al objeto.

60.1.2.2.3 Protocolo SNMP (Simple Network Management Protocol)

El Simple Network Management Protocol (SNMP) está diseñado para monitorear el rendimiento de los protocolos de red y de los dispositivos. Las unidades de datos del protocolo SNMP (PDUs) pueden ser transportadas en un datagrama UDP, por lo que su entrega en destino no está garantizada. Los dispositivos que se administran como los routers o hosts, son objetos y cada uno tiene una definición formal y MIB adapta una base de datos de información que describe sus características. Con este protocolo un gestor de red puede encontrar donde se localizan los problemas.

Se ejecuta sobre UDP y utiliza una configuración cliente-servidor. Sus comandos definen como realizar las consultas sobre la información de un servidor o como enviar esta hacia un cliente o hacia otro servidor.

La tarea principal del protocolo SNMP es la de transportar información entre los centro de gestión y los agentes que se ejecutan en representación



de los centros de gestión. Para cada objeto MIB que se gestiona se utiliza una petición SNMP para obtener su valor o para modificarla. Si un agente recibe un mensaje no solicitado o si una interfaz o dispositivo deja de funcionar, entonces el protocolo puede informar al centro de gestión del fallo que se está produciendo.

La segunda versión de este protocolo, SNMPv2, corre por encima de varios protocolos y tiene más opciones de mensajería, lo que resulta en una gestión más eficaz de la red. Tiene siete unidades de PDU, o mensajes:

1. **GetRequest.** Se utiliza para obtener un valor de objeto MIB.
2. **GetNextRequest.** Se utiliza para obtener el siguiente valor de un objeto MIB.
3. **GetBulkRequest.** Recibe múltiples valores, lo que equivale a GetRequests múltiples, pero sin necesidad de utilizar múltiples peticiones.
4. **InformRequest.** Es un mensaje de director a director de comunicación que se envían entre sí dos centros de gestión a distancia el uno del otro.
5. **SetRequest.** Es utilizado por un centro de gestión para inicializar el valor de un objeto MIB.
6. **Response.** Es un mensaje de respuesta a una petición de tipo PDU.
7. **Trap.** Notifica a un centro de gestión de un evento inesperado.

Hay dos tipos de representación de PDUs, Get o Set y Trap.

- El formato de PDU de Get o Set es el siguiente:
 - o *PDU type*, indica uno de los siete tipos de PDU.



- o *Request ID*, es un ID que se utiliza para verificar la respuesta de una solicitud. Por lo tanto un centro de gestión puede detectar peticiones perdidas o duplicadas.
- o *Error status*, sólo es usado por PDUs *Response* para indicar tipos de errores reportados por un agente.
- o *Error index*, es un parámetro que indica a un administrador el nombre del objeto que ha causado el error.

Si las solicitudes o respuestas se pierden, el protocolo no realiza un reenvío. Los campos *Error status* and *Error index* son todo ceros excepto para las PDUs *GetBulkRequest*

- El formato de PDU de Trap es:
 - o *Enterprise*, para usar en múltiples redes.
 - o *Timestamp*, para realizar las mediciones de tiempo.
 - o *Agentaddress*, para indicar que la dirección del agente gestor está incluida en la cabecera PDU.

60.2 VIRTUALIZACIÓN DEL ALMACENAMIENTO

Gracias a la introducción de redes de gran capacidad y servidores de alto rendimiento, combinado con los nuevos sistemas de almacenamiento desarrollados en gran medida gracias al avance de las tecnologías en este campo, el campo de la virtualización orientado al almacenamiento se ha convertido en uno de los sectores más dinámicos en el campo de las TIC.

La tendencia general en las grandes empresas e instituciones hoy en día se orienta a la disposición de tecnologías de almacenamiento en red, que permitan mantenerla accesible, a la par que protegida. Las empresas, instituciones y gobiernos hoy en día dependen de la información, que no deja de ser datos sin procesar o interpretar, que en última instancia residen en algún lugar de los medios de almacenamiento. Por tanto, es necesario establecer los mecanismos adecuados para proteger esa información y facilitar su acceso a la vez que proporcionar medios para simplificar su gestión.

Aproximadamente desde los años 90, los sistemas de almacenamiento han ido sufriendo un proceso evolutivo constante. La introducción de tecnología de fibra óptica ha propiciado el despliegue de sistemas de almacenamiento distribuido, basados en NAS (Network-Attached Storage), así como agrupación de servidores de discos o acceso compartido a los sistemas de almacenamiento de cinta. Cada uno de estos avances técnicos ha ido acompañado por una ruptura en las prácticas anteriores, dado que la operativa para sustituir y trabajar con nuevos modelos de almacenamiento, a medida implicaba un cambio operacional importante.

Actualmente las nuevas soluciones tratan de simplificar este tipo de situaciones aplicando técnicas de abstracción que permiten acceder de forma transparente a los recursos de almacenamiento. Aquí es donde la

virtualización adquiere un papel importante. La virtualización pretende abstraer de forma lógica los sistemas de almacenamiento físico, y por lo tanto, cuando está bien empleado, oculta la complejidad de los dispositivos y simplificando la gestión de los sistemas de almacenamiento, lo que ayuda a reducir los costes de gestión.

En la actualidad no hay ningún organismo internacional que esté definiendo un modelo estándar para los protocolos y arquitecturas relacionadas con la virtualización del almacenamiento. El único trabajo destacable es el realizado por la SNIA (Storage Networking Industry Association), que ha redactado un informe sobre el estado actual de las tecnologías de virtualización.

60.2.1 *Concepto de virtualización de almacenamiento*

El concepto de virtualización de almacenamiento se refiere a las herramientas que se utilizan para disponer de un entorno de almacenamiento con múltiples dispositivos y multilocalización de recursos, pero presentado de forma totalmente transparente al usuario.

La virtualización de almacenamiento a menudo se apoya en servidores de discos o servidores de almacenamiento que combinen diferentes tipos de tecnologías de almacenamiento como por ejemplo medios de rotación, discos duros tradicionales, o tecnologías de estado sólido como SSD o incluso memoria de acceso aleatorio dinámico.

Según la taxonomía de la SNIA (Storage Networking Industry Association) referente a la virtualización del almacenamiento, existen tres conceptos básicos que se deben destacar en el sistema de este tipo:

- Qué es lo que se está virtualizando: La virtualización se puede aplicar a una gran variedad de dispositivos de almacenamiento. Los discos físicos, compuestos de cilindros, pistas y sectores, se virtualizan conformando un disco virtual. Los sistemas de cinta, formados por una o muchas unidades de cinta, pueden ser

agrupados en una única unidad. Otro ejemplo pueden ser los sistemas de archivo que mediante virtualización pueden hacer de forma transparente el acceso a puntos del sistema de ficheros que se encuentren en máquinas remotas.

- **Dónde se realiza la virtualización:** Se refiere a la localización espacial en la cual se realiza la implementación ya que esta puede realizarse mediante matrices de almacenamiento, o en red a través de switches inteligentes o dispositivos conectados a SAN.
- **Cómo se implementa:** Hace referencia a cómo proporcionar los medios para construir servicios de alto nivel que oculten la complejidad de los componentes subyacentes y se permitan la automatización de las operaciones de almacenamiento de datos.

La idea es que ni clientes ni servidores necesiten saber donde están los archivos que se están procesando escondiendo la red física que existe entre ellos. Esto proporciona las siguientes funcionalidades:

- Permite sistemas de archivos distribuidos.
- Los dispositivos de almacenamiento remoto aparecen como si estuviesen conectados directamente al sistema.
- El sistema local no conoce dónde se encuentran o qué tipo de almacenamiento son.

Un ejemplo de virtualización de almacenamiento basado en host es la administración de volúmenes. La gestión de volúmenes permite presentar

una única vista lógica de un recurso de almacenamiento que puede estar formado por distintos dispositivos físicos.

Las principales ventajas de la virtualización del almacenamiento incluyen la optimización y reaprovechamiento de la capacidad de almacenamiento, la posibilidad de añadir o eliminar almacenamiento sin afectar a la disponibilidad de las aplicaciones, y la migración de datos sin interrupción.

Se aconseja la implantación de virtualización del almacenamiento en las organizaciones cuando se desean alcanzar los siguientes objetivos:

- Alta disponibilidad /Recuperación frente a desastres.
- En caso de que exista virtualización de aplicaciones.
- Cuando se necesita un acceso continuo a aplicaciones y datos y existe un sólo dispositivo e de almacenamiento. Conectado en red, mediante virtualización se pueden mejorar las prestaciones y la escalabilidad además de ofrecer mecanismos de tolerancia a fallos.
- Las políticas en las que se contemple procesamiento paralelo, o en las que se tenga en cuenta una escalabilidad global del sistema, deben contemplar virtualización del almacenamiento.
- Cuando múltiples sistemas trabajan en una tarea contra una única unidad de almacenamiento, puede disminuir notablemente el rendimiento de la misma. Mediante virtualización podemos conseguir que la carga de trabajo se extienda por una única unidad lógica de almacenamiento repartida en varias unidades físicas, lo que proporciona un mejor balanceo de la carga de trabajo.

60.2.2 *Tipos de virtualización de almacenamiento*

La virtualización del almacenamiento trata de proporcionar los mecanismos necesarios para asignar unidades de almacenamiento lógicas a usuarios y aplicaciones, independientemente de la ubicación de los dispositivos físicos, realizando las operaciones de forma transparente. La virtualización puede realizarse siguiendo la filosofía SAN o NAS. La principal diferencia es que en los entornos de virtualización SAN, la virtualización se aplica a nivel de bloque, mientras que en NAS se aplica a nivel de archivo.

- Virtualización a nivel de archivo (NAS): a este nivel, la virtualización se basa en la eliminación de las dependencias entre los datos de acceso a nivel de archivo y la ubicación donde se almacenan físicamente. Esto permite optimizar la utilización del almacenamiento y la consolidación de servidores para realizar migraciones con seguridad.
- Virtualización a nivel de bloque (SAN): en este nivel, se proporciona una capa de traducción en la SAN entre los usuarios y las matrices de almacenamiento que albergan los dispositivos físicos de almacenamiento. Cuando se accede a las unidades de almacenamiento, en lugar de redirigirse a la matriz de almacenamiento física identificada por un LUN (Logical unit number), se redirige hacia un LUN virtual, que reorganiza las matrices de almacenamiento físicas (identificadas por los LUN físicos), en función de las necesidades organizacionales. El dispositivo de virtualización es el que se encarga de realizar la traducción entre los LUN virtuales y LUN físicos.

60.2.3 *Otros tipos de virtualización*

Además del almacenamiento, la virtualización ha existido en la industria de las Tecnologías de la Información durante muchos años, y en diferentes formas. La idea de la virtualización representa, además de un mecanismo de abstracción, una técnica para el ahorro y la utilización eficiente de ciertos recursos críticos de la máquina. Dentro de las técnicas de virtualización aplicables a otros factores, destacan la virtualización de la red, virtualización de memoria, y en combinación virtualización de servidores.

60.2.3.1 *Virtualización de Memoria*

Aunque el coste de la memoria ha disminuido gracias a los avances tecnológicos, sigue siendo un recurso costoso. La virtualización de la memoria posibilita que las aplicaciones dispongan de su propia memoria continua, de forma independiente de los recursos de memoria física que exista en la máquina anfitriona.

Una de las implementaciones más habituales de memoria virtual es la conocida como paginación. En ésta, el espacio de direcciones de la memoria se divide en bloques contiguos de tamaño fijo que se denominan marcos de páginas. A su vez, los programas en ejecución se dividen también en trozos o páginas. Esto permite que el sistema operativo disponga de un proceso denominado Gestor de Memoria Virtual (VMM, Virtual Memory Manager) que permite optimizar el uso de la memoria recuperando de forma eficiente los “trozos” de las aplicaciones en ejecución a la memoria principal, y derivando a un almacenamiento secundario los “trozos” inactivos.

El sistema asigna al VMM un espacio en el disco, conocido como archivo SWAP, o partición SWAP. La SWAP conforma el espacio de intercambio, en

el que el VMM mantiene almacenadas las páginas en las que se dividen los procesos, guardando su contexto e información de estado. Esta parte del disco actúa como una memoria física (RAM) para el sistema operativo.

60.2.3.2 Redes de virtualización

La virtualización de redes se refiere al hecho de que cada aplicación que haga uso de la red para su funcionamiento pueda generar su propia red lógica e independiente de la red física. Un ejemplo concreto de este tipo de virtualización podrían ser las VLAN, que presenta un mecanismo de gestión de las redes menos costosa y más flexible.

Con una virtualización de tipo VLAN, un conjunto de usuarios de una red con unos requisitos de acceso a recursos similares, se pueden agrupar en la misma red virtual, permitiendo acceder a los recursos de esa VLAN sin importar en que red física real se encuentren esos recursos. Esto implica que todas las conexiones inter-red que se tengan que realizar para el acceso a los recursos compartidos, se harán de forma transparente, dando la impresión de que el acceso a los recursos se hace siempre a nivel local.

60.2.3.3 Virtualización a nivel de servidores

La virtualización de servidores aborda los problemas que existen en un entorno de servidor físico. La capa de virtualización ayuda a superar conflictos de recursos que permiten aislar aplicaciones que se ejecutan en diferentes sistemas operativos en la misma máquina. Además, la virtualización de servidores permite, de forma dinámica destinar los recursos de hardware al lugar donde más se necesiten.

60.3 GESTIÓN DEL CICLO DE VIDA DE LA INFORMACIÓN (ILM)

60.3.1 Gestión del Ciclo de Vida de los Datos

La gestión del ciclo de vida de los datos o DLM (Data Lifecycle Management) es un enfoque de la gestión de la información desde el punto de vista del manejo del flujo de los datos de un sistema de información durante todo su ciclo de vida, desde que se crean y se produce su primer almacenamiento, hasta que son declarados obsoletos y eliminados del sistema.

Los productos para la gestión del ciclo de vida de los datos tratan de automatizar los procesos que forman parte de este ciclo de vida. Organizan los datos en distintos niveles siguiendo unas políticas especificadas, y automatizan la migración o intercambio de los datos entre unos niveles y otros basándose para ello en los criterios especificados de cada uno.

Como norma general, los datos más recientes y aquellos a los que se accede con más frecuencia se tienden a almacenar en medios de almacenamiento más rápidos, pero también más caros, mientras que los datos de un nivel menos crítico se almacenan en los dispositivos más baratos y más lentos.

Las arquitecturas que gestionan el ciclo de vida de los datos suelen incluir un sistema de archivos que indexa toda aquella información crítica y aquella considerada no tan crítica pero que guarda relevancia o relación que esta. Con esta información crea copias de respaldo, los almacena en ubicaciones seguras para evitar manipulaciones pero que puedan ser accesibles de una manera segura y confiable.

Estas arquitecturas también se encargan de las posibles duplicaciones de datos y de la comprensión de los mismos para garantizar un correcto y eficiente uso del espacio de almacenamiento disponible.

Desafortunadamente, muchas implementaciones de DLM de negocios se han estancado, principalmente porque las empresas no han logrado definir ni las políticas de migración adecuadas ni el archivado de datos. Dado que esas políticas necesitan reflejar las prioridades de regulación y de negocio, en sus definiciones es necesario una colaboración que involucre no solo a miembros del departamento de tecnologías de la información, sino también a miembros de diferentes departamentos del negocio.

Por otro lado, el criterio más sencillo para realizar una migración de la información a un sistema de almacenamiento más económico es el temporal, es decir, los datos más antiguos en los sistemas más lentos y baratos. Sin embargo, las empresas en industrias altamente reguladas a menudo quieren ir más lejos, estableciendo la clasificación de los datos en función de la rapidez con la que se precisen, o la frecuencia con la que se accede a ellos, o en base a quien los ha enviado o recibido, o en base a un conjunto de palabras clave o cadenas numéricas, etc. Entonces el reto está en conseguir definirlos de tal manera que sea viable realizarlo en el tiempo y mediante la menor intervención humana.

60.3.2 *Gestión del Ciclo de Vida de la Información*

La gestión del ciclo de vida de la información o ILM (Information Lifecycle Management) es un enfoque integral para el manejo del flujo de los datos de un sistema de información y los metadatos asociados desde su creación y almacenamiento inicial hasta el momento en que estos se vuelven obsoletos y son borrados.

A diferencia de anteriores enfoques para la gestión de almacenamiento de datos, ILM abarca todos los aspectos en los que se tratan los datos,

partiendo de las prácticas de los usuarios, en lugar de la automatización de los procedimientos de almacenamiento y en contraste con los sistemas más antiguos, ILM permite criterios mucho más complejos para la realización de la gestión del almacenamiento que la antigüedad de los datos o la frecuencia de acceso a ellos.

Es importante destacar que ILM no es sólo una tecnología sino que integra los procesos de negocio y TI con el fin de determinar cómo fluyen los datos a través de una organización, permitiendo a los usuarios y administradores gestionar los datos desde el momento que se crean hasta el instante en el que ya no son necesarios.

Aunque los términos gestión del ciclo de vida de los datos (DLM) y gestión del ciclo de vida de la información (ILM) a veces se utilizan indistintamente, ILM se considera un proceso más complejo.

La clasificación de los datos en función de valores del negocio es una parte integral y muy importante del proceso ILM. Esto quiere decir que ILM reconoce que la importancia de los datos no se basa únicamente en su antigüedad o en su frecuencia de acceso, sino que ILM espera que sean los usuarios y los administradores los que especifiquen distintas directivas para que los datos vayan variando de una manera decreciente su relevancia o grado de importancia para la organización, o que puedan conservar su importancia durante todo su ciclo de vida, etc.

Para una exitosa y eficiente implementación de ILM se necesita que la organización identifique requisitos de seguridad de los datos críticos e incluirlos en sus procesos de clasificación. Los usuarios de los datos, tanto los individuos como las aplicaciones, deben de ser identificados y categorizados en función de las necesidades asociadas con sus tareas.

Algunas de las mejores prácticas relacionadas con la implementación de ILM comparten enfoques como:

- Se centran en la productividad del usuario con el fin de obtener una ventaja estratégica a través del acceso a los datos necesarios.
- Proteger los datos contra el robo, la mutilación, la divulgación involuntaria, o la eliminación.
- Crear múltiples capas de seguridad, sin crear una gestión excesivamente compleja.
- Asegurarse que los procesos de seguridad están incorporados en los procesos generales del negocio y en los procesos de TI.
- Utilizar estándares y modelos de referencias con el fin de satisfacer únicamente las necesidades de seguridad de la organización.

Por supuesto, cada organización deberá desarrollar e implementar su propia solución de seguridad de almacenamiento, que debe seguir evolucionando, adaptándose a las nuevas oportunidades, amenazas y capacidades.

60.3.3 *Alguna soluciones para la gestión*

60.3.3.1 Microsoft

Microsoft Identity Lifecycle Manager ofrece una solución integrada y completa para la gestión del ciclo de vida de las identidades de usuario y sus credenciales asociadas. Esta solución aporta la sincronización de identidades, los certificados y administración de contraseñas y suministro de usuarios. La solución funciona bajo plataformas Windows y otros sistemas organizacionales.

60.3.3.2 IBM

Las soluciones de IBM para la gestión del ciclo de vida de la información se han agrupado en cinco categorías (IBM, 2008):

- *Archivo de correo electrónico* (IBM DB2 CommonStore, VERITAS Enterprise Vault, OpenText-IXOS Livelink)
- *Aplicación y base de datos de archivo* (Archivo Activo de Princeton Softech),
- *Gestión del ciclo de vida de los datos* (TotalStorage de IBM SAN File System)
- *Gestión de contenidos* (repositorio de administración de contenido, DB2 Content Manager)
- *Gestión de registros* (IBM DB2 Records Manager).

60.3.3.3 Oracle

Oracle ILM Assistant es una herramienta que se basa en una interfaz gráfica de usuario para la gestión de entorno de ILM. Ofrece la posibilidad de crear definiciones de ciclo de vida, que se asignan a las tablas en la base de datos. Posteriormente basándose en las políticas establecidas sobre el ciclo de vida, ILM Assistant informa cuando es el momento para mover, archivar o suprimir los datos. También muestra las necesidades de almacenamiento y el ahorro de costes asociados con el cambio de ubicación de los datos.

Otras capacidades de Oracle ILM Assistant incluyen la habilidad de mostrar cómo particionar una tabla basada en una definición del ciclo de vida, y poder simular los eventos para comparar el resultado en caso de que la tabla fuera particionada.

60.4 BIBLIOGRAFÍA

- G. Somasundaram, Alok Shirvastava “Information, Storage and Management: Storing, Managin and Protecting Digital Information”. John Wiley & Sons. April 06, 2009. ISBN:978-0-470-29421-5
- Jason Buffington “Data protection for Virtual Data Centers”. Sybex. August 02, 2010. ISBN: 978-0-4705-7214-6
- Doug Lowe “Networking for Dummies”. John Willey & sons. May 29, 2007. ISBN: 978-0-470-05620-2
- Mani Subramanian, Timothy A. Gonsalves, N. Usha Rani “Network Management: Principles and Practice”. Pearson Education India. 2010. ISBN: 978-8-131-72759-1
- Nader F. Mir “Computer and Communication Networks”. Prentice Hall. November 02, 2006. ISBN: 978-0-13-174799-9
- Theo Schlossnagle, “Scalable Internet Architectures”. Sams. July 21, 2006. ISBN:978-0-672-32699-8
- Tom Petrocelli “Data Protection and Information Lifecycle Management”. Prentice Hall. September 23, 2005. ISBN: 978-0-13-192757-5

Autor: Francisco Javier Rodriguez Martínez

Subdirector de Sistemas Escola Superior Enxeñaría Informática Ourense

Colegiado del CPEIG

**61. REDUNDANCIA HARDWARE.
ALTA DISPONIBILIDAD A NIVEL
DE SISTEMA OPERATIVO.
SISTEMAS DE CLÚSTER Y
BALANCEO DE CARGA. ALTA
DISPONIBILIDAD EN
SERVIDORES DE
APLICACIONES Y SERVIDORES
DE BASES DE DATOS. ALTA
DISPONIBILIDAD A NIVEL DE
APLICACIÓN. DISPONIBILIDAD
EN ENTORNOS
VIRTUALIZADOS. CENTROS DE
PROTECCIÓN GEOGRÁFICOS.
PLANES DE CONTINGENCIA.**

Tema 61: Redundancia hardware. Alta disponibilidad a nivel de sistema operativo. Sistemas de clúster y balanceo de carga. Alta disponibilidad en servidores de aplicaciones y servidores de bases de datos. Alta disponibilidad a nivel de aplicación. Disponibilidad en entornos virtualizados. Centros de protección geográficos. Planes de contingencia.

ÍNDICE

61.1 REDUNDANCIA HARDWARE.....	2
61.1.1 REDUNDANCIA EN DISCO RAID.....	4
61.1.1.1 RAID 0.....	4
61.1.1.2 RAID 1.....	5
61.1.1.3 RAID 5.....	6
61.2 ALTA DISPONIBILIDAD A NIVEL DE SISTEMA OPERATIVO.....	8
61.2.1 ALTA DISPONIBILIDAD.....	8
61.2.2 ALTA DISPONIBILIDAD A NIVEL DE SISTEMA OPERATIVO.....	8
61.3 SISTEMAS DE CLÚSTER Y BALANCEO DE CARGA.	10
61.3.1 CONCEPTO DE CLÚSTER.....	12
61.3.2 TIPOS DE CLUSTERS.....	14
<i>Clusters HPCC (High Performance Computing Cluster): Cluster de Alto Rendimiento</i>	14
<i>Clusters HA (High Availability): Cluster de Alta Disponibilidad.....</i>	16
61.3.3 BALANCEO DE CARGA.....	18
61.4 ALTA DISPONIBILIDAD EN SERVIDORES DE APLICACIONES Y SERVIDORES DE BASES DE DATOS.....	20
61.4.1 ALTA DISPONIBILIDAD EN SERVIDORES DE APLICACIONES.....	20

61.4.2 ALTA DISPONIBILIDAD A NIVEL DE BASES DE DATOS.....	21
61.5 ALTA DISPONIBILIDAD EN ENTORNOS VIRTUALIZADOS.....	25
61.5.1 VIRTUALIZACIÓN DE HARDWARE.....	25
61.5.2 VIRTUALIZACIÓN DE SISTEMA OPERATIVO.....	26
61.6 CENTROS DE PROTECCIÓN GEOGRÁFICOS.....	26
61.7 PLANES DE CONTINGENCIA.....	29
61.7.1 CICLO DE VIDA.....	30
61.7.2 CARACTERÍSTICAS.....	31
61.7.3 OBJETIVO.....	32
61.7.4 PUNTOS CLAVE.....	32
61.7.5 ELEMENTOS.....	33
61.8 BIBLIOGRAFÍA.....	34

61.1 Redundancia Hardware

La redundancia de hardware consiste en la replicación de elementos hardware de reserva en la configuración de un determinado sistema para proporcionar tolerancia a fallos, de forma que a en un caso de contingencia por fallo de alguno de los componentes principales, alguna de las réplicas se active para seguir proporcionando servicio sin que el sistema se caiga.

Dentro de los sistemas de protección contra fallos basados en la redundancia de hardware, existen un cierto tipo de componentes determinados como críticos que suelen ser los que se replican:

Fuentes de alimentación: La idea de replicación de fuentes de alimentación consiste básicamente en replicar las fuentes de alimentación interna del servidor o máquina sobre la que estamos implementando la tolerancia a fallos. Además, y como medidas de apoyo, puede instalarse

unidades de alimentación eléctrica ininterrumpida (SAI) para mitigar las caídas de suministro eléctrico de la red, o incluso, la instalación de grupos electrógenos alternativos para los casos en los que tratamos con centros de proceso de datos con varios servidores o unidades que controlan sistemas críticos.

Núcleos de proceso: Es habitual, sobre todo con las nuevas unidades de microprocesadores multinúcleo, replicar las unidades de proceso que se integran en los servidores proporcionando mecanismos de control para la degradación del sistema que consisten en gestionar el fallo de los microprocesadores balanceando la carga de proceso a las unidades restantes que quedan activas.

Dispositivos de conexión a la red: Al igual que en los casos anteriores, la idea consiste en eliminar el cuello de botella que puede suponer el disponer de una única toma de conexión a la red que presenta la interfaz de conexión a la máquina y a los servicios que presta. Por ello la tendencia suele ser establecer como mínimo dos interfaces de red físicas en la máquina para poder disponer de una interfaz alternativa en caso de contingencia, que nos permita mantener en sistema en línea.

Dispositivos de almacenamiento: En cuanto a la replicación de los sistemas de almacenamiento, la tendencia general consiste en la replicación de los dispositivos de almacenamiento masivo como los discos duros o cintas magnéticas. En el caso de los discos duros que se encuentran en los servidores, la tendencia general es aplicar una configuración de tipo RAID en alguno de sus niveles avanzados, que presentan redundancia de datos y tolerancia a fallos con ciertas garantías.

Cabe destacar que, la mayoría de los sistemas operativos sobre servidores deben implementar una característica, de alta disponibilidad, que permita realizar mantenimiento y sustitución de elementos hardware replicados que hayan sufrido algún fallo, sin necesidad de detener el sistema.

61.1.1 Redundancia en Disco RAID

Las estrategias de backup que hacen uso de discos habitualmente siguen algún modelo de sistema RAID (Redundant Array of Independent Disks, conjunto redundante de discos independientes). La estrategia consiste en utilizar un conjunto de discos en los cuáles se distribuyen o replican los datos. Existen diferentes configuraciones o niveles de RAID que determinan las características de la arquitectura y definen una serie de ventajas con respecto al uso de un único disco o al uso de otros niveles de RAID inferiores. Estas ventajas están relacionadas con la integridad de los datos, la tolerancia a fallos, la capacidad y el rendimiento.

Habitualmente los niveles de RAID se gestionan mediante controladoras especializadas a nivel de hardware, creando desde el nivel más simple hasta niveles complejos, matrices redundantes de discos independientes, que a alto nivel se reflejan como unidades lógicas únicas.

Los modelos de RAID estándar son los Niveles 0 a 6, y sus combinaciones o anidaciones que dan lugar a los niveles 0+1 y 1+0 o RAID10. Existen más niveles de RAID por combinación o anidación de los estándares existentes, así como soluciones o modelos propietarios. Dentro de todo el abanico de posibilidades que existen, los más habituales son los niveles RAID0, RAID1 y RAID5.

61.1.1.1 RAID 0

El nivel RAID 0, también conocido como striping, consiste en la utilización de dos o más discos entre los que se distribuye la información de forma equitativa. Es un modelo o nivel en el que no existe información adicional de paridad ni se proporciona redundancia, por lo que en algunos círculos esta configuración no se considera como modelo de RAID original. Como contrapartida, este modelo proporciona un alto rendimiento dado que permite la escritura y acceso a los datos de forma simultánea en tantos dispositivos como estén configurados.

La configuración mostrará una única unidad virtual (dos o más discos físicos subyacentes) cuyo tamaño total dependerá del disco físico que

tenga menor capacidad dentro del conjunto de los discos utilizados. Es decir, si disponemos de un nivel de RAID 0 con tres discos A, B y C, y cada uno de ellos con 400GB, 350GB y 300GB respectivamente, nuestro nivel RAID 0 presentará una única unidad lógica con una capacidad de 900GB.

Esto implica que es posible la configuración de un nivel de RAID 0 con discos de diferente capacidad. Sin embargo, lo recomendable siempre para este tipo de configuraciones es el uso de capacidades similares.

Para determinar la fiabilidad de un RAID 0 existe una fórmula sencilla que consiste en calcular la fiabilidad media de cada disco entre el número de discos utilizados en la configuración.

61.1.1.2

RAID 1

En RAID 1, también conocido como mirroring, se crea una copia exactamente igual de un conjunto de datos en uno o más discos. Este modelo proporciona un alto rendimiento en cuanto a lectura además de incrementar la fiabilidad global del sistema dado que ambos discos son una copia exactamente igual. En contraposición existe un menor desaprovechamiento del espacio dado que sólo se utiliza el equivalente al espacio de un disco físico.

La implementación de técnicas de splitting o duplexing, consistentes en configurar cada uno de los discos en controladoras independientes, maximiza ese rendimiento mejorado en cuanto a la lectura de datos, dado que se pueden estar leyendo de ambos dispositivos de forma simultánea.

Para las operaciones de escritura, el conjunto se comporta como un único disco dado que los datos deben ser escritos en todos los discos del RAID 1.

El RAID 1 proporciona una gran ventaja en cuanto a la administración en entornos de producción continua, dado que permite la posibilidad de inactivar uno de los discos espejo para realizar sobre él copias de

seguridad, sin necesidad de tener que apagar el sistema y proporcionando tiempo de servicio extra para ese tipo de tareas de mantenimiento.

61.1.1.3

RAID 5

El RAID 5 se compone de un mínimo de 3 discos para su implementación. Es un sistema RAID muy popular gracias a que proporciona, además de eficiencia en operaciones de lectura y escritura, redundancia a un coste realmente muy bajo.

RAID 5 realiza una división de los datos en forma de bloques (stripes), distribuyendo cada bloque por uno de los discos físicos que forman el RAID 5. Además, realiza un control de paridad de cada conjunto de bloques distribuidos por los discos. El almacenamiento de estos bloques de paridad se va alternando entre los diferentes discos que forman el RAID, de forma que permite establecer un sistema de redundancia con garantías.

La idea es que cada vez que un bloque de datos se escribe en un RAID 5, se genera un bloque de paridad dentro de la misma división. En caso de modificar los datos del bloque, o añadir datos nuevos al bloque, la paridad se recalcula y se escribe en su espacio asignado. El bloque utilizado para escribir la paridad está escalonado en cada división. Por tanto todos los discos que forman parte de un RAID 5 albergan bloques de datos y bloques de paridad. De ahí el término de “bloques de paridad distribuidos”.

La desventaja de este nivel de RAID es que las operaciones de escritura son costosas, dado que hay que realizar el coproceso de cálculo de paridad para la escritura. De hecho, en las implementaciones de RAID 5 se presenta un rendimiento malo en el caso de realizar muchas operaciones de escritura cuyo tamaño del bloque es menor que el tamaño de una división. En las operaciones de lectura, el bloque de paridad asociado no se lee, a no ser que se produzca un error en la comprobación de paridad de los datos leídos.

En caso de fallo de uno de los bloques de datos durante la lectura, automáticamente se recupera la paridad asociada a ese bloque para recuperar los datos y reconstruir el sector erróneo de forma transparente al

usuario. De la misma forma, si uno de los discos de RAID 5 falla, los bloques de paridad restantes de los demás discos permiten reconstruir los bloques de datos bajo demanda del disco que ha fallado. De ahí que al menos se necesiten tres discos para una implementación de este nivel de RAID. El fallo de un segundo disco dentro de RAID 5 provoca la pérdida completa de los datos.

Teóricamente, en número máximo de discos que se pueden utilizar para implementar un RAID5 es ilimitado, sin embargo la tendencia general consiste en limitar ese número dado que a mayor cantidad de discos, mayor probabilidad de fallo simultáneo.

61.2 Alta disponibilidad a nivel de sistema operativo.

61.2.1 Alta disponibilidad

El concepto de alta disponibilidad, o High Availability en inglés, consiste en el diseño de arquitecturas de sistemas cuyas implementaciones aseguren un grado de continuidad de las operaciones que lleven a cabo. Se trata fundamentalmente de prever contingencias que puedan desembocar en la suspensión de los servicios proporcionados por el sistema que se diseña, de forma que puedan ser controlables, y dichos mecanismos de control permitan que el sistema mantenga todas las funcionalidades que se ponen a disposición de los usuarios. Además de contingencias, se tratan de prever y soportar otras tareas que en un sistema normal provocan la suspensión temporal, como pueden ser tareas de mantenimiento o actualización. Los sistemas que habitualmente necesitan garantizar grados absolutos de alta disponibilidad son aquellos destinados al control de tareas críticas.

Como se detalla a continuación, existen diferentes orientaciones a la hora de dotar a los sistemas de alta disponibilidad, que pueden estar implementadas a nivel de sistema operativo, a nivel de aplicaciones, o incluso haciendo uso transparente de redundancia de equipos mediante la configuración de clústers.

61.2.2 Alta disponibilidad a nivel de sistema operativo

Los sistemas operativos proporcionan también los mecanismos necesarios para complementar las funcionalidades que proporcionan alta disponibilidad del sistema. Los más habituales suelen ser los siguientes:

Capacidad para poder gestionar réplicas a nivel software de volúmenes o particiones del sistema. Consiste básicamente en una simulación del nivel 1 de RAID basado en software.

El sistema de ficheros además debe permitir la generación de tablas con las que pueda localizar archivos redundantes en otras estructuras redundantes, de forma que proporcione las operaciones de acceso de

Algunos ejemplos componentes software que proporcionan esta funcionalidad a nivel de sistema operativo son:

HP MirrorDisk/UX basada en Unix para servidores de la casa HP.

Sun Solaris Volume Manager para sistemas operativos basados en Solaris de Sun

Windows Disk Administrator para sistemas operativos Windows.

Todas estas herramientas basan su funcionamiento en la gestión de discos dinámicos, facilitando la creación y gestión de volúmenes que proporcionan la creación de espejos, implementando un nivel de RAID 1 por software.

En los sistemas operativos que se basan en Unix, la capacidad de gestionar un sistema de ficheros que permite redundancia viene proporcionada por el sistema de ficheros NFS (Network File System). Mediante la agrupación de máquinas en forma de clúster se posibilita a nivel hardware la alta disponibilidad mediante replicación de máquinas. El sistema operativo interviene al implementar NFS como servicio, permitiendo integrar en el clúster servidores de ficheros ofreciendo de forma transparente una interfaz que permite utilizar un único sistema de ficheros redundante sobre el clúster.

Otra característica a nivel de sistema operativo que proporciona la capacidad de alta disponibilidad consiste en la implementación de journaling. El journaling es una característica de los sistemas de gestión de ficheros transaccionales que mantiene un fichero de log en el que se almacenan los cambios que se van produciendo en el disco. Esto proporciona la posibilidad de poder realizar una recuperación de los datos en caso de que se produzca un error en el sistema. En caso de fallo, el procedimiento consiste en la reconstrucción de ese fichero de log principal, comúnmente llamado journal, para recuperar la integridad de todo el sistema de ficheros. Entre los sistemas de ficheros que implementan las características de journaling se encuentran algunos como Ext3, Ext4 y JFS de Linux, NTFS de Windows, UFS de SUN Solaris, y HFS de Mac OS X.

Otras características que permiten mantener una alta disponibilidad de los sistemas consisten en:

Capacidad para aplicación de parches y actualizaciones sin necesidad de reiniciar el sistema. Esto proporciona que disminuya el tiempo en las tareas de mantenimiento así como evitar los cortes del servicio en caso de actualización.

Capacidad del sistema operativo para la gestión de dispositivos hardware que puedan ser conectados y agregados en caliente, es decir, sin necesidad de tener que apagar el sistema.

Otra característica implementada es la tolerancia a fallos provocados por hardware, implementando lo que se conoce como sistemas degradables, que permiten gestionar estos fallos de hardware sin que se produzca una detención de los servicios proporcionados a los usuarios ni una detención del sistema.

61.3 Sistemas de clúster y balanceo de carga.

El concepto de clúster sirve para definir un conjunto de ordenadores contruidos utilizando componentes de hardware comunes y que se agrupan proporcionando la vista lógica de un único equipo para realizar tareas de procesamiento. Gracias al avance de la tecnología de clustering, actualmente esta filosofía de construcción de centros de procesamiento permite su aplicación en campos que abarcan desde la supercomputación, sistemas críticos, servidores Web o comercio electrónico, hasta bases de datos de alto rendimiento. En la actualidad, los principios de clustering y la creación agrupaciones de máquinas para el procesamiento de datos desempeña un papel importante para la resolución de problemas de cálculo y modelado de simulaciones en todos los campos científicos y de conocimiento.

La utilización de clusters viene derivada del desarrollo de tecnológico actual, en el que la disponibilidad de microprocesadores económicos e infraestructura de comunicaciones de alta velocidad proporcionan la base hardware necesaria para su diseño, y el desarrollo de herramientas de software para cómputo distribuido de alto rendimiento proporciona los mecanismos para la puesta en producción. Por tanto, podemos entender los clústers como un conjunto de múltiples equipos interconectados a través de una red de datos habitualmente de alta velocidad, y que forman una vista lógica de equipo único. Esta vista lógica proporcionada presenta un ordenador mucho más potente, y con ciertas capacidades intrínsecas que permiten proporcionar alta disponibilidad y gran capacidad de proceso, a un coste comparativo mucho más reducido que un equipo real con las mismas características de procesamiento.

Según el tipo de ordenadores que forman parte de un clúster, éstos pueden seguir tres tendencias:

- Si todos tienen los equipos tienen misma configuración hardware y sistema operativo, hablamos de un clúster homogéneo.
- Si el hardware es distinto, pero la arquitectura y sistemas operativos son similares, entonces hablamos de un clúster semi-homogéneo.
- Finalmente, si el hardware y sistema operativo de cada equipo es diferente hablamos de un clúster heterogéneo.

Esta versatilidad a la hora de escoger entre las máquinas que finalmente formarán parte del clúster es lo que proporciona flexibilidad económica y facilidad para su construcción.

El último elemento que se necesita para que un clúster finalmente se ponga en producción es el sistema de manejo del clúster. Este sistema será

el que se encargue de interactuar con el usuario y los procesos que corren en el propio clúster, para optimizar el funcionamiento distribuyendo las cargas de proceso y proporcionando al usuario la vista transparente de equipo único.

Debido a que existen una diferente tipología de clusters que se pueden configurar, el tipo de software final que gestione esas capacidades debe ser específico. Independientemente de las diferentes especializaciones, existen dos modelos generales a la hora de desarrollar software que compone el clúster:

- **Software a nivel de aplicación:** En el que habitualmente se utilizan bibliotecas que permiten realizar la abstracción de un nodo a un sistema integral, facilitando el desarrollo de aplicaciones distribuidas. Estas bibliotecas proporcionan funciones para la construcción de rutinas. Estas rutinas serán tratadas por el clúster como unidades que pueden ser procesadas de forma independiente en cualquiera de los nodos del clúster, realizando la comunicación a través de la red.
- **Software a nivel de sistema:** En este tipo, habitualmente el propio sistema operativo cuenta con implementación interna para la gestión de este tipo de tareas. Suelen ser sistemas operativos específicos para la construcción de clústers.

61.3.1

Concepto de clúster

La definición de clúster es compleja y para nada sencilla, hasta el punto de que en la actualidad, incluso el personal especializado en el campo de la supercomputación y clustering tiene problemas para delimitar realmente cuáles son los límites de la definición.

A nivel general, podemos definir un clúster como un conjunto de ordenadores unidos por una red de alta capacidad y que realizan tareas de procesamiento conjunto. Según el tipo de tareas a las que el clúster esté orientado, se pueden distinguir clústers de alta disponibilidad, alto rendimiento o clústers dedicados al balanceo de carga..

También se hace referencia a la arquitectura utilizada para la configuración de los clústers, distinguiendo entre clústers SMP y clusters formados por nodos monoprocesadores. Hay arquitecturas clusters que se denominan constelaciones y se caracterizan por que cada nodo contiene más procesadores que el número de nodos. A pesar de todo, las constelaciones siguen siendo clusters de componentes o nodos aventajados y caros. De hecho entre las máquinas que aparecen en el top500 existen unos pocos clusters que pertenecen a organizaciones que no son gigantes de la informática, lo cual indica el precio que pueden llegar a tener estos sistemas.

La definición que tomaremos como formal y más aproximada al conjunto de definiciones que se pueden encontrar en la bibliografía general que versa sobre el tema es la siguiente:

Un clúster consiste en un conjunto de máquinas denominadas nodos, que en conjunto alcanza una gran capacidad de proceso y que está orientado al procesamiento paralelo de grandes cantidades de datos, realizándolo de forma transparente.

61.3.2

Tipos de clusters

Clusters HPCC (High Performance Computing Cluster): Cluster de Alto Rendimiento

Un clúster de alto rendimiento será aquel tipo de clúster que está especialmente diseñado para ofrecer una gran capacidad de cálculo. A la hora de enfrentarse a un problema fundamentalmente basado en la realización de cálculo, las principales fortalezas que nos proporcionan los clústers están ligadas a dos aspectos:

- El tamaño del problema por resolver: En muchas ocasiones, los problemas tienden a redefinirse y recalcularse, o a generar nuevas especificaciones para validar, incrementando notablemente el tamaño del problema final que necesita ser procesado.
- El precio de la máquina necesaria para resolverlo: Si se plantean especificaciones necesarias acerca de la capacidad de cálculo necesario para obtener resultados en un margen de tiempo aceptable, en la mayoría de los casos el coste asociado a una única máquina que satisfaga esas especificaciones es muy superior al de un clúster formado por equipos de menor rendimiento.

Otro aspecto que se debe tener en cuenta es que para garantizar esta capacidad de cálculo los problemas necesitan ser paralelizables. Los clústers utilizan la división de tareas y asignación a los diferentes nodos de proceso de esas tareas, como mecanismo para agilizar el proceso de cálculo. Los problemas deben ser subdivididos en problemas más pequeños para que se pueda distribuir su proceso entre los diferentes nodos de cómputo. Si un problema no cumple con esa característica, entonces el clúster no puede ser utilizado para resolverlo. El objetivo, por lo tanto es mejorar el rendimiento en la obtención de resultados de un problema,

obteniendo una mejora del rendimiento en base al tiempo de respuesta o en base a la precisión de los propios resultados.

La implementación necesaria para abordar estos problemas sigue dos tendencias. Se puede implementar a nivel de sistema operativo y se puede implementar mediante el uso de librerías.

Dentro de esta definición no se engloba restricción concreta. Esto supone que cualquier clúster que haga que el rendimiento del sistema aumente respecto al de uno de los nodos individuales puede ser considerado clúster HP. Generalmente estos problemas de cómputo suelen estar ligados a:

- *Cálculos matemáticos*
- *Renderizaciones de gráficos*
- *Compilación de programas*
- *Compresión de datos*
- *Descifrado de códigos*
- *Rendimiento del sistema operativo, (incluyendo en él, el rendimiento de los recursos de cada nodo)*

Existen otros muchos problemas más que se pueden solucionar con clusters HP, donde cada uno aplica de una manera u otra las técnicas necesarias para habilitar la paralelización del problema, su distribución entre los nodos y obtención del resultado. Las técnicas utilizadas dependen de a qué nivel trabaje el clúster.

Habitualmente las tendencias de diseño de implementación de clusters a nivel de aplicación y a nivel de balanceo de carga son excluyentes, es decir, si se construyen a nivel de aplicación, no implementan el balanceo de carga. Suelen basar todo su funcionamiento en una política de localización que sitúa las tareas en los diferentes nodos del clúster, y las comunica mediante las librerías abstractas. Resuelven problemas de cualquier tipo de los que se han visto en el apartado anterior, pero se deben diseñar y codificar aplicaciones propias para cada tipo para poderlas utilizar en estos clusters.

Otro tipo de implementación de los sistemas alto rendimiento consiste en implementarlos a nivel de sistema. Este tipo de clusters basa todo su funcionamiento en comunicación y colaboración de los nodos a nivel de sistema operativo. Esto implica que generalmente que son clusters de nodos de la misma arquitectura, proporcionando una ventaja importante en lo relativo al factor de acoplamiento. Basan su funcionamiento en la compartición de recursos a cualquier nivel, y en el balanceo de la carga de procesamiento de manera dinámica. Para ello utilizan funciones de planificación especiales que se encargan de gestionar los nodos de procesamiento agregados al clúster.

Clusters HA (High Availability): Cluster de Alta Disponibilidad

Los clústers de alta disponibilidad son un tipo de clústers totalmente diferentes a los de alto rendimiento, basándose esta diferencia en el objetivo hacia el que están diseñados. La idea es que este tipo de clústers deben proporcionar una mejora de los servicios ofrecidos, permitiendo mantener con garantía dichos servicios en el tiempo a pesar del incremento de factores que desvirtúen el rendimiento o incluso a pesar de que exista alguna contingencia. Este hecho hace que sean los clústers más demandados actualmente por las empresas.

Estos clusters están diseñados para proporcionar la máxima disponibilidad sobre los servicios integrados que está proporcionando el clúster, y suponen una competencia que abarata los sistemas redundantes, ofreciendo una serie de servicios durante el mayor tiempo posible. Para poder dar estos servicios los clusters de este tipo se implementan en base a dos factores.

- **Alta disponibilidad de infraestructura:** Si se produce un fallo de hardware en alguna de las máquinas del clúster, el software de alta disponibilidad es capaz de arrancar automáticamente los servicios en cualquiera de las otras máquinas del clúster (failover). Y cuando la máquina que ha fallado se recupera, los servicios son nuevamente migrados a la máquina original (failback). Esta capacidad de recuperación automática de servicios nos garantiza la alta disponibilidad de los servicios ofrecidos por el clúster, minimizando así la percepción del fallo por parte de los usuarios.
- **Alta disponibilidad de aplicación:** Si se produce un fallo del hardware o de las aplicaciones de alguna de las máquinas del clúster, el software de alta disponibilidad es capaz de arrancar automáticamente los servicios que han fallado en cualquiera de las otras máquinas del clúster. Y cuando la máquina que ha fallado se recupera, los servicios son nuevamente migrados a la máquina original. Esta capacidad de recuperación automática de servicios nos garantiza la integridad de la información, ya que no hay pérdida de datos, y además evita molestias a los usuarios, que no tienen por qué notar que se ha producido un problema.

Gran parte de la problemática asociada está ligada a la necesidad de que el servicio proporcionado sea ininterrumpido, proporcionando total disponibilidad constante a los clientes o usuarios de dicho servicio. En entorno de producción real se suelen producir fallos inesperados en los servidores, y estos fallos provocan la aparición de dos eventos en el

tiempo: el tiempo en el que el servicio está inactivo y el tiempo de reparación del problema. Entre las opciones que solucionan este tipo de contingencias tenemos:

- Sistemas de información redundante
- Sistemas tolerantes a fallos
- Balanceo de carga entre varios servidores
- Balanceo de conexiones entre varios servidores

La adopción de este tipo de sistemas está vinculada con dos fuentes de necesidad de cualquier organización. La primera es el poder disponer de un servicio activo y ahorrar económicamente todo lo que sea posible. El servicio puede ser de diversa índole, desde un sistema de ficheros distribuidos de carácter muy barato, hasta grandes clusters de balanceo de carga y conexiones para los grandes portales de Internet. Cualquier funcionalidad requerida en un entorno de red puede ser colocada en un clúster e implementar mecanismos para hacer que esta obtenga la mayor disponibilidad posible.

Se basan en principios muy simples que pueden ser desarrollados hasta crear sistemas complejos especializados para cada entorno particular. En cualquier caso, las técnicas de estos sistemas suelen basarse en excluir del sistema aquellos puntos críticos que pueden producir un fallo y por tanto la pérdida de disponibilidad de un servicio. Para esto se suelen implementar desde enlaces de red redundantes hasta disponer de N máquinas para hacer una misma tarea de manera que si caen N-1 máquinas el servicio permanece activo sin pérdida de rendimiento.

61.3.3 ***Balanceo de carga***

Aunque el término de balanceo de carga puede hacer referencia a un tipo de clústering concreto, puede asumirse como una característica que

forma parte de un gran número de implementaciones de clústering diferentes. El término en sí hace referencia a la capacidad para subdividir el trabajo de procesamiento de forma equilibrada entre un conjunto de nodos que forman parte de un sistema multiproceso, siendo el término aplicado a sistemas de clústering o a otro tipo de sistemas multiproceso.

El balanceo de carga se utiliza frecuentemente apoyándose en la gestión dinámica del tráfico de la red existente entre distintos servidores. La aplicación más común del balanceo de carga es evitar que un solo servidor se encuentre saturado mientras otros similares estén disponibles.

Mediante el uso de balanceo de carga, los servidores aparecen como uno solo para el usuario. Un servidor o máquina realiza una monitorización continua de cada servidor para determinar el mejor camino a dónde enrutar las peticiones de los clientes de acuerdo a los recursos de los servidores que gestionan.

De esta forma se consigue que los sistemas sigan funcionando aunque alguno de los servidores no esté operativo. Si los servidores se encuentran físicamente en distintas ubicaciones el balanceo de carga se convierte en una forma de mantener los sistemas funcionando aunque uno de los centros de datos no se encuentre operativo.

El término habitualmente se confunde con el concepto de alta disponibilidad, y ciertamente, sistemas donde primen la alta disponibilidad o el balanceo de carga habitualmente tienen objetivos similares. Sin embargo, el concepto de balanceo de carga está ligado a la unificación de sistemas separados.

En el caso de los clústers de alta disponibilidad, pueden entenderse como un conjunto de máquinas independientes bajo una arquitectura distribuida que permite que si un nodo se cae, otro en reserva se active para asumir las competencias del nodo que ha dejado de funcionar. Sin embargo el concepto de balanceo de carga, independientemente de que también proporciona redundancia y tolerancia a fallos, se centra más en el uso compartido de los recursos para alcanzar metas globales.

61.4 Alta disponibilidad en servidores de aplicaciones y servidores de bases de datos.

61.4.1 *Alta disponibilidad en servidores de aplicaciones*

Un servidor de aplicaciones se define como un equipo o máquina que contiene un conjunto de aplicaciones software que permiten ofrecer servicios de aplicación a diferentes clientes. En la actualidad el concepto se encuentra asociado a servidores de aplicaciones basados en Java, como J2EE (Java 2 Enterprise Edition), Websphere de IBM o WebLogic de Oracle.

En su arquitectura interna, el servidor de aplicaciones no es más que un contenedor de aplicaciones formadas por componentes que interactúan entre sí. Estos componentes tienen una gran capacidad de reutilización permitiendo su combinación para la implementación de nuevas aplicaciones que aporten diferentes servicios.

En el caso de los servidores de aplicaciones basados en J2EE, este tipo de componentes están escritos en Java y se clasifican según la funcionalidad que vayan a desempeñar en la arquitectura de la aplicación, distinguiéndose entre los Servlets, las Java Server Pages (JSPs) y por último los Enterprise Java Beans (EJBs). Estos elementos permiten construir aplicaciones en diferentes capas, facilitando las operaciones de reutilización, reimplementación, extensibilidad y escalabilidad de las aplicaciones. El diseño en capas de las aplicaciones permite separar la

interfaz de usuario de funciones de lógica de negocio, gestión de las sesiones del usuario o el acceso a las bases de datos del sistema. Además, en el caso de los servidores de aplicaciones basados en Java, que siguen el estándar J2EE, se permite la creación de clústers de servicios ampliando las características de escalabilidad y proporcionando una interfaz para integrar alta disponibilidad para el sistema de aplicaciones basado en la gestión transparente de conjuntos de servidores.

Un ejemplo concreto de servidor de aplicaciones es el WebLogic Server, basado en Java, que proporciona mecanismos para integrar un clúster de servicios, generando copias replicadas de todos los servicios a los clientes del sistema. En caso de que un servicio se caiga, automáticamente se notifica y se redireccionan las solicitudes pendientes a las réplicas del servicio que existen en el clúster.

Algunos de los requisitos que se deben cumplir para garantizar la alta disponibilidad son:

Que en cada instancia del servidor del clúster existan los mismos componentes de aplicación.

Que el mecanismo de recuperación pueda determinar la ubicación en el clúster de todos los objetos de la aplicación.

Que se conozca el estado de ejecución de las distintas tareas de cada uno y de los componentes. Esto permite que si un componente falla, la tarea la pueda completar otro servicio partiendo del mismo punto en el que se detuvo por fallo, y posibilitando que no se dupliquen los datos de carácter persistente.

61.4.2 *Alta disponibilidad a nivel de bases de datos*

La alta disponibilidad a nivel de bases de datos hace referencia a la disponibilidad de los servicios de acceso a las bases de datos por parte de los clientes, garantizando un grado absoluto de funcionamiento continuo de los sistemas gestores de bases de datos.

Existe un amplio repertorio de sistemas que necesitan alta disponibilidad de sistemas de gestión de bases de datos. Este tipo de sistemas abarcan desde sistemas de tiempo real y sistemas embebidos hasta aplicaciones web u otro tipo de sistemas online. Habitualmente estos entornos requieren un compromiso de nivel de servicio mínimo y robustez para hacer frente a posibles contingencias que eviten, no sólo la pérdida de datos, sino la suspensión del servicio.

A menudo, los sistemas de alta disponibilidad en general centran sus esfuerzos en garantizar que el servicio ofrecido se mantenga de forma constante pese a que surjan imprevistos o fallos que deben controlarse. Sin embargo, en la implementación de la alta disponibilidad a nivel de bases de datos debe tenerse en cuenta un aspecto importante; no sólo se pretende mantener el sistema activo, sino que se pretenden mantener los datos actualizados y disponibles para todos los clientes. Debe de poder asegurarse la integridad de la base de datos.

Los sistemas de alta disponibilidad que implementan los servicios de bases de datos deben cumplir las siguientes características:

Robustez frente a fallos del servidor y capacidad de recuperación.

Tiempo de caída del sistema tiene que ser reducido o eliminado.

Niveles de servicio obligatorios en caso de fallo o alta densidad de tráfico.

Asociado a los sistemas de alta disponibilidad a nivel de base de datos entra en juego el concepto de Punto de Fallo. Este término hace referencia a determinados componentes del sistema que pueden fallar, y cuyo fallo es independiente de otros componentes. Por tanto puedes considerarse puntos de riesgo a tener en cuenta en una planificación y diseño del sistema de alta disponibilidad.

Existen tres principales puntos de conflicto o Puntos de Fallo en una implementación de un servicio de bases de datos:

El propio servidor de la base de datos, es decir el motor software o Sistema Gestor de la Base de Datos y la plataforma hardware que lo sustenta.

La base de datos física, es decir, el dispositivo o dispositivos físicos que albergan los datos, como discos duros o memorias.

Los enlaces y conexiones externas que permiten a los usuarios realizar las peticiones, entendiendo como tales los enlaces físicos (red cableada) y lógicos (servicios levantados).

Cada componente tiene su propio tipo de fallo y reducción de servicio, así como sus protocolos específicos de actuación para intentar reducir y/o subsanar las contingencias provocadas por esos fallos.

Las principales soluciones que intentan mitigar las posibles contingencias que se provoquen en los puntos de fallo consisten fundamentalmente en tres:

Backup Online: Se basa en implementaciones del server que permiten proteger los datos frente a fallos del disco, manteniendo registro de cambios del log en dispositivos separados.

Replicación: implica la implementación de otro servidor gemelo utilizando técnicas de mirroring. Mediante la duplicidad del servicio mediante un segundo punto de acceso, es posible derivar peticiones entre servidores en caso de que uno falle o se produzca un cuello de botella que deniegue el servicio a alguno de ellos. El mecanismo de replicación utiliza dos bases de datos diferentes; la principal (activa) y la secundaria (espejo), que corren en máquinas diferentes, cada una en un servidor, pero ambas conteniendo representaciones idénticas de los mismos datos.

Recuperación ante fallos: La recuperación ante fallos consiste básicamente en una mejora del mecanismo de replicación. Consiste en establecer los mecanismos necesarios para que, en caso de fallo, mediante la réplica situada en otra máquina, el sistema que ha caído pueda recuperar el punto actual mediante la sincronización automática de los sistemas.

61.5 Alta disponibilidad en entornos virtualizados.

La alta disponibilidad en entornos virtualizados puede verse desde dos ópticas distintas; la primera de ellas implica alta disponibilidad de servidores que contienen una virtualización de servicios, o bien desde el punto de vista de asegurar alta disponibilidad de servicios mediante la virtualización de servidores.

En el primero de los casos, las medidas referentes a la disposición de alta disponibilidad pasan por la implementación de soluciones basadas en redundancia de hardware, o implementación de sistemas que garanticen alto rendimiento a nivel de sistema operativo.

En cuanto a asegurar alta disponibilidad mediante servicios de virtualización, es un campo complejo que tiene a ser la idea general de implantación en los grandes centros de cómputo y proceso de datos, dadas las grandes ventajas que presenta.

Mediante la virtualización se pueden manejar todos los componentes que forman parte de cada uno de los servidores o nodos que van a componer el centro de procesamiento, permitiendo interoperabilidad entre los componentes de los mismos, y administrando y gestionando la memoria y recursos como CPU y discos. Las dos tendencias fundamentales que se siguen son la virtualización de hardware o la virtualización de Sistema Operativo.

61.5.1 Virtualización de hardware

Mediante la virtualización de hardware (Ilustración 4) se emula el hardware original del servidor en cada una de las máquinas virtuales. Una vez emulada la máquina anfitriona, cada una de estas instancias virtualizadas se convertirá en un servidor privado que puede albergar diferentes sistemas operativos y diferentes servicios. El gestor de virtualización permitirá configurar políticas de recuperación frente a fallos, permitiendo levantar instancias y/o recuperar instancias de máquinas que alberguen servicios y se hayan detenido en caso de alguna contingencia.

61.5.2 *Virtualización de sistema operativo*

Por el contrario, en la virtualización de los SO (Ilustración 5), se establece una configuración base del sistema operativo sobre el hardware nativo de la máquina, estableciendo instancias de ese sistema y virtualizado mediante la generación de instancias idénticas al hardware y sistema operativos originales de la máquina. En última instancia, todos los recursos son procesados y controlados por el sistema operativo nativo, dado que no existe virtualización de hardware. Esto reduce la complejidad de configuración de diferentes dispositivos en diferentes sistemas operativos, pero tiene como consecuencia que en caso de fallo de un dispositivo por mala configuración, se verán afectadas todas las instancias virtuales que corran sobre ese servidor físico.

61.6 **Centros de Protección Geográficos**

Cuando es un requisito indispensable el hecho de mantener una alta disponibilidad de determinados servicios de 24 horas al día durante los 7 días del año (24x7), es imprescindible hacer uso de elementos que proporcionen respaldo de la información o de los recursos a distintos niveles: alta disponibilidad de servicios, redundancia de sistemas, replicación de datos y centro de respaldo.

Entonces, para poder garantizar que un servicio o recurso va a tener una disponibilidad de 24x7, será necesario emplear sistemas redundantes y estos deben de encontrarse en ubicaciones físicas situadas a una considerable distancia para ofrecer de esta manera respuesta a ciertas situaciones de contingencia de carácter muy grave producidas por un desastre a nivel físico, como puede ser un incendio, un terremoto o simplemente un fallo total en los sistemas de energía.

A su vez, la disponibilidad e integridad de los datos asociados a los servicios son vitales para poder garantizar que los servicios tengan una disponibilidad 24x7. Entonces para garantizar una disponibilidad 24x7:

Los datos han de estar replicados de una manera eficiente entre los diferentes centros geográficos, garantizando que en caso de que se produzca cualquier tipo de incidencia o catástrofe se disponga de una copia exacta, fiable y actualizada de los mismos. Esta réplica, a su vez, ha de encontrarse disponible para ser utilizada y poder hacer uso de ella en los servicios en producción.

Los trabajos para la recuperación de los servicios se han de automatizar, disminuyendo así los posibles tiempos de indisponibilidad. Para ello se llevan a cabo operaciones en los servidores para la detección de fallos, para detener algún servicio y para levantar otros. Además se ha de establecer una coordinación entre los sistemas de almacenamiento de los datos con el fin de garantizar tanto la disponibilidad del servicio como el hecho de que la información se está replicando de una manera adecuada. Esta tarea se realiza con el fin de ofrecer una copia exacta de la información en un estado óptimo para ser utilizada de forma automática una vez ocurrido un desastre.

Siguiendo estos puntos, un servicio que se encuentre en régimen de disponibilidad 24x7 en el cual se ofrecen diversos centros geográficos para la protección de los servicios y de la información, se ha de contemplar la alta disponibilidad de una manera integrada. Esta alta disponibilidad ha de gestionar en bloque aquellas operaciones que tengan relación tanto con los servicios, como con los sistemas o con el almacenamiento de los datos.

Un ejemplo donde el Centro de Datos 1 se presta el servicio XYZ y tiene asociados un conjunto de servidores y de dispositivos de almacenamiento, los cuales se replican contra los dispositivos de almacenamiento situados en el Centro de Datos 2. En el Centro de Datos 2, existen servidores que se encuentran en disposición de proporcionar los mismos servicios que en el Centro de Datos 1, en caso de que en este se produzca algún tipo de fallo o desastre.

Si se produce algún tipo de contingencia, todas las operaciones que se llevan a cabo en el Centro de Datos 1 de servicios, de aplicaciones, de servidores y de replicación de datos han de estar coordinadas y automatizadas para que se produzca un cambio en la ejecución de los servicios, es decir, que el Centro de Datos 2 tome el mando de los servicios y comience a servir en el menor tiempo posible como se muestra en la siguiente ilustración. Cuando se produce este cambio y los servicios comienzan a ser prestados desde el Centro de Datos 2, también se ha de producir una inversión en el sentido de la replicación de los datos.

61.7

Planes de Contingencia

Un plan de contingencia es una herramienta para emplear en la gestión de las Tecnologías de la Información y las Comunicaciones y aporta una serie de reglas o medidas que proporciona una garantía de continuidad del negocio y de los procesos de una organización. Estas medidas pueden ser:

Técnicas: Extintores contra incendios, detectores de humo, salidas de emergencia, equipos informáticos de respaldo.

Humanas: Formación de actuación ante un incendio, designación de responsables de las salas, asignación de roles y responsabilidades para la copia de respaldo.

Organizativas: Seguro de incendio, precontrato de alquiler de equipos informáticos y ubicación alternativa, procedimiento de copia de respaldo, procedimiento de actuación ante un incendio, contratación de servicios de auditorías de riesgos laborales.

Podría definirse como una planificación de las acciones a tomar cuando se produzca un evento o condición que no esté recogido dentro del proceso de planificación formal. Se trata de una serie de procedimiento para el restablecimiento de los procesos de negocio en caso de producirse un desastre.

Todo plan de contingencia ha de comprender tres subplanes, que determinaran el conjunto de procedimientos o contramedidas que se aplicaran en cada momento en función de la aparición de una amenaza. Estos subplanes son:

Plan de respaldo: contramedidas antes de la aparición de una amenaza para evitar que se produzca.

Plan de emergencia: en él se reflejan los procedimientos a seguir en el momento que se produce una amenaza o justamente después para paliar los efectos que pueda provocar la amenaza.

Plan de recuperación tras un desastre: refleja las contramedidas que

daños ocasionados por el desastre, definiendo desastre como toda interrupción del acceso a la información o de su procesado, necesaria para el normal funcionamiento de todos los procesos de negocio.

Un plan de contingencia se divide en tres partes según las tareas que se lleven a cabo:

Prevención: Conjunto de acciones que se han de realizar como prevención ante cualquier posible problema que provoque la continuidad de los procesos de negocio de forma parcial o total. Con ello se minimizarán los daños en caso de producirse el problema, proporcionando una mejor respuesta que restablezca los servicios en un menor tiempo.

Detección: Grupo de acciones encargadas de contener el impacto en el momento de la aparición de un problema intentando limitarlos tanto como sea posible.

Recuperación: Acciones que van desde el mantenimiento de partes críticas mientras se está produciendo la pérdida de los servicios y los recursos, hasta su recuperación o restauración.

61.7.1

Ciclo de Vida

Todo plan de contingencia ha de seguir un ciclo de vida iterativo, en continua evolución, PDCA (Plan-Do-Check-Act, Planificar-Hacer-Comprobar-Actuar). Este ciclo de vida proporciona la identificación de las amenazas que pueden provocar una ruptura en la continuidad de los procesos de negocio de una organización.

Una vez identificadas las amenazas se establecen una serie de medidas o procedimientos para afrontarlas. El plan de contingencia recoge estas medidas además de indicar los recursos necesarios para poder ejecutarlas.

A lo largo del ciclo de vida de un plan de contingencia, éste sufre numerosas revisiones, que resultan de un nuevo análisis de las posibles amenazas que se pueden llegar a producir.

Cuando se plantea una amenaza, el plan de contingencia se ve también afectado, provocando sobre él una serie de actuaciones:

Amenaza establecida y acciones eficaces: se realizan los cambios menores que se consideren para mejorar la eficacia del plan de contingencia ante el mismo tipo de situaciones.

Amenaza establecida y acciones ineficaces: se vuelve a realizar un análisis de las causas del error y se proponen nuevas medidas a tomar.

Amenaza no prevista: se llevara a cabo un nuevo análisis de riesgos, aunque las medidas adoptadas contra una amenaza no detectada fueran eficaces.

61.7.2

Características

El plan de contingencia ha de contemplar dos aspectos:

Operacional: cada usuario ha de conocer qué función ha de desempeñar una vez detectado el problema y saber a quién avisar en caso de que este se produzca. En el plan de contingencia también se ha de especificar los encargados de la toma de decisiones durante el proceso de recuperación y se establezca la disponibilidad y el entrenamiento del personal experimentado.

Administrativo: en el aspecto administrativo se contempla

- o La definición de los riesgos y los porcentajes de aparición de los mismos
- o Los procedimientos de recuperación de la información
- o Los responsables de los medios de respaldo
- o La localización de los medios de respaldo y del software de reemplazo.
- o La especificación de alternativas de respaldo
- o La información, bases de datos, servicios, etc. prioritarios que deben de ser restablecidos primero.

61.7.3

Objetivo

El objetivo prioritario de un plan de contingencia es garantizar que una organización y sus procesos e negocio o actividades operacionales sigan en funcionamiento a pesar de haberse producido una situación de desastre. Para poder conseguir esto, el plan de contingencia habilita a la organización para poder responder y superar problemas críticos o incluso catastróficos, de tal manera que permite una temprana recuperación de la situación normal de trabajo.

61.7.4

Puntos Clave

Los puntos clave de un plan de contingencia pueden enfocarse hacia algunas de las siguientes áreas:

Facilidad de Destrucción. El equipo encargado de realizar la planificación ha de tener en cuenta que se puede producir una total destrucción de los sistemas organizacionales o un colapso total de los servicios de la misma. El plan de contingencia también debe de contemplar revisiones para realizar en caso de que se produzca una destrucción parcial.

Disponibilidad del personal. Se ha de determinar en el plan de contingencia un organigrama para una situación de desastre, el cual deberá estar formado por personal de toda la organización, identificando las posiciones clave para la ejecución del plan.

Determinar los tiempos del desastre. Se deben tomar las consideraciones oportunas para cada uno de los diversos momentos en que puede producirse un desastre, tratando de identificar los momentos en los que se pueda producir un mayor impacto para la organización. Este factor depende del tipo de organización, puesto que una organización puede desarrollar el 70 % de su producción o de su actividad en las primeras horas de un día, mientras que otras su mayor actividad se produce de madrugada. También se pueden considerar periodos de tiempo, mayor impacto a principio de mes que a finales, etc.

Instalaciones fuera del centro operacional. Se puede tener en cuenta desastres que afecte por completo a partes del sistema presentes en el centro de operaciones. El hecho de tener una instalación externa, como un centro de almacenamiento o una réplica del sistema, garantiza una considerable reducción del impacto que puede ocasionar una contingencia o un desastre.

Un plan de contingencia ha de ser dinámico y estar en continua evolución, viéndose modificado cada vez que se produzca, cambio de equipo de instalación cambio de algún sistema, variaciones en los contratos de mantenimiento, cambios de personal, etc.

61.7.5 *Elementos*

En un plan de contingencia se pueden identificar tres tipos de elemento o tipos de acciones que se pueden identificar:

Acciones de Emergencia. Tratan de solventar el daño en el momento de ocurrir la incidencia, así como evitar el mayor impacto posible.

Acciones de Recuperación. Realizan tareas de mantenimiento durante la pérdida del servicio y recursos, y tareas de recuperación.

Acciones de Respaldo. Se llevan a cabo una vez que se presenta una contingencia que afecte a la continuidad operativa de la organización con el fin de reducir su impacto, posibilitando el restablecimiento de los servicios interrumpidos en el menor tiempo posible.

61.8

Bibliografía

Alta disponibilidad de los servicios en la SGTIC del MEH. Emilio Raya López y Marcos Llama Pérez.

Disaster Recovery and Business Continuity: A Quick Guide for Small Organizations and Busy Executives Second Edition. Thejendra BS

Computer Security Handbook. Seymor Bosworth, Michel E. Kabay

Information Storage and Management: Storing, Managing, and Protecting Digital Information. G. Somasundaram, Alok Shrivastava

System & Disaster Recovery Planning. Richard Dolewski

Scalable Internet Architectures. Theo Schlossnagle

Autor: Francisco Javier Rodriguez Martínez

Subdirector de Sistemas Escola Superior Enxeñaría Informática Ourense

Colegiado del CPEIG