

## **NOTA INFORMATIVA EN RELACIÓN COA PUBLICACIÓN DOS TEMARIOS DOS PROCESOS SELECTIVOS CONVOCADOS POLA XUNTA DE GALICIA NO DIARIO OFICIAL DE GALICIA Nº 142 DE 26 /07/11**

O Diario Oficial de Galicia nº 142, de 26 de xullo de 2011, publica distintas ordes da Consellería de Facenda polas que se convocan diferentes procesos selectivos para o ingreso na Administración autonómica de Galicia.

Cumprindo co compromiso adquirido, a EGAP, continúa coa publicación dos temarios correspondentes aos distintos procesos selectivos convocados formalmente.

Tendo en conta, por unha banda, o volume e complexidade na elaboración dun material didáctico que sirva de referencia básica e, por outra, o interese da EGAP para que os posibles usuarios dispoñan á maior brevidade posible de dito material, a publicación do mesmo na páxina web da Escola (<http://egap.xunta.es>), irase producindo da seguinte maneira:

- 1) **Lexislación**, actualizada e consolidada á data de publicación no DOG do nomeamento do tribunal do proceso (Base II.1 da convocatoria<sup>1</sup>), correspondente aos procesos selectivos para o ingreso no corpo superior da Administración da Xunta de Galicia, subgrupo A1; corpo de xestión da Administración da Xunta de Galicia, subgrupo A2; corpo superior da Administración da Xunta de Galicia, subgrupo A1, escala de sistemas e tecnoloxía da información; corpo de xestión da Administración da Xunta de Galicia, subgrupo A2, escala de xestión e sistemas de información e corpo auxiliar da Xunta de Galicia, subgrupo C2.

A data prevista para dita publicación é de 5 de agosto de 2011.

- 2) **Temarios específicos**, iranse publicando na páxina web da Escola, a medida que os procesos de elaboración e revisión vaian concluíndo.

Sen prexuízo da súa publicación nas dúas linguas oficiais e a fin de facilitar á maior brevidade posible este material aos usuarios, os temas iranse publicando na web no idioma orixinalmente empregado por cada un dos autores.

Para maior información pódense poñer en contacto co servizo de Estudos e Publicacións a través do correo electrónico [temarios.egap@xunta.es](mailto:temarios.egap@xunta.es), e teléfono 881 997 251.

A Escola reitera que os temarios por ela facilitados non teñen carácter oficial, polo que en ningún caso vincularán aos opositores ou aos tribunais; senón que se trata de instrumentos complementarios que servirán de apoio e axuda como textos de referencia pero nunca de forma exclusiva e excluín-te.

Santiago de Compostela, 4 de agosto de 2011

---

<sup>1</sup> II. Proceso selectivo.  
II.1. Procedemento de oposición.  
(...)

Teranse en conta as normas de dereito positivo relacionadas co contido do programa que no momento de publicación no DOG do nomeamento do tribunal do proceso contén con publicación oficial no boletín ou diario correspondente.

**1. GOBERNANZA DAS TIC.  
PLANIFICACIÓN, DIRECCIÓN E  
CONTROL DAS TIC. COBIT  
(«CONTROL OBJECTIVES FOR  
INFORMATION AND RELATED  
TECHNOLOGY»), OBXECTIVOS  
DE CONTROL E MÉTRICAS.  
PROPOSTAS DE PROXECTOS  
(CASOS DE NEGOCIO OU  
«BUSINESS CASE»), ANÁLISE  
DE CUSTOS/BENEFICIOS,  
ANÁLISE DE RISCOS,  
FACTORES CRÍTICOS DE  
ÉXITO. VALIT.**

**Tema 1. Gobernanza das TIC. Planificación, dirección e control das TIC. CoBIT («Control Objectives for Information and Related Technology»), obxectivos de control e métricas. Propostas de proxectos (casos de negocio ou «business case»), análise de custos/beneficios, análise de riscos, factores críticos de éxito. ValIT.**

## **ÍNDICE**

- 1.1 Gobernanza das TIC. Planificación, dirección e control das TIC.
- 1.2 CoBIT («Control Objectives for Information and related Technology»), obxectivos de control e métricas.
  - 1.2.1 Marco de traballo COBIT
    - 1.2.1.1 Orientado ao negocio
    - 1.2.1.2 Orientado a procesos
    - 1.2.1.3 Baseado en controis
    - 1.2.1.4 Impulsado pola medición
  - 1.2.2 Modelos de madurez
  - 1.2.3 Medición do desempeño
- 1.3 Propostas de proxectos (casos de negocio ou «business case»), análise de custos/beneficios, análises de riscos, factores críticos de éxito. ValIT.
  - 1.3.1 Introducción
    - 1.3.1.1 Obxectivo de ValIT
    - 1.3.1.2 A necesidade de ValIT
    - 1.3.1.3 Unha nova perspectiva
  - 1.3.2 O marco ValIT
    - 1.3.2.1 Principios de ValIT
    - 1.3.2.2 Procesos de ValIT
  - 1.3.3 ValIT. O caso de negocio
    - 1.3.3.1 Introducción: A importancia do caso de negocio
    - 1.3.3.2 Estrutura do caso de negocio

## **1.1 GOBERNANZA DAS TIC. PLANIFICACIÓN, DIRECCIÓN E CONTROL DAS TIC.**

Gobernanza das TIC é o aliñamento das Tecnoloxías da información e a comunicación (TIC) coa estratexia do negocio. Traslada as metas e a estratexia a todos os departamentos da empresa, e prové o mellor uso da tecnoloxía e das súas estruturas organizacionais para alcanzalas.

Para moitas empresas, a información e a tecnoloxía que as soporta representan os seus máis valiosos activos, aínda que con frecuencia son pouco entendidos. As empresas exitosas recoñecen os beneficios da tecnoloxía da información e utilízana para impulsar o valor dos seus interesados (*stakeholders*). Estas empresas tamén entenden e administran os riscos asociados, tales como o aumento en requirimentos regulatorios, así como a dependencia crítica de moitos procesos de negocio en TI.

A necesidade do aseguramento do valor de TI, a administración dos riscos asociados a TI, así como o incremento de requirimentos para controlar a información, enténdense agora como elementos clave do Goberno Corporativo. O valor, o risco e o control constitúen a esencia do goberno de TI.

O goberno de TI é responsabilidade dos executivos, do consello de directores e consta de liderado, estruturas e procesos organizacionais que garanten que TI na empresa sostén e estende as estratexias e obxectivos organizacionais. Máis aínda, o goberno de TI integra e institucionaliza as boas prácticas para garantir que TI na empresa soporta os obxectivos do negocio. Deste xeito, o goberno de TI facilita que a empresa aproveite ao máximo a súa información, maximizando así os beneficios, capitalizando as oportunidades e gañando vantaxes competitivas.



As organizacións deben satisfacer a calidade, os requirimentos fiduciarios e de seguridade da súa información, así como de todos os seus activos. A dirección tamén debe optimizar o uso dos recursos dispoñibles de TI, incluíndo aplicacións, información, infraestrutura e persoas. Para descargar estas responsabilidades, así como para lograr os seus obxectivos, a dirección debe entender o status da súa arquitectura empresarial para TI e decidir que tipo de goberno e de control debe aplicar.

## **1.2 CoBIT («CONTROL OBJECTIVES FOR INFORMATION AND RELATED TECHNOLOGY»), OBXECTIVOS DE CONTROL E MÉTRICAS.**

Para que TI teña éxito á hora de satisfacer os requirimentos do negocio, a dirección debe implantar un sistema de control interno ou un marco de traballo. O marco de traballo de control COBIT contribúe a estas necesidades do seguinte xeito:

- Establecendo un vínculo cos requirimentos do negocio.
- Organizando as actividades de TI nun modelo de procesos xeralmente aceptado.
- Identificando os principais recursos de TI que deben ser utilizados.
- Definindo os obxectivos de control xerenciais que cómpre considerar.

A orientación ao negocio que enfoca COBIT consiste en aliar as metas de negocio coas metas de TI, brindando métricas e modelos de madurez para medir os seus logros e identificando as responsabilidades asociadas dos donos dos procesos de negocio e de TI.

O enfoque cara a procesos de COBIT ilústrase cun modelo de procesos, o cal subdivide TI en 34 procesos de acordo ás áreas de responsabilidade de planificar, construír, executar e monitorar, ofrecendo

unha visión de punta a punta da TI. Os conceptos de arquitectura empresarial axudan a identificar aqueles recursos esenciais para o éxito dos procesos; é dicir, aplicacións, información, infraestrutura e persoas.

En resumo, para proporcionar a información que a empresa precisa para lograr os seus obxectivos, os recursos de TI deben ser administrados por un conxunto de procesos agrupados de forma natural.

Pero, como pode a empresa poñer baixo control TI de tal xeito que xere a información que a empresa necesita? Como pode administrar os riscos e asegurar os recursos de TI dos cales depende tanto? Como pode a empresa asegurar que TI logre os seus obxectivos e soporte os do negocio? Primeiro, a dirección require obxectivos de control que definan a meta final de implantar políticas, procedementos, prácticas e estruturas organizacionais deseñadas para brindar unha seguridade razoable de que:

- Se alcanzan os obxectivos do negocio.
- Se preveñan ou se detecten e corrixan os eventos non desexados.

En segundo lugar, nos complexos ambientes de hoxe en día, a dirección busca continuamente información oportuna e condensada para tomar decisións difíciles respecto de riscos e controis, de maneira rápida e exitosa. Que se debe medir e como? As empresas requiren unha medición obxectiva de onde se atopan e onde se requiren melloras, e deben implementar unha caixa de ferramentas xerenciais para monitorar esta mellora.

Unha resposta aos requirimentos de determinar e monitorar o nivel apropiado de control e desempeño de TI son as definicións específicas de COBIT dos seguintes conceptos:

- Benchmarking da capacidade dos procesos de TI, expresada como modelos de madurez, derivados do Modelo de Madurez da Capacidade do Instituto de Enxeñería de Software.
- Metas e métricas dos procesos de TI para definir e medir os seus resultados e o seu desempeño, baseados nos principios de Balanced Scorecard de Negocio de Robert Kaplan e David Norton.
- Metas de actividades para controlar estes procesos, con base nos obxectivos de control detallados de COBIT.

A avaliación da capacidade dos procesos baseada nos modelos de madurez de COBIT é unha parte clave da implementación do goberno de TI.

Despois de identificar os procesos e controis críticos de TI, o modelo de madurez permite identificar e demostrarlle á dirección as brechas na capacidade. Entón pódense crear plans de acción para levar estes procesos ata o nivel obxectivo de capacidade desexado.

COBIT dálle soporte ao goberno de TI ao brindar un marco de traballo que garante que:

- TI está aliñada co negocio.
- TI habilita o negocio e maximiza os beneficios.
- Os recursos de TI úsanse de maneira responsable.
- Os riscos de TI adminístranse apropiadamente.

A medición do desempeño é esencial para o goberno de TI. COBIT dálle soporte e inclúe o establecemento e a monitorización de obxectivos que se poidan medir, referentes ao que os procesos de TI requiren xerar (resultado do proceso) e a como o xeran (capacidade e desempeño do proceso). Moitos estudos identificaron que a falta de transparencia nos custos, valor e riscos de TI é un dos máis importantes impulsores para o

gobierno de TI. Namentres as outras áreas consideradas contribúen, a transparencia lógrase de forma principal por medio da medición do desempeño.

Estas áreas de enfoque de goberno de TI describen os puntos nos que a dirección executiva esixe poñer atención para gobernar a TI nas súas empresas. A dirección operacional usa procesos para organizar e administrar as actividades cotiás de TI.

COBIT brinda un modelo de procesos xenéricos que representa todos os procesos que normalmente se atopan nas funcións de TI, ofrecendo un modelo de referencia común entendible para os xerentes operativos de TI e do negocio. Establecéronse equivalencias entre os modelos de procesos COBIT e as áreas de enfoque do goberno de TI, ofrecendo así unha ponte entre o que os xerentes operativos deben realizar e o que os executivos desexan gobernar.

Para lograr un goberno efectivo, os executivos esperan que os controis que serán implantados polos xerentes operativos se atopen dentro dun marco de control definido para todos os procesos de TI. Os obxectivos de control de TI de COBIT están organizados por proceso de TI; polo tanto, o marco de traballo brinda un aliñamento claro entre os requirimentos de goberno de TI, os procesos de TI e os controis de TI.

COBIT céntrase en qué se require para lograr unha administración e un control adecuado de TI, e sitúase nun nivel alto. COBIT foi aliñado e harmonizado con outros estándares e mellores prácticas máis detallados de TI. COBIT actúa como un integrador de todos estes materiais guía, resumindo os obxectivos clave baixo un mesmo marco de traballo integral que tamén se aliña cos requirimentos de goberno e de negocios.

COSO (e marcos de traballo compatibles semellantes) é normalmente aceptado como o marco de traballo de control interno para as empresas. COBIT é o marco de traballo de control interno normalmente aceptado para TI. Os produtos COBIT organizáronse en tres niveis deseñados para darlles soporte a:

- Administración e consellos executivos.
- Administración do negocio e de TI.
- Profesionais en Goberno, aseguramento, control e seguridade.

COBIT é un marco de referencia e un xogo de ferramentas de soporte que lle permiten á xerencia cerrar a brecha respecto dos requirimentos de control, temas técnicos e riscos de negocio, e comunicarlles ese nivel de control aos Interesados.

COBIT actualízase e harmonízase con outros estándares. Polo tanto, COBIT converteuse no integrador das mellores prácticas de TI e no marco de referencia xeral para o goberno de TI, e axuda a comprender e administrar os riscos e beneficios asociados con TI.

A estrutura de procesos de COBIT e o seu enfoque de alto nivel orientado ao negocio brindan unha visión completa de TI e das decisións que cómpre tomar acerca da mesma.

Os beneficios de implantar COBIT como marco de referencia de goberno sobre TI inclúen:

- Mellor aliñamento, baseándose no seu enfoque de negocios.
- Unha visión, entendible para a xerencia, do que fai TI.
- Propiedade e responsabilidades claras, baseándose na súa orientación a procesos.

- Aceptación xeral de terceiros e reguladores.
- Entendemento compartido entre todos os Interesados, baseándose nunha linguaxe común.
- Cumprimento dos requirimentos COSO para o ambiente de control de TI.

### **1.2.1 MARCO DE TRABALLO COBIT**

O marco de traballo COBIT creouse coas características principais de ser orientado a negocios, orientado a procesos, baseado en controis e impulsado por medicións.

#### **1.2.1.1 ORIENTADO AO NEGOCIO**

A orientación a negocios é o tema principal de COBIT. Está deseñado para ser utilizado non só por provedores de servizos, usuarios e auditores de TI, senón tamén e principalmente, como guía integral para a xerencia e para os donos dos procesos de negocio.

O marco de traballo COBIT baséase no seguinte principio: Para proporcionar a información que a empresa require para lograr os seus obxectivos, a empresa necesita investir en, administrar e controlar os recursos de TI usando un conxunto estruturado de procesos que provean os servizos que entregan a información empresarial requirida.

#### **1.2.1.2 ORIENTADO A PROCESOS**

COBIT define as actividades de TI nun modelo xenérico de procesos organizado en catro dominios. Estes dominios son Planear e Organizar, Adquirir e Implantar, Entregar e Dar Soporte e Monitorar e Avaliar. Os dominios equipáranse ás áreas tradicionais de TI de planificar, construír, executar e monitorar. O marco de traballo de COBIT proporciona un modelo

de procesos de referencia e unha linguaxe común para que todos na empresa visualicen e administren as actividades de TI. A incorporación dun modelo operativo e unha linguaxe común para todas as partes dun negocio involucradas en TI é un dos pasos iniciais máis importantes de cara a un bo goberno. Tamén brinda un marco de traballo para a medición e monitorización do desempeño de TI, comunicándose cos provedores de servizos e integrando as mellores prácticas de administración. Un modelo de procesos fomenta a propiedade dos procesos, permitindo que se definan as responsabilidades.

### *PLANIFICAR E ORGANIZAR (PO)*

Este dominio cobre as estratexias e as tácticas e ten que ver con identificar a maneira en que TI pode contribuír do mellor xeito ao logro dos obxectivos do negocio. Ademais, a realización da visión estratéxica require ser planificada, comunicada e administrada desde diferentes perspectivas. Finalmente, débese implantar unha estrutura organizacional e unha estrutura tecnolóxica apropiada. Este dominio cobre os seguintes cuestionamentos típicos da xerencia:

- Están alineadas as estratexias de TI e do negocio?
- A empresa está alcanzando un uso óptimo dos seus recursos?
- Entenden todas as persoas dentro da organización os obxectivos de TI?
- Enténdense e adminístranse os riscos de TI?
- É apropiada a calidade dos sistemas de TI para as necesidades do negocio?

### *ADQUIRIR E IMPLANTAR (AI)*

Para levar a cabo a estratexia de TI, as solucións de TI precisan ser identificadas, desenvolvidas ou adquiridas, así como implantadas e integradas nos procesos do negocio. Este dominio cobre os seguintes cuestionamentos da xerencia:

- É probable que os novos proxectos xeren solucións que satisfagan as necesidades do negocio?
- É probable que os novos proxectos sexan entregados a tempo e dentro do orzamento?
- Traballarán adecuadamente os novos sistemas así que sexan implementados?
- Os cambios non afectarán ás operacións actuais do negocio?

### *ENTREGAR E DAR SOPORTE (DS)*

Este dominio cobre a entrega en si dos servizos requiridos, o que inclúe a prestación do servizo, a administración da seguridade e da continuidade, o soporte do servizo aos usuarios e a administración dos datos e das instalacións operativas.

Polo xeral, cobre as seguintes preguntas da xerencia:

- Estando entregando os servizos de TI de acordo coas prioridades do negocio?
- Están optimizados os custos de TI?
- É capaz a forza de traballo de utilizar os sistemas de TI de maneira produtiva e segura?
- Están implantadas de forma adecuada a confidencialidade, a integridade e mais a dispoñibilidade?

### *MONITORAR E AVALIAR (MA)*

Todos os procesos de TI deben avaliarse de forma regular no tempo en canto á súa calidade e cumprimento dos requirimentos de control. Este dominio abrangue a administración do desempeño, a monitorización do control interno, o cumprimento regulatorio e a aplicación do goberno. Polo xeral, abrangue as seguintes preguntas da xerencia:

- Mídese o desempeño de TI para detectar os problemas antes de que sexa demasiado tarde?
- A Xerencia garante que os controis internos son efectivos e eficientes?



- Pódese vincular o desempeño do que TI realizou coas metas do negocio?
- Mídense e comunícanse os riscos, o control, o cumprimento e o desempeño?

Ao longo destes catro dominios, COBIT identificou 34 procesos de TI usados normalmente. Namentres a maioría das empresas definiu as responsabilidades de planificar, construír, executar e monitorar para TI, e a maioría teñen os mesmos procesos clave, poucas teñen a mesma estrutura de procesos ou aplicaron todos os 34 procesos de COBIT. COBIT proporciona unha lista completa de procesos que pode ser utilizada para verificar que se completan as actividades e responsabilidades; con todo, non é necesario que se apliquen todas, e, aínda máis, pódense combinar segundo necesite cada empresa.

Para cada un destes 34 procesos ten un enlace ás metas de negocio e TI que soporta. Información de como se poden medir as metas, tamén se proporcionan cales son as súas actividades clave e entregables principais, e quen é o responsable delas.

### **1.2.1.3 BASEADO EN CONTROIS**

COBIT define obxectivos de control para os 34 procesos, así como para o proceso xeral e os controis de aplicación.

Control defínese como as políticas, procedementos, prácticas e estruturas organizacionais deseñadas para brindar unha seguridade razoable de que os obxectivos de negocio se alcanzarán, e os eventos non desexados serán previstos ou detectados e corrixidos.

A xerencia de operacións usa os procesos para organizar e administrar as actividades de TI en curso. COBIT brinda un modelo xenérico de procesos que representa todos os procesos que normalmente se atopan nas funcións de TI, proporcionando un modelo de referencia xeral e entendible para a xerencia de operacións de TI e para a xerencia de negocios. Para lograr un goberno efectivo, os xerentes de operacións deben implantar os controis necesarios dentro dun marco de control definido para todos os procesos TI. Xa que os obxectivos de control de TI de COBIT están organizados por procesos de TI, o marco de traballo brinda vínculos claros entre os requirimentos de goberno de TI, os procesos de TI e os controis de TI.

Cada un dos procesos de TI de COBIT ten un obxectivo de control de alto nivel e varios obxectivos de control detallados. Como un todo, representan as características dun proceso ben administrado.

Os obxectivos de control detallados identifícanse por dous caracteres que representan o dominio (PO, AI, DS e MA), máis un número de proceso e un número de obxectivo de control. Ademais dos obxectivos de control detallados, cada proceso COBIT ten requirimentos de control xenéricos que se identifican con PCn, que significa Control de Proceso número. Débense tomar como un todo, xunto cos obxectivos de control do proceso para ter unha visión completa dos requirimentos de control.

#### *PC1 Metas e Obxectivos do Proceso*

Definir e comunicar procesos, metas e obxectivos específicos, medibles, accionables, reais, orientados a resultado e en tempo (SMARRT) para a execución efectiva de cada proceso de TI, asegurando que están enlazados ás metas de negocio e que se soportan por métricas adecuadas.

#### *PC2 Propiedade do Proceso*

Asignar un dono para cada proceso de TI e definir claramente os roles e responsabilidades do dono do proceso. Inclúe, por exemplo, responsabilidade do deseño do proceso, interacción con outros procesos, rendición de contas dos resultados finais, medición do desempeño do proceso e a identificación de mellora das oportunidades.

### *PC3 Proceso Repetible*

Diseñar e establecer cada proceso clave de TI de tal maneira que sexa repetible e consecuentemente produza os resultados esperados. Prover unha secuencia lóxica pero flexible e escalable de actividades que leve aos resultados desexados e que sexa o suficientemente áxil para manexar as excepcións e urxencias. Usar procesos consistentes, cando sexa posible, e axustalos só cando non se poida evitar.

### *PC4 Roles e Responsabilidades*

Definir as actividades clave e entregables finais do proceso. Asignar e comunicar roles e responsabilidades non ambiguas para a execución efectiva e eficiente das actividades clave e a súa documentación, así como a rendición de contas para os entregables finais do proceso.

### *PC5 Políticas, Plans e Procedementos*

Definir e comunicar como todas as políticas, plans e procedementos que dirixen os procesos de TI están documentados, revisados, mantidos, aprobados, almacenados, comunicados e usados para o adestramento. Asignar responsabilidades para cada unha destas actividades e, en momentos oportunos, revisar se se executan correctamente. Asegurar que as políticas, plans e procedementos son accesibles, correctos, entendidos e actualizados.

### *PC6 Desempeño do Proceso*

Identificar un conxunto de métricas que proporcionen visión das saídas e o desempeño do proceso. Establecer obxectivos que se reflectan

nas metas do proceso e os indicadores de desempeño de tal xeito que permitan o logro das metas dos procesos.

#### **1.2.1.4 IMPULSADO POLA MEDICIÓN**

Unha necesidade básica de toda empresa é entender o estado dos seus propios sistemas de TI e decidir que nivel de administración e control debe proporcionar. Para decidir o nivel correcto, a xerencia debe preguntarse: Ata onde debemos ir?, e está o custo xustificado polo beneficio?

A obtención dunha visión obxectiva do nivel de desempeño propio dunha empresa non é sinxela. Que se debe medir e como? As empresas deben medir onde se atopan e onde se requiren melloras, e implantar un xogo de ferramentas xerenciais para monitorar esta mellora. COBIT atende estes temas a través de:

- Modelos de madurez que facilitan a avaliación por medio de benchmarking e a identificación das melloras necesarias na capacidade.
- Metas e medicións de desempeño para os procesos de TI, que demostran como os procesos satisfán as necesidades do negocio e de TI, e como se usan para medir o desempeño dos procesos internos baseados nos principios dun marcador de puntuación balanceado (*balanced scorecard*).
- Metas de actividades para facilitar o desempeño efectivo dos procesos.

#### **1.2.2 MODELOS DE MADUREZ**

Cada vez con máis frecuencia pídeselles aos directivos de empresas corporativas e públicas que consideren ata que punto se está administrando correctamente TI. Como resposta a isto, débese desenvolver un plan de negocio para mellorar e alcanzar o nivel apropiado de

administración e control sobre a infraestrutura de información. Aínda que poucos argumentarían que isto non é algo bo, débese considerar o equilibrio do custo/beneficio e estas preguntas relacionadas:

- Que está facendo a nosa competencia na industria e como estamos situados en relación con eles?
- Cales son as mellores prácticas aceptables na industria e como estamos situados respecto destas prácticas?
- Partindo destas comparacións, pódese dicir que estamos facendo abondo?
- Como identificamos o que cómpre facer para acadar un nivel adecuado de administración e control sobre os nosos procesos de TI?

Pode resultar difícil proporcionar respostas significativas a estas preguntas. A xerencia de TI está buscando constantemente ferramentas de avaliación para benchmarking e ferramentas de autoavaliación como resposta á necesidade de saber qué facer de maneira eficiente. Comezando cos procesos e os obxectivos de control de alto nivel de COBIT, o dono do proceso débese poder avaliar de forma progresiva comparándoo cos obxectivos de control. Isto responde a tres necesidades:

1. Unha medición relativa de onde se encontra a empresa.
2. Un xeito de decidir cara a onde ir de forma eficiente.
3. Unha ferramenta para medir o avance comparándoo coa meta.

O modelo de madurez para a administración e o control dos procesos de TI baséase nun método de avaliación da organización, de tal forma que se poida avaliar a si mesma desde un nivel de non-existente (0) ata un nivel de optimizado (5). Este enfoque derívase do modelo de madurez que o Software Engineering Institute definiu para a madurez da capacidade do desenvolvemento de software. Calquera que sexa o modelo, as escalas non deben ser demasiado granulares, xa que iso faría que o sistema fose difícil de usar e suxeriría unha precisión que non é xustificable debido a que, en

xeral, o fin é identificar onde se atopan os problemas e como fixar prioridades para as melloras. O propósito non é avaliar o nivel de adherencia aos obxectivos de control.

Os niveis de madurez están deseñados como perfís de procesos de TI que unha empresa recoñecería como descricións de estados posibles actuais e futuros. Non están deseñados para seren usados como un modelo limitante, onde non se pode pasar ao seguinte nivel superior sen cumprir todas as condicións do nivel inferior. Cos modelos de madurez de COBIT, ao revés da aproximación do CMM orixinal de SEI, non hai intención de medir os niveis de forma precisa ou de probar a certificar que un nivel se conseguiu con exactitude. Unha avaliación da madurez de COBIT resultará nun perfil onde as condicións relevantes a diferentes niveis de madurez se conseguiron.

### **1.2.3 MEDICIÓN DO DESEMPEÑO**

As métricas e as metas defínense en COBIT a tres niveis:

- As metas e métricas de TI que definen o que o negocio espera de TI (o que o negocio usaría para medir a TI).
- Metas e métricas de procesos que definen o que o proceso de TI debe xerar para darlles soporte aos obxectivos de TI (cómo sería medido o dono do proceso de TI).
- Métricas de desempeño dos procesos (miden con que nivel de corrección se desempeña o proceso para indicar se é probable alcanzar as metas).

## **1.3 PROPOSTAS DE PROXECTOS (CASOS DE NEGOCIO OU «BUSINESS CASE»), ANÁLISE DE CUSTOS/BENEFICIOS, ANÁLISE DE RISCOS, FACTORES CRÍTICOS DE ÉXITO. VALIT.**

### **1.3.1 INTRODUCCIÓN**

#### **1.3.1.1 OBXECTIVO DE VAL IT**

A iniciativa Val IT, na que se inclúen investigacións, publicacións e servizos de soporte, ten como obxectivo axudarlle á xerencia a garantir que as organizacións logren un valor óptimo dos investimentos de negocio posibilitados por TI a un custo económico, e cun nivel coñecido e aceptable de risco. Val IT proporciona guías, procesos e prácticas de soporte para axudarlles ao consello e á dirección executiva a comprender e desempeñar os seus roles relacionados cos devanditos investimentos. Aínda que é aplicable a todas as decisións de investimento, Val IT está dirixido principalmente aos investimentos de negocio posibilitados por TI: investimentos de negocio importantes no mantemento, crecemento ou transformación do negocio cun compoñente crítico de TI, onde TI é un medio para conseguir un fin, sendo o fin o de contribuír ao proceso de creación de valor na empresa. En concreto, Val IT céntrase na decisión de investir (estamos facendo o correcto?) e na realización de beneficios (estamos obtendo beneficios?). COBIT, o estándar normalmente aceptado internacionalmente para o control sobre TI, céntrase especificamente na execución (estámolo facendo correctamente e estámolo logrando ben?).

A aplicación eficaz dos principios, procesos e prácticas contidos en Val IT ha permitirlles ás organizacións:

- Aumentar o coñecemento e transparencia dos custos, riscos e beneficios, dando como resultado unhas decisións de xestión moito mellor informadas.
- Aumentar a probabilidade de seleccionar investimentos que teñen o potencial de xerar a maior rendibilidade.
- Aumentar a probabilidade de éxito ao executar os investimentos elixidos de modo que logren ou sobrepasen a súa rendibilidade potencial.

- Reducir custos non facendo cousas que non se deben facer e tomando rapidamente medidas correctivas, ou terminando investimentos que non están cumprindo o seu potencial esperado
- Reducir o risco de fracaso, especialmente o fracaso de alto impacto.
- Reducir sorpresas en relación co custo e entrega de TI, e desa forma aumentar o valor do negocio, reducir custos innecesarios e aumentar o nivel global de confianza en TI.

#### **1.3.1.2 A NECESIDADE DE VAL IT**

O nivel de investimento en TI é significativo e segue aumentando. Son poucas as organizacións que hoxe en día poderían funcionar durante moito tempo sen a súa infraestrutura de TI. Así e todo, aínda que hai moitos exemplos de organizacións que xeran valor investindo en TI, ao mesmo tempo hai moitos executivos que se preguntan se o valor de negocio realizado é proporcional ao nivel de investimento. Polo tanto, non sorprende que exista cada vez máis demanda por parte dos consellos e dirección executiva dunhas guías xeralmente aceptadas sobre a toma de decisións de investimento e a realización de beneficios. Os investimentos de negocio posibilitados por TI, cando se xestionan ben dentro dun marco de goberno efectivo, supoñen para as organizacións unhas oportunidades importantes para crear valor. Moitas organizacións prósperas crearon valor seleccionando os investimentos oportunos e xestionándoos con éxito desde o concepto, pasando pola implantación ata a realización do valor esperado. Sen un goberno efectivo e unha boa xestión, os investimentos de negocio posibilitados por TI xeran unha oportunidade igualmente importante para destruír valor. A mensaxe é clara. Os investimentos de negocio posibilitados por TI poden reportar enormes beneficios.

#### **1.3.1.3 UNHA NOVA PERSPECTIVA**

Unha lección fundamental que cómpre aprender das experiencias citadas e de moitas outras é que co investimento en TI xa non se trata de



implantar solucións de TI, senón que se trata de implantar o cambio posibilitado por TI. O valor de negocio xérao o que fan as organizacións con TI e non a tecnoloxía en si. Isto entraña maior complexidade e maior risco que no pasado. As prácticas de xestión que se aplicaron tradicionalmente xa non son suficientes. Existe un claro incentivo para a dirección, para que garanta o establecemento dos procesos adecuados de goberno e xestión que optimicen a creación de valor. Un compoñente esencial do goberno da empresa é garantir a obtención de valor dos investimentos posibilitados por TI. Implica unha selección acertada dos investimentos e a súa xestión como activo ou servizo durante todo o seu ciclo de vida. En COBIT establécese un marco global para a xestión e entrega de servizos de alta calidade baseados na tecnoloxía de información. Fíxanse mellores prácticas para os medios de contribuír ao proceso de creación de valor. Agora en Val IT engádense as mellores prácticas para o fin, proporcionando así os medios para medir, monitorar e optimizar de forma inequívoca o rendemento, tanto financeiro como non financeiro, do investimento en TI. Está comprobado que a aplicación intelixente de procesos, segundo están definidos en COBIT e Val IT, pode axudarlles ás empresas a mellorar de forma significativa o rendemento dos seus investimentos. Non obstante, non é abondo ter simplemente os procesos establecidos. Existen probas empíricas de que o impacto máis importante na creación de valor, no que se refire á rendibilidade accionarial total, á eficiencia do capital ou ás rendas de activos, o produce a crecente madurez do proceso, segundo está definida no Modelo de Madurez de Capacidades (CMM), en combinación con economías de escala e alcance. Estas conclusións corrobóranse un recente estudo onde se comprobou que os investimentos en TI teñen pouco impacto a menos que vaian acompañados de prácticas de xestión de alta calidade, e que aquelas compañías que combinan boas prácticas de xestión con investimentos en TI son as que mellores resultados obteñen.

Val IT complementa a COBIT desde o punto de vista financeiro e de negocio e ha axudar a todos aqueles con un interese na entrega de valor a

partir de TI. É relevante para todos os niveis de dirección en todos os sectores do negocio e TI, desde o CEO e o consello ata todos aqueles implicados directamente nos procesos de selección, aprovisionamento, desenvolvemento, implantación, despregamento e obtención de beneficios. Val IT contén guías esenciais para todos.

### **1.3.2 O MARCO VALIT**

#### **1.3.2.1 PRINCIPIOS DE VAL IT**

Os principios de Val IT son:

- Os investimentos posibilitados por TI débense xestionar como carteira de investimentos.
- Os investimentos posibilitados por TI incluírán o alcance total de actividades que son necesarias para lograr o valor de negocio.
- Os investimentos posibilitados por TI débense xestionar ao longo do seu ciclo de vida económico completo.
- Nas prácticas de entrega de valor, cómpre recoñecer que existen distintas categorías de investimento cuxa avaliación e xestión será diferente.
- Nas prácticas de entrega de valor, débense definir e monitorar as métricas claves e responder rapidamente a calquera cambio ou desviación.
- As prácticas de entrega de valor implicarán a todos os socios e hase asignar a responsabilidade correspondente para a entrega de capacidades e a obtención de beneficios do negocio.
- Cómpre facer unha monitorización, avaliación e mellora continua das prácticas de entrega de valor.

#### **1.3.2.2 PROCESOS DE VAL IT**

Para obter a rendibilidade do investimento, os socios dos investimentos posibilitados por TI deberán aplicarles os principios de Val IT aos seguintes procesos:

- Goberno de Valor (VG). O goberno de valor ten como obxectivo optimizar o valor dos investimentos posibilitados por TI dunha organización:

- Establecendo o marco de goberno, monitorización e control.
- Marcando a dirección estratéxica para os investimentos.
- Definindo as características da carteira de investimentos.

- Xestión de Carteira (PM). A xestión de carteira ten como obxectivo asegurar que a carteira global de investimentos posibilitados por TI dunha organización estea aliñada cos obxectivos estratéxicos da mesma mediante:

- O establecemento e xestión de perfís de recursos.
- A definición de limiares para o investimento.
- A avaliación, priorización e selección, aprazamento ou rexeitamento de novos investimentos.
- A xestión da carteira global.
- A monitorización e informes sobre o rendemento da carteira.

- Xestión de Investimentos (IM). A xestión de investimentos ten como obxectivo asegurar que os programas individuais de investimentos posibilitados por TI entreguen un valor óptimo a un custo económico e cun nivel coñecido e aceptable de risco, mediante:

- A identificación de necesidades de negocio.
- Un claro entendemento dos programas de investimento candidatos.
- A análise das alternativas.
- A definición do programa e a documentación dun caso de negocio detallado, incluíndo detalles dos beneficios.

- A asignación clara de responsabilidade e propiedade.
- A xestión do programa durante todo o seu ciclo de vida económico.
- A monitorización e informes sobre o rendemento do programa.

Esta publicación ten como enfoque un elemento clave do proceso de xestión de investimentos: o caso de negocio. As sementes do éxito ou fracaso prenden no caso de negocio. Así e todo, as organizacións en xeral non son moi hábiles no desenvolvemento e documentación de casos de negocio completos e comparables. O caso de negocio contén un conxunto de opinións e suposicións sobre como se pode crear valor. Para garantir a consecución dos resultados esperados, é necesario que as devanditas opinións e suposicións estean ben probadas. Uns indicadores cualitativos e cuantitativos permiten a validación do caso de negocio e dan ideas para as decisións de investimento no futuro. Aquí é onde empeza todo. En Val IT facilítanse guías para maximizar a calidade dos casos de negocio, poñendo especial énfase na definición de indicadores claves, tanto financeiros (valor neto actual, taxa interna de rendibilidade e período de recuperación) como non financeiros, e na avaliación e valoración global do risco de perdas.

O caso de negocio non é un documento puntual e estático, senón unha ferramenta operativa que hai que actualizar continuamente para reflectir a realidade actual e para darlle soporte ao proceso de xestión de carteira.

### **1.3.3 VAL IT. O CASO DE NEGOCIO**

#### **1.3.3.1 INTRODUCCIÓN: A IMPORTANCIA DO CASO DE NEGOCIO**

O caso de negocio —desestimado con demasiada frecuencia como obstáculo burocrático que hai que superar co mínimo esforzo posible— é unha das ferramentas máis valiosas dispoñibles para a dirección, para guiala na creación de valor de negocio. A experiencia demostra que a calidade do caso de negocio e dos procesos implicados na súa creación e uso durante todo o ciclo de vida económico dun investimento ten un

impacto enorme na creación de valor. Os casos de negocio baséanse nas expectativas dos sucesos futuros e teñen que dar resposta aos «Catro Interrogatorios»:

- Estamos facendo o correcto? Que se propón e para que resultado de negocio, e como contribúen os proxectos dentro do programa?
- Estámolo facendo correctamente? Como se vai facer e que se está facendo para asegurar que encaixe con outras capacidades actuais ou futuras?
- Estámolo logrando ben? Que plan temos para facer o traballo, e que será necesario en canto a recursos e financiamento?
- Estamos obtendo os beneficios? Como se van entregar os beneficios? Cal é o valor do programa?

O proceso de desenvolvemento do caso de negocio debe ser propiedade do promotor do negocio e implicar a todos os socios claves no desenvolvemento e documentación dun coñecemento completo e compartido dos resultados de negocio esperados (resultados tanto intermedios como finais) dun investimento. Debe describir como se van medir os resultados do negocio, así como o pleno alcance das iniciativas necesarias para lograr os resultados esperados. Entre estas iniciativas débese incluír calquera cambio necesario na natureza do negocio da empresa, os procesos de negocio, as habilidades e competencias persoais, a tecnoloxía impulsora e a estrutura organizacional. No caso de negocio, identifícase a natureza da contribución de cada iniciativa, como se vai medir esta contribución, e todas as suposicións claves. No caso de negocio débense establecer tamén as métricas ou indicadores similares para a monitorización da validez das devanditas suposicións. Tamén é necesario identificar e documentar os riscos principais, tanto para a realización con éxito das iniciativas individuais como para a consecución dos resultados desexados, xunto coas accións de mitigación. A decisión de proceder ou

non cun investimento posibilitado por TI tómase primeiro a nivel de programa individual por parte do promotor do negocio, determinando se o caso de negocio é abondo sólido para a súa avaliación a nivel de carteira. A nivel de carteira, valórase o valor relativo do programa fronte a outros programas activos e candidatos. Para facilitar este proceso debe haber un método establecido para chegar a un valor normalizado, ou a un conxunto de beneficios de aliñamento, financeiros e non financeiros, e puntuacións de risco para os casos de negocio individuais.

Con frecuencia, a reacción á presentación dos casos de negocio neste contexto é que se están complicando demasiado as cousas. É importante distinguir entre os procesos de reflexión que se deben seguir á hora de emprender un investimento importante posibilitado por TI e o nivel de rigor e detalle necesario para darlle soporte e documentar a devandita reflexión. No marco de Val IT, introdúcese o concepto de categorías de investimento con distintos niveis de complexidade e graos de liberdade á hora de asignar fondos. A categoría do investimento, as súas dimensións, o impacto do seu fracaso e a súa posición no ciclo de vida económico, todos son factores que permiten determinar a que partes do caso de negocio hai que prestarlles maior atención e que nivel de detalle é necesario.

### **1.3.3.2 ESTRUCTURA DO CASO DE NEGOCIO**

O desenvolvemento do caso de negocio consiste en oito pasos:

#### Paso 1 - Elaboración da Folla de Datos

A folla de datos do caso de negocio contén todos os datos necesarios para a análise do aliñamento estratéxico, os beneficios financeiros e non financeiros, e os riscos do programa. Para cada partida, polo que respecta ás etapas de elaboración, implementación, operación e retiro, recóllense os

datos dos escenarios de caso mellor / caso peor, segundo corresponda, para o investimento posibilitado por TI.

### Paso 2 - Análise de Aliñamento

Case sempre haberá máis oportunidades de investimento nunha organización que recursos para asumilas. A análise de aliñamento constitúe un método para garantir a utilización efectiva e eficiente de recursos escasos.

### Paso 3 - Análise Financeira Baseada no Incremento de 'Cash Flows' Descontados

Un obxectivo clave da elaboración dun caso de negocio é o de expresar os beneficios en termos financeiros, e débese intentar na medida do razoablemente posible. Pódese soportar o exercicio en técnicas avanzadas tales como a valoración do valor real da opción, así como en investigacións empíricas con datos de valoración obtidas doutros investimentos posibilitados por TI.

### Paso 4 - Análise de Beneficios non Financeiros

Aínda que un obxectivo clave da elaboración dun caso de negocio é o de expresar os beneficios en termos financeiros e débese intentar na medida do razoablemente posible, non se debe pasar por alto os beneficios non financeiros. De feito, no sector público e en organizacións sen ánimo de lucro, moitos dos resultados de negocio desexados son de carácter non financeiro.

### Paso 5 - Análise de Risco

Os programas non son iguais no que se refire á probabilidade de que entreguen o valor de negocio esperado ou á probabilidade de que cumpran cos obxectivos de custo e prazo. Dous programas co mesmo nivel de aliñamento estratéxico e valor financeiro previsto poden ter características de risco moi diferentes.

### Paso 6 - Optimización do Risco e Rendemento

A decisión de proceder ou non cun investimento posibilitado por TI tómaa primeiro o promotor do negocio a nivel de programa individual, determinando se o caso de negocio é o suficientemente sólido para a súa valoración a nivel de carteira. A nivel de carteira, contrástase o valor relativo do programa cos programas activos e candidatos. Para facilitar este proceso, debe haber un proceso establecido para chegar a un valor normalizado, ou a un conxunto de puntuacións normalizadas de aliñamento global, de beneficios financeiros e non financeiros e de risco para os casos de negocio individuais.

### Paso 7 - Documentar o Caso de Negocio

A categoría do investimento, as súas dimensións, o impacto do seu fracaso e a súa posición no ciclo de vida económico son factores que permiten determinar os compoñentes do caso de negocio aos que lles hai que prestar maior atención, así como o nivel de detalle necesario.

### Paso 8 - Manter o Caso de Negocio

Un caso de negocio non é máis que unha fotografía nun momento dado. Non debe ser creado e revisado só unha vez para determinar se proceder ou non cun investimento para logo ignoralo ou, no mellor dos casos, volver consideralo na revisión post-implementación. É unha ferramenta operacional que debe ser actualizada continuamente durante



todo o ciclo de vida económico dun investimento e aproveitada para darlles soporte á implantación e execución dun programa, incluíndo a obtención 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

Colexiado do CPEIG

## **2. XESTIÓN ESTRATÉXICA DAS TIC. FERRAMENTAS DE PLANIFICACIÓN E CONTROL: CADROS DE MANDO INTEGRAL («BALANCED SCORECARDS»), MAPAS ESTRATÉXICOS, XESTIÓN DE COÑECEMENTOS E INNOVACIÓN.**

## **Tema 2. Xestión estratéxica das TIC. Ferramentas de planificación e control: cadros de mando integral (“balanced scorecards”), mapas estratéxicos, xestión do coñecemento e innovación.**

### **INDICE**

- 2.1 Ferramentas de planificación e control: cadros de mando integral (“balanced scorecards”)
  - 2.1.1 Perspectivas do cadro de mando integral
  - 2.1.2 Deseño do cadro de mando integral
    - 2.1.2.1 Análise da situación actual
    - 2.1.2.2 Desenvolvemento da estratexia xeral do negocio
    - 2.1.2.3 Descomposición en obxectivos
    - 2.1.2.4 Creación do mapa estratéxico da organización
    - 2.1.2.5 Definición das métricas de performance
    - 2.1.2.6 Identificación e deseño de novas iniciativas
  - 2.1.3 Implantación do cadro de mando integral
- 2.2 Mapas estratéxicos
  - 2.2.1 Plan estratéxico
- 2.3 Xestión do coñecemento e innovación
  - 2.3.1 O coñecemento e a súa xestión
  - 2.3.2 A Creatividade
  - 2.3.3 A innovación
    - 2.3.3.1 Tipos de innovación
    - 2.3.3.2 Xestión da innovación

### **2.1 FERRAMENTAS DE PLANIFICACIÓN E CONTROL: CADROS DE MANDO INTEGRAL (“BALANCED SCORECARDS”)**

O Cadro de Mando Integral é unha ferramenta de Xestión Estratéxica cuxa implantación pode axudar a unha empresa a clarificar os seus obxectivos a longo prazo, comunicalos a toda a empresa e traducilos en accións concretas.

### **2.1.1 PERSPECTIVAS DO CADRO DE MANDO INTEGRAL**

O Cadro de Mando Integral, ou Balance ScoreCard (BSC), desenvolvido por Kaplan e Norton, permite transmitir as estratexias definidas por unha organización dun xeito claro e eficiente a todos os integrantes da mesma e, ao tempo, poder traducir ditas estratexias en obxectivos, indicadores e accións concretas.

As estratexias definidas polas máximas autoridades da empresa baséanse en moitos factores, como a análise da posición da empresa no mercado, os recursos cos que conta, os obxectivos a curto e longo prazo e a visión de futuro baseada na intuición do empresario.

O Cadro de Mando Integral formula que primeiro se deben definir as estratexias, é dicir, a onde se quere chegar e como se vai medir o éxito das mesmas. Logo preséntanse os obxectivos intermedios e, para rematar, cómo se van alcanzar.

Estas definicións quedan claras para todos os integrantes da organización, como se formasen parte dun grande equipo, e é unha forma de saber se as súas accións para lograr os devanditos obxectivos son correctas ou non. Todas as empresas teñen sistemas para verificar a marcha das súas actividades.

Máis ou menos automatizados, todas teñen os seus medios, compostos por reportes de vendas, de produción, balances contables, etc. Este conxunto de informes e reportes chámase “Sistemas de Medición de Performance”.

O valor agregado do Cadro de Mando Integral é que os sistemas de medición de performance están asociados de forma coherente á estratexia

xeral definida pola dirección da empresa. Neste caso, primeiro formúlase cara a onde se dirixe a empresa e, logo, qué se debe controlar para saber se a marcha é a correcta; para tal fin implántanse os sistemas de información.

A visión e a estratexia xeral da empresa ordénanse mediante o Cadro de Mando Integral ao redor de catro perspectivas básicas: finanzas, clientes, procesos internos, e aprendizaxe e crecemento:

- A perspectiva **finanzas** enfócase en producir mellores ganancias para os accionistas ou donos das organizacións. Cando se trata dunha organización sen fins de lucro, esta perspectiva vese como o obxectivo de maximizar a utilización do orzamento. Todo o esforzo de aplicar un programa de Cadro de Mando Integral vai dirixido a mellorar este aspecto a través de melloras na xestión do resto das perspectivas.

- A perspectiva **clientes** inclúe aqueles obxectivos estratéxicos que teñen en conta a satisfacción do cliente. Un cliente máis satisfeito consumirá máis os nosos servizos ou produtos, mellorará a nosa imaxe e situaranos mellor ante a nosa competencia. Xa que logo, unha mellora neste aspecto repercutirá directamente nas ganancias da nosa empresa, é dicir, na perspectiva financeira.

- A perspectiva **procesos** internos refírese a que para mellorar a satisfacción do cliente ou para mellorar a utilización dos nosos recursos, vía redución de custos ou gastos, seguramente se deben mellorar os procesos internos en canto á cadea de valor. Calquera mellora neste aspecto ten un impacto nas perspectivas de clientes e finanzas.

- A perspectiva de aprendizaxe e crecemento inclúe aqueles aspectos relacionados cos recursos humanos necesarios para poder implantar as melloras no resto das perspectivas. Adoita mostrarse como a

base do resto das estratexias, tanto nos aspectos operativos, para poder cumprir coas metas de mellora nos procesos internos, como na satisfacción dos empregados, condición necesaria para mellorar a atención aos clientes.

A combinación das catro perspectivas nun sistema integrado compoñerán o Cadro de Mando Integral. Imos ver un exemplo de aplicación das perspectivas dun Cadro de Mando Integral: Supoñamos unha entidade con sucursais con atención a clientes na que queremos reducir o tempo medio de permanencia no local de 20 a 10 minutos. A estratexia é mellorar a atención aos clientes e o obxectivo é a redución de tempo. En canto á perspectiva financeira, as melloras van dirixidas a que a mellor atención dea como resultado que máis clientes queiran utilizar os nosos servizos. Desa maneira obteremos mellores resultados financeiros.

A mellora na calidade de atención relacionada coa perspectiva clientes, resultará nunha maior satisfacción dos mesmos. A mellora nos procesos necesarios para poder atender máis rápido, xa sexa pola diminución de pasos na cadea de procesos que non agregan valor, ou ben por cambios na loxística de Atención, está relacionada coa perspectiva de procesos internos.

Todas as accións necesarias para realizar estes cambios están relacionadas entre si, e unhas non poden ser desenvolvidas sen a colaboración das outras. Ao tempo, non se pode implantar un programa de melloras sen considerar os riscos que poden aparecer se se lle dá máis importancia a unha perspectiva ca a outra.

Concluíndo, o Cadro de Mando Integral serve para comunicar a visión e a estratexia da organización, transformándoa en accións concretas.

### **2.1.2 DESEÑO DO CADRO DE MANDO INTEGRAL**

O Cadro de Mando Integral non é só o sistema informático que brinda unha serie de medidas a controlar, senón que implica un cambio no *management* estratéxico de toda a organización e, xa que logo, debe ser impulsado pola máis alta Dirección.

Un programa de Cadro de Mando Integral non ten data de terminación definida e todas as persoas da empresa deben participar do mesmo. Non hai diferenzas con outras iniciativas estratéxicas de melloras de performance ou calidade.

A seguinte é a enumeración das etapas a seguir no deseño do Cadro de Mando Integral:

1. Análise da situación actual.
2. Desenvolvemento da estratexia xeral de negocio.
3. Descomposición en obxectivos.
4. Creación do mapa estratéxico da organización.
5. Definición das métricas de performance.
6. Identificación e deseño de novas iniciativas.

#### **2.1.2.1 ANÁLISE DA SITUACIÓN ACTUAL**

É a etapa inicial do programa; a que implica ver onde está situada a empresa e onde se quere chegar. Adoita incluír unha análise DAFO (Debilidades, Ameazas Fortalezas e Oportunidades), unha análise de mercado, unha análise económica-financeira dos últimos 6 meses e unha análise de capacidade operativa que indique os recursos materiais, de infraestrutura e humanos cos que conta a empresa. Esta análise será a base do compromiso de inicio e da definición da misión e visión da organización.



A misión da organización é o propósito da mesma, é dicir, a razón de ser da empresa. A visión é o obxectivo cara a onde apuntan todas as accións que se desenvolverán; é dicir, a onde se quere chegar.

#### **2.1.2.2 DESENVOLVEMENTO DA ESTRATEXIA XERAL DE NEGOCIO**

Unha vez definidas a misión e a visión da organización, hai que definir a estratexia xeral de negocio, é dicir, os obxectivos a longo prazo, entre 3 e 5 anos. A estratexia consiste en definir de qué forma se vai acadar a visión. Un exemplo de estratexia pode ser “desenvolver novos produtos”.

Ao mesmo tempo que se presentan as estratexias ou obxectivos a longo prazo, deben establecerse metas numéricas para eses obxectivos, metas que adoitan expresarse en termos de porcentaxe.

Poden utilizarse moitas ferramentas, entre elas a matriz DAFO de estratexias combinadas.

Nela pártese dunha análise DAFO convencional, onde se identifican Fortalezas, Oportunidades, Debilidades e Ameazas e, logo, por cada cruzamento de características, elabóranse as estratexias que aproveitan as oportunidades de mellora que blindan ditos cruces.

#### **2.1.2.3 DESCOMPOSICIÓN EN OBXECTIVOS**

Unha vez definida a estratexia global, cómpre definirmos os obxectivos máis detallados e a curto prazo. Estes obxectivos deben estar distribuídos nas catro perspectivas: finanzas, clientes, procesos internos, e aprendizaxe e crecemento. Para cada unha das perspectivas existen certos obxectivos comúns á maioría de empresas, e outros máis específicos, que

dependen da situación da empresa e do xiro de negocio específico da mesma.

Canto aos temas estratéxicos para a perspectiva finanzas, hai que tratar de mellorar o valor financeiro das accións da empresa e do Retorno do Investimento (ROI). Isto conseguíremolo mediante o crecemento das ganancias e do mix de produtos, o incremento da produtividade e a redución de custos e algunhas melloras na utilización dos arquivos e a estratexia de investimento.

Canto aos temas estratéxicos para a perspectiva clientes, cabe salientar que mellorando as variables relacionadas cos clientes mellorarán as nosas ganancias financeiras, ao ser os clientes nosa principal fonte de ingresos. Con respecto á relación da nosa empresa cos clientes e co mercado, hai que ter en conta os seguintes aspectos: participación de mercado, retención de clientes, adquisición de clientes, satisfacción do cliente e rendibilidade do cliente. Ademais, hai que ter en conta algunhas características relacionadas co que pensamos que o cliente valora da nosa empresa e que imos chamar “proposicións de valor”. Trátase dos atributos do produto ou servizo, a relación co cliente e a imaxe e reputación da empresa.

As estratexias relacionadas coa perspectiva de procesos internos defínense en función da cadea de valor do produto. A cadea de valor dos procesos internos dunha empresa está relacionada co ciclo de vida do produto e descomponse en tres etapas: procesos de innovación, procesos operativos e procesos de servizo posvenda. Estes procesos abarcan desde que se detecta a necesidade do cliente ata que as necesidades do cliente quedan satisfeitas.

Nos procesos de innovación, as estratexias van dirixidas á forma en que a organización manexa os custos e os investimentos en investigación

básica, investigación aplicada, desenvolvemento do produto e marketing. Nos procesos operativos trátase de mellorar as tarefas que van desde producir, fabricar un produto ou a estandarización na metodoloxía para prestar un servizo, ata a distribución ou entrega dos servizos. Nos procesos posvenda céntranse nos servizos e produtos que se ofrezan ao cliente trala venda, tales como garantías, políticas de devolución, etc.

Canto aos temas estratéxicos para a perspectiva de aprendizaxe e crecemento, se queremos introducir cambios no xeito de facer as cousas, o noso persoal debería estar motivado para realizar ditos cambios e capacitado para executar as tarefas de forma apropiada. Ademais, hai que contar cos recursos materiais necesarios para efectuar as tarefas indicadas. Os devanditos recursos inclúen, por exemplo, os sistemas informáticos adecuados, as ferramentas, os uniformes, etcétera. Non podemos pretender clientes satisfeitos se primeiro non temos empregados satisfeitos.

#### **2.1.2.4 CREACIÓN DO MAPA ESTRATÉXICO DA ORGANIZACIÓN**

Unha vez definidos os obxectivos e as estratexias a longo prazo, dentro de cada unha das perspectivas, hai que analizar cómo cada un deses obxectivos se vai encadeando e afectando entre si. Ao tomar unha decisión nun dos aspectos, esa decisión vai afectando ao resto das dimensións nun efecto cadoiro. Para a creación do mapa estratéxico hai que ir relacionando os obxectivos, utilizando conexións lóxicas (se...entón) nas perspectivas correspondentes a cada un deles. Ditas relacións utilizaranse para determinar os indicadores e métricas que informarán cando unha estratexia ha ter éxito ou non.

#### **2.1.2.5 DEFINICIÓN DAS MÉTRICAS DE PERFORMANCE**

Tras crear o mapa estratéxico, onde poderemos observar cómo se relacionan cada un dos obxectivos, hai que analizar cales serán as métricas ou indicadores clave, que permitirán coñecer en que medida se está alcanzando cada obxectivo.

O proceso de definir estas medidas é iterativo, é dicir, por cada unha das relacións e obxectivos faise un listado que logo se vai refinando ata quedar co máis significativo. Tamén se pode determinar primeiro as cinco máis importantes e logo amplialas.

Recoméndase non exceder as 25 medidas que, ademais, deben estruturarse en indicadores causa (porque afectan a outro obxectivo co que están relacionados) e indicadores efecto (que miden a consecución dun obxectivo). As medidas deben estar ben definidas, o valor obtido ten que ser sempre o mesmo, sen importar quen realice a medición, e teñen que ser correctamente entendidas no marco da nosa estratexia.

#### **2.1.2.6 IDENTIFICACIÓN E DESEÑO DE NOVAS INICIATIVAS**

É o último paso no deseño do Cadro de Mando Integral e consiste en definir cales van ser as iniciativas e actividades a desenvolver para poder implantar a nosa estratexia. Cada unha das iniciativas estará unida a un conxunto de métricas ou medidas que permitirán coñecer a súa evolución. Ditas iniciativas deben ser comprendidas como un medio para alcanzar os obxectivos estratéxicos e non coma un fin en si mesmas.

#### **2.1.3 IMPLEMENTACIÓN DO CADRO DE MANDO INTEGRAL**

Unha vez definido o Cadro de Mando Integral, hai moitas opcións para implantalo na práctica como unha ferramenta efectiva. A mellor solución depende de cada empresa en particular, e non existe unha regra xeral. A

maioría de empresas poden crear o seu Cadro de Mando Integral utilizando as ferramentas de automatización de oficina dispoñibles.

Recordemos que o Cadro de Mando Integral debe:

- Axudarnos na definición de estratexias, obxectivos, medidas, metas e accións.
- Facilitarnos a comunicación da dirección estratéxica e axudar a transmitir o que debe facer cada integrante da organización para que as súas accións individuais favorezan o cumprimento dos obxectivos.
- Permitirnos comparar a evolución das metas e o seu cumprimento.
- Ser simple de entender e fácil de manexar para o usuario final e fácil de manter para os administradores.

Se as ferramentas non están integradas nun só sistema informático, todo o anterior será difícil de cumprir e, xa que logo, o Cadro de Mando Integral fracasará.

Entre os factores de risco que poden poñer en perigo o éxito dun programa de Cadro de Mando Integral, atópanse:

- Falta de compromiso da Dirección: se a Dirección non se involucra ao comezo do proceso e delega a responsabilidade en xerentes ou mandos medios, hase xerar unha falta de autoridade no líder do proxecto.
- Falta de continuidade: o Cadro de Mando Integral debe ser un programa de longo prazo, realizando os axustes diarios necesarios.
- Sistema de comunicación deficiente: a información debe fluír en ambos sentidos (proporcionar a información para o Cadro de Mando Integral e distribuír os resultados a todas as áreas) para que as persoas vexan os beneficios e non tomen o proxecto como un intento de controlar as súas actividades en lugar dunha ferramenta para o crecemento de toda a organización.

- Definicións débiles: se ao definir os indicadores non se unifica a linguaxe e se fai unha especificación dura que non dea posibilidade a dobres interpretacións, cada persoa fará a súa propia interpretación e iso xerará controversias, co que o programa perderá fiabilidade.
- Problemas na escalabilidade: cando a empresa ten certa envergadura, implántase o Cadro de Mando Integral en certas unidades de negocio, escollidas pola súa importancia, e logo esténdese a toda a organización. Neste caso, o Cadro de Mando Integral componse de varios cadros para cada unidade de negocio. A medida que se vaian agregando máis áreas ao Cadro de Mando Integral será máis complicado manter a integridade da información e a súa actualización.

Na mesma medida, agregaranse potenciais usuarios, e se non temos un sistema que permita a conexión de moitos usuarios, aparecerán problemas de performance ou inconvenientes na distribución (se non é un só sistema integrado). Se implantamos un sistema informático que contemple todas as etapas na explotación do Cadro de Mando Integral, estes factores de risco mencionados poden desaparecer, axudando ao éxito do programa.

Existen unha serie de estándares que tratan sobre qué debe posuír un sistema para poder articular un Cadro de Mando Integral, elaborados pola Balanced Scorecard Collaborative Inc, unha organización fundada polos creadores deste concepto (Kaplan e Norton). Os requisitos funcionais básicos especificados no estándar divídense en catro seccións: deseño do Cadro de Mando Integral; capacitación estratéxica e comunicación; explotación do negocio; e *feedback* e aprendizaxe.

- Deseño do Cadro de Mando Integral: a aplicación debe permitir o desenvolvemento de todas as etapas do deseño do Cadro de Mando Integral.

- Capacitación estratéxica e comunicación: un dos obxectivos do Cadro de Mando Integral é facilitar a comprensión das estratexias da compañía mediante a comunicación e a capacitación, polo que se debe manter a documentación das definicións de obxectivos, medidas, metas e iniciativas aliñadas coas estratexias.
- Explotación do negocio: as iniciativas ou programas de acción son a aplicación concreta para cumprir as metas formuladas e, por ende, os obxectivos estratéxicos. Unha ferramenta que cumpra os estándares do Cadro de Mando Integral debe permitir relacionar as iniciativas cos obxectivos estratéxicos.
- Feedback e aprendizaxe: unha ferramenta de Cadro de Mando Integral efectiva debe facilitar a análise das medidas a controlar mediante unha interface que mostre tanto valores numéricos coma indicadores gráficos.

Existen outros factores que debemos ter en conta á hora de elixir o software que cómpre adquirir ou decidirnos a desenvolver o noso propio software. Entre estes factores inclúese:

- Envergadura da empresa: determina a cantidade de posibles usuarios do sistema, o nivel de automatización e os recursos económicos dos que dispón. Unha empresa pequena é probable que non necesite un gran desenvolvemento informático, o que non significa que non se poida construír un Cadro de Mando Integral utilizando plantillas de cálculo e bases de datos relacionais pequenas.
- Alcance das capacidades funcionais e integración con outros sistemas: se analizamos os estándares para o Cadro de Mando Integral, vemos que en canto ás capacidades de análises, só mencionan a habilidade de mostrar a evolución dos indicadores. Con todo, non mencionan as capacidades de *drill-down* e *drill-up* por diferentes dimensións, como tampouco acerca da integración con

outros sistemas, como taboleiros de control ou *data warehouse*. Se estes existen e son fonte de datos, é posible que os usuarios queiran poder estender as súas análises estratéxicas a análises tácticas, mediante a navegación polo detalle da información.

A implantación ou automatización do Cadro de Mando Integral debe afrontarse como un proxecto máis de sistemas. Como tal, é conveniente aplicar algunha metodoloxía de enxeñería de software que permita:

- Determinar o alcance e obxectivos.
- Analizar a factibilidade e alternativas de solución.
- Estimar correctamente a duración do proxecto.
- Facilitar o mantemento e os cambios na definición.
- Permitir a reutilización e conxunción entre o resto dos sistemas.
- Mellorar a calidade, reducir custos e mellorar o aproveitamento de recursos.

Unha das alternativas posibles é utilizar Métrica III (metodoloxía impulsada polo Ministerio de Administracións Públicas), que se basea nas teorías máis modernas de Enxeñería de Software moderno. As súas etapas son:

- Planificación (PSI)
- Desenvolvemento, que inclúe:
  - Estudo da viabilidade (EVS)
  - Análise (ASI)
  - Deseño (DSI)
  - Construción (CSI)
  - Implantación e aceptación (IAS)
- Mantemento (MSI)



## **2.2 MAPAS ESTRATÉXICOS**

O mapa estratéxico é o primeiro paso para a introdución da metodoloxía de Balanced Scorecard. Que é e para que serve?

O primeiro paso do Balanced Scorecard é a construción do mapa estratéxico, unha ferramenta que debe servir como guía en momentos de incerteza. O mapa constrúese en función do que a organización pensa hoxe con respecto ao futuro. Esta representación gráfica permite ir aprendendo sobre os cambios a medida que se xeran, especialmente en situacións onde non existen certezas.

Os mapas estratéxicos son unha representación visual da estratexia dunha organización e demostran claramente por que unha imaxe é máis poderosa ca mil palabras (ou ata máis poderosa que 25 indicadores de desempeño).

Estes mapas deséñanse baixo unha arquitectura específica de causa e efecto, e serven para ilustrar como interactúan as catro perspectivas do Balanced Scorecard.

1) Os resultados financeiros conséguense unicamente se os clientes están satisfeitos. É dicir, a perspectiva financeira depende de como se constrúa a perspectiva do cliente.

2) A proposta de valor para o cliente describe o método para xerar vendas e consumidores fieis. Por iso se atopa intimamente ligada coa perspectiva dos procesos necesarios para que os clientes queden satisfeitos.

3) Os procesos internos constitúen a engrenaxe que leva á práctica a proposta de valor para o cliente. Con todo, sen o respaldo dos activos intanxibles é imposible que funcionen eficazmente.

4) Se a perspectiva de aprendizaxe e crecemento non identifica claramente qué tarefas (capital humano), qué tecnoloxía (capital da información) e qué contorna (cultura organizacional) se necesitan para apoiar os procesos, a creación de valor non se producirá. Polo tanto, en última instancia, tampouco se cumprirán os obxectivos financeiros.

Neste contexto, alinear os obxectivos destas catro perspectivas é a clave da creación de valor e dunha estratexia focalizada e internamente consistente. Unha vez creados, os mapas estratéxicos son excelentes ferramentas de comunicación, xa que permiten que todos os empregados comprendan a estratexia e a traduzan en accións específicas para contribuír ao éxito da empresa.

O mapa estratéxico do BSC proporciona un marco para ilustrar de qué modo a estratexia vincula os activos intanxibles cos procesos de creación de valor. Vexamos con maior detalle os elementos de cada unha das perspectivas:

A perspectiva financeira describe os resultados tanxibles da estratexia en termos financeiros. Os indicadores clave para avaliar o éxito ou fracaso da estratexia son a rendibilidade do investimento (ROI), o valor para os accionistas, o crecemento dos ingresos e o custo por unidade.

A perspectiva do cliente, pola súa banda, define a proposta de valor para os "clientes target". Se os clientes valoran a calidade constante e a entrega puntual, daquela, as habilidades, os sistemas e os procesos de desenvolvemento de novos produtos e servizos de gran funcionalidade

adquieren un gran valor. A aliñación de accións e capacidades coa proposta de valor para o cliente é o núcleo da execución da estratexia.

A perspectiva de procesos internos identifica os poucos procesos críticos que se espera que teñan o maior impacto sobre a estratexia. Por exemplo, unha organización pode aumentar os seus investimentos en I + D e reestruturar os seus procesos de desenvolvemento para obter produtos innovadores e de alto desempeño. Outra empresa, coa idea de ofrecer a mesma proposta de valor, podería desenvolver novos produtos a través de alianzas estratéxicas con outros fabricantes.

A perspectiva de aprendizaxe e crecemento identifica os activos intanxibles máis importantes para a estratexia. Os obxectivos desta perspectiva céntranse nas tarefas, os sistemas e o tipo de ambiente requiridos para apoiar os procesos internos de creación de valor. Estes activos deben estar agrupados e aliñados cos procesos internos críticos.

En síntese, o mapa estratéxico proporciona o marco visual para integrar todos os obxectivos da empresa. A comprensión dos procesos críticos como xestión de operacións, innovación e relacións sociais, promove o logro das metas de produtividade.

Para rematar, o mapa identifica as capacidades específicas relacionadas cos activos intanxibles da organización (capital humano, de información e organizacional) para obter un desempeño excepcional

### **2.2.1 PLAN ESTRATÉXICO**

O plan estratéxico é unha actividade administrativa que ten como obxectivo conducir o rumbo da organización para conseguir a súa sustentabilidade, producindo respostas consistentes ás tres cuestións fundamentais: Onde estamos? Onde queremos chegar? Como imos facer

para acadalo? É un proceso de dirección que xestiona, en relación coa formulación de obxectivos, a selección de programas de acción e a súa execución, levando o seguimento das condicións internas e externas á empresa e a evolución esperada.

Tamén considera premisas básicas que a empresa debe respectar para que todo o proceso teña coherencia e sexa sustentable.

O establecemento dun plan estratéxico envolve seis actividades:

- definición da misión corporativa
- análise da situación
- formulación de obxectivos
- formulación de estratexias
- implantación
- seguimento, aprendizaxe e control.

É cada vez maior o número de empresas no escenario global que, ante a complexidade do escenario empresarial e das turbulencias e incertezas, están recollendo modelos de xestión para que as auxilien no desempeño e perfeccionamento do proceso de dirección.

A elaboración dun Plan Estratéxico engloba varios temas fundamentais:

- **Misión:** razón de ser da organización. Expresa as necesidades ás que atende, de qué grupos de persoas e con qué competencias básicas.
- **Visión:** definición de onde e como a organización deberá estar no futuro – nun horizonte medio de tempo de 5 anos.

- Políticas: guías (con carácter de permanencia) para a toma de decisións sobre aspectos importantes da organización.
- Obxectivos: resultados parciais – horizonte de 1 ano – en dirección ao proposto pola visión de futuro
- Estratexias: vías/camiños escollidos para a realización da visión.
- Plan de acción: conxunto de programas e proxectos propostos para o cumprimento da misión e en dirección á visión de futuro

## **2.3 XESTIÓN DO COÑECEMENTO E INNOVACIÓN.**

Actualmente estamos confrontados cun novo paradigma onde o coñecemento se está a converter no principal activo dunha empresa. A chamada “sociedade do coñecemento”, na cal estamos vivindo, esixe un esforzo orientado ao mellor e total aproveitamento do capital intelectual, entendido este como a suma resultante do coñecemento dos integrantes dunha empresa.

A valoración dos activos intanxibles é unha característica da sociedade do coñecemento, a mesma que mesmo presenta un desafío ás prácticas contables; así, se temos dúas empresas “A” e “B” coas mesmas instalacións, a mesma maquinaria, a mesma tecnoloxía e o mesmo capital, nun balance patrimonial non aparecería diferenza algunha. Con todo, se na empresa “A” os traballadores son altamente especializados, cunha capacitación continua, participación, sinerxía e pensamento sistémico, mentres que na empresa “B” non atopamos tales características nos recursos humanos, entón é evidente que a empresa “A” sería máis valorada no mercado de accións, por exemplo, porque é nela onde existe maior integración e mellor utilización do coñecemento. E máis aínda: a empresa “A” estará máis preparada para innovar e, por conseguinte, competir nunha economía cada vez máis globalizada.

A sociedade do coñecemento é a terceira fase produtiva pola que atravesamos a sociedade. A primeira fase, que foi moi longa, estaba baseada na produción rural e artesanal; logo dun tempo houbo un tránsito da sociedade rural á sociedade industrial. A sociedade industrial baseábase na produción en serie; o centro produtivo era a fábrica e a filosofía que a orientaba era a do predominio da razón sobre o sentimento; a sociedade industrial foi optimizada e organizada por Taylor mediante a produción científica, onde separaba o traballo intelectual do operacional para evitar o desperdicio de tempo e isto foi perfeccionado pola enxeñería de métodos e movementos; na sociedade industrial existía unha orientación cara ao produto que despois é ofrecido ao mercado que o aceptará.

A actual terceira fase produtiva, ou sexa a sociedade do coñecemento, caracterízase pola importancia dada ao coñecemento, o predominio dos traballadores intelectuais e onde o traballo repetitivo é delegado ás máquinas, robots e/ou computadoras.

Así, o traballador ten máis tempo para pensar, sentir, emocionarse, ser creativo e innovar. Na sociedade do coñecemento as empresas están orientadas ao mercado, buscando identificar os sinais do mesmo, e para isto fan uso da intelixencia competitiva.

Unha empresa na sociedade do coñecemento enfróntase aos seguintes desafíos:

- A desestruturación do tempo e do espazo, onde deixa de ser importante a permanencia do traballador durante 8 horas no espazo físico da empresa; pasa a ser importante o resultado creativo que o traballador pode achegar desde a súa casa mediante o teletraballo; é dicir, o traballo transcende os límites da fábrica porque a resposta creativa aparece en calquera momento e en calquera lugar.

- A calidade de vida, que é condición *sine qua non* da creatividade; o traballador para identificarse cos obxectivos da empresa debe ter unha calidade de vida que lle permita poder dar o mellor da súa produción intelectual ao equipo do cal forma parte.

- A valoración dos activos intanxibles e a xestión do coñecemento.

### **2.3.1 O COÑECEMENTO E A SÚA XESTIÓN.**

Unha xestión do coñecemento vainos levar a preguntarnos cal é o coñecemento dispoñible na empresa e cal é o coñecemento que necesitamos. E deste xeito comezamos coa identificación do coñecemento dispoñible dentro da organización.

O coñecemento dispoñible no interior da organización, así como a capacidade de incrementalalo, é o activo intanxible de tal organización. Este coñecemento dispoñible vai ser o coñecemento acumulado, vai estar na forma das prácticas compartidas na empresa, na forma de produtos e procesos desenvolvidos pola empresa, no coñecemento do mercado e dos seus clientes, na forma en que a empresa interactúa con outras organizacións, no coñecemento tácito dos traballadores da empresa. É importante, nesta fase, diferenciar o coñecemento tácito do coñecemento explícito.

O coñecemento tácito é aquel froito da experiencia e adquirido en forma práctica, en tanto que o coñecemento explícito é aquel coñecemento xa codificado dispoñible para a súa captación e/ou transmisión en manuais ou textos. Para intercambiar ese coñecemento é necesario ver formas de xerenciar e optimizar tal proceso.

O coñecemento ten un carácter acumulativo, é dicir o que unha empresa fará no futuro é determinado, dalgunha forma, polo que a

empresa fixo no pasado, ou sexa a capacidade tecnolóxica non xorde da noite para a mañá.

Para conservar e dispoñer os coñecementos dunha organización faise necesario contar con formas versátiles de almacenamento do coñecemento, en manuais de procedementos, nun proxecto de xestión do coñecemento e intelixencia competitiva, e mediante a xestión estratéxica dun sistema de información.

É dicir, faise necesario ter unha memoria organizada da empresa para non perder nin o coñecemento tácito nin o explícito que a empresa foi acumulando no transcurso dos anos.

### **2.3.2 A CREATIVIDADE.**

Ademais do coñecemento, que está estreitamente ligado ao razoamento lóxico, ao pensamento cartesiano, temos a creatividade, a cal, en contrapartida, se atopa máis próxima ao que sería a intuición, a imaxinación e a subxectividade.

Entendemos a creatividade como a adaptación ao cambio resultado dun problema que nos desafía. Nunha época en que o cambio e a incerteza son as constantes, a resposta creativa significará a evolución dos produtos, procesos e servizos.

### **2.3.3 A INNOVACIÓN.**

#### Que é a Innovación?

Podemos definir a innovación como "o proceso no cal, a partir dunha idea, invención ou recoñecemento dunha necesidade se desenvolve un



produto, técnica ou servizo útil ata que sexa comercialmente aceptado". De acordo con este concepto, innovar non é máis que o proceso de desenvolver algo novo ou que non se coñecía a partir do estudo metódico dunha necesidade, xa sexa persoal, grupal ou organizacional, para lograr unha meta económica. Isto quere dicir que a innovación xera ideas que poden venderse nun mercado específico.

Para innovar é necesario un amplo coñecemento dunha necesidade; non todas as ideas innovadoras teñen éxito e, por conseguinte, é necesario xogar con todas as ferramentas necesarias para que a innovación non só sorprenda senón que tamén funcione.

Para que aconteza a innovación na empresa serían necesarios os dous ingredientes anteriormente vistos, isto é: o coñecemento e a creatividade. Desta forma poderíamos establecer a seguinte ecuación que nos axudaría a presentar o concepto:

$$\text{COÑECEMENTO} + \text{CREATIVIDADE} = \text{INOVACION} ==> \text{COMPETITIVIDADE}$$

### Por que é importante a innovación?

Innovación e competitividade van da man, pero non necesariamente a unha existe sen a outra. Pódese ser competitivo sen ser innovador con só manter sistemas de mellora continua, pero os procesos de mellora non chegan a ser suficientes cando o mercado se atopa saturado, cando a demanda é alta e cando existen necesidades que os produtos ou servizos existentes non logran liquidar.

Neste punto, a innovación convértese nun proceso fundamental para alcanzar a competitividade, debido a que os esforzos por mellorar chegaron ao seu límite e xa non son suficientes para seguir adiante.

Pero hai que entender que a innovación, por si soa, non garante necesariamente que se alcance a competitividade. Débense establecer metodoloxías e estratexias definidas para poder innovar. Será fundamental realizar un estudo metódico dos factores que interveñen no proceso para a innovación e das oportunidades existentes nos diferentes escenarios.

### **2.3.3.1 TIPOS DE INNOVACIÓN**

Segundo a súa aplicación:

- Innovación de PRODUTO: Comercialización dun produto tecnoloxicamente distinto ou mellorado; a innovación dáse cando as características dun produto cambian.
- Innovación de PROCESO: Ocorre cando hai un cambio significativo na tecnoloxía de produción dun produto ou servizo; tamén ocorre cando se producen cambios significativos no sistema de dirección e/ou métodos de organización; reenxeñería de procesos, planificación estratéxica, control de calidade, etc.

Segundo o seu grado de orixinalidade:

- Innovación RADICAL: aplicacións novas dunha tecnoloxía ou combinación orixinal de novas tecnoloxías.
- Innovación INCREMENTAL: melloras que se realizan sobre un produto, servizo ou método existente.

### **2.3.3.2 XESTIÓN DA INNOVACIÓN**

Tradicionalmente considérase que a innovación é o resultado dunha idea feliz e que só a poden xerar empresas con grandes presupostos de I+D; que para innovar cómpre ser un creativo... Sen negar parte de razón a estes argumentos, a realidade é que a maior parte das innovacións que

coñecemos son o resultado dun traballo sistemático de procura de ideas-oportunidades e a súa transformación en realidade; parafraseando a Peter Drucker: Hai innovacións que xorden dun instante de xenialidade, pero a maioría destas, especialmente as de máis éxito, son o resultado da procura consciente e deliberada de oportunidades.

Daquela, nunha contorna como a actual, na que a innovación é un factor clave de supervivencia, o reto de toda empresa é innovar de forma sistemática, facendo que esta sexa unha actividade máis, en definitiva xestionando a innovación a través dun proceso específico, o denominado proceso de innovación.

A innovación sistemática será o resultado dunha correcta xestión deste proceso e dunha adecuada utilización de metodoloxías e técnicas.

A capacidade innovadora da empresa dependerá da forma en que organicemos e xestionemos o proceso de innovación, o cal está constituído por catro etapas principais:

1. Xerar ideas. Deberemos converternos nunha organización observadora, capaz de mirar ao seu redor, detectar os cambios que se están producindo e descubrir o xeito de aproveitalos.
2. Seleccionar. Deberemos dispoñer de sistemas para avaliar a viabilidade das ideas que xeremos, para así seleccionar e executar aquelas con maiores posibilidades de éxito.
3. Desenvolver. Deberemos dispoñer de persoas capaces de executar os proxectos de innovación de forma efectiva, utilizando metodoloxías de xestión adecuadas.
4. Medir. Se non nos medimos non saberemos se o estamos a facer ben e, xa que logo, deberemos medir tanto o éxito como o fracaso das innovacións xeradas.

Bibliografía:

Bibliografía:

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

Kaplan, Robert S. e 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, Rodríguez, Esteban, Rodríguez-Patón, Alfonso e 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

Colexiado do CPEIG

**3. DIRECCIÓN E XESTIÓN DE  
PROXECTOS. XESTIÓN DA  
INTEGRACIÓN. O PLAN XERAL  
DO PROXECTO. XESTIÓN DO  
ALCANCE. XESTIÓN DO CUSTO.  
ORZAMENTOS. XESTIÓN DO  
TEMPO. TÉCNICAS DE  
PLANIFICACIÓN. XESTIÓN DA  
CALIDADE. PLAN DE  
CALIDADE. XESTIÓN DE RRHH.  
CAPACIDADES DO XEFE DE  
PROXECTO. XESTIÓN DAS  
COMUNICACIÓNS. XESTIÓN DO  
RISCO. CONTINXENCIAS.  
XESTIÓN DA  
SUBCONTRATACIÓN E  
ADQUISICIÓNS.**

**Tema 3. Dirección e xestión de proxectos. Xestión da integración. O plan xeral do proxecto. Xestión do alcance. Xestión do custo. Orzamentos. Xestión do tempo. Técnicas de planificación. Xestión da calidade. Plan de calidade. Xestión de RRHH. Capacidades do xefe de proxecto. Xestión das comunicacións. Xestión do risco. Continxencias. Xestión da subcontratación e adquisicións.**

## **ÍNDICE**

- 3.1 Dirección e xestión de proxectos
- 3.2 Xestión da integración do proxecto
  - 3.2.1 O plan xeral do proxecto
- 3.3 Xestión do alcance do proxecto
- 3.4 Xestión do tempo do proxecto
  - 3.4.1 Técnicas de planificación
- 3.5 Xestión dos custos do proxecto
  - 3.5.1 Orzamentos
- 3.6 Xestión da calidade do proxecto
  - 3.6.1 Plan de calidade
- 3.7 Xestión dos recursos humanos do proxecto
  - 3.7.1 Capacidades do xefe de proxecto.
- 3.8 Xestión das comunicacións do proxecto
- 3.9 Xestión dos riscos do proxecto
  - 3.9.1 Continxencias
- 3.10 Xestión das adquisicións do proxecto

## **3.1 DIRECCIÓN E XESTIÓN DE PROXECTOS**

A dirección de proxectos é a aplicación de coñecementos, habilidades, ferramentas e técnicas ás actividades do proxecto para cumprir cos requisitos do mesmo. Lógrase mediante a aplicación e integración adecuadas dos 42 procesos da dirección de proxectos, agrupados lxicamente, que conforman os 5 grupos de procesos. Estes 5 grupos de procesos son:



- Iniciación
- Planificación
- Execución
- Seguimento e Control
- Peche

Dirixir un proxecto polo xeral implica:

- identificar requisitos;
- abordar as diversas necesidades, inquietudes e expectativas dos interesados segundo se planifica e efectúa o proxecto;
- equilibrar as restricións contrapostas do proxecto que se relacionan, entre outros aspectos, con:
  - o alcance
  - a calidade
  - o cronograma
  - o orzamento
  - os recursos
  - o risco

### **3.2 XESTIÓN DA INTEGRACIÓN DO PROXECTO**

A Xestión da Integración do Proxecto inclúe os procesos e actividades necesarios para identificar, definir, combinar, unificar e coordinar os diversos procesos e actividades da dirección de proxectos dentro dos grupos de procesos de dirección de proxectos. No contexto da dirección de proxectos, a integración inclúe características de unificación, consolidación, articulación, así como as accións integradoras que son cruciais para a terminación do proxecto, a xestión exitosa das expectativas dos interesados e o cumprimento dos requisitos. A xestión da integración do

proxecto implica tomar decisións en canto á asignación de recursos, equilibrar obxectivos e alternativas contrapostas, e manexar as interdependencias entre as áreas de coñecemento da dirección de proxectos.

Procesos de Xestión da Integración do Proxecto:

**Desenvolver a Acta de Constitución do Proxecto**—É o proceso que consiste en desenvolver un documento que autoriza formalmente un proxecto ou unha fase e en documentar os requisitos iniciais que satisfagan as necesidades e expectativas dos interesados.

**Desenvolver o Plan para a Dirección do Proxecto**—É o proceso que consiste en documentar as accións necesarias para definir, preparar, integrar e coordinar todos os plans subsidiarios.

**Dirixir e Xestionar a Execución do Proxecto**—É o proceso que consiste en executar o traballo definido no plan para a dirección do proxecto co fin de cumprir cos obxectivos do mesmo.

**Monitorar e Controlar o Traballo do Proxecto**—É o proceso que consiste en monitorar, revisar e regular o avance co fin de cumprir cos obxectivos de desempeño definidos no plan para a dirección do proxecto.

**Realizar o Control Integrado de Cambios**—É o proceso que consiste en revisar todas as solicitudes de cambio e en aprobar e xestionar os cambios nos entregables, nos activos dos procesos da organización, nos documentos do proxecto e no plan para a dirección do proxecto.

**Pechar Proxecto ou Fase**—É o proceso que consiste en finalizar todas as actividades en todos os grupos de procesos de dirección de proxectos para completar formalmente o proxecto ou unha fase deste.

Nos casos de interacción de procesos individuais, a necesidade dunha xestión da integración do proxecto tórnase evidente. Por exemplo, unha estimación de custos necesaria para un plan de continxencias implica a integración dos procesos nas áreas de coñecemento relativas ao custo, ao tempo e aos riscos. A identificación de riscos adicionais, asociados a



diversas alternativas de adquisición de persoal, pode xerar a necesidade de reconsiderar un ou varios destes procesos. Tamén pode ser necesario integrar os entregables do proxecto nas operacións en curso, xa sexa por parte da organización executante ou da organización do cliente, ou na planificación estratéxica a longo prazo, que ten en conta os problemas e oportunidades futuros. A xestión da integración do proxecto tamén abrangue as actividades necesarias para xestionar os documentos do proxecto, para asegurar a coherencia co plan para a dirección do proxecto e os entregables do produto.

### **3.2.1 O PLAN XERAL DO PROXECTO**

Desenvolver o Plan para a Dirección do Proxecto é o proceso que consiste en documentar as accións necesarias para definir, preparar, integrar e coordinar todos os plans subsidiarios. O plan para a dirección do proxecto define a maneira en que o proxecto se executa, se monitora, se controla e se pecha. O contido do plan para a dirección do proxecto variará en función da área de aplicación e da complexidade do proxecto. O plan para a dirección do proxecto desenvólvese a través dunha serie de procesos integrados ata chegar ao peche do proxecto.

Este proceso dá lugar a un plan para a dirección do proxecto que se elabora gradualmente por medio de actualizacións, e contrólase e apróbase a través do proceso Realizar o Control Integrado de Cambios.

### **3.3 XESTIÓN DO ALCANCE DO PROXECTO**

A Xestión do Alcance do Proxecto inclúe os procesos necesarios para garantir que o proxecto inclúa todo (e unicamente todo) o traballo requirido para completalo con éxito. O obxectivo principal da Xestión do Alcance do Proxecto é definir e controlar qué se inclúe e qué non se inclúe no proxecto.

Procesos da Xestión do Alcance do Proxecto:

**Recompilar Requisitos**—É o proceso que consiste en definir e documentar as necesidades dos interesados co fin de cumprir cos obxectivos do proxecto.

**Definir o Alcance**—É o proceso que consiste en desenvolver unha descrición detallada do proxecto e do produto.

**Crear a EDT**—É o proceso que consiste en subdividir os entregables e o traballo do proxecto en compoñentes máis pequenos e máis fáciles de manexar.

**Verificar o Alcance**—É o proceso que consiste en formalizar a aceptación dos entregables do proxecto que se completaron.

**Controlar o Alcance**—É o proceso que consiste en monitorar o estado do alcance do proxecto e do produto, e en xestionar cambios na liña base do alcance.

Estes procesos interactúan entre si e cos procesos das outras áreas de coñecemento.

Cada proceso pode implicar o esforzo dunha ou máis persoas, dependendo das necesidades do proxecto. Cada proceso execútase polo menos unha vez en cada proxecto e nunha ou máis fases do proxecto, no caso de que o mesmo estea dividido en fases. Aínda que os procesos se presentan aquí como compoñentes diferenciados con interfaces ben definidas, na práctica superpóñense e interactúan de formas que non se detallan aquí.

No contexto do proxecto, o termo ‘alcance’ pódese referir a:

- **Alcance do produto.** As características e funcións que definen un produto, servizo ou resultado.
- **Alcance do proxecto.** O traballo que se debe realizar para entregar un produto, servizo ou resultado coas características e funcións especificadas.

Os procesos usados para xestionar o alcance do proxecto, así como as ferramentas e técnicas asociadas, varían segundo a área de aplicación e normalmente se definen como parte do ciclo de vida do proxecto. A Declaración do Alcance do Proxecto, detallada e aprobada, e a súa EDT asociada, xunto co dicionario da EDT, constitúen a liña base do alcance do proxecto. Esta liña base do alcance monitórase, verifícase e contrólase durante todo o ciclo de vida do proxecto.

Aínda que non se presenta aquí como un proceso diferenciado, o traballo implicado na execución dos cinco procesos de xestión do alcance do proxecto está precedido por un esforzo de planificación por parte do equipo de dirección do proxecto. Este esforzo de planificación forma parte do proceso Desenvolver o Plan para a Dirección do Proxecto, cuxo resultado é un plan para a Xestión do Alcance do Proxecto que proporciona unha guía acerca de como se definirá, documentará, verificará, xestionará e controlará o alcance do proxecto. Dependendo das necesidades do proxecto, o plan para a xestión do alcance do proxecto pode ser formal ou informal, moi detallado, ou formulado de modo xeral.

### **3.4 XESTIÓN DO TEMPO DO PROXECTO**

A Xestión do Tempo do Proxecto inclúe os procesos requiridos para administrar a finalización do proxecto a tempo.

Procesos de Xestión do Tempo do Proxecto:

**Definir as Actividades**—É o proceso que consiste en identificar as accións específicas que deben realizarse para elaborar os entregables do proxecto.

**Secuenciar as Actividades**—É o proceso que consiste en identificar e documentar as interrelacións entre as actividades do proxecto.

**Estimar os Recursos das Actividades**—É o proceso que consiste en estimar o tipo e as cantidades de materiais, persoas, equipos ou subministracións requiridos para executar cada actividade.

**Estimar a Duración das Actividades**—É o proceso que consiste en establecer aproximadamente a cantidade de períodos de traballo necesarios para finalizar cada actividade cos recursos estimados.

**Desenvolver o Cronograma**—É o proceso que consiste en analizar a secuencia das actividades, a súa duración, os requisitos de recursos e as restricións do cronograma para crear o cronograma do proxecto.

**Controlar o Cronograma**—É o proceso polo que se lle dá seguimento ao estado do proxecto para actualizar o avance deste e xestionar cambios na liña do base do cronograma.

No caso dalgúns proxectos, especialmente os de menor alcance, a definición das actividades, o establecemento da súa secuencia, a estimación dos seus recursos, a estimación da súa duración e o desenvolvemento do cronograma son procesos tan estreitamente vinculados que son vistos como un proceso único que pode realizar unha soa persoa nun período relativamente curto. Estes procesos preséntanse aquí como procesos distintos porque as ferramentas e técnicas requiridas para cada un deles son diferentes.

Os procesos de Xestión do Tempo do Proxecto e as súas ferramentas e técnicas asociadas documéntanse no plan de xestión do cronograma. Este está contido no plan para a dirección do proxecto ou é un plan subsidiario do mesmo.

O desenvolvemento do cronograma utiliza as saídas dos procesos Definir as Actividades, Secuenciar as Actividades, Estimar os Recursos das Actividades e Estimar a Duración das Actividades en combinación coa ferramenta de planificación para elaborar o cronograma. O cronograma finalizado e aprobado constitúe a liña base que se utilizará no proceso Controlar o Cronograma conforme se van executando as actividades do proxecto; a maior parte do esforzo na área de coñecemento da Xestión do Tempo do Proxecto debe realizarse durante o proceso Controlar o Cronograma para asegurar que o traballo do proxecto se complete de modo oportuno.

### **3.4.1 TÉCNICAS DE PLANIFICACIÓN**

#### Análise da Rede do Cronograma

A análise da rede do cronograma é unha técnica utilizada para xerar o cronograma do proxecto. Emprega diversas técnicas analíticas, tales como o método da ruta crítica, o método da cadea crítica, a análise “Que pasa se...?” e a nivelación de recursos para calcular as datas de inicio e finalización temperás e tardías para as partes non completadas das actividades do proxecto. Algúns camiños de rede poden ter puntos de converxencia ou diverxencia de rutas que se poden identificar e empregar na análise de compresión do cronograma ou noutras análises.

#### Método da Ruta Crítica

O método da ruta crítica calcula as datas teóricas de inicio e finalización temperás e tardías para todas as actividades, sen considerar as limitacións de recursos, realizando unha análise que percorre cara adiante e cara atrás toda a rede do cronograma. As datas de inicio e finalización temperás e tardías resultantes non constitúen necesariamente o cronograma, senón que máis ben indican os períodos dentro dos cales se poden planificar as actividades, tendo en conta as duracións das actividades, as relacións lóxicas, os adiantos, os atrasos e outras restricións coñecidas. As datas de inicio e finalización temperás e tardías calculadas poden verse afectadas pola folgura total da actividade, que proporciona flexibilidade ao cronograma e cuxo valor pode ser positivo, negativo ou nulo. En calquera camiño de rede, a flexibilidade do cronograma mídese pola diferenza positiva entre as datas temperás e tardías, o cal se coñece como “folgura total”. As rutas críticas teñen unha folgura total igual a cero ou negativa e as actividades do cronograma nunha ruta crítica reciben o nome de “actividades críticas”.

#### Método da Cadea Crítica

A cadea crítica é unha técnica de análise da rede do cronograma que permite modificar o cronograma do proxecto para adaptalo aos recursos limitados.

Inicialmente, o diagrama de rede do cronograma do proxecto elabórase mediante os estimados da duración, coas dependencias requiridas e as restricións definidas como entradas. Entón calcúlase a ruta crítica. Unha vez que se identificou a ruta crítica, ingrésase a dispoñibilidade de recursos e determínase o resultado do cronograma con recursos limitados. A miúdo, o cronograma resultante presenta unha ruta crítica modificada.

A ruta crítica con restricións de recursos coñécese como cadea crítica. O método da cadea crítica agrega colchóns de duración, que son actividades do cronograma que non requiren traballo e que se utilizan para manexar a incerteza.

### Nivelación de Recursos

A nivelación de recursos é unha técnica de análise da rede do cronograma que se lle aplica a un cronograma que xa foi analizado por medio do método da ruta crítica. A nivelación de recursos pode utilizarse cando os recursos compartidos ou críticos necesarios só están dispoñibles en certos momentos ou en cantidades limitadas, ou para manter a utilización de recursos nun nivel constante. A nivelación de recursos é necesaria cando os recursos foron sobreasignados, é dicir, cando un recurso se lles asignou a dous ou máis tarefas para o mesmo período, ou cando os recursos compartidos ou críticos necesarios só están dispoñibles en certos períodos ou en cantidades limitadas. A nivelación de recursos ocasiona a miúdo cambios na ruta crítica.

### Análise “Que pasa se...?”

Este é unha análise da pregunta “Que pasa se se produce a situación representada polo escenario ‘X’?” Realízase unha análise da rede do cronograma usando o cronograma para calcular os diferentes escenarios,

tales coma un atraso na entrega dun compoñente principal, a prolongación da duración dun deseño específico ou a introdución de factores externos, como unha folga ou un cambio no procedemento para a obtención de permisos.

### Aplicación de Adiantos e Atrasos

Os adiantos e atrasos son refinamentos que se aplican durante a análise da rede para desenvolver un cronograma viable.

### Compresión do Cronograma

A compresión do cronograma reduce o calendario do proxecto *sen* modificar o seu alcance para cumprir coas restricións do cronograma, as datas impostas ou outros obxectivos do cronograma. As técnicas de compresión do cronograma inclúen:

- **Compresión.** Unha técnica de compresión do cronograma na cal se analizan as concesións entre custo e cronograma para determinar como obter a maior compresión co menor incremento de custo. A compresión non sempre resulta unha alternativa viable e pode ocasionar un incremento do risco e/ou do custo.
- **Execución rápida.** Unha técnica de compresión do cronograma na cal as fases ou actividades que normalmente se realizarían en forma secuencial se realizan en paralelo.

## **3.5 XESTIÓN DOS CUSTOS DO PROXECTO**

A Xestión dos Custos do Proxecto inclúe os procesos implicados en estimar, orzamentar e controlar os custos de modo que se complete o proxecto dentro do orzamento aprobado.

Procesos da xestión dos custos do proxecto:

**Estimar os Custos**—É o proceso que consiste en desenvolver unha aproximación dos recursos financeiros necesarios para completar as actividades do proxecto.

**Determinar o Orzamento**—É o proceso que consiste en sumar os custos estimados de actividades individuais ou paquetes de traballo para establecer unha liña base de custo autorizada.

**Controlar os custos**—É o proceso que consiste en monitorar a situación do proxecto para actualizar o orzamento do mesmo e xestionar cambios na liña base de custo.

Nalgúns proxectos, especialmente naqueles de alcance máis pequeno, a estimación de custos e a preparación do orzamento de custos están tan estreitamente ligadas que se consideran un só proceso, que pode realizar unha soa persoa nun período de tempo relativamente curto. A capacidade de influír nos custos é moito maior nas primeiras etapas do proxecto, o que fai que a definición temperá do alcance do proxecto sexa crítica.

Os procesos de Xestión dos custos do Proxecto, así como as súas ferramentas e técnicas asociadas, selecciónanse normalmente durante a definición do ciclo de vida do proxecto e documéntanse no plan de xestión de custos. Por exemplo, o plan de xestión de custos pode establecer o seguinte:

- **Nivel de exactitude.** As estimacións do custo das actividades axustaranse a un redondeo de datos segundo unha precisión establecida (p. ex., \$100, \$1.000), dependendo do alcance das actividades e da magnitude do proxecto, e poden incluír unha cantidade para continxencias.
- **Unidades de medida.** Todas as unidades que se utilizan nas medicións (tales como as horas ou días de traballo do persoal, a semana laboral ou a suma global) defínense para cada un dos recursos.
- **Enlaces cos procedementos da organización.** A estrutura de desagregación do traballo (EDT) establece o marco para o plan de xestión de custos, permitindo a consistencia cos estimados de custos, os orzamentos e o control de custos. O compoñente da EDT que se utiliza para a contabilidade dos custos do proxecto denomínase conta de control (CA).



A cada conta de control asígnaselle un código único ou un número de conta vinculado directamente ao sistema de contabilidade da organización executante.

- **Limiars de control.** Para monitorar o desempeño dos custos, poden definirse limiars de variación que establecen unha cantidade acordada de variación permitida antes de que sexa necesario realizar unha acción. Os limiars exprésanse habitualmente como unha porcentaxe de desviación respecto da liña base do plan.

- **Regras para a medición do desempeño.** Establécense regras para a medición do desempeño grazas á xestión do valor gañado (EVM). Por exemplo, o plan de xestión de custos podería:

- Definir a EDT e os puntos onde se realizará a medición das contas de control.

- Establecer as técnicas que se empregarán para medir o valor gañado (p. ex., fitos ponderados, fórmula fixa, porcentaxe completada, etc.).

- Especificar as fórmulas de cómputo de xestión do valor gañado (EVM ) para determinar a estimación á conclusión (EAC) proxectada e outras metodoloxías de seguimento.

- **Formatos dos informes.** Defínense os formatos e a frecuencia de presentación dos diferentes informes de custos.

- **Descricións dos procesos.** Documéntanse as descricións de cada un dos tres procesos de Xestión dos custos do Proxecto.

Toda esta información se inclúe no plan de xestión de custos, que é un compoñente do plan para a dirección do proxecto, ben como texto dentro do corpo do plan ou como anexos.

### **3.5.1 ORZAMENTOS**

#### Ferramentas e Técnicas

#### Suma de custos

As estimacións de custos súmanse por paquetes de traballo, de acordo coa EDT. Despois, as estimacións de custos dos paquetes de traballo súmanse para os niveis superiores de compoñentes da EDT, tales coma as contas de control, e finalmente para todo o proxecto.

### **Análise de Reserva**

A análise de reserva do orzamento pode establecer tanto as reservas para continxencias como as reservas de xestión do proxecto. As reservas para continxencias son asignacións para cambios non planificados, pero potencialmente necesarios, que poden resultar de riscos identificados no rexistro de riscos. As reservas de xestión son orzamentos reservados para cambios non planificados no alcance e no custo do proxecto. O director do proxecto pode necesitar obter a aprobación antes de comprometer ou gastar a reserva de xestión. As reservas non forman parte da liña base de custo, pero poden incluírse no orzamento total do proxecto. As reservas non se inclúen como parte dos cálculos da medición do valor gañado.

### **Xuízo de Expertos**

Un xuízo que se brinda sobre a base da experiencia nunha área de aplicación, unha área de coñecemento, unha disciplina, unha industria, etc., segundo resulte apropiado para a actividade que se está desenvolvendo e que debe utilizarse para determinar o orzamento. Esta experiencia pode ser proporcionada por calquera grupo ou persoa cunha educación, coñecemento, habilidade, experiencia ou capacitación especializada. O xuízo de expertos pode provir de diversas fontes, entre outras:

- outras unidades dentro da organización executante
- consultores
- interesados, incluíndo clientes
- asociacións profesionais e técnicas
- grupos industriais

### **Relacións Históricas**

Calquera relación histórica que dea como resultado estimacións paramétricas ou análogas implica o uso de características (parámetros) do

proxecto para desenvolver modelos matemáticos que permitan predicir os custos totais do proxecto. Estes modelos poden ser simples (p. ex., a construción dunha vivenda residencial custará unha certa cantidade por metro cadrado de espazo útil) ou complexas (p. ex., un modelo de custo de desenvolvemento de software utiliza varios factores de axuste separados, onde cada un destes factores entraña numerosos criterios).

Tanto o custo como a exactitude dos modelos análogos e paramétricos poden variar en gran medida. É máis probable que sexan fiables cando:

- a información histórica utilizada para desenvolver o modelo é exacta;
- os parámetros utilizados no modelo son facilmente cuantificables;
- os modelos son escalables, de modo que funcionan tanto para un proxecto grande como para un pequeno, e para as fases dun proxecto.

### **Conciliación do Límite do Financiamento**

O gasto de fondos debe conciliarse cos límites de financiamento establecidos sobre o desembolso de fondos para o proxecto. Unha variación entre os límites de financiamento e os gastos planificados esixirá nalgúns casos a reprogramación do traballo para regular os devanditos gastos. Isto pódese realizar aplicando restricións de data impostas para o traballo no cronograma do proxecto.

## **3.6 XESTIÓN DA CALIDADE DO PROXECTO**

A Xestión da Calidade do Proxecto inclúe os procesos e actividades da organización executante que determinan responsabilidades, obxectivos e políticas de calidade co fin de que o proxecto satisfaga as necesidades pola cales foi emprendido. Implanta o sistema de xestión de calidade por medio de políticas e procedementos, con actividades de mellora continua dos procesos levados a cabo durante todo o proxecto, segundo corresponda.

Procesos de Xestión da Calidade do Proxecto:

**Planificar a Calidade**—É o proceso polo cal se identifican os requisitos de calidade e/ou normas para o proxecto e o produto, documentando a maneira en que o proxecto demostrará o cumprimento dos mesmos.

**Realizar o Aseguramento de Calidade**—É o proceso que consiste en auditar os requisitos de calidade e os resultados das medidas de control de calidade para asegurar que se utilicen as normas de calidade apropiadas e as definicións operacionais.

**Realizar o Control de Calidade**—É o proceso polo que se monitoran e rexistran os resultados da execución de actividades de control de calidade co fin de avaliar o desempeño e recomendar cambios necesarios

A Xestión da Calidade do Proxecto trata sobre a xestión tanto da calidade do proxecto como do produto do proxecto. Aplícaselles a todos os proxectos, independentemente da natureza do seu produto. As medidas e técnicas relativas á calidade do produto son específicas do tipo de produto xerado polo proxecto. Por exemplo, namentres que a xestión de calidade de produtos de software implica enfoques e medidas diferentes dos que se utilizan para as centrais nucleares, os enfoques de Xestión da Calidade do Proxecto aplícanse a ambos. En calquera caso, o incumprimento dos requisitos de calidade do produto ou do proxecto pode ter consecuencias negativas graves para algúns interesados no proxecto e mesmo para todos. Por exemplo:

- Facer que o equipo do proxecto traballe en exceso para cumprir coas esixencias do cliente pode ocasionar un importante desgaste dos empregados, erros ou reprocesos.
- Realizar apresuradamente as inspeccións de calidade planificadas para cumprir cos obxectivos do cronograma do proxecto pode xerar erros non detectados.

A calidade e o grao non son o mesmo. A calidade é “o nivel no que un conxunto de características inherentes satisfai os requisitos”. O grao é unha categoría que se lles asigna a produtos ou servizos que teñen o

mesmo uso funcional pero características técnicas diferentes. Namentres que un nivel de calidade que non cumpre cos requisitos de calidade é sempre un problema, un grao baixo pode non o ser. Por exemplo, un produto de software pode ser de alta calidade (sen defectos evidentes, manual lexible) e baixo grao (un número limitado de características), ou de baixa calidade (con moitos defectos, a documentación do usuario deficientemente estruturada) e alto grao (numerosas características). O director do proxecto e o equipo de dirección do proxecto son responsables de determinar as concesións necesarias para cumprir cos niveis requiridos, tanto de calidade como de grao.

Precisión e exactitude non son equivalentes. Precisión significa que os valores de medicións repetidas están agrupados e teñen pouca dispersión. Exactitude significa que o valor medido é moi próximo ao valor verdadeiro. As medicións precisas non son necesariamente exactas. Unha medición moi exacta non é necesariamente precisa.

O equipo de dirección do proxecto debe determinar os niveis apropiados de exactitude e precisión.

O enfoque básico da xestión de calidade que se describe nesta sección pretende ser compatible co da Organización Internacional de Normalización (ISO).

Tamén é compatible con enfoques propietarios sobre a xestión de calidade, tales como os recomendados por Deming, Xuran, Crosby e outros, así como con enfoques que non son propietarios, como a Xestión da Calidade Total (TQM), Six Sigma, Análise de Modos de Fallo e Efectos, Revisións do Deseño, Opinión do Cliente, Custo da Calidade (COQ) e Mellora Continua.

A xestión moderna da calidade complementa a dirección de proxectos. Ambas as disciplinas recoñecen a importancia de:

- **A satisfacción do cliente.** Entender, avaliar, definir e xestionar as expectativas, de modo que se cumpran os requisitos do cliente. Isto require unha combinación de conformidade cos requisitos (para asegurar que o

proxecto produza aquilo para o que foi emprendido) e adecuación para o seu uso (o produto ou servizo debe satisfacer necesidades reais).

- **A prevención antes que a inspección.** Un dos preceptos fundamentais da xestión moderna da calidade establece que a calidade se planifica, se diseña e se integra (e non se inspecciona). Polo xeral, o custo de previr erros é moito menor que o de corrixilos cando son detectados por unha inspección.
- **A mellora continua.** O ciclo planificar-facer-revisar-actuar é a base para a mellora da calidade, segundo a definición de Shewhart, modificada por Deming. Ademais, as iniciativas de mellora da calidade emprendidas pola organización executante, tales como TQM e Six Sigma, deben mellorar tanto a calidade da dirección do proxecto como a do produto do proxecto. Os modelos de mellora de procesos inclúen Malcolm Baldrige, OPM3® (Organizational Project Management Maturity Model) e CMMI® (Capability Maturity Model Integration).
- **A responsabilidade da dirección.** O éxito require a participación de todos os membros do equipo do proxecto, pero proporcionar os recursos necesarios para lograr o devandito éxito segue a ser responsabilidade da dirección.

### **3.6.1 PLAN DE CALIDADE**

O plan de xestión de calidade describe como o equipo de dirección do proxecto implantará a política de calidade da organización executante. É un compoñente ou un plan subsidiario do plan para a dirección do proxecto. O plan de xestión de calidade proporciona entradas ao plan xeral para a dirección do proxecto e aborda o control de calidade, o aseguramento da calidade e métodos de mellora continua dos procesos do proxecto.

O plan de xestión de calidade pode ser formal ou informal, moi detallado ou formulado de modo xeral. O formato e o grao de detalle determínanse en función dos requisitos do proxecto. O plan de xestión de calidade débese revisar nunha etapa temperá do proxecto para asegurarse

de que as decisións estean baseadas en informacións precisas. Os beneficios desta revisión poden incluír a redución do custo e sobrecustos no cronograma ocasionados polo reproceso.

### **3.7 XESTIÓN DOS RECURSOS HUMANOS DO PROXECTO**

A Xestión dos Recursos Humanos do Proxecto inclúe os procesos que o equipo do proxecto organiza, xestiona e conduce. O equipo do proxecto está conformado por aquelas persoas ás que se lles asignaron roles e responsabilidades para completar o proxecto. O tipo e a cantidade de membros do equipo do proxecto poden variar con frecuencia, a medida que o proxecto avanza. Os membros do equipo do proxecto tamén se poden denominar persoal do proxecto. Aínda que se lle asignan roles e responsabilidades específicos a cada membro do equipo do proxecto, a participación de todos os membros na toma de decisións e na planificación do proxecto pode resultar beneficiosa. A intervención e a participación temperás dos membros do equipo enriquecen coa súa experiencia profesional o proceso de planificación e fortalecen o seu compromiso co proxecto.

Procesos de Xestión dos Recursos Humanos do Proxecto:

**Desenvolver o Plan de Recursos Humanos**—É o proceso polo cal se identifican e documentan os roles dentro dun proxecto, as responsabilidades, as habilidades requiridas e as relacións de comunicación e se crea o plan para a dirección de persoal.

**Adquirir o Equipo do Proxecto**—É o proceso polo cal se confirman os recursos humanos dispoñibles e se forma o equipo necesario para completar as asignacións do proxecto.

**Desenvolver o Equipo do Proxecto**—É o proceso que consiste en mellorar as competencias, a interacción dos membros do equipo e o ambiente xeral do equipo para lograr un mellor desempeño do proxecto.

**Dirixir o Equipo do Proxecto**—É o proceso que consiste en darlle seguimento ao desempeño dos membros do equipo, proporcionar retroalimentación, resolver problemas e xestionar cambios co fin de optimizar o desempeño do proxecto. O equipo de dirección do proxecto é un subgrupo do equipo do proxecto e é responsable das actividades de liderado e dirección do proxecto, tales como iniciar, planificar, executar, monitorar, controlar e cerrar as diversas fases do proxecto. Este grupo pódese denominar tamén equipo central, equipo executivo ou equipo líder. Para proxectos máis pequenos, as responsabilidades da dirección de proxectos poden ser compartidas por todo o equipo ou administradas unicamente polo director do proxecto. O patrocinador do proxecto traballa co equipo de dirección do proxecto, colaborando polo xeral en asuntos tales como o financiamento do proxecto, aclarando cuestións referidas ao alcance, monitorando o avance e exercendo influencia sobre outros interesados para beneficio do proxecto.

Dirixir e liderar o equipo do proxecto tamén inclúe, entre outros aspectos:

- **Influír no equipo do proxecto.** Estar atento aos factores de recursos humanos que poderían ter un impacto no proxecto e influír neles cando sexa posible. Isto inclúe o ambiente de equipo, a localización xeográfica dos membros do equipo, a comunicación entre os interesados, as políticas internas e externas, os asuntos de índole cultural, a singularidade da organización e outros factores humanos que poderían alterar o desempeño do proxecto.
- **Comportamento profesional e ético.** O equipo de dirección do proxecto debe estar atento a que todos os membros do equipo adopten un comportamento ético, adoptalo igualmente e asegurarse de que así sexa.

### **3.7.1 CAPACIDADES DO XEFE DE PROXECTO**



### Habilidades Interpersoais

Os directores de proxecto usan unha combinación de habilidades técnicas, humanas e conceptuais para analizar as situacións e interactuar de maneira apropiada cos membros do equipo. O uso de habilidades interpersoais axeitadas axuda aos directores de proxecto a tiraren proveito dos puntos fortes dos membros do equipo.

Existe un amplo conxunto de coñecementos relativo ás habilidades interpersoais apropiadas para o traballo dentro e fóra do proxecto.

Algunhas das habilidades interpersoais utilizadas con maior frecuencia polos directores do proxecto descríbense brevemente deseguido.

- **Liderado.** Os proxectos exitosos requiren fortes habilidades de liderado. O liderado é importante en todas as fases do ciclo de vida do proxecto. É particularmente importante comunicar a visión e inspirar ao equipo do proxecto co fin de acadar un alto desempeño.

- **Influencia.** Dado que a miúdo a autoridade directa dos directores do proxecto sobre os membros do seu equipo é escasa ou nula nun ambiente matricial, a súa capacidade de influír oportunamente nos interesados resulta vital para o éxito do proxecto. Entre as habilidades clave de influencia atópanse:

- Ter a habilidade para persuadir e expresar con claridade os puntos de vista e as posicións asumidas.
- Contar con grande habilidade para escoitar de forma activa e eficaz.
- Ter en conta as diversas perspectivas en calquera situación.
- Recompilar información relevante e crítica a fin de abordar os asuntos importantes e lograr acordos, mantendo á vez a confianza mutua.

• **Toma de decisións eficaz.** Isto implica ter a habilidade de negociar e influír sobre a organización e o equipo de dirección do proxecto. Algunhas pautas en materia de toma de decisións inclúen:

- centrarse nos obxectivos perseguidos
- seguir un proceso de toma de decisións
- estudar os factores ambientais
- desenvolver as calidades persoais dos membros do equipo
- fomentar a creatividade do equipo
- xestionar as oportunidades e os riscos

### **3.8 XESTIÓN DAS COMUNICACIÓNS DO PROXECTO**

A Xestión das Comunicacóns do Proxecto inclúe os procesos requiridos para garantir que a xeración, a recompilación, a distribución, o almacenamento, a recuperación e a disposición final da información do proxecto sexan adecuados e oportunos. Os directores do proxecto pasan a maior parte do tempo comunicándose cos membros do equipo e outros interesados no proxecto, tanto se son internos á organización (en todos os niveis desta) como externos á ela. Unha comunicación eficaz crea unha ponte entre os diferentes interesados implicados nun proxecto, conectando diferentes contornos culturais e organizacionais, diferentes niveis de experiencia, e perspectivas e intereses diversos na execución ou resultado do proxecto.

Procesos de Xestión das Comunicacóns do Proxecto:

**Identificar aos Interesados**—É o proceso que consiste en identificar a todas as persoas ou organizacións implicadas no proxecto, e en documentar información relevante relativa aos seus intereses, participación e implicación no éxito do mesmo.

**Planificar as Comunicaci3ns**—É o proceso para determinar as necesidades de informaci3n dos interesados no proxecto e definir como abordar as comunicaci3ns con eles.

**Distribuir a Informaci3n**—É o proceso de poñer a informaci3n relevante a disposici3n dos interesados no proxecto, de acordo co plan establecido.

**Xestionar as Expectativas dos Interesados**—É o proceso de comunicarse e traballar en conxunto cos interesados para satisfacer as súas necesidades e abordar os problemas conforme se presentan.

**Informar o Desempeño**—É o proceso de recompilaci3n e distribuci3n da informaci3n sobre o desempeño, incluíndo os informes de estado, as medic3ns do avance e as proxecci3ns.

As dimensi3ns posibles da actividade de comunicaci3n son, entre outras:

- interna (dentro do proxecto) e externa (cliente, outros proxectos, medios de comunicaci3n, p3blico);
- formal (informes, memorandos, instrucci3ns) e informal (correos electr3nicos, conversaci3ns *ad hoc*);
- vertical (cara arriba e abaixo dentro da organizaci3n) e horizontal (entre colegas);
- oficial (boletíns, informe anual) e non oficial (comunicaci3ns extraoficiais);
- escrita e oral;
- verbal e non verbal (inflexi3ns de voz, linguaxe corporal).

A maioría das habilidades de comunicaci3n son com3ns á direcci3n en xeral e á direcci3n de proxectos. Entre estas habilidades, inclúese:

- escoitar de xeito activo e eficaz;
- formular preguntas, indagar en ideas e situaci3ns para garantir unha mellor comprensi3n;
- educar para aumentar o coñecemento do equipo a fin de que sexa máis eficaz;
- investigar para identificar ou confirmar informaci3n;

- identificar e xestionar expectativas;
- persuadir a unha persoa ou organización para que leve a cabo unha acción;
- negociar a fin de lograr acordos entre partes que resulten mutuamente aceptables;
- resolver conflitos para previr impactos negativos;
- resumir, recapitular e identificar as próximas etapas.

### **3.9 XESTIÓN DOS RISCOS DO PROXECTO**

A Xestión dos Riscos do Proxecto inclúe os procesos relacionados con levar a cabo a planificación da xestión, a identificación, a análise, a planificación de resposta aos riscos, así como a súa monitorización e control nun proxecto. Os obxectivos da Xestión dos Riscos do Proxecto son aumentar a probabilidade e o impacto de eventos positivos e diminuír a probabilidade e o impacto de eventos negativos para o proxecto.

Procesos de Xestión dos Riscos do Proxecto:

**Planificar a Xestión de Riscos**—É o proceso polo cal se define como realizar as actividades de xestión dos riscos para un proxecto.

**Identificar os Riscos**—É o proceso polo cal se determinan os riscos que poden afectar ao proxecto e se documentan as súas características.

**Realizar a Análise Cualitativa de Riscos**—É o proceso que consiste en priorizar os riscos para realizar outras análises ou accións posteriores, avaliando e combinando a probabilidade de ocorrencia e o impacto dos devanditos riscos.

**Realizar a Análise Cuantitativa de Riscos**—É o proceso que consiste en analizar numericamente o efecto dos riscos identificados sobre os obxectivos xerais do proxecto.

**Planificar a Resposta aos Riscos**—É o proceso polo cal se desenvolven opcións e accións para mellorar as oportunidades e reducir as ameazas aos obxectivos do proxecto.

**Monitorar e Controlar os Riscos**—É o proceso polo cal se implantan plans de resposta aos riscos, se rastrexan os riscos identificados, se monitoran os riscos residuais, se identifican novos riscos e se avalía a efectividade do proceso contra riscos a través do proxecto.

Os riscos dun proxecto sitúanse sempre no futuro. Un risco é un evento ou condición incerta que, se sucede, ten un efecto en polo menos un dos obxectivos do proxecto. Os obxectivos poden incluír o alcance, o cronograma, o custo e a calidade. Un risco pode ter unha ou máis causas e, se sucede, un ou máis impactos. Unha causa pode ser un requisito, un suposto, unha restrición ou unha condición que crea a posibilidade de consecuencias tanto negativas como positivas. Por exemplo, as causas poderían ser o requisito de obter un permiso ambiental para realizar o traballo, ou contar cunha cantidade limitada de persoal asignado para o deseño do proxecto. O evento de risco é que a axencia que outorga o permiso poida tardar máis do previsto en emitir o permiso ou, no caso dunha oportunidade, que a cantidade limitada de persoal dispoñible asignado ao proxecto poida realizar o traballo a tempo e, por conseguinte, efectuar o traballo cunha menor utilización de recursos. Se algún destes eventos incertos se produce, pode haber un impacto no custo, no cronograma ou no desempeño do proxecto. As condicións de risco poderían incluír aspectos do contorno do proxecto ou da organización que poidan contribuír a poñer en risco o proxecto, tales como prácticas deficientes de dirección de proxectos, a falta de sistemas de xestión integrados, a concorrencia de varios proxectos ou a dependencia de participantes externos que non poden ser controlados.

### **3.9.1 CONTINXENCIAS**

Algunhas estratexias están deseñadas para seren usadas unicamente se se presentan determinados eventos. Para algúns riscos, resulta apropiado para o equipo do proxecto elaborar un plan de resposta que só se executará baixo determinadas condicións predefinidas, se se cre que haberá suficientes sinais de advertencia para implantar o plan. Os eventos que disparan a resposta para continxencias, tales como non cumprir con fitos intermedios ou obter unha prioridade máis alta cun proveedor, deben definirse e rastrexarse.

### **3.10 XESTIÓN DAS ADQUISICIÓNS DO PROXECTO**

A Xestión das Adquisicións do Proxecto inclúe os procesos de compra ou adquisición dos produtos, servizos ou resultados que é necesario conseguir fóra do equipo do proxecto. A organización pode ser a compradora ou vendedora dos produtos, servizos ou resultados dun proxecto. A Xestión das Adquisicións do Proxecto inclúe os procesos de xestión do contrato e de control de cambios requiridos para desenvolver e administrar contratos ou ordes de compra emitidas por membros autorizados do equipo do proxecto. A Xestión das Adquisicións do Proxecto tamén inclúe a administración de calquera contrato emitido por unha organización externa (o comprador) que lle estea adquirindo o proxecto á organización executante (o vendedor), así como a administración das obrigas contractuais contraídas polo equipo do proxecto en virtude do contrato.

Procesos de Xestión das Adquisicións do Proxecto:

**Planificar as Adquisicións**—É o proceso de documentar as decisións de compra para o proxecto, especificando a forma de facelo e identificando posibles vendedores.

**Efectuar as Adquisicións**—É o proceso de obter respostas dos vendedores, seleccionar un vendedor e adxudicar un contrato.

**Administrar as Adquisicións**—É o proceso de xestionar as relacións de adquisicións, monitorar a execución dos contratos e efectuar cambios e correccións segundo sexa necesario.

**Pechar as Adquisicións**—É o proceso de completar cada adquisición para o proxecto.

Os procesos de Xestión das Adquisicións do Proxecto implican contratos, que son documentos legais que se establecen entre un comprador e un vendedor. Un contrato representa un acordo vinculante para as partes en virtude do cal o vendedor se obriga a prover os produtos, servizos ou resultados especificados, e o comprador obrígase a proporcionar diñeiro ou calquera outra contraprestación válida. O acordo pode ser simple ou complexo, e pode reflectir a simplicidade ou complexidade dos entregables e o esforzo requirido.

Un contrato de adquisición inclúe termos e condicións e pode incorporar outros aspectos especificados polo comprador para establecer o que o vendedor debe realizar ou proporcionar. É responsabilidade do equipo de dirección do proxecto asegurar que todas as adquisicións satisfagan as necesidades específicas do proxecto, á vez que se respectan as políticas da organización en materia de adquisicións.

Segundo a área de aplicación, os contratos tamén se poden denominar acordos, convenios, subcontratos ou ordes de compra. A maioría das organizacións contan con políticas e procedementos documentados que definen especificamente as regras de adquisición, así como quen está autorizado a asinar e administrar os devanditos acordos no nome da organización.

Aínda que todos os documentos do proxecto están suxeitos a algún tipo de revisión e aprobación, o carácter xuridicamente vinculante dun contrato polo xeral significa que estará suxeito a un proceso de aprobación máis exhaustivo. En todos os casos, o obxectivo principal do proceso de

revisión e aprobación é asegurar que a linguaxe do contrato describa os produtos, servizos ou resultados que han satisfacer a necesidade identificada do proxecto.

O equipo de dirección do proxecto pode buscar canto antes o apoio de especialistas en contratación, adquisicións, dereito e asuntos técnicos. A devandita participación pode ser mandatoria segundo a política de cada organización.

As diferentes actividades implicadas nos procesos de Xestión das Adquisicións do Proxecto conforman o ciclo de vida dun contrato. Se se xestiona activamente o ciclo de vida do contrato e se redactan coidadosamente os termos e condicións das adquisicións, algúns riscos identificables do proxecto poden evitarse, mitigarse ou transferirse a un vendedor. Celebrar un contrato por produtos ou servizos é un método de asignar a responsabilidade de xestionar ou de compartir posibles riscos.

Un proxecto complexo pode supoñer a xestión simultánea ou secuencial de múltiples contratos ou subcontratos. En tales casos, o ciclo de vida de cada contrato pode finalizar durante calquera fase do ciclo de vida do proxecto. A Xestión das Adquisicións do Proxecto abórdase dentro da perspectiva da relación entre o comprador e o vendedor.

A relación comprador-vendedor pode existir a moitos niveis en calquera proxecto, e entre organizacións internas e externas á organización compradora.

Dependendo da área de aplicación, o vendedor pode ser denominado contratista, subcontratista, provedor, provedor de servizos ou distribuidor. Dependendo da posición do comprador no ciclo de adquisición do proxecto, este pode denominarse cliente, contratista principal, contratista, organización compradora, organismo governamental, solicitante de servizos ou simplemente comprador. Durante o ciclo de vida do contrato, o vendedor pode ser considerado primeiro licitador, logo a fonte seleccionada e, finalmente, o provedor ou vendedor contratado.



Bibliografía:

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

Sitios web:

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

Autor:

Ramón Seoane Freijido

Director de Sistemas de Información Molduras del Noroeste

Colexiado do CPEIG



## **4. SISTEMAS DE XESTIÓN DE CALIDADE. NORMALIZACIÓN E CERTIFICACIÓN. EFQM. SERIE ISO 9000.**

## **Tema 4. Sistemas de Xestión de Calidade. Normalización e certificación. EFQM. Serie ISO 9000.**

### **ÍNDICE**

#### **4.1 Normalización e certificación**

##### **4.1.1 Normalización. Conceptos básicos**

##### **4.1.2 Certificación. Pasos**

#### **4.2 EFQM. Modelo EFQM de excelencia**

##### **4.2.1 Introducción ao modelo**

##### **4.2.2 Que é a EFQM?**

##### **4.2.3 Historia da EFQM**

##### **4.2.4 Que é o modelo EFQM?**

##### **4.2.5 Para que serve o modelo EFQM?**

##### **4.2.6 Composición do modelo EFQM**

##### **4.2.7 Vantaxes de adoptar o modelo EFQM**

##### **4.2.8 Cambios que orixina a excelencia en xestión**

#### **4.3 Serie ISO 9000**

##### **4.3.1 Introducción**

##### **4.3.2 A familia de normas ISO 9000**

##### **4.3.3 Principios de xestión**

##### **4.3.4 Versións específicas da norma ISO 9000**

##### **4.3.5 Custos e beneficios de establecer un sistema de xestión da calidade**

##### **4.3.6 Implantación dun sistema de xestión da calidade**

### **4.1 NORMALIZACIÓN E CERTIFICACIÓN.**

#### **4.1.1 NORMALIZACIÓN. CONCEPTOS BÁSICOS.**

Que se entende por normalización?

A normalización é unha actividade colectiva encamiñada a establecer solucións a situacións repetitivas.

En particular, esta actividade consiste na elaboración, difusión e aplicación de normas.

A normalización ofrece importantes beneficios, como consecuencia de adaptar os produtos, procesos e servizos aos fins aos que se destinan, protexer a saúde e o medio ambiente, previr os obstáculos ao comercio e facilitar a cooperación tecnolóxica.

### Que é unha norma?

As normas son documentos técnicos coas seguintes características:

- Conteñen especificacións técnicas de aplicación voluntaria.
- Son elaborados por consenso das partes interesadas:
- Están baseados nos resultados da experiencia e o desenvolvemento tecnolóxico.
- Son aprobados por un Organismo Nacional/Rexional/Internacional de Normalización recoñecido.
- Están dispoñibles para o público.

As normas ofrecen unha linguaxe común de comunicación entre as empresas, a Administración e os usuarios e consumidores, establecen un equilibrio socioeconómico entre os distintos axentes que participan nas transaccións comerciais, base de calquera economía de mercado, e son un patrón necesario de confianza entre cliente e proveedor.

### Que vantaxes ofrece a normalización?

a) Para os consumidores:

- Establece niveis de calidade e seguridade dos produtos e servizos.
- Informa das características do produto.

- Facilita a comparación entre diferentes ofertas.
- b) Para os fabricantes:
- Racionalizar variedades e tipos de produtos.
  - Diminúe o volume de existencias en almacén e os custos de produción.
  - Mellora a xestión e o deseño.
  - Axiliza o tratamento dos pedidos.
  - Facilita a comercialización dos produtos e a súa exportación.
  - Simplifica a xestión de compras.
- c) Para a Administración:
- Simplifica a elaboración de textos legais.
  - Establece políticas de calidade, medioambientais e de seguridade.
  - Axuda ao desenvolvemento económico.
  - Axiliza o comercio.

### Que se pode normalizar?

O campo de actividade das normas é tan amplo como a propia diversidade de produtos ou servizos, incluídos os seus procesos de elaboración.

Así, normalízanse os Materiais (plásticos, aceiro, papel, etc.), os Elementos e Produtos (parafusos, televisores, ferramentas, tubos, etc.), as Máquinas e Conxuntos (motores, ascensores, electrodomésticos, etc.), Métodos de Ensaio, Temas Xerais (medio natural, calidade da auga, regras de seguridade, estatística, unidades de medida, etc.), Xestión e Aseguramento da Calidade, Xestión Medioambiental (xestión, auditoría, análise do ciclo de vida, etc.), Xestión de prevención de riscos no traballo (xestión e auditoría), etc.

### Que clases de normas existen?

Os documentos normativos poden ser de diferentes tipos dependendo do organismo que os elaborou.

Na clasificación tradicional de normas distínguese entre:

- Normas nacionais. Son elaboradas, sometidas a un período de información pública e sancionadas por un organismo recoñecido legalmente para desenvolver actividades de normalización nun ámbito nacional. En España estas normas son as normas UNE, aprobadas por AENOR, que é o organismo recoñecido pola Administración Pública española para desenvolver as actividades de normalización no noso país (Real Decreto 2000/1995).
- Normas rexionais. Son elaboradas no marco dun organismo de normalización rexional, normalmente de ámbito continental, que agrupa a un determinado número de Organismos Nacionais de Normalización. As máis coñecidas, aínda que non as únicas, son as normas europeas elaboradas polos Organismos Europeos de Normalización (CEN, CENELEC, ETSI), e preparadas coa participación de representantes acreditados de todos os países membros. AENOR é o organismo nacional de normalización español membro de CEN e CENELEC e, xa que logo, a organización a través da cal canalizar os intereses e a participación dos axentes socioeconómicos do noso país na normalización europea.
- Normas internacionais. Teñen características similares ás normas rexionais canto á súa elaboración, pero distínguense delas en que o seu ámbito é mundial. As máis representativas polo seu campo de actividade son as normas CEI/IEC (Comité Electrotécnico Internacional) para a área eléctrica, as UIT/ITU (Unión Internacional de Telecomunicacións) para o sector das telecomunicacións e as normas ISO (Organización Internacional de Normalización) para o resto. AENOR é o organismo nacional de normalización español membro de ISO e CEI e, xa que logo, a organización

a través da cal canalizar os intereses e a participación dos axentes socioeconómicos do noso país na normalización internacional.

### Que é unha norma UNE?

Unha norma UNE é unha especificación técnica de aplicación repetitiva ou continuada cuxa observancia non é obrigatoria, establecida con participación de todas as partes interesadas, que aproba AENOR, organismo recoñecido a escala nacional e internacional pola súa actividade normativa (Lei 21/1992, do 16 de xullo, de Industria).

### Como se elabora unha norma UNE?

A elaboración dunha norma UNE, incluída a adopción de normas europeas, lévase a cabo no seo dos Comités Técnicos de Normalización (CTN) a través das seguintes fases:

- Traballos preliminares (recompilación de documentación, discusión sobre o contido...) previos á toma en consideración dunha nova iniciativa;
- Elaboración do proxecto de norma; inclúe todas aquelas actividades que se desenvolven polo Comité ata a aprobación dun documento como proxecto de norma, buscando sempre o consenso de todas as partes;
- Información pública no BOE; anuncio da existencia do proxecto de norma, tanto nacional como europea, para que calquera persoa, física ou xurídica, poida remitir ao mesmo as observacións que estime oportunas;
- Elaboración da proposta de norma; unha vez superada a fase anterior, e recibidas en AENOR as posibles observacións ao proxecto, o CTN procede ao estudo das mesmas e aprobación da proposta de norma final, para a súa consideración e adopción por AENOR;

- Rexistro, edición e difusión da norma UNE; publicación da norma UNE por AENOR, notificación a BOE, promoción e comercialización, a través dos servizos comerciais de AENOR.

#### **4.1.2 CERTIFICACIÓN. PASOS.**

O proceso de certificarse con base na ISO 9001, e de manter este status unha vez conseguido, implica os pasos seguintes:

##### 1. Como seleccionar un organismo de certificación

As organizacións que desexen obter un certificado, deben presentar unha solicitude ao organismo de certificación da súa elección. Os aspectos a considerar ao seleccionar o organismo de certificación inclúen:

- Se a natureza da acreditación do organismo de certificación é aceptable no mercado ao cal a organización desexa exportar.
- A imaxe do organismo de certificación no mercado.
- Cotizacións das tarifas de certificación e auditorías, etc.

##### 2. Preparación para a avaliación

De acordo coa ISO 9001, o primeiro requisito é definir os procesos da organización que afectan á calidade, de maneira que o primeiro paso é que o auditor do organismo de certificación se reúna coa alta dirección da organización, co fin de que aquel obteña unha comprensión clara acerca dos procesos da organización.

##### 3. Auditoría

Os auditores recollen evidencia de conformidade ou non conformidade mediante a observación de actividades, o exame de procedementos/rexistros, observacións das condicións de manexo da empresa, a través de entrevistas cos directores e persoal involucrado da organización, etc. A información recompilada mediante as entrevistas é



verificada ou ensaiada polos auditores mediante a recolección da mesma información doutras fontes, tales como observacións físicas ou medicións realizadas no produto e os seus rexistros relacionados. Os auditores visitan e verifican a conformidade co SGC en todos os departamentos e funcións dentro do alcance do SGC.

#### 4. Non conformidades

A evidencia recollida polos auditores é comparada cos criterios da auditoría (políticas e obxectivos da compañía, manuais, procedementos, instrucións, contratos, regulamentacións, etc.) e as conclusións das auditorías, incluídas as non conformidades, se as hai, son aclaradas e reportadas á alta dirección ao final da auditoría no sitio, nunha reunión formal coa alta dirección, chamada “Reunión de Peche”. As non conformidades (NC) son clasificadas polos auditores como “maiores” ou “menores”. As “observacións” tamén se rexistran.

#### 5. Outorgamento do certificado ISO 9000

Con base ás recomendacións do auditor e logo da revisión independente destas recomendacións por parte do organismo certificador, este expide un certificado á organización. O certificado expídese para o alcance específico do negocio e para os produtos ou servizos para os cales a organización implantou un SGC.

#### 6. Auditorías de seguimento

O certificado outórgase inicialmente por un período de tres anos. Durante este tempo, o organismo de certificación realiza auditorías de seguimento periódicas (unha ou dúas veces ao ano), en datas acordadas mutuamente. O organismo de certificación informa previamente un plan de auditoría de tres anos, no que se indique o alcance de cada auditoría de seguimento. Estas auditorías planifícanse de maneira que todos os aspectos do SGC se auditen nun período de tres anos. Logo dos tres anos

lévase a cabo unha auditoría de re-certificación usando os pasos 2 e 5 anteriores.

## **4.2 EFQM. MODELO EFQM DE EXCELENCIA**

### **4.2.1 INTRODUCCIÓN Ao MODELO**

O Modelo EFQM de Excelencia é un marco de traballo non-prescriptivo que ten nove criterios. Os criterios que fan referencia a un Axente Facilitador tratan sobre o que a organización fai. Os criterios que fan referencia aos Resultados tratan sobre o que a organización logra. Os Resultados son consecuencia dos Axentes Facilitadores.

O Modelo, que recoñece que a Excelencia en todo o referente a resultados e rendemento dunha organización pódese lograr de xeito sostido mediante distintos enfoques, fundaméntase en que:

"Os resultados excelentes con respecto ao Rendemento da Organización, aos Clientes, as Persoas e a Sociedade lógranse mediante un Liderado que dirixa e impulse a Política e Estratexia, as Persoas da organización, as Alianzas e Recursos, e os Procesos."

### **4.2.2 QUE É A EFQM?**

EFQM (European Foundation for Quality Management ou Fundación Europea para a Xestión da Calidade).

MISSION: Ser a forza que impulsa a Excelencia nas organizacións europeas de xeito sostido.

VISION: Un mundo no que as organizacións europeas sobresaian pola súa Excelencia

EFQM é unha organización sen ánimo de lucro cuxo ámbito é Europa e a súa sé está en Bruxelas.

EFQM é o creador e o xestor do premio á Excelencia EEA (EFQM Excellence Award) que recoñece a Excelencia en Xestión nas organizacións.

EFQM é a propietaria do Modelo de Excelencia EFQM e a encargada de actualizala coas boas prácticas que se están levando nas organizacións de vangarda no tema da Excelencia en Xestión.

#### **4.2.3 HISTORIA DA EFQM**

1988 Foi creada a Fundación Europea para a Xestión da Calidade (EFQM) sendo unha organización sen ánimo de lucro formada por 14 organizacións europeas (Bosch, BT, Bull, Ciba-Geigy, Dassault, Electrolux, Fiat, KLM, Nestlé, Olivetti, Philips, Renault, Sulzer e Volkswagen)

1989 É establecida a misión, visión e obxectivos do EFQM e comézanse os traballos de desenvolvemento do Modelo Europeo de Calidade. Ademais, engadíronse outras 53 empresas.

1991 Nace o Modelo de Excelencia EFQM e lánzase o primeiro Premio Europeo de Calidade para empresas

1992 Preséntase o Premio Europeo de Calidade

1995 Adáptase o Modelo e lanza o Premio Europeo para o sector público

1996 Simplifícase o Modelo e lanza o Premio Europeo para PEMEs e unidades operativas

2003 Actualízase o Modelo de Excelencia

2005 Lánzase o sistema 2005+ para a presentación de memorias e avaliación para o Premio EFQM á Excelencia (EEA)

#### **4.2.4 QUE É O MODELO EFQM?**

O Modelo EFQM de Excelencia é un instrumento práctico que axuda ás organizacións a establecer un sistema de xestión apropiado, medindo en qué punto se atopan dentro do camiño cara á excelencia, identificando posibles carencias da organización e definindo accións de mellora.

#### **4.2.5 PARA QUE SERVE O MODELO EFQM?**

É un marco que as organizacións poden utilizar para axudarse a desenvolver a súa visión e as metas para o futuro dun xeito tanxible.

É un instrumento que as organizacións poden utilizar para identificar e entender a natureza do seu negocio, é dicir, as relacións entre os distintos axentes presentes na actividade, e as relacións causa-efecto.

É unha ferramenta que permite establecer unha mesma linguaxe e modo de pensar en toda a organización.

É unha ferramenta de diagnóstico para determinar a saúde actual da organización, detectando puntos de mellora e implantando accións que a axuden a mellorar.

É a base para a concesión do Premio EFQM á Excelencia, isto é, un proceso de avaliación que permite a Europa recoñecer ás súas organizacións mellor xestionadas e promovelas como modelos de excelencia das que as demais organizacións poidan aprender.

#### **4.2.6 COMPOSICIÓN DO MODELO EFQM**

O Modelo de Excelencia EFQM é un marco non preceptivo baseado en nove criterios.

Cinco destes son “Axentes Facilitadores” (O que a organización fai. Inclúe 24 subcriterios) e catro son “Resultados” (O que a organización logra. Inclúe 8 subcriterios). Total: 9 CRITERIOS, 32 subcriterios e 298 áreas a contemplar.

##### **CRITERIO 1: LIDERADO**

Como os líderes desenvolven e facilitan a consecución da misión e a visión, desenvolven os valores necesarios para alcanzar o éxito a longo prazo e implantan todo iso na organización mediante as accións e os comportamentos adecuados, estando implicados persoalmente en asegurar que o sistema de xestión da organización se desenvolve e implanta.

##### **Subcriterios**

- 1a. Desenvolvemento da misión, visión e valores por parte dos líderes, que actúan como modelo de referencia dentro dunha cultura de Excelencia.
- 1b. Implicación persoal dos líderes para garantir o desenvolvemento, implantación e mellora continua do sistema de xestión da organización.
- 1c. Implicación dos líderes con clientes, partners e representantes da sociedade.
- 1d. Reforzo por parte dos líderes dunha cultura de Excelencia entre as persoas da Organización.
- 1e. Os cambios na organización son definidos e impulsados polos líderes.

## CRITERIO 2: POLÍTICA E ESTRATEXIA

Cómo implanta a organización a súa misión e visión mediante unha estratexia claramente centrada en todos os grupos de interese e apoiada por políticas, plans, obxectivos, metas e procesos relevantes.

### Subcriterios

- 2a. As necesidades e expectativas actuais e futuras dos grupos de interese son o fundamento da política e estratexia
- 2b. A información procedente das actividades relacionadas coa medición do rendemento, investigación, aprendizaxe e creatividade son o fundamento da política e estratexia
- 2c. Desenvolvemento, revisión e actualización da política e estratexia
- 2d. Comunicación e despregue da política e estratexia a través dun esquema de procesos clave

## CRITERIO 3: PERSOAS

Cómo xestiona, desenvolve e aproveita a organización o coñecemento e todo o potencial das persoas que a compoñen, tanto a escala individual, como de equipos ou da organización no seu conxunto; e cómo planifica estas actividades en apoio da súa política e estratexia e do eficaz funcionamento dos seus procesos

#### Subcriterios

- 3a. Planificación, xestión e mellora dos recursos humanos
- 3b. Identificación, desenvolvemento e mantemento do coñecemento e a capacidade das persoas da organización
- 3c. Implicación e asunción de responsabilidades por parte das persoas da organización
- 3d. Existencia dun diálogo entre as persoas da organización
- 3e. Recompensa, recoñecemento e atención ás persoas da organización

#### CRITERIO 4: ALIANZAS E RECURSOS

Cómo planifica e xestiona a organización as súas alianzas externas e os seus recursos internos en apoio da súa política e estratexia e do eficaz funcionamento dos seus procesos

#### Subcriterios

- 4a. Xestión das alianzas externas
- 4b. Xestión dos recursos económicos e financeiros
- 4c. Xestión dos edificios, equipos e materiais
- 4d. Xestión da tecnoloxía
- 4e. Xestión da información e do coñecemento

#### CRITERIO 5: PROCESOS

Cómo diseña, xestiona e mellora a organización os seus procesos para apoiar a súa política e estratexia e para satisfacer plenamente, xerando cada vez maior valor, aos seus clientes e outros grupos de interese.

#### Subcriterios

- 5a. Deseño e xestión sistemática dos procesos
- 5b. Introducción das melloras necesarias nos procesos mediante a innovación, a fin de satisfacer plenamente a clientes e outros grupos de interese, xerando cada vez maior valor

5c. Deseño e desenvolvemento dos produtos e servizos baseándose nas necesidades e expectativas dos clientes

5d. Produción, distribución e servizo de atención, dos produtos e servizos

5e. Xestión e mellora das relacións cos clientes

## CRITERIO 6: RESULTADOS NOS CLIENTES

Qué logros está alcanzando a organización en relación cos seus clientes externos.

### Subcriterios

#### 6a. Medidas de percepción

Refírense á percepción que teñen os clientes da organización, e obtéñense, por exemplo, das enquisas a clientes, grupos focais, clasificacións de provedores existentes no mercado, felicitacións e reclamacións.

#### 6b. Indicadores de rendemento

Son medidas internas que utiliza a organización para supervisar, entender, predicir e mellorar o rendemento, así como para anticipar a percepción dos seus clientes externos.

## CRITERIO 7: RESULTADOS NAS PERSOAS

Qué logros está alcanzando a organización en relación coas persoas que a integran.

### Subcriterios

#### 7a. Medidas de percepción

Refírense á percepción da organización por parte das persoas que a integran, e obtéñense, por exemplo, de enquisas, grupos focais, entrevistas e avaliacións de rendemento estruturadas.

#### 7b. Indicadores de rendemento

Son medidas internas que utiliza a organización para supervisar, entender, predicir e mellorar o rendemento das persoas que a integran, así como para anticipar as súas percepcións.

## CRITERIO 8: RESULTADOS NA SOCIEDADE

Qué logros está alcanzando a organización na sociedade.

### Subcriterios

#### 8a. Medidas de percepción

Refírense á percepción da organización por parte da sociedade, e obtéñense, por exemplo, de enquisas, informes, reunións públicas, representantes sociais e autoridades gobernativas.

#### 8b. Indicadores de rendemento

Son medidas internas que utiliza a organización para supervisar, entender, predicir e mellorar o seu rendemento, así como para anticipar as percepcións da sociedade.

## CRITERIO 9: RESULTADOS CLAVE

Qué logros está alcanzando a organización con relación ao rendemento planificado

### Subcriterios

#### 9a. Resultados Clave do Rendemento da Organización

Estas medidas son os resultados clave planificados pola organización e, dependendo do obxecto e dos obxectivos da mesma, poden facer referencia a:

- Resultados económicos e financeiros
- Resultados non económicos

#### 9b. Indicadores Clave do Rendemento da Organización

Son as medidas operativas que utiliza a organización para supervisar, entender, predicir e mellorar os probables resultados clave do rendemento da mesma.

### **4.2.7 VANTAXES DE ADOPTAR O MODELO EFQM**



Aumentar a competitividade da organización:

- Sendo máis rendibles
- Logrando un bo clima de traballo
- Ofrecendo unha excelente calidade de servizo, tendo en conta tanto os requisitos legais como as necesidades e expectativas dos clientes.

#### **4.2.8 CAMBIOS QUE ORIXINA A EXCELENCIA EN XESTIÓN**

Concepto tradicional

- Descoñecemento do cliente
- Os empregados buscan satisfacer aos xefes
- A calidade refírese á produción e ás materias primas
- O departamento de calidade é o que asegura a calidade
- Existe unha reticencia cara ao cambio
- A organización está dividida en departamentos
- Non hai involucración entre departamentos
- A participación e a involucración non é prioritario e mesmo é sancionada
- Os xefes son os que deciden
- Xestión cualitativa

Concepto Excelente

- O cliente é o que manda
- Toda a organización busca satisfacer aos clientes
- A calidade concirne a todas as persoas da organización
- Cada empregado garante a calidade
- A contorna é cambiante e, por conseguinte, o cambio é natural nas empresas
- A organización está integrada e cohesionada
- Estimúlase e prémíase a participación e a involucración
- Os líderes delegan

- Xestión con datos, os indicadores sinalan oportunidades de mellora

## **4.3 SERIE ISO 9000.**

### **4.3.1 INTRODUCCIÓN.**

A Norma Internacional UNE NISO 9001 é un método de traballo considerado como o mellor para a mellora da calidade e da satisfacción do cliente. Na súa última revisión, ISO 9001:2008 clarifícanse algúns aspectos do seu anterior revisión (ISO 9001:2000), mantendo a esencia da mesma, sen ampliar a súa especificación.

O Estándar ISO 9000 está baseado nun modelo de xestión por procesos que desenvolve os oitos principios da Xestión da Calidade.

A nova versión da norma ISO 9001:2008 foi publicada en 2008, froito do traballo realizado polo Comité ISO TC/176/SC2.

A norma ISO 9001:2008 mantén de forma xeral a filosofía do enfoque a procesos e os oito principios de xestión da calidade, á vez que seguirá sendo xenérica e aplicable a calquera organización independentemente da súa actividade, tamaño ou o seu carácter público ou privado.

Aínda que os cambios abarcan practicamente a totalidade dos apartados da norma, estes non supoñen un impacto para os sistemas de xestión da calidade das organizacións baseados na ISO 9001:2000, xa que fundamentalmente están enfocados a mellorar ou enfatizar aspectos como:

- Importancia relevante do cumprimento legal e regulamentario.
- Aliñación cos elementos comúns dos sistemas ISO 14001
- Maior coherencia con outras normas da familia ISO 9000
- Mellora do control dos procesos subcontractados.

- Aumento de comprensión na interpretación e entendemento dos elementos da norma para facilitar o seu uso.

#### **4.3.2 A FAMILIA DE NORMAS ISO 9000**

*ISO 9000, Quality management systems – Fundamentals and vocabulary (Sistemas de xestión da calidade – Fundamentos e vocabulario)*

Esta norma describe os conceptos dun Sistema de Xestión da Calidade (SGC) e define os termos fundamentais usados na familia ISO 9000. A norma tamén inclúe os oito principios de xestión da calidade que se usaron para desenvolver a ISO 9001 e a ISO 9004.

*ISO 9001, Quality management systems - Requirements (Sistemas de xestión da calidade – Requisitos)*

Esta norma especifica os requisitos dun SGC, co cal unha organización busca avaliar e demostrar a súa capacidade para subministrar produtos que cumpran cos requisitos dos clientes e os regulamentarios aplicables, e con iso aumentar a satisfacción dos seus clientes.

*ISO 9004, Quality management systems – Guidelines for performance improvements (Sistemas de xestión da calidade – Directrices para a mellora do desempeño)*

Esta norma proporciona orientación para a mellora continua e pódese usar para mellorar o desempeño dunha organización. Mentres que a ISO 9001 busca brindar o aseguramento da calidade aos procesos de fabricación de produtos e aumentar a satisfacción dos clientes, a ISO 9004 asume unha perspectiva máis ampla de xestión da calidade e ofrece orientación para melloras futuras. As directrices para autoavaliación incluíronse no Anexo A da ISO 9004. Este anexo brinda un enfoque sinxelo e de fácil uso para determinar o grado relativo de madurez do SGC dunha organización e identificar as principais áreas de mellora.

A ISO 9000 é un punto de partida para entender as normas, xa que define os termos fundamentais usados na “familia” ISO 9000, ou no grupo de normas relativas a xestión da calidade. A ISO 9001 especifica os requisitos para un sistema de xestión da calidade co cal se poida demostrar a capacidade de subministrar produtos que cumpran os requisitos dos clientes, do mesmo xeito que os requisitos aplicables; tamén busca incrementar a satisfacción dos clientes. A ISO 9004 bríndalle orientación sobre a mellora continua do seu sistema de xestión da calidade, de maneira que se cumpran as necesidades e expectativas de todas as partes interesadas. Dentro das partes interesadas inclúense os clientes e os usuarios finais; os directores e persoal da organización; os propietarios e investidores; os provedores e socios, e a sociedade en xeral.

A ISO 9001 e a ISO 9004 son un “par coherente” de normas que relacionan a xestión da calidade moderna cos procesos e actividades dunha organización, e enfatizan na promoción da mellora continua e o logro da satisfacción do cliente. A ISO 9001, que se enfoca na eficacia do sistema de xestión da calidade para cumprir os requisitos dos clientes, úsase para certificación ou para acordos contractuais entre provedores e compradores. Por outra lado, a ISO 9004 non se pode usar para certificación, xa que non establece requisitos senón que proporciona orientación sobre a mellora continua do desempeño dunha organización. A ISO 9001 enfócase na “eficacia”, é dicir, en facer o correcto, mentres que a ISO 9004 fai énfase tanto na “eficacia” como na “eficiencia”, é dicir, en facer o correcto na forma correcta.

#### **4.3.3 PRINCIPIOS DE XESTIÓN**

A ISO 9000 baséase nos 8 principios de xestión:

- Enfoque ao cliente, que dá como resultado o cumprimento dos requisitos dos clientes e o esforzo por excedelos.

- Liderado, que apunta a crear un ambiente interno no cal as persoas estean totalmente involucradas.
- Participación do persoal, que é a esencia dunha organización.
- Enfoque baseado en procesos, que dá como resultado a mellora da eficiencia para obter os resultados desexados.
- Enfoque de sistema para a xestión, que conduce á mellora da eficiencia e a eficacia por medio da identificación, comprensión e xestión de procesos interrelacionados.
- Mellora continua, que se converte nun obxectivo permanente da organización.
- Enfoque baseado en feitos para a toma de decisións, baseado na análise de datos e información, e
- Relacións mutuamente beneficiosas co proveedor, baseado na comprensión da súa interdependencia

Para o manexo dunha organización, a ISO 9000 estimula a adopción do enfoque baseado en procesos. Para o modelo de procesos revisado na ISO 9000 considéranse cinco áreas principais:

- Sistema de xestión da calidade
- Responsabilidade da alta dirección
- Xestión de recursos
- Realización do produto
- Medición, análise e mellora

O modelo de proceso usado nas normas é completamente compatible co ben coñecido ciclo de PLANIFICAR, FACER, VERIFICAR, ACTUAR.

A xestión de calidade debe incluír os procesos requiridos para lograr calidade, e resaltar a interacción entre eles. A alta xerencia debe asumir a responsabilidade polo liderado, compromiso e participación activa para desenvolver e manter o sistema de calidade. A alta dirección debería subministrar os recursos adecuados, de maneira que os clientes obteñan o

que se acordou mutuamente. É necesario contar con procesos ben definidos, tanto operacionais como de soporte, para poder realizar o produto. A satisfacción dos clientes débese medir e analizar de maneira que a organización poida mellorar continuamente.

#### **4.3.4 VERSIÓNS ESPECÍFICAS DA NORMA ISO 9000**

As normas para “sectores específicos” son normas de xestión da calidade destinadas a unha industria específica, un produto ou grupo de produtos. Por exemplo, existen normas de xestión de calidade específicas para a industria automotriz, a industria de alimentos e bebidas, a industria das telecomunicacións, etc.

A familia de normas ISO 9000, xenérica por natureza, é aplicable a calquera tipo de produto ou servizo e pode ser implantada por calquera industria. Xa que logo, a ISO (Organización Internacional de Normalización), busca limitar a proliferación de normas no campo da xestión da calidade. O comité técnico ISO 176 (ISO/TC 176), responsable do desenvolvemento da familia de normas ISO 9000, apoia o desenvolvemento de normas para sectores específicos, unha vez que se estableceu que hai necesidade delas.

#### **4.3.5 CUSTOS E BENEFICIOS DE ESTABLECER UN SISTEMA DE XESTIÓN DA CALIDADE**

##### 1. Custos...

A implantación de custos en que incorren as compañías pódese detallar en custos directos e indirectos.

Os custos directos inclúen, entre outros, os seguintes:

- Contratación de formadores ou consultores externos, se cómpre.
- Envío de persoal para recibir formación externa.
- Adquisición das normas nacionais e internacionais pertinentes da familia ISO 9000, e os libros e publicacións relacionadas, e

- Adquisición de equipos adicionais, instrumentos e outros recursos que identifique a compañía.

Os custos indirectos inclúen, entre outros, os seguintes:

- Tempo empregado pola dirección e demais persoal, para o desenvolvemento do sistema.
- Reorganización dos procesos, incluídas as melloras no manexo da empresa, se cómpre.
- Custos de calibración externa dos equipos, co fin de asegurar a trazabilidade das medicións comparado con patróns de medición trazables a patróns de medición nacionais ou internacionais.
- Organización da formación interna.
- Tempo gastado polos auditores internos para as auditorías internas periódicas.
- Accións correctivas, incluída a actualización de manuais e procedementos, se cómpre.
- Gastos en dixitalización de documentos, papelería e outros artigos de consumo requiridos para a preparación de manuais e documentación de procesos, etc.

Algúns factores que poden axudar a reducir os custos anteriores inclúen:

- Facer que o persoal da compañía se familiarice cos requisitos do SGC.
- Contar con actividades documentadas relacionadas co sistema, por exemplo instrucións de traballo, plans de calidade, procedementos, etc., xa implantadas.
- A contratación de consultores unicamente para actividades específicas tales como "análises de brechas", formación de auditores, auditorías de preavaliación, etc., e contar con persoal interno para supervisar as actividades restantes.

Doutra parte, hai factores que poden significar custos de implantación maiores para a compañía. Por exemplo, se a súa compañía

realiza actividades en diferentes lugares, ou está involucrada no deseño e desenvolvemento de produtos, isto pode aumentar os custos.

## 2. ... e beneficios de obter unha certificación con base na ISO 9000

A implantación dun sistema de xestión de calidade xera beneficios internos á maioría de organizacións, do mesmo xeito que oportunidades con relación ao mundo exterior.

Os beneficios internos para a compañía inclúen:

- Enfoque mellorado cara ao cliente e orientación aos procesos dentro da compañía.
- Maior compromiso da dirección e mellor toma de decisións.
- Condicións de traballo melloradas para os empregados.
- Aumento de motivación por parte dos empregados.
- Custo reducido de fallas internas (menores tarifas de reprocesos, rexeitamento, etc.) e fallas externas (menos devolucións dos clientes, substitucións, etc.), e último, aínda que non o menos importante,
- A mellora continua do sistema de xestión da calidade.

Xéranse os seguintes beneficios externos:

- Os clientes teñen máis confianza en que recibirán produtos conformes aos seus requisitos, o que, á súa vez, redunda en maior satisfacción do cliente.
- Unha mellor imaxe da compañía.
- Publicidade máis agresiva, xa que os clientes poden estar informados dos beneficios de realizar negocios cunha compañía que manexa a calidade dos seus produtos.
- Máis confianza en que os produtos da compañía cumpren os requisitos regulamentarios pertinentes.
- Mellor evidencia obxectiva para defenderse contra demandas por obrigación civil, se os clientes chegasen a presentar algunha.



#### **4.3.6 IMPLANTACIÓN DUN SISTEMA DE XESTIÓN DA CALIDADE**

Un sistema de xestión de calidade con base na ISO 9000 pódese implantar nos seguintes pasos:

##### 1. Avaliar a necesidade e metas da organización con relación á implantación dun SGC

A necesidade pode xurdir a raíz de queixas repetidas dos clientes, devolucións frecuentes por garantía, entregas atrasadas, altos inventarios, atrasos frecuentes na produción, un alto nivel de reprocesos, ou rexeitamento de produtos ou servizos. Nesta etapa, identifique as metas que quixese alcanzar a través dun SGC, tales como a satisfacción dos seus clientes, unha maior participación no mercado, mellores comunicacións e moral da organización, unha maior eficiencia e rendibilidade, etc.

Outro obxectivo de implantar un SGC pode ser a demostración de conformidade por medio dunha certificación por terceira parte, que pode solicitar un cliente importante, ou que se esixe para poder rexistrarse como provedor de grandes compañías, por exemplo, os fabricantes de equipos orixinais (OEMs).

##### 2. Obter información acerca da familia ISO 9000

As persoas identificadas para iniciar o desenvolvemento dun SGC con base na ISO 9000 necesitan entender os requisitos da ISO 9001, conxuntamente coa ISO 9000 e a ISO 9004.

A información de soporte, por exemplo os principios de xestión de calidade, preguntas frecuentes (FAQ), orientación sobre o numeral 1.2 (aplicación) da ISO 9001, orientación sobre os requisitos de documentación da ISO 9001 e outros folletos, atópanse dispoñibles na páxina web da ISO: <http://www.iso.org>

##### 3. Nomear un consultor, se é necesario

Se dentro da organización non se conta coa competencia adecuada para desenvolver un SGC, pódese contratar un consultor. Antes de facelo é conveniente verificar os seus coñecementos e experiencia; o coñecemento deste acerca dos procesos de realización do produto da súa organización, e a súa experiencia en axudar a outras organizacións a alcanzar as súas metas establecidas, incluída a certificación.

#### 4. Toma de conciencia e formación

Hai que espertar a conciencia acerca dos requisitos do SGC entre todo o persoal que realiza actividades que afectan á calidade. Tamén planificar e brindar formación específica acerca de como desenvolver Manuais de Calidade, como planificar un SGC, como identificar e implantar procesos de mellora, e sobre como auditar a conformidade co SGC.

#### 5. Realizar a análise de brechas (Gap analysis)

Débense avaliar as brechas que hai entre o sistema de xestión da calidade existente e os requisitos da ISO 9001 para o SGC, e preparar o xeito de pechar estas brechas, incluída a planificación dos recursos adicionais requiridos. A análise destas brechas pódese levar a cabo mediante unha autoavaliación ou un consultor externo.

#### 6. Procesos de realización do produto

Examinar o numeral 7 da ISO 9001 relativo a realización "do produto", para determinar como os requisitos se aplican ou non ao SGC da compañía. Os procesos que se atopan baixo este numeral inclúen:

- Procesos relacionados co cliente.
- Deseño e desenvolvemento.
- Compras.
- Produción e subministración do servizo.
- Control de dispositivos de medición e seguimento

#### 7. Subministrar o persoal

Decidir sobre as responsabilidades das persoas que estarán involucradas no desenvolvemento e documentación do seu SGC, incluído o nomeamento dun representante da dirección, quen supervisará a implantación do SGC. A creación dun Comité Director do proxecto tamén pode ser útil para supervisar o progreso e subministrar os recursos cando estes requíranse.

### 8. Elaborar o cronograma

Preparar un plan completo con fin de pechar as brechas identificadas no Paso 5 para desenvolver os procesos do SGC. Neste plan incluír as actividades por realizar, os recursos requiridos, as responsabilidades e un tempo de finalización estimado para cada actividade. Os numerais 4.1 e 7.1 da ISO 9001 brindan información que se debería usar ao desenvolver o plan. O tempo total requirido para cada fase (planificación, documentación, implantación e avaliación) depende da extensión das brechas na súa SGC existente.

### 9. Redactar o Manual de Calidade

No Manual de Calidade:

- Incluir cómo se aplica o SGC aos produtos, procesos, instalacións e departamentos da organización.
- Excluir calquera requisito que se decidiu no paso 6, coa súa respectiva xustificación.
- Facer referencia ou incluír procedementos documentados para o seu SGC.
- Describir a interacción entre os procesos do SGC, por exemplo, a interacción entre os procesos de realización do produto e outros procesos de xestión, medición e mellora, e
- Redactar a política de calidade e os obxectivos de calidade da organización.

O persoal involucrado na organización debería revisar o Manual de Calidade e os procedementos documentados, de maneira que os seus comentarios e suxestións poidan terse en conta antes de que o Manual de Calidade e os procedementos sexan aprobados para publicación e uso. Tamén se debería chegar a unha decisión acerca da data de implantación.

#### 10. Realización de auditorías internas

Durante a fase de implantación, de aproximadamente tres a seis meses despois de que se escribe a documentación, os auditores adestrados deberían levar a cabo unha ou dúas auditorías internas que cubran todas as actividades do SGC, e a dirección involucrada debería emprender sen demora as accións correctivas sobre os achados de auditoría. Cando se requira, actualizar os manuais, os procedementos e os obxectivos. Logo de cada auditoría interna, a alta dirección debería revisar a eficacia do sistema e subministrar os recursos necesarios para as accións correctivas e melloras.

#### 11. Solicitude da certificación

Unha vez finalizado satisfactoriamente o Paso 10, e se a compañía decide obter unha certificación por unha terceira parte, pódese solicitar unha certificación a un organismo de certificación acreditado.

#### 12. Realización de avaliacións periódicas

Logo da certificación, a organización debería realizar periodicamente auditorías internas para revisar a eficacia do SGC e ver como se pode “mellorar continuamente”. A organización debería avaliar periodicamente se o propósito e metas (ver o Paso 1) para os cales se desenvolveu o SGC se están a lograr, incluída a súa mellora 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

Colexiado do CPEIG



# **5. A BIBLIOTECA DE INFRAESTRUTURA TI (ITIL). SOPORTE AO SERVIZO. ENTREGA DE SERVIZOS. ISO 20.000. OBXECTIVOS DA NORMA. MAPA E DESCRICIÓN DOS PROCESOS.**

## **Tema 5. A biblioteca de infraestrutura TI (ITIL). Soporte ao servizo. Entrega de servizos. ISO 20.000. Obxectivos da norma. Mapa e descrición dos procesos.**

### **INDICE**

#### **5.1 A biblioteca de infraestrutura TI (ITIL)**

##### **5.1.1 Introducción**

##### **5.1.2 Antecedentes**

##### **5.1.3 Que é ITIL?**

###### **5.1.3.1 Obxectivos**

###### **5.1.3.2 Beneficios**

###### **5.1.3.3 Estrutura**

##### **5.1.4 Libros de ITIL V3**

##### **5.1.5 Conclusións**

#### **5.2 Soporte ao servizo. Entrega de servizos.**

##### **5.2.1 Soporte ao servizo**

###### **5.2.1.1 Procesos**

##### **5.2.2 Entrega de servizos**

###### **5.2.2.1 Procesos**

#### **5.3 ISO 20.000. Obxectivos da norma**

##### **5.3.1 Que é ISO 20.000?**

##### **5.3.2 Utilidades do certificado ISO 20.000**

##### **5.3.3 ISO 20.000 e ITIL**

##### **5.3.4 Que representa exactamente ser conforme a ISO 20.000?**

#### **5.4 Deseño do mapa de procesos ITIL**

##### **5.4.1 Utilidade do modelo de referencia de ITIL**

### **5.1 A BIBLIOTECA DE INFRAESTRUTURA TI (ITIL)**

#### **5.1.1 INTRODUCCIÓN**

Na actualidade, a dependencia polas TI é un factor crítico no desenvolvemento das organizacións. O depender das TI soamente poderá ser visto como positivo a condición de que exista unha forma de operar que permita aproveitar as TI e que as converta nunha vantaxe que proporcione funcionalidade e flexibilidade institucional. Para lograr o anteriormente descrito, é indispensable que existan estándares internacionais que orienten as organizacións respecto de como é posible organizar e estruturar, da mellor maneira e aos mellores custos, todos os servizos de TI que xiran arredor da organización, ademais de lograr que se comuniquen os principais actores que interveñen no desenvolvemento da estratexia do negocio.

Por esa razón existen actualmente unha serie de estándares ou aliñamentos definidos por diversas institucións de recoñecido prestixio que pretenden ofrecerlles ás organizacións un marco de traballo que lles permita adoptar novas políticas interinstitucionais para a administración organizada e estruturada dos Servizos de TI. Entre os estándares comunmente recoñecidos a nivel mundial atópanse ISO 9000, COBIT, BS-15000, ITIL, ISO 20000, etc.

ITIL (Information Technology Infrastructure Library), considerado como un modelo que permite adoptar “mellores prácticas” nas organizacións, é o resultado da unión de varias librerías estandarizadas dedicadas a unha práctica en particular dentro da Xestión de Servizos de TI; ofrece ferramentas que facilitan a administración e optimización das TI nas organizacións. É unha estratexia que se pode aplicar en todo tipo de organizacións, pois o seu propósito final é implantar boas prácticas na prestación de servizos de TI.

### **5.1.2 ANTECEDENTES**



O incremento na dependencia das Tecnoloxías de Información (TI), así como a adopción de estándares propios para xestionar a información — incorrendo algunhas veces na duplicidade de esforzos nos proxectos ou en maiores custos— xunto coa calidade dos servizos TI que ofrecía o goberno británico, levaron a que no ano 1980 a Central Computer and Telecommunications Agency (CCTA) desenvolvese unhas primeiras recomendacións que facilitasen a administración e optimización das TI, recomendacións que actualmente se coñecen como ITIL (Information Technology Infrastructure Library). Esta iniciativa converteuse nun marco de traballo conformado por numerosos volumes, que ten probado a súa utilidade non soamente en organizacións gobernamentais senón en todos os sectores, converténdose na base para todo tipo de empresas, grandes ou pequenas, que tivesen a disposición de implantar Mellores Prácticas.

Inicialmente, a CCTA centrouse en recompilar información tendente a verificar como as organizacións dirixían a administración dos seus servizos, logrando analizar e filtrar os diferentes problemas que se xeraban; logo, comprobaron a utilidade e os beneficios das súas recomendacións. Na década dos 90, moitas empresas do goberno europeo adoptaron este marco de traballo, converténdose nunha boa práctica para a administración dos servizos de TI.

No ano 2001, a CCTA e todas as actividades que estaban baixo o seu control pasaron a formar parte da OGC (Office of Government Commerce), oficina do Ministerio de Facenda Británico, que, desta maneira, se converteu na nova entidade propietaria de ITIL, que tiña como finalidade axudar a modernizar a provisión de TI do goberno británico a través do uso de boas prácticas, logrando deste xeito o mellor valor monetario nas súas relacións comerciais. Posteriormente, a OGC publicaría novas versións de librerías de boas prácticas, escritas por expertos internacionais de diversas organizacións do sector público e privado.

En 1991, créase no Reino Unido a rede mundial de grupos de usuarios das TI que ofrecen mellores prácticas e guías baseadas en estándares para a Xestión de Servizos de TI; esta rede é denominada itSMF (Information Technology Service Management Forum); é o único grupo dedicado exclusivamente a este tipo de xestión e é recoñecido internacionalmente.

Está presente en varios países de Europa e nalgúns de América Latina, traballando en asociación coa OGC, BSI (British Standard Institute), o Information Systems Examination Board (ISEB) e o Examination Institute of the Netherlands (EXIN), e contribuíndo deste xeito á industria das Mellores Prácticas. Os capítulos desenvolvidos por itSMF fomentan o intercambio de información e experiencias vividas, orientando as organizacións de TI na implantación de boas prácticas e melloras nos servizos que ofrecen.

### **5.1.3 QUE É ITIL?**

ITIL (Information Technology Infrastructure Library) considérase unha colección de guías especializadas en temas organizacionais enfocadas á planificación, á subministración e ao soporte de servizos de TI. Recoñécese como un estándar global que resume as mellores prácticas para a área da Xerencia de Servizos de TI, orientadas especificamente a describir qué funcións ou procesos son os que se recomenda desenvolver, mais non como desenvolvelos; para isto último, é responsabilidade da organización definir as estratexias e métodos necesarios para implantalas, a condición de que se adapten ao tamaño, á cultura e ás necesidades internas da organización.

ITIL ofrece un marco de traballo para as actividades da área de TI proporcionando unha descrición dos roles, tarefas, procedementos e responsabilidades que poden ser adaptados en organizacións de TI cuxa finalidade sexa mellorar a Xestión dos seus Servizos; grazas á cantidade de



temas que abarca, considérase un elemento de referencia útil para as organizacións, xa que permite fixar novos obxectivos de mellora para a organización de TI baseándose na calidade do servizo e no desenvolvemento dos procesos dun modo eficaz e eficiente.

En varias ocasións, as mellores prácticas consideráronse como procesos que abranguen as actividades máis importantes que cómpre ter en conta dentro das organizacións de servizos de TI, polo que se pode afirmar que ITIL é unha colección coherente das mellores prácticas desenvolvidas na industria e non soamente pode ser adaptada ao sector público senón tamén ao privado.

As publicacións de ITIL describen como poden ser optimizados e coordinados dun mellor xeito todos aqueles procesos que foron previamente identificados e que interveñen na administración e operación da infraestrutura de TI, tales como o desenvolvemento do servizo, a xestión da infraestrutura e a provisión e soporte dos servizos; de igual maneira, revelan como estes poden ser formalizados dentro dunha organización, brindando un marco de traballo que facilita unificar a terminoloxía relevante dentro da organización e que lles permite ás persoas falaren unha linguaxe común, axudando así a definir obxectivos claros e a identificar os recursos e o esforzo necesarios para o seu cumprimento.

#### **5.1.3.1 OBXECTIVOS**

Especificamente, ITIL concéntrase en ofrecer servizos de alta calidade dándolles especial importancia ás relacións establecidas cos Clientes, para o cal o departamento de TI debe prover e cumprir con todos os acordos de servizos previamente definidos con eles, e para logralo é preciso que exista unha forte relación entre estes dous; por esta razón algúns dos obxectivos de ITIL están relacionados con:

- Promover a visión de IT como provedor de servizos.



- Xerar melloras na calidade da subministración dos servizos de TI.
- Fomentar a redución de custos dos servizos de TI.
- Aliñar a prestación dos servizos de TI coas necesidades actuais e futuras do negocio das organizacións, ademais de mellorar a relación cos Clientes.
- Estandarizar os procesos que forman parte da Xestión de Servizos de TI.
- Promover o uso dunha linguaxe común por parte das persoas para mellorar a comunicación dentro das organizacións.
- Servir de base para a certificación das persoas e das organizacións que desexan adoptar este estándar.
- Mellorar a eficiencia, aumentando a efectividade.
- Reducir os posibles riscos que se poidan presentar.

#### **5.1.3.2 BENEFICIOS**

ITIL centra os seus esforzos na satisfacción dos requirimentos organizacionais coa mellor relación custo/beneficio a través da descrición dun enfoque sistémico e profesional da Xerencia de Servizos de TI. Algúns dos beneficios que se logran coa adopción das mellores prácticas manexadas en ITIL están relacionados directamente co Cliente e coa organización; principalmente teñen que ver con:

- A subministración dos servizos de TI oríntase especialmente ao Cliente e os acordos sobre a calidade do servizo melloran a relación entre o departamento de TI e o Cliente.
- A mellora nos niveis de satisfacción dos Clientes por medio de medidas obxectivas e eficacia na dispoñibilidade e desempeño da calidade dos servizos de TI.
- Implantación de estándares que permitan realizar o control, a administración e operación dos recursos da organización.
- Os servizos ofrecidos son descritos nunha linguaxe máis cómoda e con maiores detalles para os Clientes.

- Xestíonanse dun mellor xeito a calidade, dispoñibilidade, fiabilidade e custo dos servizos ofrecidos na organización.
- Melloras na comunicación co departamento de TI no momento de acordar os puntos de contacto.
- O departamento de TI xera unha estrutura clara, centrada nos obxectivos corporativos dun modo eficaz.
- Soporte aos procesos de negocio e ás actividades dos decisores de TI.
- O departamento de TI conta cun maior control sobre a infraestrutura e os servizos que ten a cargo, obténdose unha visión clara da capacidade do departamento; ademais, permite administrar os cambios dun xeito sinxelo e fácil de manexar.
- A definición de funcións, roles e responsabilidades na área dos servizos.
- É posible identificar, a través dunha estrutura procedemental, a externalización dalgúns dos elementos dos servizos de TI.
- Subministración de servizos de TI que satisfagan as necesidades de negocio da organización.
- Incremento e melloras na produtividade e eficiencia organizacional a través das experiencias vividas e os coñecementos adquiridos.
- Xera un cambio cultural cara á provisión de servizos e sustenta a introdución dun sistema de xestión de calidade.
- Establece un marco de traballo coherente para as comunicacións tanto internas como externas, permitindo contar coa identificación e estandarización dos procedementos que deben seguirse.
- Melloras na satisfacción do persoal da organización reducindo notablemente a súa rotación.
- Melloras na comunicación entre o persoal de TI e os seus clientes.
- Xera o intercambio das experiencias obtidas coa súa adopción.

### **5.1.3.3 ESTRUCTURA**

O marco de traballo de ITIL está conformado por cinco (5) elementos principais que teñen directa relación entre si, xa que o éxito de cada un deles depende da súa interacción e coordinación cos demais.

Estes elementos son:

- The Business Perspective (A Perspectiva do Negocio)
- Managing Applications (Administración de Aplicacións)
- Deliver IT Services (Entrega de Servizos de TI)
- Support IT Services (Soporte aos Servizos de TI)
- Manage the Infrastructure (Xestión da Infraestrutura)

Cada unha das publicacións de ITIL céntrase en documentar un a un os elementos do marco de traballo; realízase unha descrición xeral do que se require para estruturar a Xestión de Servizos de TI e defínense os obxectivos, as actividades, os roles, os fluxos de comunicación necesarios e as entradas e saídas de cada un dos procesos que son indispensables nunha organización de TI.

Leváronse a cabo tres publicacións das mellores prácticas de ITIL; a primeira versión (V1) desenvolveuse inicialmente na década de 1980 e estaba conformada por dez (10) libros básicos que se centraban en describir a Xestión do Servizo, especificamente nas súas dúas áreas principais: (i) a entrega do servizo de TI e (ii) o soporte aos devanditos servizos; ampliouse posteriormente con trinta (30) libros complementarios que abarcaban diversos temas, desde o Cableado ata a Xestión de Continuidade do Negocio. Debido á cantidade de información existente, nace a segunda versión (V2), a cal empezou a ser reestruturada entre 1999 e 2001, cando ITIL se converte na pedra angular para a Xestión do Servizo, e se reorganizou dun xeito máis sinxelo, onde a maioría da información relacionada coa entrega do servizo e o soporte dos servizos se converte na base do marco de traballo e se agrupa en dous grandes volumes, eliminando desta forma a duplicidade na información existente na primeira versión; de tal maneira que esta versión queda reorganizada

aproximadamente en dez (10) libros. Na terceira versión (V3), publicada en maio de 2007, reducíronse os exemplares a cinco (5) volumes articulados que se centran principalmente no concepto e desenvolvemento do ciclo de vida do Servizo de TI. Ese ciclo iníciase cunha definición da estratexia do servizo; logo, céntrase en describir o deseño do servizo; posteriormente, inicia un período de transición onde se busca levar a cabo o desenvolvemento e a implantación do servizo; deseguido, realízase a operación do servizo e finalmente concéntrase en prover unha mellora continua do servizo, a cal está relacionada permanentemente coas demais etapas do ciclo de vida.

#### **5.1.4 LIBROS DE ITIL V3**

##### Service Strategy

Encárgase de asegurar que a estratexia do servizo sexa definida, se manteña e se implante; introdúcense novos conceptos, tales como a consecución do valor, a definición do mercado e o espazo de solución; céntrase no desenvolvemento de prácticas que permitan a toma de decisións baseado na comprensión do servizo activo, as estruturas e os servizos da economía co obxectivo final de incrementar a vida económica dos servizos; busca obter o aliñamento entre as TI e o negocio, non como se viña traballando anteriormente, onde soamente as TI eran as que se debían adaptar ao negocio.

Algúns dos conceptos xerais que se abordan neste libro teñen que ver coa definición do servizo, a estratexia do Service Management e a planificación do valor; a identificación da dirección e do goberno dos servizos das TI, a correspondencia existente entre os plans de negocio e as estratexias dos servizos de TI, algúns arquetipos de servizos e tipos de provedores de servizos, e o máis importante, qué debe formularse, implantarse e revisarse como estratexia do negocio.

##### Service Design

Este libro concéntrase en definir como se deseñará o servizo identificado previamente na estratexia a través do desenvolvemento de plans que a convertan en realidade. Para o deseño de servizos de TI adecuados e innovadores é necesario establecer e implantar políticas de TI, arquitecturas e algunha documentación pertinente. Dentro dos aspectos abordados no novo proceso de Xestión de Provedores que forma parte do deseño do servizo, atópanse o aproveitamento da dispoñibilidade, a capacidade, a continuidade e administración do SLA, así como os conceptos de garantía do servizo e utilidade, os cales son considerados como aspecto fundamental polos Clientes.

Outros conceptos que son traballados neste volume están asociados co ciclo de vida do servizo, obxectivos e elementos no deseño dos servizos, selección dun modelo de servizos apropiado, identificación de servizos, persoas, procesos, ferramentas, etc., modelo de custos, unha análise de riscos e beneficios, e a implantación do deseño do servizo.

### Service Transition

Ten como obxectivo minimizar dun xeito eficaz a brecha existente entre os proxectos e as operacións; céntrase nas accións que interveñen unha vez que o servizo deseñado debe poñerse en produción, orientándose especialmente ao papel que desempeña o Change Management e explicando as prácticas existentes para un correcto Release Management dun modo amplo e con visión a longo prazo, permitindo que se consideren todos os factores que participan, tales coma mecanismos de entrega, riscos, beneficios e facilidade na posterior operación continua do servizo deseñado.

A transición do servizo ten que ver coa calidade e o control da entrega das operacións e proporciona modelos para apoiar a transición orientando a forma para reducir variacións na entrega.



### Service Operation

O ciclo de vida de calquera servizo culmina coa súa operación, a cal debe ser tan robusta e efectiva que permita obter unha estabilidade na xestión do servizo en todo momento e de extremo a extremo. Neste volume explícanse as actividades necesarias para garantir operatividade no día a día, abarca moitas das disciplinas e conceptos definidos na V2 de ITIL, e especificamente concéntrase nos libros de Service Support e Service Delivery. A través dos coñecementos que se adquiren coa prestación real do servizo, pode chegar a influír na estratexia do servizo, o deseño, a transición e a mellora continua do servizo.

### Continual Service Improvement

Este libro abrangue a calidade do servizo no contexto de mellora continua; ademais, céntrase tamén en ofrecer mellora continua do servizo aínda cando este se encontre próximo a ser retirado. Un dos maiores beneficios deste libro é que indica explicitamente as accións que cómpre levar a cabo para a revisión e mellora dos procesos, información que na V2 non era tan clara.

Algúns dos conceptos que considera este libro están relacionados cos principios da mellora continua do servizo, a implantación da mellora de servizos, algúns elementos do negocio e da tecnoloxía que poden levar á mellora continua do servizo, e os beneficios xerados que favorecen o negocio, a organización e o aspecto financeiro.

## **5.1.5 CONCLUSIÓN**

As mellores prácticas de ITIL ofrecen un marco de traballo que lles permite ás organizacións melloraren o nivel de calidade nos servizos de TI ofrecidos; por este motivo, a súa adopción é un paso fundamental e transcendental que hai que tomar, xa que os beneficios que se van obter,

non soamente no mediano senón no longo prazo, van permitir que se perciba unha mellora continua dende o punto de vista da empresa.

A adopción dun estándar como o de ITIL entraña o desenvolvemento disciplinado dun proceso centrado no ciclo de vida do servizo de TI, no cal interveñen varios actores da organización, tanto internos como externos, e onde a achega e contribución de cada un deles ao cumprimento das políticas e actividades definidas para todos os procesos favorecen de xeito significativo o éxito da súa implantación. A estrutura das publicacións que foron liberadas desta metodoloxía na súa V3 permítelles ás organizacións adaptáreno dun mellor xeito, xa que ofrece as ferramentas necesarias que se deben ter en conta durante a definición e implantación dos procesos de TI; dado que o obxectivo central é o Ciclo de Vida dos Servizos de TI, presenta dunha maneira organizada e centralizada todas as actividades que deben ser consideradas durante a súa implantación, desde a definición da estratexia do servizo, o deseño do servizo, o período de transición polo que debe pasar, a operación do servizo, ata chegar a obter unha mellora continua do servizo.

Cada un dos procesos que se identificaron para ITIL teñen estreita relación entre eles mesmos, e da súa interacción e comunicación depende en gran parte o éxito da implantación das mellores prácticas; o simple feito de que algúns dos elementos necesarios nos procesos non cumpra cos aliñamentos establecidos no estándar, incrementa as posibilidades de que a adopción se converta nun fracaso.

Cada vez son máis as organizacións que entran a formar parte da familia de ITIL, o que deu lugar a que agora os Xerentes se empecen a preocupar por identificar como deben planificar, implantar e administrar exitosamente estas mellores prácticas, converténdose nun dos seus retos laborais e persoais. Tamén son varias as organizacións que xa teñen implantadas con éxito as mellores prácticas de ITIL e grazas ás experiencias que cada un deles viviu coa súa adopción púidose enriquecer

este modelo, ofrecendo valiosos tipos ás novas organizacións que a están implantando.

## **5.2 SOPORTE AO SERVIZO. ENTREGA DE SERVIZOS.**

A Xestión dos Servizos de TI está conformada por dúas grandes áreas: Entrega do Servizo (Service Delivery) e Soporte ao Servizo (Service Support). En libros independentes trabállase todo o relacionado coa perspectiva do negocio, a xestión da infraestrutura, a planificación que se require para implantar a xestión do servizo, a xestión da seguridade e a xestión das aplicacións.

### **5.2.1 SOPORTE AO SERVIZO**

É considerado como un dos eixes principais da Xestión do Servizo de TI; o contido do libro céntrase en describir os procesos necesarios para manter as operacións funcionando no día a día; explica como o Service Desk é o responsable e soporta a Xestión de Incidentes, proporcionando unha base para o soporte ás solicitudes e problemas que se lle poden presentar aos usuarios nunha organización. Así mesmo, encárgase de explicar como a Xestión de Problemas ten que ser, en certo modo, proactiva e reactiva, ademais de expoñer os beneficios que se poden obter cando se realiza unha análise efectiva das causas fundamentais dos problemas, ofrecendo unha ampla visión da redución do impacto que se produce cando existe unha suspensión do servizo aos usuarios.

En resumo, encárgase de describir a maneira en que os clientes e usuarios poden acceder aos servizos que lles permitan apoiar o desenvolvemento das súas actividades diarias e as do negocio, así como a forma en que os devanditos servizos deben ser soportados; ademais, céntrase en todos os aspectos que interveñen para garantir que o servizo

ofrecido aos usuarios sexa un servizo continuo, que estea dispoñible e que sexa de calidade.

### **5.2.1.1 PROCESOS**

#### Service Desk

É o único punto de contacto entre o cliente e os usuarios cos provedores de servizos de TI para todo o relacionado coa subministración de servizos de TI; tamén é o punto de partida encargado de informar sobre os Incidentes e de anotar as solicitudes de servizo realizadas polos usuarios. A súa obriga é manter informados os usuarios do servizo sobre os eventos, accións e oportunidades que poden chegar a afectar dalgún modo á dispoñibilidade do servizo e, por conseguinte, á continuidade na subministración do servizo no día a día. Todo o anterior é posible a través do rexistro, resolución e monitorización de problemas.

Dentro do marco de traballo das mellores prácticas de ITIL, o Service Desk non foi concibido como un proceso senón como unha función por desenvolver dentro da organización do servizo; algunhas das tarefas ao seu cargo inclúen: ser o punto primario de contacto (SPOC) cos clientes e usuarios; recibir e atender todas as solicitudes, consultas e inquietudes dos clientes e usuarios relacionadas coa subministración dos servizos de TI; documentar, priorizar e realizar un seguimento adecuado ás solicitudes de modificacións ou cambios realizadas polos usuarios; atender todos os procesos da Xerencia de Servizos definidos por ITIL; manter informados sobre o estado e progreso das solicitudes aos usuarios que as realizaron; clasificar as solicitudes recibidas e iniciar o seu proceso segundo os acordos do nivel de servizo (SLA) e procedementos establecidos; cando se requira dun soporte de segundo nivel, deberá encargarse de realizar a coordinación do soporte e a subministración do servizo, así como a dos provedores ou participación de terceiros; xestionar a reiniciación dos servizos co mínimo impacto no negocio, segundo os SLA e prioridades do

negocio establecidas; cerrar as solicitudes de servizo realizadas polos usuarios aplicando a avaliación de satisfacción do cliente; realizar seguimento aos SLA definidos levando a cabo as accións necesarias en caso de presentarse incumprimentos; proporcionar a información solicitada pola Xerencia de TI para manter e mellorar a calidade nos servizos ofrecidos.

De acordo coas mellores prácticas de ITIL, o Service Desk clasifícase en tres tipos: Call Center (Centro de Chamadas), Help Desk (Mesa de Axuda ) e Service Desk (Centro de Soporte); pola súa banda, o Help Desk está categorizado en: Service Desk Local, a través do cal se busca canalizar localmente todas as necesidades do negocio, resultando práctico en varios sitios que requiren servizos de soporte, pero podendo chegar a incorrer en grandes custos, xa que o servizo é ofrecido en diferentes lugares, o cal esixe a definición dun estándar operacional; o Service Desk Central, que pretende que todos os requirimentos do servizo sexan rexistrados nunha localización central, minimizando custos operacionais, xa que existe soamente unha mesa de axuda a nivel organizacional que atende a todos os requirimentos; e o Service Desk Virtual, que ten por finalidade ofrecer o servizo en calquera parte do mundo a través da rede, sen importar a súa localización física, xa que o servizo se atopa dispoñible en todo momento, e o seu éxito dáse a condición de que todos os usuarios da organización contén con infraestrutura tecnolóxica para poder acceder a ela. En conclusión, a implantación exitosa e execución do proceso de Service Desk xerará maiores beneficios na organización, representados na satisfacción dos clientes, minimización de custos, compromiso persoal e profesionalidade.

### Configuration Management

Coñecida tamén como Xestión da Configuración, é parte integral de todos os demais procesos da Xestión do Servizo; ten por obxectivo controlar os activos e elementos de configuración que forman parte da

infraestrutura de TI, polo cal se encarga de todos os procesos, ferramentas e técnicas necesarias para logralo; tamén é a súa responsabilidade proporcionar información fiable e actualizada non soamente dos elementos específicos da infraestrutura (Elementos de Configuración ou CI) necesarios para executar os procesos do negocio, senón tamén sobre as relacións entre eles mesmos, asegurando a integración coas demais disciplinas da Xestión do Servizo. Permite o desenvolvemento dos servizos informáticos de mellor calidade dun modo viable economicamente e proporciona información importante para o cálculo dos custos e a facturación dos servizos executados. As solicitudes de cambio sobre os CI rexístranse nunha base de datos creada para a Xestión da Configuración denominada Configuration Management Database (CMDB); nesta base de datos atópanse rexistrados todos os datos dos CI requiridos para a prestación do servizo, desde a súa descrición e interconexión ata un nivel de detalle que inclúe a categoría, as relacións, os atributos e os posibles estados nos cales poden estar en determinado momento; é necesario actualizar a CMDB cada vez que se realiza un cambio na infraestrutura e o devandito cambio está relacionado coa xestión da configuración.

### Incident Management

O obxectivo deste proceso é resolver calquera incidente que xere unha interrupción na prestación do servizo, restaurándoo novamente da maneira máis rápida e efectiva posible; este proceso non se detén en buscar, avaliar e analizar cales foron as causas que desencadearon a ocorrencia do devandito incidente, que xerou unha interrupción no servizo, senón simplemente límitase a solucionalo temporalmente e a restaurar o servizo de calquera xeito, o que probablemente pode chegar a xerar novas interrupcións do servizo polo mesmo incidente; os incidentes rexístranse sobre os CI.

Unha das maiores contribucións que se lles atribúen ás mellores prácticas de ITIL foi a de establecer a diferenza que existe entre os

incidentes e os problemas, onde se distingue entre a reiniciación rápida do servizo (Incident Management) e a identificación e corrección total da causa que ocasionou o incidente (Problem Management), pero destácase a articulación que debe existir entre estes dous procesos, do mesmo xeito que con Change Management (Xestión de Cambios) e o Service Desk. Recoméndase que todas as modificacións realizadas aos incidentes sexan relacionadas na mesma CMDB, igual que os rexistros de problemas, erros coñecidos e cambios, pois desta forma será máis fácil identificar se a ocorrencia do incidente pode converterse posteriormente nun problema, o que permitirá analizar e buscar a súa solución definitiva ou corrección total, ademais de que se evita a ocorrencia de novos incidentes como consecuencia dos cambios implantados. Algunhas das tarefas a cargo deste proceso teñen que ver con: identificación e documentación de todos os rexistros que se realizaron dos incidentes ocorridos, incluíndo informes e investigacións; priorizar e categorizar os rexistros dos incidentes que se xeraron; proporcionar unha análise inicial do incidente ofrecendo un soporte de primeiro nivel; escalar, cando sexa necesario, a execución de soporte de segundo e terceiro nivel; cando se encontre en risco o cumprimento dos SLA, é necesario incrementar a asignación de recursos que traballan na solución do incidente; resolver a situación no menor tempo posible, restaurando o servizo; cerrar e documentar os incidentes ocorridos; realizar un seguimento exhaustivo a cada un dos incidentes que se presentan (monitorización, revisión e comunicación do progreso); realizar unha avaliación dos incidentes rexistrados, analizalos e xerar informes sobre posibles melloras ao servizo.

### Problem Management

Este proceso dedícase a identificar as causas (orixe) que ocasionan os problemas que se presentan na infraestrutura de TI e a súa solución definitiva para evitar novas ocorrencias. Cando existe un incidente que se repite máis dunha vez, é posible que posteriormente se poida converter nun problema, aínda que a intención é evitar que isto suceda sendo

proactivos e previndo novas ocorrencias cando sexa posible; por iso se fala da xestión de problemas proactiva, onde os incidentes son detectados con suficiente anterioridade de tal xeito que permite adoptar as medidas preventivas necesarias garantindo que o servizo permaneza dispoñible e non se vexa afectado en ningún momento.

Como resultado da identificación temperá dos incidentes, as medidas preventivas que se recomenda adoptar tradúcense na execución de cambios nos CI, interactuando desta forma coa Xestión de Cambios; este proceso tamén se relaciona coa Xestión de Incidentes, xa que require dun rexistro preciso e completo de todos os incidentes co fin de identificar eficiente e eficazmente a súa causa e as tendencias na súa ocorrencia. Ademais, unha vez se atopa a solución a un problema, os incidentes que previamente foran consignados e que tiñan directa relación coas causas do problema poderán pasar a un estado Pechado ou Dados de Baixa.

### Change Management

Este proceso ten unha estreita relación co proceso de Configuration Management, xa que partindo da exactitude dos datos dos elementos da infraestrutura (CMDB) é posible garantir que a análise do impacto é realizada e coñecida, logrando tramitar deste xeito os cambios necesarios a través de procesos e procedementos estandarizados e consistentes; encárgase de obter a aprobación para realizar calquera cambio, así como de controlar a implantación dos cambios da infraestrutura de TI.

Dentro dos seus obxectivos atópanse: realizar unha valoración dos cambios e garantir que se poden executar ocasionando o mínimo impacto na prestación dos servizos de TI e na infraestrutura actual ou nova, e asegurar de maneira simultánea a trazabilidade dos cambios; implantar os cambios autorizados e requiridos para o cumprimento dos SLA de maneira eficiente, efectiva, económica e oportuna; minimizar os cambios, evitando que se leven a cabo cambios non autorizados.



### Release Management

A implantación dos cambios pode ter como resultado a instalación de novo hardware, a instalación de novas versións de software ou simplemente a actualización ou xeración de nova documentación; por ese motivo todas estas accións deben ser controladas e distribuídas dun modo organizado, como parte dun novo paquete ou versión.

Este proceso está asociado coa correcta implantación de todas as versións dos CI requiridas para a prestación dun SLA, proporcionando un marco de traballo para a coordinación, o control e a introdución física dun cambio; encárgase de levar o control de todos os cambios e novas versións que se xeraron como resultado da implantación dun cambio ou dunha nova adquisición (ex. Novo software instalado nunha máquina). É importante ter claras as relacións que existen entre os CI para que cando se realice un cambio de versión se saiba con certeza que accións ou consideracións é necesario ter en conta e a que outros CI se está afectando, ademais de manter os rexistros actualizados na CMDB.

## **5.2.2 ENTREGA DE SERVIZOS**

Considerado outro dos eixes fundamentais da Xestión do Servizo de TI, o Service Delivery céntrase en describir todos os aspectos que cómpre ter en conta para realizar unha planificación e mellora continua do servizo de TI a longo prazo e en todos os procesos que interveñen, para que a prestación do servizo se manteña e se provea de tal xeito que satisfaga as necesidades actuais e futuras do negocio. Algúns dos aspectos que describe están relacionados coa xestión dos niveis do servizo, os niveis de seguridade requiridos, a viabilidade financeira dos servizos, a súa capacidade, continuidade e dispoñibilidade, entre outros.

### **5.2.2.1 PROCESOS**

### Availability Management

Este proceso encárgase de garantir que os servizos de TI poidan ser accedidos dun xeito fiable e se atopen dispoñibles e funcionando correctamente cada vez que os Clientes ou usuarios así o requiran, enmarcados nos SLA que se defínisen para a prestación do servizo.

Dentro dos obxectivos definidos para este proceso atópase realizar o deseño dos servizos de TI co nivel de dispoñibilidade esixido polo negocio; garantir que exista unha dispoñibilidade non soamente nos servizos de TI senón tamén na súa infraestrutura, de tal forma que cumpra cos SLA establecidos; xerar informes de dispoñibilidade que demostren que o sistema é fiable e que se mantén, e minimizar a frecuencia e o tempo que tarda en solucionarse un incidente.

### Capacity Management

O obxectivo deste proceso é asegurar a existencia de certa capacidade en canto á infraestrutura de TI, a cal debe atoparse dispoñible constantemente para satisfacer os requirimentos do negocio respecto do volume de transaccións, o tempo de proceso, o tempo de resposta e, ante todo, contemplar a súa viabilidade cuantitativa e económica para non incorrer en custos desproporcionados.

Como o seu nome indica, a xestión da capacidade céntrase en verificar e garantir que todos os servizos de TI estean soportados coa suficiente capacidade de proceso e almacenamento, e que ademais estea dimensionada de tal modo que non supoña custos innecesarios para a organización, pero que tampouco xere insatisfacción nos Clientes ou usuarios debido á escasa calidade na prestación do servizo.

### Financial Management for IT Services

Céntrase en realizar un adecuado manexo do recurso financeiro (ingresos e gastos) asociado ao que implica a prestación dos servizos de TI,

sempre orientándose ao cumprimento dos SLA definidos; determina cal é o manexo financeiro asociado a cada un dos recursos que participan na subministración dun servizo, buscando manter un equilibrio permanente. Mantén unha estreita relación coa xestión da capacidade, a xestión da configuración e a xestión de niveis de servizo, e a través da información que cada un deles prové, é posible determinar exactamente cal é o custo real dun servizo.

### IT Service Continuity Management

A función principal deste proceso é evitar que unha grave e imprevista interrupción no servizo atente contra a continuidade do negocio, polo que se centra na preparación e planificación das medidas que se deben tomar para recuperar o servizo no caso de que aconteza algún desastre.

Pretende asegurar a dispoñibilidade do servizo a través da adopción de medidas preventivas que se orienten a reducir a probabilidade de fallos, e de que no caso de que ocorra algún fenómeno considerado como catastrófico ou desastre, o servizo poida ser restablecido no menor tempo posible e coas menores perdas de información para a organización.

### Service Level Management (SLM)

Encárgase de definir os servizos de TI ofrecidos, formalizándoos a través de Acordos de Niveis de Servizo (SLA) e Acordos de Nivel Operativo (SLO). Realiza unha avaliación do impacto que ocasionan os cambios sobre a calidade do servizo e os SLA unha vez que estes cambios son propostos e implantados, asegurando deste xeito que calquera impacto negativo sobre a calidade dos servizos de TI sexa relativamente baixo; tamén se encarga da creación de plans e emisión de informes respecto da calidade do servizo que se está ofrecendo.

Explica a importancia de establecer unha boa relación cos Clientes e así asegurar que as necesidades das empresas sexan entendidas; por isto Service Level Management céntrase tamén en coñecer as necesidades dos Clientes, definir correctamente os servizos que lles serán ofrecidos e monitorar a calidade dos servizos ofrecidos por medio dos SLA definidos.

Algúns dos aspectos máis importantes que se deben considerar na definición dos SLA están relacionados coa descrición do servizo e as súas características de funcionamento, coa dispoñibilidade do servizo —é dicir, durante canto tempo a organización se compromete a manter o servizo dispoñible para os seus Clientes—, para o cal tamén é indispensable que se acorden tempos de reacción (mínimos e máximos) na resolución de incidentes, e por esa razón os SLA dependen da solución dos incidentes nos tempos acordados. Outro aspecto que hai que ter en conta ten que ver cos obxectivos de dispoñibilidade, seguridade e continuidade do servizo, as obrigas que recaen tanto nos Clientes coma nos Provedores, e as horas críticas do negocio, entre outros.

### **5.3 ISO 20.000. OBXECTIVOS DA NORMA**

#### **5.3.1 QUE É ISO 20.000?**

ITIL mostra todo o que se debe facer para que os usuarios ofrezan servizos de TI adecuados cumprindo cos procesos da súa empresa. Para persoas individuais é posible obter certificacións de ITIL pero ata o momento non foi posible para unha organización de TI presentar probas de que traballa segundo as recomendacións de ITIL.

As normas ISO foron concibidas para encher este baleiro. En base a ITIL, as organizacións itSMF e BSI (British Standard Institute) elaboraron unha normativa que define os requisitos da xestión de servizos para as organizacións de TI.

Na actualidade, a normativa do BSI coñécese internacionalmente como normativa ISO 20000 e une os enfoques de ITIL e COBIT. ISO 20000 abre as portas ás organizacións de TI para que poidan obter por primeira vez unha certificación.

Aquelas organizacións que aspiren a lograr unha certificación segundo ISO 20000 deben cumprir os requisitos formulados na normativa —UNE-ISO/IEC 20000, Parte 1: Especificacións nas que se fixan os requisitos obrigatorios que debe cumprir toda organización que desexe unha certificación segundo esta normativa.

Os requisitos centrais da normativa ISO 20000 para unha organización de TI son:

- o O aliñamento dos procesos de TI segundo as normas de ISO 20000, que corresponden esencialmente ás recomendacións da Xestión do Servizo de ITIL (en especial tras a introdución de ITIL V3).
- o O uso dun método de xestión na organización de TI segundo as normas ISO 9001, baseado nos principios da xestión de procesos e dirixido a unha mellora continua da calidade.

A norma contén así mesmo dúas partes máis con carácter recomendatorio:

- UNE-ISO/IEC 20000, Parte 1: Anexo A (Informativo) mostra a correspondencia entre a norma ISO/IEC 20000-1:2005 e a norma ISO 9001:2008.
- UNE-ISO/IEC 20000, Parte 2: Código de boas prácticas que ofrece recomendacións sobre procesos da Xestión de Servizos de TI para organizacións que desexen unha certificación.

### **5.3.2 UTILIDADES DO CERTIFICADO ISO 20.000**

Un certificado ISO 20000 demostra que unha organización de TI:

- está orientada ás necesidades dos clientes;
- está en condicións de prestar servizos que cumpren cos obxectivos de calidade fixados;
- utiliza os seus recursos de forma económica.

Este certificado supón sempre unha vantaxe sobre a competencia. Cada vez hai máis clientes que esperan unha certificación ISO 20000 do seu provedor de TI, de tal xeito que este certificado se converte nunha condición imprescindible para gañar cota de mercado.

Pero tamén para a empresa mesma traballar segundo os principios de ISO 20000 (e ITIL) supón unha serie de beneficios. A normativa ten como obxectivo fornecer os negocios cos servizos de TI que realmente necesite e ocuparse sempre de que isto suceda de forma eficiente.

Empezar unha iniciativa ISO 20000 é unha boa forma de impulsar a introdución de mellores prácticas na organización de TI e manter a longo prazo a motivación para a súa implantación.

### **5.3.3 ISO 20.000 E ITIL**

ISO 20000 fixa requisitos para os procesos sen ocuparse de como deben ser conformados tales procesos de forma concreta.

Aí é onde aparece en escena ITIL: ITIL (e máis especialmente a nova versión 3) oríntase á normativa ISO 20000 e presenta un grande abano de

recomendacións de mellores prácticas, o que supón unha base de partida ben fundamentada para deseñar procesos conforme a ISO 20000.

A introdución de ITIL é, polo tanto, a mellor forma de prepararse para unha certificación ISO 20000.

### **5.3.4 QUE REPRESENTA EXACTAMENTE SER CONFORME A ISO 20000?**

Obter unha certificación ISO 20000 é un proxecto laborioso. A condición máis importante ao iniciar un proxecto así é determinar que obxectivo se persegue. Concretamente debe responderse á pregunta: Como debe ser a organización de TI ao final do proxecto?

Non obstante, a normativa deixa aberta esta cuestión, limitándose só a nomear os requisitos sen especificar como se deben cumprir. Por iso non existe unha resposta válida á pregunta sobre o que representa “ser conforme a ISO 20000”.

Así as cousas, non é de estrañar que ao empezar unha iniciativa ISO 20000 se faga evidente un gran problema: non queda claro como se debe estruturar de forma concreta o labor dunha organización de TI para cumprir cos requirimentos da normativa ISO e, xa que logo, non é fácil determinar os cambios que se precisan facer con ese obxectivo.

Aquí é onde ITIL pode prestar unha axuda decisiva, xa que ISO 20000 está orientada a ITIL.

Os coñecementos sobre ITIL adquírense normalmente mediante libros ou, de forma alternativa, co Mapa de Procesos ITIL® V3 en combinación co ITIL - ISO 20000 Bridge.

## **5.4 DESEÑO DO MAPA DE PROCESOS ITIL**

O Mapa de Procesos ITIL® V3 é un modelo de referencia íntegro de ITIL. Contén a descrición completa de forma gráfica de todos os procesos estándar na Xestión de Servizos de TI segundo ITIL V3. O modelo de procesos mostra como funciona ITIL na práctica: aforra traballo á hora de converter en procesos implantables as múltiples normas recollidas na bibliografía sobre ITIL.

O Mapa de Procesos ITIL® V3 foi creado para organizacións de TI e provedores de servizos de TI que:

- teñan previsto introducir por primeira vez, parcial ou totalmente, a Xestión de Servizos de TI segundo ITIL V3;
- desexen revalorar os procesos xa introducidos de ITIL baseándose en ITIL V3;
- queiran orientarse segundo ISO 20000 e/ou se estean preparando para unha certificación segundo ISO 20000.

### **5.4.1 UTILIDADE DO MODELO DE REFERENCIA DE ITIL**

O Mapa de Procesos ITIL® V3 está organizado para prestar un apoio óptimo en todos os pasos de calquera proxecto ITIL ou ISO 20000, desde a primeira planificación ata unha organización de TI que funcione segundo os principios das mellores prácticas. O seu uso ofrece vantaxes decisivas:

- O tratamento gráfico e navegable dos contidos de ITIL facilita a comprensión dos procesos ITIL e das súas interrelacións. Co modelo de procesos de ITIL pode aclarar ITIL a todos os colaboradores da súa organización de TI dunha forma moi efectiva e económica.
- Os modelos de procesos, claramente estruturados, e as guías complementarias serven de fío condutor á hora de que a organización incorpore o seu proxecto á implantación de ITIL e o leve a cabo. Na definición e documentación de procesos reducirase o seu traballo, xa que



adaptará os procesos de referencia existentes ás necesidades da súa organización sen ter que empezar cunha folla en branco.

- O Mapa de Procesos é unha documentación de procesos profesional coa que a xestión de TI estará na vantaxosa situación de poder demostrarlles aos clientes que a organización de TI realiza o seu labor de forma planificada, orientada ao cliente e de calidade.

Bibliografía:

Sitios web:

<http://www.iti1-officialsite.com/>

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

<http://iso20000enespanol.com/>

Autor:

Ramón Seoane Freijido

Director de Sistemas de Información Molduras del Noroeste

Colexiado do CPEIG



**6. AUDITORÍA INFORMÁTICA.  
MARCO XERAL. METODOLOXÍA.  
AUDITORÍA DOS GRANDES  
SISTEMAS INFORMÁTICOS.  
AUDITORÍA DA INFORMÁTICA  
PERSOAL E AS REDES DE  
ÁREA LOCAL. ASPECTOS  
LEGAIS.**

## **Tema 6. Auditoría informática. Marco xeral. Metodoloxía. Auditoría dos grandes sistemas informáticos. Auditoría da informática persoal e as redes de área local.**

### **INDICE**

#### **6.1 Auditoría Informática. Marco xeral.**

##### **6.1.1 Introducción**

##### **6.1.2 Definicións**

##### **6.1.3 Bases sobre as que se sustenta a auditoría informática**

##### **6.1.4 Carácter interdisciplinar de A.I.**

##### **6.1.5 Obxectivos**

##### **6.1.6 Controis**

##### **6.1.7 Conclusións**

#### **6.2 Metodoloxía**

#### **6.3 Auditoría dos grandes sistemas informáticos**

##### **6.3.1 Regulación internacional sobre auditoría de sistemas de información**

#### **6.4 Auditoría das redes de área local**

##### **6.4.1 Etapas a implantar na auditoría de redes**

#### **6.5 Auditoría da informática persoal**

##### **6.5.1 Análise forense**

###### **6.5.1.1 Introducción**

###### **6.5.1.2 Fases da análise forense**

### **6.1 AUDITORÍA INFORMÁTICA**

#### **6.1.1 INTRODUCCIÓN**

Na actualidade, as tecnoloxías da información están presentes en todas as áreas das organizacións. Esta implantación xeneralizada de Sistemas Informáticos (SI) realizouse en moitos casos sen a necesaria planificación, en parte porque os conceptos necesarios non estaban

suficientemente desenvolvidos. A tendencia cara aos sistemas abertos, a interconexión global e o desexo por parte dos consumidores de independizarse dos fabricantes, traen consigo a necesidade dun estudo máis profundo dos SI antes de tomar decisións. Polo tanto, faise necesario mellorar a planificación de futuras implantacións, a compatibilidade entre sistemas e a organización do persoal e da empresa.

Nas organizacións modernas, tanto públicas como privadas, a misión das tecnoloxías da información é facilitar a consecución dos seus obxectivos estratéxicos. Para iso, invístese unha considerable cantidade de recursos en persoal, equipos e tecnoloxía, ademais dos custos derivados da posible organización estrutural que moitas veces comporta a introdución destas tecnoloxías. Este importante investimento debe ser constantemente xustificado en termos de eficacia e eficiencia. Polo tanto, o propósito a alcanzar por unha organización que contrata a auditoría de calquera parte dos seus SI é asegurar que os seus obxectivos estratéxicos son os mesmos que os da propia organización, e que os sistemas prestan o apoio axeitado á consecución destes obxectivos, tanto no presente como na súa evolución futura.

### **6.1.2 DEFINICIÓNS**

A auditoría pode definirse como o exame comprensivo e construtivo da estrutura organizativa dunha empresa, dunha institución, ou de calquera outra entidade e dos seus métodos de control, medios de operación e emprego que dea aos seus recursos humanos e materiais.

Auditoría en Informática é a revisión e avaliación dos controis, sistemas, procedementos de informática, dos equipos de cómputo, a súa utilización, eficiencia e seguridade, da organización que participa no procesamento da información, a fin de que por medio da indicación de

cursos alternativos se acade unha utilización máis eficiente e segura da información que servirá para a adecuada toma de decisións.

### **6.1.3 BASES SOBRE AS QUE SE SUSTENTA A AUDITORÍA INFORMÁTICA**

Na actualidade os temas relativos á auditoría informática cobran cada vez máis relevancia, debido a que a información se converteu no activo máis importante das empresas, representando a súa principal vantaxe estratéxica, polo que estas invisten enormes cantidades de diñeiro e tempo na creación de sistemas de información, co fin de obter a maior produtividade e calidade posibles.

Así, de igual modo que se esixe para os outros activos da empresa, os requirimentos de calidade, controis, seguridade e información, son indispensables. A xerencia, polo tanto, debe establecer un sistema de control interno adecuado e tal sistema debe soportar debidamente os procesos do negocio.

Atendendo a estas tendencias, a Organización ISACA (Information Systems Audit and Control Association), a través da súa Fundación, publicou en decembro de 1995 o COBIT, como resultado de catro anos de intensa investigación e do traballo dun gran equipo de expertos internacionais, sendo esta metodoloxía o marco dunha definición de estándares e conduta profesional para a xestión e o control dos SI, en todos os seus aspectos, unificando diferentes estándares, métodos de avaliación e controis anteriores.

Adicionalmente, esta metodoloxía achega a orientación cara ao negocio e está deseñada non só para ser utilizada por usuarios e auditores, senón tamén como unha extensa guía para xestionar os procesos de negocios.

#### **6.1.4 CARÁCTER INTERDISCIPLINAR DE A.I.**

Auditoría Informática non é só unha prolongación da auditoría tradicional, senón que é un aspecto importante na seguridade e bo funcionamento da empresa.

Pódese considerar A.I. como a intersección de catro disciplinas: Auditoría Tradicional, Ciencias do Comportamento, Xestión de Sistemas de Información e Informática.

##### Auditoría Tradicional

Proporciona coñecemento e experiencia en Técnicas de Control Interno. É dicir, aspectos sobre como controlar as actividades da empresa. Un SPD ten compoñentes manuais e mecanizados, que serán obxecto de control.

- Os manuais están suxeitos aos principios de Control Interno da auditoría tradicional: separación de tarefas, persoal fiable, definición clara de responsabilidades, etc.
- Os mecanizados poden utilizar controis “clásicos”, desde o punto de vista informático: totais de control, cadres, balances, etc.

Outra achega da auditoría tradicional constitúena as metodoloxías de recolleita e avaliación de evidencias, aínda que o aspecto máis importante é que a auditoría tradicional proporciona un “saber facer”, un “modus operandi”, para examinar os datos e procesos con mente crítica, cuestionando a capacidade dun SPD de salvagardar os bens, e de manter a integridade dos datos dun xeito eficaz e eficiente.

##### Xestión de Sistemas de Información

Nos comezos da era informática houbo grandes fracasos ao implantar Sistemas de Proceso de Datos por non dispoñer de técnicas e ferramentas

axeitadas. Por desgraza, isto ás veces segue ocorrendo nos nosos días... por non utilizalas.

Hoxe en día dispoñemos de mellores técnicas: Programación Estruturada, Estándares de Xestión de Proxectos, Equipos de Traballo, Metodoloxías de Análises e Desenvolvemento, etc.

A causa final da existencia destas técnicas é a de simplificar o mantemento dos SPD's. Todos estes avances teñen un impacto en A.I. porque afectan directamente ás funcións de A.I..

### Ciencias do comportamento

A razón principal do fallo dos SPD's é o descoñecemento dos problemas do comportamento organizativo no deseño e implantación dos Sistemas de Información.

O auditor debe de coñecer as condicións que orixinan problemas de comportamento e que poden causar fallos no Sistema. É dicir, é necesario coñecer os problemas das persoas nas organizacións.

Alguns investigadores están aplicando a Teoría das Organizacións ao desenvolvemento e implantación dos Sistemas de Información. É dicir, débese de considerar, de modo concorrente, o impacto dun SPD tanto en:

- O cumprimento das tarefas (que se faga o que se espera)
- O sistema técnico (que teñamos recursos técnicos para realizar as tarefas)
- O sistema social (a calidade de traballo das persoas; que haxa un bo ambiente de traballo)

### Informática

A última das disciplinas base de A.I. é a Informática. Os informáticos tamén están fortemente involucrados nas funcións de A.I..

En Enxeñería do Software desenvolvéronse investigacións sobre:

- Como desenvolver software con “cero erros”





- Como manter a integridade global do hardware e o software: Programación Estruturada, Teoría de Fiabilidade, Teoría de Control, etc.

E estas disciplinas incorporáronse en A.I., xa que deben ser coñecidas polo auditor informático. No entanto, este coñecemento tecnolóxico de alto nivel ocasiona beneficios e desvantaxes a A.I., xa que:

- Permite ao auditor despreocuparse da fiabilidade dalgúns compoñentes do Sistema, xa que supón que funcionarán correctamente.
- Se hai “abuso” será moi difícil de detectar. Xa que non ten os coñecementos necesarios para detectalos.
- A fraude perpetrada por un programador altamente cualificado será moi difícil de detectar por un auditor que non teña ese alto grao de coñecemento técnico.

### **6.1.5 OBXECTIVOS**

Distinguimos entre dous tipos de Auditoría en función dos seus obxectivos:

- Auditoría externa: que se centra en obxectivos de seguridade: salvagarda de bens e integridade de datos, principalmente.
- Auditoría interna: que, ademais de nos obxectivos anteriores, céntrase en obxectivos de xestión, é dicir garantir que as tarefas se realicen nuns graos axeitados de efectividade e eficiencia.

#### Obxectivos de salvagarda de bens

Consideraremos como “bens” dun Centro de Proceso de Datos (CPD) o hardware, software, persoas, datos (ficheiros, bases de datos, etc.),

documentación, subministracións, etc. O hardware pode ser danado por accidente ou á mantenta; o software, do mesmo xeito que os datos, pode ser roubado ou destruído; as subministracións poden ser usadas con fins alleos aos da empresa, etc.

Ademais, estes bens concéntranse todos nun mesmo sitio, o ámbito físico do CPD, polo que deben de ser especialmente protexidos por un sistema de control interno, e a súa protección debe ser un obxectivo importante.

### Obxectivos de integridade de datos

Un dos aspectos que debemos coidar especialmente é a integridade dos datos, pero realizar esta tarefa vainos supoñer un custo fronte aos beneficios esperados ao implantar unhas medidas de seguridade. Desde un punto de vista puramente empresarial, estes beneficios deben superar os custos de implantación para que sexa rendible a súa utilización. Mais, disposicións legais poden obrigar a establecer controis, á marxe da súa rendibilidade.

Para determinar os custos e beneficios, estudaremos dous factores que afectan ao valor dun dato para a empresa:

1. O valor da información que proporciona o dato. Este valor depende da capacidade que esta teña para reducir a ambigüidade nunha toma de decisións. É dicir, os datos que inflúen directamente na toma de decisións serán os máis importantes e deberán ser especialmente protexidos.

2. As ocasións nas que o dato é usado por persoas que toman decisións. Se o dato é compartido, a súa falta de integridade afectará a todos os usuarios, polo que nun medio compartido é vital manter esta integridade.

### Obxectivos de efectividade do sistema

Para ver se un SPD (Sistema de Proceso de Datos) é efectivo, hai que coñecer as características do usuario e o tipo de decisións que se van

tomar. Non se debe avaliar de igual xeito a efectividade dun SPD dunha gran empresa que a dun pequeno comercio, por exemplo.

Para saber se o sistema está traballando correctamente, e para poder medir a súa efectividade, é necesario esperar a que o sistema leve funcionando un certo tempo, tralo cal normalmente a xerencia solicita unha auditoría para saber se o sistema alcanza os obxectivos que se programaran.

Como resultado da auditoría saberase se hai que descartar o SPD, modificalo, ou se o debemos deixar como está. Téñase en conta que esta auditoría tamén se pode facer durante a fase de Deseño do Sistema. Ademais, é posible que a xerencia solicite unha auditoría independente.

#### Obxectivos de eficiencia do sistema

Un SPD eficiente é o que utiliza o mínimo de recursos (tempo de máquina, periféricos, canles, software de sistemas, man de obra, etc.) para alcanzar os seus obxectivos.

En calquera sistema os recursos son escasos e hai que compartilos, polo que saber se se están a utilizar os recursos de forma eficiente non sempre é doado. Ademais, non se pode considerar a eficiencia dun sistema por si só, senón en conxunto cos demais sistemas dentro da organización.

Suboptimización: Prodúcese cando un sistema se optimiza a expensas doutros. Exemplo: Dedicar exclusivamente un recurso a un sistema (que non o utiliza a tempo completo) penalizará a outros sistemas que necesiten o recurso.

A eficiencia vólvese crítica cando o ordenador comeza a estar escaso de recursos (escaseza de capacidade de almacenamento en discos, de memoria, de procesador, etc.), polo que, se ademais os recursos son caros, hai que saber se se esgotaron porque as aplicacións son ineficientes, porque existen tapóns, ou simplemente porque o crecemento natural das aplicacións reduciu os devanditos recursos.

### **6.1.6 CONTROIS**

Estando nun medio informático no que o ordenador realiza de forma automática as tarefas, teremos que controlar se o que fai é o que realmente queremos que faga.

Os ordenadores xogan un papel moi importante ao axudármonos no proceso de datos, polo que hai que controlar o seu uso, xa que no procesamento de datos é un dos puntos onde se pode producir a fraude con maior facilidade.

Estes controis son necesarios xa que os medios abusan da capacidade do proceso de datos, dando lugar a intercambio de datos privados entre empresas ou fraudes por falta de controis nos sistemas.

Por todo iso é necesario establecer mecanismos de Control e Auditoría de Ordenadores nas organizacións, e deste xeito evitar:

- Custos pola perda de datos nas organizacións

Na actualidade, os datos son recursos críticos para a continuidade das funcións de calquera empresa, e a súa importancia dependerá do vitais que sexan para a organización.

Para poder protexer estes recursos será necesario establecer unha política no ámbito da organización, de copias de seguridade e recuperación.

- Toma de decisións incorrecta

Os datos vannos a permitir entre outras cousas realizar tomas de decisión. Pero para que as decisións tomadas a partir dos datos sexan correctas, teremos que garantir que os datos que nos son fornecidos son así mesmo correctos.

A importancia da veracidade dos datos vén dada polo tipo de decisións que se toman a partir deles. Por exemplo:

- En plans estratéxicos a longo prazo: Os datos que facilitan a toma de decisións poden ser “algo” imprecisos, posto que o resultado é global, xenérico. Pódense utilizar “grandes números”, é dicir, cantidades brutas aproximadas, sen importar o detalle.
- En cambio, en control de operacións e en control de xestión necesítanse datos totalmente precisos.

- Abuso Informático ou Abuso do Ordenador

Poderíase pensar que o abuso informático constitúe a causa principal da necesidade de A.I.. Mais, tras estudos intensivos chegouse á conclusión de que existen outras dúas causas de problemas, que son aínda máis importantes que o abuso informático:

- 1) Erros e omisións que orixinan perdas: frecuentemente, son o motivo de toma de decisións erróneas. Por exemplo: un simple erro no inventario que indique que existen 500 unidades dun determinado produto, cando en realidade hai 5.000, pode inducir a realizar un novo pedido, co conseguinte custo de adquisición, almacenamento ou perdas se o produto é perecedoiro.
- 2) Destrución de datos ocasionada por desastres naturais (auga, lume, e fallos de enerxía)

Isto obríganos a indicar solucións para estas dúas causas en primeiro lugar, antes mesmo que ao abuso informático.

De todos os xeitos, non podemos deixar de establecer controis para evitar o abuso informático, dado que os custos derivados deste adoitan ser moi superiores aos producidos polo abuso “manual”, ou aos derivados das dúas causas anteriormente citadas. En xeral, as fraudes que se poden realizar cos ordenadores producen máis perdas que as que se realizan con sistemas manuais.

- Perda de privacidade dos datos

Desde sempre se recolleron datos de persoas para o seu uso comercial: datos persoais, médicos, de impostos, etc. Pero desde a chegada dos ordenadores a difusión “incontrolada” destes datos converteuse nun serio problema, principalmente debido a que crear, actualizar e difundir unha base de datos con datos persoais de posibles clientes é moito máis fácil agora que cando os sistemas eran manuais.

En moitos países a privacidade dos datos é un dereito. No noso país, a Lei de protección de datos de carácter persoal asegura a confidencialidade dos datos e protexe aos propietarios dos mesmos do uso ilexítimo deles por terceiras persoas.

O que temos é que garantir que isto non ocorra, e que os datos só se utilicen co propósito para o que foron dados polo seu propietario, fin último da Auditoría Informática.

### **6.1.7 CONCLUSIÓN**

Os cambios na tecnoloxía inflúen en qué auditar e en como auditar, polo que inevitablemente, a auditoría cambiou de xeito drástico nos últimos anos co gran impacto que xeraron as técnicas informáticas na forma de procesala.

Os procesos de negocios, que se levan a cabo dentro das unidades dunha organización, se coordinan en función dos procesos de xestión básicos de planificación, execución e supervisión. O control que prové a auditoría é parte dos mencionados procesos e está integrado neles, permitindo o seu funcionamento adecuado e supervisando o seu comportamento e aplicabilidade en cada momento, co que constitúe unha ferramenta útil para a xestión, pero non un substituto da mesma.

## **6.2 METODOLOXÍA.**

O método de traballo do auditor pasa polas seguintes etapas:

- Alcance e Obxectivos da Auditoría Informática.
- Estudo inicial do medio auditable.
- Determinación dos recursos necesarios para realizar a auditoría.
- Elaboración do plan e dos Programas de Traballo.
- Actividades propiamente ditas da auditoría.
- Confección e redacción do Informe Final.

### Definición de Alcance e Obxectivos

O alcance da auditoría expresa os límites da mesma. Debe existir un acordo moi preciso entre auditores e clientes sobre as funcións, as materias e as organizacións a auditar.

Aos efectos de acoutar o traballo, resulta moi beneficioso para ambas partes expresar as excepcións de alcance da auditoría, é dicir cales materias, funcións ou organizacións non van ser auditadas. Tanto os alcances como as excepcións deben figurar ao comezo do Informe Final.

As persoas que realizan a auditoría teñen que coñecer coa maior exactitude posible os obxectivos aos que a súa tarefa debe chegar. Deben comprender os desexos e pretensións do cliente, de maneira que as metas fixadas poidan ser cumpridas.

Unha vez definidos os obxectivos (obxectivos específicos), estes engadiranse aos obxectivos xerais e comúns a toda auditoría Informática: A operatividade dos Sistemas e os Controis Xerais de Xestión Informática.

### Estudo Inicial

Para realizar o mencionado estudo cómpre examinar as funcións e actividades xerais da informática.

Para o equipo auditor, o coñecemento de quen ordena, quen diseña e quen executa é fundamental. Para realizar isto o auditor deberá fixarse en:

#### A- A Organización:

1) Organigrama: O organigrama expresa a estrutura oficial da organización a auditar.

2) Departamentos: O equipo auditor describirá brevemente as funcións de cada un deles.

3) Relacións Xerárquicas e funcionais entre órganos da Organización: O equipo auditor verificará se se cumpren as relacións funcionais e Xerárquicas previstas polo organigrama.

#### B- Medio Operacional:

1) Arquitectura e configuración de Hardware e Software: Os auditores, no seu estudo inicial, deben ter no seu poder a distribución e interconexión dos equipos.

O auditor solicitará información escrita, onde figuren todos os elementos físicos e lóxicos da instalación. En canto ao Hardware figurarán as CPUs, unidades de control local e remotas, periféricos de todo tipo, etc.

O inventario de software debe conter todos os produtos lóxicos do Sistema, desde o software básico ata os programas de utilidade adquiridos ou desenvolvidos internamente. Adoita ser habitual clasificalos en facturables e non facturables.

2) Comunicación e Redes de Comunicación: No estudo inicial os auditores dispoñerán do número, situación e características principais das



liñas, así como dos accesos á rede pública de comunicacións. Igualmente, posuirán información das Redes Locais da Empresa.

3) Aplicacións de bases de datos e ficheiros: O auditor solicitará información de tamaño e características das Bases de Datos, clasificándoas en relación e xerarquías.

Estes datos proporcionan unha visión aceptable das características da carga informática.

### Determinación de recursos da auditoría Informática

Mediante os resultados do estudo inicial realizado procédese a determinar os recursos humanos e materiais que se empregarán na auditoría.

#### Recursos materiais

É moi importante a súa determinación, por canto a maioría deles son proporcionados polo cliente.

#### Recursos Humanos

A cantidade de recursos depende do volume auditable. As características e perfís do persoal seleccionado dependen da materia auditable.

### Elaboración do Plan e dos programas de traballo

Unha vez asignados os recursos, o responsable da auditoría e os seus colaboradores establecen un plan de traballo. Decidido este, procédese á programación do mesmo.

O plan elabórase tendo en conta, entre outros criterios, os seguintes:

a) Se a Revisión debe realizarse por áreas xerais ou áreas específicas. No primeiro caso, a elaboración é máis complexa e custosa.

b) Se a auditoría é global, de toda a Informática, ou parcial. O volume determina non soamente o número de auditores necesarios, senón as especialidades necesarias do persoal.

Unha vez elaborado o Plan, procédese á Programación de Actividades.

### Actividades da Auditoría Informática

Para completar as distintas actividades propias da auditoría informática, o auditor pode facer uso das seguintes técnicas e ferramentas:

#### Técnicas de Traballo:

- Análise da información solicitada do auditado.
- Análise da información propia.
- Entrevistas.
- Simulación.
- Mostraxe.

#### Ferramentas:

- Cuestionario xeral inicial.
- Cuestionario *Checklist*.
- Estándares.
- Monitores.
- Simuladores (Xeradores de datos).
- Paquetes de auditoría (Xeradores de Programas).
- Matrices de risco.

### Informe Final

A función da auditoría materialízase exclusivamente por escrito. Polo tanto a elaboración final é o expoñente da súa calidade.

Resulta evidente a necesidade de redactar borradores e informes parciais previos ao informe final, que son elementos de contraste de opinión entre auditor e auditado e que poden descubrir fallos de apreciación no auditor.

### **6.3 AUDITORÍA DOS GRANDES SISTEMAS INFORMÁTICOS**

A auditoría dos SI deberá comprender non só a avaliación dos equipos de cómputo, dun sistema ou procedemento específico, senón que ademais haberá de avaliar os sistemas de información en xeral desde as súas entradas, procedementos, controis, arquivos, seguridade e obtención de información.

A auditoría dos SI é de vital importancia para o bo desempeño dos sistemas de información, xa que proporciona os controis necesarios para que os sistemas sexan fiables e cun bo nivel de seguridade. Ademais debe avaliar todo (informática, organización de centros de información, hardware e software).

Para facer unha axeitada planificación da auditoría dos SI, hai que seguir unha serie de pasos previos que permitirán dimensionar o tamaño e características do organismo a auditar, os seus sistemas, organización e equipo.

#### **6.3.1 REGULACIÓN INTERNACIONAL SOBRE AUDITORÍA DE SISTEMAS DE INFORMACIÓN**

En materia de Auditoría de Sistemas de Información existen varias metodoloxías desde o enfoque de control a nivel internacional. Algunhas das máis importantes para os profesionais da auditoría son:

#### A) ISACA-COBIT

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

ISACA propón a metodoloxía COBIT ® (Control Objectives for Information and related Technology). É un documento realizado no ano de 1996 e revisado posteriormente, dirixido a auditores, administradores e usuarios de sistemas de información, que ten como obxectivos de control a efectividade e a eficiencia das operacións; confidencialidade e integridade da información financeira e o cumprimento das leis e regulacións.

#### B) COSO

The Committee of Sponsoring Organizations of the Treadway Commission's Internal Control - Integrated Framework (COSO). Publicado en 1992 fai recomendacións aos contables de xestión de como avaliar, informar e implantar sistemas de control, tendo como obxectivo de control a efectividade e eficiencia das operacións, a información financeira e o cumprimento das regulacións que explica nos compoñentes do ambiente de control, valoración de riscos, actividades de control, información e comunicación, e a monitoraxe.

#### C) AICPA-SAS

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

Proporcióنالles unha guía aos auditores externos sobre o impacto do control interno na planificación e desenvolvemento dunha auditoría de

estados financeiros das empresas, presentado como obxectivos de control a información financeira, a efectividade e eficiencia das operacións e o cumprimento de regulacións, que desenvolve nos compoñentes de ambiente de control, valoración de risco, actividades de control, información, comunicación e monitoraxe.

#### D) IFAC - NIA

A Federación Internacional de Contables IFAC (<http://www.ifac.org>) emitiu as Normas Internacionais de Auditoría NIA 15, 16 e 20 en 1991.

IFAC mostra na NIA 15 (Auditoría en Medios Informatizados) unha referencia de controis para procesamento electrónico de datos e a necesidade destes cando estamos en medios onde os instrumentos tradicionais do papel e demais pistas de auditoría non son visibles para os contables no momento de realizar o seu traballo.

A NIA 16 (Técnicas de Auditoría Asistida por Computador) describe técnicas e procedementos de auditoría que se poden facer en medios informatizados con axuda dos computadores e outras tecnoloxías.

A NIA 20 preséntanos os efectos dun medio informatizado na avaliación de sistemas de información contables. Xunto coas demais normas dan unha guía ao auditor dos controis en xeral a ter en conta nun ambiente informatizado e nas aplicacións que procesan a información, así como técnicas de auditoría asistidas por computador e a súa importancia.

#### E) SAC

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

Realizado en 1991 e revisado posteriormente. Ofrece unha guía de estándares e controis para os auditores internos na área de auditoría de sistemas de información e tecnoloxía. Ten como obxectivos de control da

efectividade e eficiencia das operacións, a integridade da información financeira e o cumprimento de normas e regulacións que explica no medio de control, sistemas manuais e automatizados e procedementos de control.

#### F) MARGERIT

Consello superior de informática do ministerio de administracións públicas de España MARGERIT (Metodoloxía de Análise e Xestión de Riscos dos Sistemas de Información). 1997

É unha metodoloxía de análise e xestión de riscos dos sistemas de información das administracións públicas, emitida no ano 1997 polo consello superior de informática e recolle as recomendacións das directivas da Unión Europea en materia de seguridade de sistemas de información. Esta metodoloxía presenta un obxectivo definido no estudo dos riscos que afectan aos sistemas de información e ao seu medio facendo unhas recomendacións das medidas apropiadas que deberían adoptarse para coñecer, previr, avaliar e controlar os riscos investigados. Margerit desenvolve o concepto de control de riscos nas guías de procedementos, técnicas, desenvolvemento de aplicacións, persoal e cumprimento de normas legais.

#### G) EDP

A E.D.P. Auditors Foundation (EDPAF) fundada en 1976, é outra entidade de carácter educativo e investigador nos temas sobre estándares para a auditoría dos sistemas de información.

Esta fundación investigou sobre controis nos sistemas de información, xerando os dez estándares xerais de auditoría de sistemas e o código de ética para os auditores de sistemas que relacionamos a continuación.

## **6.4 AUDITORÍA DAS REDES DE ÁREA LOCAL.**

Unha Auditoría de Redes é, en esencia, unha serie de mecanismos mediante os cales ponse a proba unha rede informática, avaliando o seu desempeño e seguridade, a fin de lograr unha utilización máis eficiente e segura da información. O primeiro paso para iniciar unha xestión responsable da seguridade é identificar a estrutura física (hardware, topoloxía) e lóxica (software, aplicacións) do sistema (sexa un equipo, rede, intranet, extranet), e facerlle unha Análise de Vulnerabilidade para saber en que grao de exposición nos atopamos; así, feita esta "radiografía" da rede, procédese a localizar as súas carencias máis críticas, para propoñer unha Estratexia de Saneamento das mesmas; un Plan de Contención ante posibles incidentes; e un Seguimento Continuo do desempeño do sistema de agora en diante.

### **6.4.1 ETAPAS A IMPLANTAR NA AUDITORÍA DE REDES**

#### Análise de Vulnerabilidade

Este é sen dúbida o punto máis crítico de toda a Auditoría, xa que del dependerá directamente o curso de acción a tomar nas seguintes etapas e o éxito das mesmas.

#### Estratexia de Saneamento

Identificadas as "brechas" na rede, procédese a "parchealas", ben sexa actualizando o software afectado, ou volvendo a configuralo dun mellor xeito ou substituíndoo por outro que consideremos máis seguro e de mellor desempeño.

As bases de datos, os servidores internos de correo, as comunicacións sen cifrar, as estacións de traballo... todos os puntos críticos deben reducir o risco. Nos casos máis extremos, a mesma infraestrutura física da rede deberá ser reformulada, reorganizando e volvendo configurar os seus switches, routers e firewalls.

### Plan de Contención

A rede foi reformulada, o software foi reconfigurado (ou redeseñado) e o risco foi reducido; aínda así, constantemente estase informando de novos fallos de seguridade e a posibilidade de intrusión sempre está latente. Un disco pode fallar, unha base de datos pode corromperse ou unha estación de traballo pode ser infectada por un virus; para iso hai que elaborar un "Plan B", que prevexa un incidente aínda despois de tomadas as medidas de seguridade, e que dea resposta ante posibles eventualidades.

### Seguimento Continuo

A seguridade non é un produto, é un proceso. Constantemente xorden novos fallos de seguridade, novos virus, novas "ferramentas" (exploits) que facilitan a intrusión en sistemas, como así tamén novas e máis efectivas tecnoloxías para previr estes problemas; por todo iso, a actitude ante a seguridade debe ser activa, procurando estar "ao corrente" do que estea sucedendo na materia, para ir cubrindo as novas brechas que vaian xurdindo e -cando menos- para facerlle o traballo máis difícil aos nosos atacantes.

## **6.5 AUDITORÍA DA INFORMÁTICA PERSOAL**



Entre os distintos servizos de auditoría (interna, perimetral, test de intrusión, etc.) que se poden aplicar ao ámbito da Informática persoal, destaca a Análise forense como disciplina en auxe debido á proliferación de ataques informáticos así como a exposición dos datos contidos nos arquivos persoais como consecuencia da "necesidade" de estar conectados a redes públicas para o desempeño do traballo ou o lecer.

Son innumerables os medios de acceder aos dispositivos persoais (desde ordenadores persoais a terminais móbiles) e o risco de ser "espiado" aumenta se non se toman unhas medidas mínimas de seguridade, como software *anti-malware*, actualización de parches de seguridade, configuración do *firewall*, política de contrasinais, etc. Se estas medidas fallan, ou ben se accede por unha nova vulnerabilidade da que aínda non hai constancia, os nosos equipos persoais pasan a estar controlados por terceiros e toda a información neles contida pode ser utilizada de forma fraudulenta (contas bancarias, claves de servizos web, imaxes, vídeos, correos persoais, etc.)

Cando hai sospeita de que o noso equipo foi utilizado para levar a cabo actividades ilícitas (reenvío de *spam* no noso nome, anexar a nosa máquina a unha *botnet* para executar ataques tipo Denegación de Servizo, etc.) ou ben deixou de funcionar ao ser obxecto dun ataque (por virus, borrado de ficheiros por un terceiro, etc) deberemos obter evidencias que certifiquen o ocorrido.

## **6.5.1 ANÁLISE FORENSE**

### **6.5.1.1 INTRODUCCIÓN**

A informática forense ocúpase da investigación de acontecementos sospeitosos relacionados con sistemas informáticos, o esclarecemento de situacións creadas e os seus autores, a través da identificación,

preservación, análise e presentación de evidencias dixitais. Os servizos da informática forense non se limitan a achegar probas en procesos xudiciais ou administrativos. Tamén se aplica a recuperar evidencias para o seu estudo e á reconstrución de determinados feitos con fins privados, empresariais, etc.

Coa aplicación de métodos científicos na informática forense é posible estandarizar os procedementos e dotalos de maior consistencia.

A informática forense aplícase alí onde:

- Se presume unha actividade delituosa en Internet, en entidades económicas, ou sociais ou no ámbito privado
- cando existen sospeitas de roubo de datos, espionaxe industrial, sabotaxe ou delitos polo estilo
- tenencia, produción e difusión de pornografía prohibida
- así como outras actividades ilícitas, as cales se executan coa axuda de ordenadores.

Os obxectivos dunha investigación forense tras unha agresión son en xeral os seguintes:

- recoñecemento dos métodos ou os puntos débiles que posibilitaron a agresión
- determinación dos danos ocasionados
- identificación do autor
- aseguramento das evidencias

Da formulación destes obxectivos derívanse as seguintes cuestións:

- Como se pode verificar o ataque?
- Como se debe asegurarse o sistema comprometido e o seu medio?
- Que métodos deben empregarse para a captura de evidencias?

- En que secuencia se deben preservar as evidencias?
- Onde se deben buscar puntos de referencia e como poden ser atopados?
- Como se pode analizar o descoñecido?

### **6.5.1.2 FASES DA ANÁLISE FORENSE**

#### **IDENTIFICACIÓN**

A investigación forense comeza coa descrición exacta da situación atopada. Xunto coa toma dos elementos existentes relativos ao caso e as primeiras presuncións, teñen que definirse os aspectos que deban ser esclarecidos. A continuación deberá estruturarse o material existente. Feito isto deberán tomarse as decisións inherentes aos medios necesarios para a preservación do material. Todo isto debe ser debidamente documentado.

#### **PRESERVACIÓN**

O primeiro paso na preservación é asegurar o lugar, o/os sistemas, os medios de almacenamento de datos externos e outras posibles fontes de evidencias. O obxectivo fundamental é garantir a integridade das probas dixitais.

#### **ANÁLISE**

Tras a toma de datos probatorios relevantes e despois de aseguralos nos medios previstos, deberá procederse ás primeiras análises. Aquí requiriranse coñecementos sobre topoloxía de rede, aplicacións, vulnerabilidades do sistema e unha gran capacidade de improvisación.

A análise forense é unha metodoloxía de estudo que se aplica unha vez ocorrido un incidente, mediante o cal se trata de reconstruír como se penetrou no sistema e valóranse os danos ocasionados.

Mediante a análise forense é posible coñecer os detalles do ocorrido e propoñer a toma de medidas oportunas para previr futuros ataques, descubrir as vulnerabilidades que fixeron posible a intrusión, a orixe, as accións realizadas e as ferramentas utilizadas.

En última instancia, é capaz de identificar ao autor, o motivo e recomendar accións legais. En caso de dúbidas, o proceso de análise debe poder ser reproducido por expertos independentes (terceiros).

A análise non se realiza nunca sobre o sistema orixinal e esixe unha documentación exhaustiva.

## PRESENTACIÓN

A presentación constitúe a conclusión da investigación forense, prepárase e redáctanse os resultados de todo o proceso. Estes deben axustarse á motivación da investigación e a quen está dirixido.

O seu contido apuntará á determinación do autor ou autores, a data e hora, a descrición dos feitos, as proporcións alcanzadas e as súas causas.

## DOCUMENTACIÓN

A documentación de todo o proceso forense é de vital importancia. Todas as accións executadas deben ser protocolizadas en detalle. Esta protocolización debe ser oportuna, inmediatamente despois das accións. Deben servir de garante da actividade efectuada e facilitar a comprensión da investigación.

As actividades que non se documentan inmediatamente, xeralmente non se rexistran. Ao salvar datos volátiles nun sistema que se mantén activo mentres se realiza o traballo forense, debe facerse con testemuñas,

as cales poden corroborar que a preservación dos datos se realice correctamente e se eviten erros.

A importancia de manter unha protocolización detallada do proceso queda demostrada cando os resultados da análise forense son presentados e xorden dúbidas sobre algún aspecto. Ademais, a presentación efectúase moito despois de executarse as accións, quizais un ou varios participantes na investigación non poidan estar presentes, ou simplemente alguén non se poida lembrar dalgún detalle relevante.

Os protocolos deben recoller informacións como:

- persoa ou grupo de persoas que detectaron o caso
- hora e data da comunicación
- o contido exacto da comunicación
- nome das persoas e organizacións que executen a investigación
- nome de quen dirixe a investigación
- definición do procedemento
- causa da investigación
- lista de todos os sistemas, aparellos e aplicacións incluídos na investigación
- lista de todos os servizos e aplicacións activos
- lista de todos os administradores relacionados co sistema
- lista detallada de todos os pasos acometidos para atopar evidencias, analizalas e preservalas
- rexistro das persoas que teñen acceso ás evidencias, incluída data e 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

Colexiado do CPEIG

**7. LEI DE ACCESO  
ELECTRÓNICO DOS CIDADÁNS  
AOS SERVIZOS PÚBLICOS.  
DECRETO 198/2010, POLO QUE  
SE REGULA O  
DESENVOLVEMENTO DA  
ADMINISTRACIÓN  
ELECTRÓNICA NA XUNTA DE  
GALICIA E NAS ENTIDADES  
DEPENDENTES. REAL  
DECRETO 3/2010, POLO QUE SE  
REGULA O ESQUEMA  
NACIONAL DE SEGURIDADE NO  
ÁMBITO DA ADMINISTRACIÓN  
ELECTRÓNICA. REAL DECRETO  
4/2010, POLO QUE SE REGULA  
O ESQUEMA NACIONAL DE  
INTEROPERABILIDADE NO  
ÁMBITO DA ADMINISTRACIÓN  
ELECTRÓNICA.**

**Tema 7.- Lei de acceso electrónico dos cidadáns aos servizos públicos. Decreto 198/2010 polo que se regula o desenvolvemento da administración electrónica na Xunta de Galicia e as súas entidades dependentes. Real decreto 3/2010 polo que se regula o esquema nacional de seguridade no ámbito da administración electrónica. Real decreto 4/2010 polo que se regula o esquema nacional de interoperabilidade no ámbito da administración electrónica.**

## **INDICE**

### 7.1 Lei de acceso electrónico dos cidadáns aos servizos públicos

#### 7.1.1 Introducción

#### 7.1.2 Obxecto da lei

#### 7.1.3 Ámbito de aplicación

#### 7.1.4 Finalidades

#### 7.1.5 Principios.

### 7.2 Decreto 198/2010 polo que se regula o desenvolvemento da administración electrónica na Xunta de Galicia e as súas entidades dependentes.

#### 7.2.1 Introducción

#### 7.2.2 Obxecto

#### 7.2.3 Estrutura

### 7.3 Real decreto 3/2010 polo que se regula o esquema nacional de seguridade no ámbito da administración electrónica

#### 7.3.1 Introducción

#### 7.3.2 Principios

#### 7.3.3 Obxectivos

#### 7.3.4 Ámbito de aplicación.

### 7.4 Real decreto 4/2010 polo que se regula o esquema nacional de interoperabilidade no ámbito da administración electrónica.

#### 7.4.1 Introducción



#### 7.4.2 Obxectivos

#### 7.4.3 Ámbito aplicación e análise

### **1.- A LEI 11/2007 DE ACCESO ELECTRÓNICO DOS CIDADÁNS AOS SERVIZOS PÚBLICOS. A CALIDADE DOS SERVIZOS PÚBLICOS E DE ATENCIÓN AO CIDADÁN.**

#### 1.1 Introducción.

Durante os últimos anos producíronse numerosos cambios moi importantes nas relacións entre Administración, Goberno e cidadáns; o progreso social, económico e tecnolóxico fomentaron o desexo de cambio e presionaron á Administración para que se adaptase aos novos problemas, ás novas competencias e ás necesidades cidadás.

A Administración Pública, —en cumprimento do seu deber de servir con obxectividade aos intereses xerais e actuar de acordo cos principios de eficacia, xerarquía, descentralización, desconcentración e coordinación, con sometemento pleno á lei e ao dereito (art. 103.1 CE) — debe ser aquí unha peza fundamental para a implantación das políticas de modernización das administracións públicas. Ten que ser capaz de adaptarse ás novas realidades para formar parte do proceso de desenvolvemento económico e social das sociedades occidentais.

A mellora, e consecuentemente, a modernización das administracións públicas, debe ser un proceso continuo, dinámico e constante no que participen todos os que forman parte do sector público.

En España, o punto de partida foi o Acordo de Consello de Ministros do 15 de novembro de 1991, xa que en 1992 se aprobaría o

Plan de Modernización da Administración do Estado, composto por unha serie de medidas que tiñan como obxectivo mellorar e modernizar a Administración Pública para responder ás necesidades cambiantes dos cidadáns.

Na actualidade, as políticas de modernización están estreitamente ligadas ao desenvolvemento da administración electrónica.

Seguindo a definición dada pola Comisión Europea: a administración electrónica non é senón “o uso das tecnoloxías nas Administracións Públicas, combinado con cambios organizativos e novas aptitudes, co fin de mellorar os servizos públicos e os procesos democráticos e de reforzar o apoio ás políticas públicas”.

Actualmente, un elemento vertebrador do desenvolvemento das tecnoloxías na Administración constitúeo o denominado PLAN AVANZA II 2011-2015 (Aprobado polo Consello de Ministros do 16 de xullo de 2010).

Tomando como punto de partida o Plan Avanza aprobado no ano 2005, así como o marco europeo no que se encadran este tipo de iniciativas, identificáronse 34 retos concretos que debe abordar España no ámbito das TIC. Neste contexto, a Estratexia 2011-2015 do Plan Avanza 2 vai centrar os seus esforzos na consecución dos seguintes 10 obxectivos que facilitarán a superación dos retos definidos:

1. Promover procesos innovadores TIC (tecnoloxías da información e comunicación) nas AAPP.
2. Estender as TIC na sanidade e o benestar social.
3. Potenciar a aplicación das TIC no sistema educativo e formativo.

4. Mellorar a capacidade e a extensión das redes de telecomunicacións.

5. Estender a cultura da seguridade entre a cidadanía e as empresas.

6. Incrementar o uso avanzado de servizos dixitais pola cidadanía.

7. Estender o uso de solucións TIC de negocio na empresa.

8. Desenvolver as capacidades tecnolóxicas do sector TIC.

9. Fortalecer o sector de contidos dixitais garantindo a mellor protección da propiedade intelectual no actual contexto tecnolóxico e dentro do marco xurídico español e europeo.

10. Desenvolver as TIC verdes.

Dentro dese campo de actuación xoga un papel decisivo no seu desenvolvemento a Lei 11/2007, do 22 de xuño, de acceso electrónico dos cidadáns aos servizos públicos.

A Lei 30/1992, de 26 de réxime xurídico das administracións públicas e do procedemento administrativo común (LRXAP-PC) na súa primeira versión recolleu, no seu artigo 45, o impulso ao emprego e a aplicación das técnicas e medios electrónicos, informáticos e telemáticos pola Administración para o desenvolvemento da súa actividade e o exercicio das súas competencias, que lles permitía aos cidadáns relacionárense coas Administracións cando fose compatible cos “medios técnicos de que dispoñan”. Ademais o seu artigo 38, e posteriormente a Lei 24/2001, pasaron da informatización dos rexistros e arquivos aos rexistros telemáticos como forma de relacionarse coa Administración, sempre que o interesado sinalase este medio como preferente.

Pásase dunha declaración de impulso da administración electrónica á obriga de empregar medios telemáticos, xa que a Lei

11/2007 reconece o dereito dos cidadáns a se relacionar coa Administración a través destes medios.

O servizo ao cidadán esixe consagrar o seu dereito a comunicarse coas administracións por medios electrónicos, xa que estas están obrigadas a facelo mediante o recoñecemento por parte da lei do dereito dos cidadáns a establecer relacións electrónicas. Por iso cada Administración (Estatal, Autonómica e Local) debe facilitarlle ao cidadán, entre outros:

- O acceso á información e servizos da súa competencia.
- Presentar solicitudes e recursos.
- Os medios para dirixirse ás demais administracións, o cal implica a colaboración entre administracións.
- Efectuar pagamentos.
- Acceder ás notificacións e comunicacións que lles remita a Administración.
- Atopar información nun punto de acceso único sobre os servizos multicanle ou aqueles que se ofrezan por máis dun medio ou plataforma.

Os puntos máis salientables da lei son:

- Os cidadáns verán recoñecidos novos dereitos nas súas relacións coas administracións públicas.
- A creación da figura do Defensor do Usuario.
- As administracións terán a obriga de facer estes dereitos efectivos a partir do 2009.
- Os trámites e xestións poderán facerse desde calquera lugar, en calquera momento.
- A Administración será máis fácil, máis áxil e máis eficaz.
- Os cidadáns pasan a tomar o mando nas súas relacións coa Administración.
- É unha lei de consenso. Na súa elaboración participaron todas as administracións, cidadáns, partidos, empresas e asociacións.

## 1.2 Obxecto da lei

- Recoñecer o dereito dos cidadáns a se relacionar coas administracións públicas por medios electrónicos.
- Regular os aspectos básicos da utilización das tecnoloxías da información na actividade administrativa, nas relacións entre as administracións públicas, así como nas relacións dos cidadáns con estas coa finalidade de garantir os seus dereitos, un tratamento común ante elas e a validez e eficacia da actividade administrativa en condicións de seguridade xurídica.
- Utilizar, por parte das AA.PP., as tecnoloxías da información de acordo co disposto na lei, asegurando a dispoñibilidade, o acceso, a integridade, a autenticidade, a confidencialidade e a conservación dos datos, informacións e servizos que xestionen no exercicio das súas competencias.

## 1.3 Ámbito de aplicación (Disposición final primeira).

- As administracións públicas, entendendo por tales a Administración Xeral do Estado, as administracións das Comunidades Autónomas e as Entidades que integran a Administración Local, así como as entidades de dereito público vinculadas ou dependentes das mesmas.
- Os cidadáns nas súas relacións coas administracións públicas.
- As relacións entre as distintas administracións públicas.

A lei non será de aplicación para as administracións públicas nas actividades que desenvolvan en réxime de dereito privado.

## 1.4 Finalidades da lei

- Facilitar o exercicio de dereitos e o cumprimento de deberes por medios electrónicos.

- Facilitar o acceso por medios electrónicos dos cidadáns á información e ao procedemento administrativo, con especial atención á eliminación das barreiras que limiten o devandito acceso.

- Crear as condicións de confianza no uso dos medios electrónicos, establecendo as medidas necesarias para a preservación da integridade dos dereitos fundamentais, e en especial os relacionados coa intimidade e a protección de datos de carácter persoal, por medio da garantía da seguridade dos sistemas, os datos, as comunicacións, e os servizos electrónicos.

- Promover a proximidade co cidadán e a transparencia administrativa, así como a mellora continuada na consecución do interese xeral.

- Contribuír á mellora do funcionamento interno das administracións públicas, incrementando a eficacia e a eficiencia das mesmas mediante o uso das tecnoloxías da información, coas debidas garantías legais na realización das súas funcións.

- Simplificar os procedementos administrativos e proporcionar oportunidades de participación e maior transparencia, coas debidas garantías legais.

- Contribuír ao desenvolvemento da sociedade da información no ámbito das administracións públicas e na sociedade en xeral.

### 1.5 Principios xerais

- Limitacións da utilización das tecnoloxías da información:
- As establecidas pola Constitución.
- O resto do ordenamento xurídico.
- Principios:

1. O respecto ao dereito á protección de datos de carácter persoal nos termos establecidos pola Lei orgánica 15/1999, de protección dos datos de carácter persoal, nas demais leis específicas

que regulan o tratamento da información e nas súas normas de desenvolvemento, así como aos dereitos ao honor e á intimidade persoal e familiar.

2. Principio de igualdade con obxecto de que en ningún caso o uso de medios electrónicos poida implicar a existencia de restricións ou discriminacións para os cidadáns que se relacionen coas administracións públicas por medios non electrónicos, tanto polo que respecta ao acceso á prestación de servizos públicos como respecto de calquera actuación ou procedemento administrativo sen prexuízo das medidas dirixidas a incentivar a utilización dos medios electrónicos.

3. Principio de accesibilidade á información e aos servizos por medios electrónicos nos termos establecidos pola normativa vixente nesta materia a través de sistemas que permitan obtelos de modo seguro e comprensible, garantindo especialmente a accesibilidade universal e o deseño para todos dos soportes, canles e contornos con obxecto de que todas as persoas poidan exercer os seus dereitos en igualdade de condicións, incorporando as características necesarias para garantir a accesibilidade daqueles colectivos que o requiran.

4. Principio de legalidade respecto do mantemento da integridade das garantías xurídicas dos cidadáns ante as administracións públicas establecidas na Lei 30/1992, de réxime xurídico das administracións públicas e do procedemento administrativo común.

5. Principio de cooperación na utilización de medios electrónicos polas administracións públicas co obxecto de garantir tanto a interoperabilidade dos sistemas e solucións adoptados por cada unha delas como, se procede, a prestación conxunta de servizos aos cidadáns. En particular, garántese o recoñecemento mutuo dos documentos electrónicos e dos medios de identificación e autenticación que se axusten ao disposto na presente lei.

6. Principio de seguridade na implantación e utilización dos medios electrónicos polas administracións públicas, en virtude do cal se esixirá polo menos o mesmo nivel de garantías e seguridade que se require para a utilización de medios non electrónicos na actividade administrativa.

7. Principio de proporcionalidade en virtude do cal se esixirán só as garantías e medidas de seguridade axeitadas á natureza e circunstancias dos distintos trámites e actuacións. Así mesmo só se requirirán dos cidadáns aqueles datos que sexan estritamente necesarios en atención á finalidade para a cal se soliciten.

## **2. DECRETO 198/2010 POLO QUE SE REGULA O DESENVOLVEMENTO DA ADMINISTRACIÓN ELECTRÓNICA NA XUNTA DE GALICIA E NAS SÚAS ENTIDADES DEPENDENTES:**

### **2.1 Introducción.**

A Administración da CCAA de Galicia non pode permanecer allea aos incesantes e cada vez máis frecuentes cambios no seo das relacións coa Administración desde o punto de vista tecnolóxico; é neste ámbito onde, tal e como se recolle na exposición de motivos do Decreto, se pretende conseguir unha Administración diferente, que terá a electrónica como elemento central na súa modernización, e onde os seus efectos reais sobre a poboación irán encamiñados á utilización de medios e formas que reduzan a brecha tecnolóxica creando as condicións de confianza precisas para o uso das tecnoloxías da información e da comunicación.

### **2.1 Obxecto**

Ten por obxecto regular o dereito dos cidadáns a relacionarse coas administracións públicas por medios electrónicos, a tramitación dos procedementos administrativos incorporados á tramitación telemática, a creación e regulación da sede electrónica, a creación da



edición electrónica do Diario Oficial de Galicia e do Rexistro Electrónico, o impulso e desenvolvemento dos servizos electrónicos e o establecemento de infraestruturas e servizos de interoperabilidade.

### 2.3 Estrutura

O Decreto consta de 40 artigos, agrupados en nove capítulos, con tres disposicións adicionais, tres transitorias, unha derogatoria e catro finais.

No capítulo I da norma recolle o seu obxecto, o de regular o dereito dos cidadáns a relacionarse coas administracións públicas por medios electrónicos, a tramitación dos procedementos administrativos incorporados á tramitación telemática, a creación e regulación da sede electrónica, a creación da edición electrónica do Diario Oficial de Galicia e do Rexistro Electrónico, o impulso e desenvolvemento dos servizos electrónicos e o establecemento de infraestruturas e servizos de interoperabilidade

Establece como medidas de carácter xeral

- Ordenar e impulsar a Administración electrónica, a fin de mellorar a eficiencia interna, as relacións intra e inter administrativas e as relacións cos cidadáns.
- Garantir o dereito dos cidadáns a relacionarse por medios electrónicos coa Administración pública autonómica.
- Contribuír ao desenvolvemento da sociedade da información no ámbito das administracións públicas de Galicia.
- Preservar a integridade dos dereitos fundamentais relacionados coa intimidade das persoas para a garantía da seguridade dos datos e das comunicacións e para a protección dos servizos prestados en soporte electrónico.

- Facilitar o acceso dos cidadáns aos servizos da administración electrónica nas oficinas telemáticas integradas de atención aos cidadáns baseadas na cooperación interadministrativa, ofrecéndolles servizos aos cidadáns en oficinas públicas, con independencia de cal sexa a administración competente para coñecer o asunto.

- Posibilitar a intermediación entre administracións públicas para a resolución de trámites administrativos solicitados aos cidadáns cando sexan de competencia da Xunta de Galicia.

O capítulo II establece que a sede electrónica é o enderezo electrónico, a través do cal os cidadáns acceden á información, servizos e trámites electrónicos, que representa unha fonte de información auténtica na que o organismo titular identificado coa sede garante responsablemente a integridade, veracidade e actualización da información e os servizos aos que se poida acceder a través da mesma.

O enderezo electrónico de referencia da sede electrónica da Xunta de Galicia será <https://sede.xunta.es>, que será accesible directamente, así como a través do portal [www.xunta.es](http://www.xunta.es), configurándose como un conxunto de páxinas web que asegurará:

- A calidade da información e a coherencia na navegación.
- A identificación e comunicación segura, mediante os correspondentes certificados electrónicos admitidos pola Xunta de Galicia.

- O acceso ao Rexistro Electrónico, ás comunicacións e notificacións e aos formularios para iniciar os procedementos administrativos ou solicitar a prestación de servizos.
- Os principios de accesibilidade de acordo coas normas establecidas, estándares abertos e, se é o caso, aqueloutros que sexan de uso xeral polos cidadáns.

O capítulo III regula a creación do Diario Oficial de Galicia na súa edición electrónica, que terá unha consideración de publicación única, dotándoa de validez xurídica, que substituirá a edición impresa.

O capítulo IV trata sobre os mecanismos de identificación e autenticación, establecendo que os cidadáns poderán utilizar os seguintes instrumentos de identificación para se relacionar coa Xunta de Galicia e as entidades incluídas no ámbito de aplicación deste Decreto:

- a. En todo caso, os sistemas de sinatura electrónica incorporados ao documento nacional de identidade, para persoas físicas.
- b. Sistemas de sinatura electrónica avanzada, incluíndo os baseados en certificado electrónico recoñecido, admitidos polas administracións públicas que teñan validez para a Xunta de Galicia e que se especifiquen na sede electrónica.
- c. Sistemas de sinatura electrónica, como a utilización de claves concertadas nun rexistro previo como persoa usuaria inscrita no rexistro de funcionarios habilitados pola Xunta de Galicia.
- d. Outros sistemas de identificación que resulten proporcionais e seguros para a identificación das persoas interesadas.

O capítulo V regula a tramitación de procedementos administrativos no ámbito da administración electrónica, establecendo que a xestión electrónica da actividade administrativa respectará o exercicio e a titularidade do órgano ou entidade que teña atribuídas as súas competencias, así como a obrigatoriedade de impulso da administración electrónica.

Regula a iniciación e tramitación do procedemento por medios electrónicos, recoñecendo que calquera persoa interesada poderá iniciar e tramitar un procedemento administrativo por medios electrónicos, ante e en relación coa Xunta de Galicia ou as entidades incluídas no ámbito de aplicación deste Decreto, conforme ás previsións destas e sen outras limitacións que as establecidas nas normas e protocolos de aplicación en atención a razóns tecnolóxicas.

Os capítulos VI e VII regulan os aspectos da xestión e tramitación dos procedementos administrativos, tanto no ámbito interno, relativo a comunicacións e notificacións, que establece que as entidades incluídas no ámbito de aplicación do presente Decreto utilizarán un sistema de notificación electrónica que acredite a data e hora de posta a disposición da persoa interesada o acto obxecto de notificación, así como a data e hora de acceso desta ao seu contido mediante sistemas de selado de tempo, como no ámbito externo relacionado, en concreto coas copias e documentos electrónicos, define o documento electrónico este nos termos que se recollen no anexo da Lei 11/2007, de administración electrónica “Información de calquera natureza en forma electrónica, arquivada nun soporte electrónico segundo un formato determinado e susceptible de identificación e tratamento diferenciado.”

O capítulo VIII trata sobre a interoperabilidade e ten por obxecto fomentar a cooperación interadministrativa; figura clave no mesmo é o denominado protocolo de interoperabilidade, que é o documento que determinará o procedemento para incorporar e consumir a información en soporte electrónico das entidades incluídas no ámbito de aplicación do presente Decreto.

O capítulo IX concreta as funcións que o órgano de dirección con competencias xerais en materia de desenvolvemento da administración electrónica leva a cabo en relación con este Decreto, en desenvolvemento das competencias e funcións que lle atribúe o Decreto 325/2009, do 18 de xuño, de estrutura orgánica dos órganos superiores dependentes da Presidencia da Xunta de Galicia para o impulso, xestión e coordinación da administración electrónica como elemento indispensable para a modernización da Administración pública, a dirección e xestión de todas as actuacións da Xunta en materia de tecnoloxías da información e as comunicacións e o establecemento das directrices tecnolóxicas que deben seguir todos os órganos da Xunta de Galicia.

### **3. REAL DECRETO 3/2010 POLO QUE SE REGULA O ESQUEMA NACIONAL DE SEGURIDADE NO ÁMBITO DA ADMINISTRACIÓN ELECTRÓNICA.**

#### **3.1 Introducción**

Ten por obxecto regular o Esquema Nacional de Seguridade establecido no artigo 42 da Lei 11/2007, do 22 de xuño, e determinar a política de seguridade que cómpre aplicar na utilización dos medios electrónicos aos que se refire a citada lei e recolle e regula os principios básicos e requisitos mínimos que permitan unha protección adecuada da información.

A finalidade do Esquema Nacional de Seguridade é crear as condicións necesarias para a confianza no uso dos medios electrónicos a través de medidas para garantir a seguridade dos sistemas, dos datos, as comunicacións e os servizos electrónicos, e que permitan o exercicio de dereitos e o cumprimento de deberes a través destes medios. Persegue fundamentar a confianza en que os sistemas de información prestarán os seus servizos e custodiarán a información de acordo coas súas especificacións funcionais, sen interrupcións ou modificacións fóra de control e sen que a información poida chegar ao coñecemento de persoas non autorizadas.

Con obxecto de crear estas condicións, o Esquema Nacional de Seguridade introduce os elementos comúns que teñen que guiar a actuación das administracións públicas en materia de seguridade das tecnoloxías da información. En particular, introduce os seguintes elementos principais:

Os principios básicos que cómpre ter en conta nas decisións en materia de seguridade.

Os requisitos mínimos que permitan unha protección adecuada da información.

O mecanismo para lograr o cumprimento dos principios básicos e requisitos mínimos mediante a adopción de medidas de seguridade proporcionadas á natureza da información, ao sistema e aos servizos que hai que protexer.

Ten en conta as recomendacións da Unión Europea e a situación tecnolóxica das diferentes administracións públicas, así como os servizos electrónicos xa existentes e a utilización de estándares abertos, así como, de ser o caso e de forma complementaria, estándares que sexan de uso xeneralizado polos cidadáns.

Na súa elaboración manexáronse, entre outros, referentes en materia de seguridade tales como directrices e guías da OCDE, recomendacións da Unión Europea, normalización nacional e internacional, normativa sobre administración electrónica, protección de datos de carácter persoal, sinatura electrónica e Documento Nacional de Identidade Electrónico, así como referentes doutros países.

Realizouse nun proceso coordinado polo Ministerio da Presidencia co apoio do Centro Criptolóxico Nacional (CCN), coa participación de todas as administracións públicas. Ao longo dos últimos tres anos máis dun centenar de expertos das administracións públicas colaborou na súa elaboración; aos que lles hai que sumar os numerosos expertos que tamén achegaron a súa opinión a través das asociacións profesionais do sector TIC; todo iso á luz das últimas innovacións tecnolóxicas e dos principais referentes en materia de seguridade da información.

### 3.2 Principios básicos do Esquema Nacional de Seguridade.

O obxecto último da seguridade da información é asegurar que unha organización administrativa poderá cumprir os seus obxectivos utilizando sistemas de información. Nas decisións en materia de seguridade deberán terse en conta os seguintes principios básicos:

- a) Seguridade integral.
- b) Xestión de riscos.
- c) Prevención, reacción e recuperación.
- d) Liñas de defensa.
- e) Reavaliación periódica.
- f) Función diferenciada.

Recolle o Real decreto os requisitos mínimos que deberán ter os sistemas de seguridade, e así o artigo 11 establece que “Todos os órganos superiores das administracións públicas deberán dispoñer formalmente da súa política de seguridade, que será aprobada polo titular do órgano superior correspondente”. Esta política de seguridade establécese en función dos principios básicos indicados e desenvólvese aplicando os seguintes requisitos mínimos:

- a) Organización e implantación do proceso de seguridade.
- b) Análise e xestión dos riscos.
- c) Xestión de persoal.
- d) Profesionalidade.
- e) Autorización e control dos accesos.
- f) Protección das instalacións.
- g) Adquisición de produtos.
- h) Seguridade por defecto.
- i) Integridade e actualización do sistema.
- j) Protección da información almacenada e en tránsito.
- k) Prevención ante outros sistemas de información interconectados.
- l) Rexistro de actividade.
- m) Incidentes de seguridade.
- n) Continuidade da actividade.
- ou) Mellora continua do proceso de seguridade.

### 3.3 Obxectivos.

Crear as condicións necesarias de confianza no uso dos medios electrónicos a través de medidas para garantir a seguridade dos sistemas, dos datos, as comunicacións e os servizos electrónicos, que



permitan aos cidadáns e ás administracións públicas o exercicio de dereitos e o cumprimento de deberes a través destes medios.

Establecer a política de seguridade na utilización de medios electrónicos no ámbito da Lei 11/2007, que estará constituída polos principios básicos e os requisitos mínimos para unha protección adecuada da información.

Introducir os elementos comúns que guiarán a actuación das administracións públicas en materia de seguridade das tecnoloxías da información.

Achegar unha linguaxe común para facilitar a interacción das administracións públicas, así como a comunicación dos requisitos de seguridade da información á industria.

No Esquema Nacional de Seguridade concíbese a seguridade como unha actividade integral na que non caben actuacións puntuais ou tratamentos conxunturais, debido a que a debilidade dun sistema vén determinada polo seu punto máis fráxil e, a miúdo, este punto é a coordinación entre medidas individualmente axeitadas pero deficientemente ensambladas.

Dada a natureza da seguridade, a consecución destes obxectivos require un desenvolvemento que teña en conta a complexidade técnica, a obsolescencia da tecnoloxía subxacente e o importante cambio que supón na operativa da Administración a aplicación da Lei 11/2007.

### 3.4 Ámbito de aplicación

O seu ámbito de aplicación é o establecido no artigo 2 da Lei 11/2007, do 22 de xuño, é dicir, tanto as administracións públicas, entendendo por tales a Administración Xeral do Estado, as administracións das Comunidades Autónomas e as Entidades que integran a Administración Local, así como as entidades de dereito

público vinculadas ou dependentes das mesmas, os cidadáns nas súas relacións coas administracións públicas e as relacións entre as distintas administracións públicas.

Estarán excluídos os sistemas que tratan información clasificada regulada pola Lei 9/1968, do 5 de abril, de segredos oficiais, modificada pola Lei 48/1978, do 7 de outubro, e normas de desenvolvemento.

#### **4. REAL DECRETO 4/2010 POLO QUE SE REGULA O ESQUEMA NACIONAL DE INTEROPERABILIDADE NO ÁMBITO DA ADMINSTRACIÓN ELECTRÓNICA.**

##### **4.1 Introducción.**

O Esquema Nacional de Interoperabilidade persegue a creación das condicións necesarias para garantir o adecuado nivel de interoperabilidade técnica, semántica e organizativa dos sistemas e aplicacións empregados polas administracións públicas que permita o exercicio de dereitos e o cumprimento de deberes a través do acceso electrónico aos servizos públicos, á vez que redunda en beneficio da eficacia e a eficiencia.

Co obxecto de crear estas condicións, o Esquema Nacional de Interoperabilidade introduce os elementos comúns que guiarán a actuación das administracións públicas en materia de interoperabilidade. En particular, introduce os seguintes elementos principais:

- Enúncianse os principios específicos da interoperabilidade.

- Considéranse as dimensións da interoperabilidade organizativa, semántica e técnica ás que se refire o artigo 41 da Lei 11/2007, do 22 de xuño.

- Trátanse as infraestruturas e os servizos comúns, elementos recoñecidos de dinamización, simplificación e propagación da interoperabilidade, á vez que facilitadores da relación multilateral.

- Trátase a reutilización, aplicada ás administracións públicas, da documentación asociada e doutros obxectos de información, dado que a voz ‘compartir’ se atopa presente na definición de interoperabilidade recollida na Lei 11/2007, do 22 de xuño, e xunto coa voz ‘reutilizar’, ambas as dúas son relevantes para a interoperabilidade e atópanse entroncadas coas políticas da Unión Europea en relación coa idea de compartir, reutilizar e colaborar.

- Trátase a interoperabilidade da sinatura electrónica e dos certificados.

- Aténdese á recuperación e conservación do documento electrónico, segundo o establecido na citada Lei 11/2007, do 22 de xuño, como manifestación da interoperabilidade ao longo do tempo, e que afecta de forma singular ao documento electrónico.

- Para rematar, créanse as normas técnicas de interoperabilidade e os instrumentos para a interoperabilidade co fin de facilitar a aplicación do Esquema.

Ten en conta as recomendacións da Unión Europea e a situación tecnolóxica das diferentes administracións públicas, así como os servizos electrónicos xa existentes e a utilización de estándares abertos, así como, de ser o caso e de forma complementaria, estándares que sexan de uso xeneralizado polos cidadáns.

Na súa elaboración manexáronse, entre outros, referentes en materia de desenvolvemento da administración electrónica e, en particular, de interoperabilidade provenientes do ámbito da Unión Europea, de actuacións semellantes noutros países, da normalización

nacional e internacional; así como a normativa sobre administración electrónica, protección de datos de carácter persoal, sinatura electrónica e Documento Nacional de Identidade Electrónico.

Realizouse nun proceso coordinado polo Ministerio da Presidencia coa participación de todas as administracións públicas. Elaborouse coa participación de todas as administracións públicas. Ao longo dos últimos tres anos colaborou na súa elaboración máis dun centenar de expertos das administracións públicas; aos que lles hai que sumar os numerosos expertos que tamén achegaron a súa opinión a través das asociacións profesionais do sector TIC; todo iso á luz das últimas innovacións tecnolóxicas e dos principais referentes en materia de interoperabilidade.

#### 4.2 Obxectivos

Os seus obxectivos son os seguintes:

- Comprender os criterios e recomendacións que deberán ser tidos en conta polas administracións públicas para a toma de decisións tecnolóxicas que garantan a interoperabilidade e que eviten a discriminación dos cidadáns por razón da súa elección tecnolóxica.
- Introducir os elementos comúns que guiarán a actuación das administracións públicas en materia de interoperabilidade.
- Achegar unha linguaxe común para facilitar a interacción das administracións públicas, así como a comunicación dos requisitos de interoperabilidade á industria.

A interoperabilidade concíbese en consecuencia desde unha perspectiva integral, de maneira que non caben actuacións puntuais ou tratamentos conxunturais, debido a que a debilidade dun sistema vén determinada polo seu punto máis fráxil e, a miúdo, este punto é a coordinación entre medidas individualmente adecuadas pero deficientemente ensambladas.

Dada a natureza da interoperabilidade, a consecución destes obxectivos require un desenvolvemento que teña en conta a complexidade técnica, a obsolescencia da tecnoloxía subxacente e o importante cambio que supón na operativa da Administración a aplicación da Lei 11/2007.

#### 4.3 Ámbito de aplicación e Análise

O seu ámbito de aplicación é o establecido no artigo 42 da Lei 11/2007, do 22 de xuño, de acceso electrónico dos cidadáns aos servizos públicos, é dicir, ás administracións públicas, entendendo por tales a Administración Xeral do Estado, as administracións das Comunidades Autónomas e as Entidades que integran a Administración Local, así como as entidades de dereito público vinculadas ou dependentes das mesmas, os cidadáns nas súas relacións coas administracións públicas, as relacións entre as distintas administracións públicas.

Non será de aplicación para as administracións públicas nas actividades que desenvolvan en réxime de dereito privado.

Como aspectos mais importantes que destacar están:

1.- Regula de forma clara os dereitos dos cidadáns en relación coa utilización dos medios electrónicos na actividade administrativa, entre eles:

- A elixir entre aquelas que en cada momento se atopen dispoñibles, a canle a través da cal se relacionar por medios electrónicos coas administracións públicas.

- A non achegar os datos e documentos que obren en poder das administracións públicas, as cales utilizarán medios electrónicos para solicitar a devandita información sempre que, no caso de datos de carácter persoal, se conte co consentimento dos interesados nos termos establecidos pola Lei Orgánica 15/1999, de protección de datos de carácter persoal, ou unha norma con rango de lei así o determine, agás que existan restricións conforme á normativa de aplicación aos datos e documentos solicitados. O citado consentimento poderá emitirse e solicitarse por medios electrónicos.
- Á igualdade no acceso electrónico aos servizos das administracións públicas.
- A coñecer por medios electrónicos o estado de tramitación dos procedementos nos que sexan interesados, salvo nos supostos en que a normativa de aplicación estableza restricións ao acceso á información sobre aqueles.
- A obter copias electrónicas dos documentos electrónicos que formen parte de procedementos nos que teñan a condición de interesado.
- Á conservación en formato electrónico polas administracións públicas dos documentos electrónicos que formen parte dun expediente.
- A obter os medios de identificación electrónica necesarios, podendo as persoas físicas utilizar en todo caso os sistemas de sinatura electrónica do Documento Nacional de Identidade para calquera trámite electrónico con calquera administración pública.

- Á utilización doutros sistemas de sinatura electrónica admitidos no ámbito das administracións públicas.
- Á garantía da seguridade e confidencialidade dos datos que figuren nos ficheiros, sistemas e aplicacións das administracións públicas.
- Á calidade dos servizos públicos prestados por medios electrónicos.
- A escoller as aplicacións ou sistemas para relacionarse coas administracións públicas a condición de que utilicen estándares abertos ou, se é o caso, aqueloutros que sexan de uso xeneralizado polos cidadáns.

Regula o réxime xurídico da administración electrónica, define a sede electrónica como aquel enderezo electrónico dispoñible para os cidadáns a través de redes de telecomunicacións cuxa titularidade, xestión e administración corresponde a unha administración pública, órgano ou entidade administrativa no exercicio das súas competencias.

Regula a identificación e autenticación, dispoñendo que as administracións públicas admitirán, nas súas relacións por medios electrónicos, sistemas de sinatura electrónica que sexan conformes ao establecido na Lei 59/2003, do 19 de decembro, de sinatura electrónica, e resulten adecuados para garantir a identificación dos participantes e, se procede, a autenticidade e integridade dos documentos electrónicos.

Os cidadáns poderán utilizar os seguintes sistemas de sinatura electrónica para relacionarse coas administracións públicas, de acordo co que cada administración determine:

- En todo caso, os sistemas de sinatura electrónica incorporados ao Documento Nacional de Identidade, para persoas físicas.
- Sistemas de sinatura electrónica avanzada, incluíndo os baseados en certificado electrónico recoñecido, admitidos polas administracións públicas.
- Outros sistemas de sinatura electrónica, como a utilización de claves concertadas nun rexistro previo como usuario, a achega de información coñecida por ambas as partes ou outros sistemas non criptográficos, nos termos e condicións que en cada caso se determinen.

Con relación aos rexistros, comunicacións e notificacións dispón que as administracións públicas crearán rexistros electrónicos para a recepción e remisión de solicitudes, escritos e comunicacións.

Os rexistros electrónicos poderán admitir: documentos electrónicos normalizados correspondentes aos servizos, procedementos e trámites que se especifiquen conforme ao disposto na norma de creación do rexistro, cubertos de acordo con formatos preestablecidos, e ademais calquera solicitude, escrito ou comunicación distinta dos mencionados no apartado anterior dirixido a calquera órgano ou entidade do ámbito da administración titular do rexistro.

Con respecto ás comunicacións, os cidadáns poderán elixir en todo momento o modo de comunicarse coas administracións públicas, sexa ou non por medios electrónicos, excepto naqueles casos nos que dunha norma con rango de lei se estableza ou infira a utilización dun medio non electrónico. A opción de comunicarse por uns ou outros



medios non vincula ao cidadán, que poderá, en calquera momento, optar por un medio distinto do inicialmente elixido.

Con respecto a documentos e copias dispón que as administracións públicas poderán emitir validamente por medios electrónicos os documentos administrativos aos que se refire o artigo 46 da Lei 30/1992, de réxime xurídico das administracións públicas e do procedemento administrativo común, sempre que incorporen unha ou varias sinaturas electrónicas.

Os documentos administrativos incluírán referencia temporal, que se garantirá a través de medios electrónicos cando a natureza do documento así o requira.

As copias realizadas por medios electrónicos de documentos electrónicos emitidos polo propio interesado ou polas administracións públicas, manténdose ou non o formato orixinal, terán inmediatamente a consideración de copias auténticas coa eficacia prevista no artigo 46 da Lei 30/1992, de réxime xurídico das administracións públicas e do procedemento administrativo común, sempre que o documento electrónico orixinal estea en poder da Administración, e que a información de sinatura electrónica e, se procede, de selado de tempo permitan comprobar a coincidencia co devandito documento.

Regula a xestión electrónica de procedementos, dispoñendo que a xestión electrónica da actividade administrativa respectará a titularidade e o exercicio da competencia pola Administración Pública, órgano ou entidade que a teña atribuída e o cumprimento dos requisitos formais e materiais establecidos nas normas que regulen a correspondente actividade. Para estes efectos, e en todo caso baixo criterios de simplificación administrativa, impulsarase a aplicación de medios electrónicos aos procesos de traballo e a xestión dos procedementos e da actuación administrativa.

Por último, establece o R D un marco institucional de colaboración entre administracións dispoñendo que o II Comité Sectorial de administración electrónica, dependente da Conferencia Sectorial de Administración Pública, é o órgano técnico de cooperación da Administración Xeral do Estado, das administracións das Comunidades Autónomas e das entidades que integran a Administración Local en materia de administración electrónica.

O Comité Sectorial da administración electrónica velará polo cumprimento dos fins e principios establecidos nesta Lei, e en particular desenvolverá as seguintes funcións:

- Asegurar a compatibilidade e interoperabilidade dos sistemas e aplicacións empregados polas Administracións Públicas.
- Preparar plans programas conxuntos de actuación para impulsar o desenvolvemento da administración electrónica en España.
- Asegurar a cooperación entre as administracións públicas para proporcionar ao cidadán información administrativa clara, actualizada e inequívoca.

Autor:

Alfonso García Magariños

Director Asesoría Xurídica Municipal Concello da Coruña

**8. LEI DE MEDIDAS DE IMPULSO  
DA SOCIEDADE DA  
INFORMACIÓN. FACTURA  
ELECTRÓNICA. LEI DE  
SINATURA ELECTRÓNICA. LEI DE  
SERVIZOS DA SOCIEDADE  
DA INFORMACIÓN E COMERCIO  
ELECTRÓNICO.  
ACCESIBILIDADE. DECRETO  
3/2010, DO 8 DE XANEIRO,  
POLO QUE SE REGULA O  
SISTEMA DE FACTURACIÓN  
ELECTRÓNICA DA XUNTA DE  
GALICIA.**

**Tema 8. Lei de medidas de impulso da sociedade da información. Factura electrónica. Lei de sinatura electrónica. Lei de servizos da sociedade da información e comercio electrónico. Accesibilidade. Decreto 3/2010 do 8 de xaneiro polo que se regula o sistema de facturación electrónica da Xunta de Galicia.**

## **ÍNDICE**

- 8.1 Lei de medidas de impulso da sociedade da información
  - 8.1.1 Introducción
  - 8.1.2 Análise da lei
- 8.2 Sinatura electrónica.
- 8.3 Lei de sinatura electrónica
  - 8.3.1 Introducción
  - 8.3.2 Análise
  - 8.3.3 Efectos xurídicos e análises
- 8.4 Lei de servizos da sociedade da información e comercio electrónico
  - 8.4.1 Introducción
  - 8.4.2 Ámbito aplicación
  - 8.4.3 Principios e requisitos de actuación
- 8.5 Accesibilidade
- 8.6 Decreto 3/2010 do 8 de xaneiro polo que se regula o sistema de facturación electrónica da Xunta de Galicia
  - 8.6.1 Introducción
  - 8.6.2 Estrutura

## **8.1 LEI DE MEDIDAS DE IMPULSO DA SOCIEDADE DA INFORMACION.**

### 8.1 1 Introducción

Con data de 29 de decembro do 2007 publícase no BOE a Lei de medidas de impulso da sociedade da información (Lei 56/2007 do 28 de decembro) que se enmarca no conxunto de medidas que constitúen o Plan 2006-2010 para o desenvolvemento da Sociedade da Información e de converxencia con Europa e entre Comunidades Autónomas e Cidades Autónomas (Plan Avanza, aprobado polo Goberno en novembro do 2005; foi complementado polo PLAN AVANZA II 2011-2015, aprobado polo Consello de Ministros do 16 de xullo do 2010.)

Principais aspectos da lei:

- Introducción de Internet nos principais servizos de interese para os cidadáns. A lei obriga as grandes empresas de determinados sectores (electricidade, auga e gas, telecomunicacións) a facilitaren un medio de interlocución telemática cos seus clientes.
- Impulso á factura electrónica. O Goberno, ou de ser o caso, as Comunidades Autónomas con competencias, elaborarán un plan para xeneralizar o seu uso.
  - Desenvolvemento do comercio electrónico en España.
  - Regulación mínima das poxas electrónicas entre empresas.
  - Regras de valoración da sinatura electrónica en xuízo.
  - Flexibilización das obrigas relativas ás comunicacións comerciais e aos requisitos para a contratación por vía electrónica; en particular, para súa adecuación á telefonía móbil de datos.

- Maior seguridade en Internet. A lei obriga os provedores de acceso a Internet a informar aos seus usuarios sobre medios técnicos que permitan a protección ante aos problemas de seguridade en Internet (virus, ferramentas para o filtrado de contidos non desexados, etc.).
- Internet máis accesible para discapacitados e persoas de idade avanzada.
- Reforzo da protección dos dereitos dos usuarios en materia de telecomunicacións. A lei tipifica de maneira expresa como infracción administrativa a vulneración por parte dos operadores dos dereitos dos consumidores e usuarios no ámbito das telecomunicacións.
- Extensión da conectividade da Banda Ancha para alcanzar a maior conectividade posible antes do 31 de decembro do 2008.
- Dispoñibilidade de nomes de dominio «.es» con caracteres propios das linguas españolas, coma o «ñ» ou o «ç».
- Mellora da información dispoñible do sector TIC en España.
- Canalizacións para o tendido de redes de comunicacións electrónicas en estradas e infraestruturas ferroviarias.
- Maior rapidez na constitución de sociedades limitadas.
- Impulso para a cesión e posta a disposición da sociedade de contidos dixitais das Administracións Públicas.
- O Ministerio de Industria planificará frecuencias para a xestión individual do servizo de televisión local de proximidade por parte de entidades sen ánimo de lucro.
- Regulación do xogo. O Goberno presentará un proxecto de lei para regular as actividades de xogo e apostas atendendo aos grupos especialmente sensibles de usuarios, así como aos consumidores en xeral. Tamén deberá establecer un sistema de tributación sobre os servizos de xogos e apostas por sistemas interactivos baseados en comunicacións electrónicas, que só se poderán exercer por aqueles operadores autorizados pola Administración competente.

Nesta liña, a presente lei, por unha banda, introduce unha serie de innovacións normativas en materia de facturación electrónica e de reforzo dos dereitos dos usuarios e, por outra banda, acomete as modificacións necesarias no ordenamento xurídico para promover o impulso da sociedade da información.

Neste sentido, introdúcense unha serie de modificacións tanto da Lei 34/2002, do 11 de xullo, de servizos da sociedade da información e de comercio electrónico, como da Lei 59/2003, do 19 de decembro, de sinatura electrónica, que constitúen dúas pezas angulares do marco xurídico no que ten lugar o desenvolvemento da sociedade da información.

A devandita revisión do ordenamento xurídico complétase con outras modificacións menores da Lei 32/2003, do 3 de novembro, xeral de telecomunicacións, da Lei 11/1998, do 24 de abril, xeral de telecomunicacións e da Lei 7/1996, do 15 de xaneiro, de ordenación do comercio retalista.

#### 8.1.2 Análise.

O capítulo I da lei introduce senllos preceptos dirixidos a impulsar o emprego da factura electrónica e o uso de medios electrónicos en todas as fases dos procesos de contratación e a garantir unha interlocución electrónica dos usuarios e consumidores coas empresas que presten determinados servizos de especial relevancia económica.

En materia de facturación electrónica, o artigo 1 establece a obrigatoriedade do uso da factura electrónica no marco da contratación co sector público estatal nos termos que se precisen no Proxecto de lei de contratos do sector público; define o concepto legal de factura electrónica e, así mesmo, prevé actuacións de complemento e profundación do uso de medios electrónicos nos procesos de contratación.

O artigo 2, pola súa banda, establece a obriga das empresas de determinados sectores con especial incidencia na actividade económica (entre outras, compañías dedicadas á subministración de electricidade, auga e gas; telecomunicacións, entidades financeiras, aseguradoras, grandes superficies, transportes, axencias de viaxe...) de facilitarlles un medio de interlocución telemática aos usuarios dos seus servizos que contén con certificados recoñecidos de sinatura electrónica.

Finalmente, o artigo 3 ten por finalidade establecer unha regulación mínima das poxas electrónicas entre empresarios (B2B) co fin de definir un marco xurídico que dote a esta técnica de compra da necesaria transparencia e seguridade xurídica.

O capítulo II da Lei engloba as modificacións lexislativas que se estimaron necesarias para promover o impulso da sociedade da información e das comunicacións electrónicas.

Estas modificacións afectan principalmente á Lei 34/2002, do 11 de xullo, de servizos da sociedade da información e de comercio electrónico e á Lei 59/2003, do 19 de decembro, de sinatura electrónica, aínda que se inclúen tamén modificacións de menor entidade da Lei 32/2003, do 3 de novembro, xeral de telecomunicacións, modifícase a Lei 7/1996, do 15 de xaneiro, de ordenación do comercio retalista para incluír un novo tipo de infracción que apoie o disposto no artigo 2 da presente lei; introdúcese unha serie de cambios na Lei 11/1998, de 24 de abril, xeral de telecomunicacións e introdúcese, así mesmo, modificacións na Lei de propiedade intelectual.

O artigo 4 da lei inclúe as diferentes modificacións necesarias no vixente texto da Lei 34/2002, do 11 de xullo, de servizos da sociedade da información e de comercio electrónico (LSSI).



Estas modificacións teñen como finalidade, en primeiro lugar, revisar ou eliminar obrigas excesivas ou innecesarias e, en segundo lugar, flexibilizar as obrigas referidas ás comunicacións comerciais e á contratación electrónica a fin de, entre outras razóns, adecuar a súa aplicación ao uso de dispositivos móbiles

O artigo 5 da Lei contempla as modificacións necesarias no articulado da Lei 59/2003, do 19 de decembro, de sinatura electrónica.

Estas modificacións teñen por obxecto clarificar as regras de valoración da sinatura electrónica en xuízo e flexibilizar a obriga dos prestadores de servizos de certificación de comprobaren os datos inscritos en rexistros públicos a fin de eliminar cargas excesivas.

O primeiro aspecto que se revisa do artigo 3 da Lei de sinatura electrónica é a definición de «documento electrónico», que se modifica para axeitala en maior medida aos conceptos utilizados noutras normas españolas de carácter xeral e nos países do noso contorno.

En segundo lugar, aclárase a redacción do apartado 8 do artigo 3, especificando que o que debe comprobarse, en caso de impugnarse en xuízo unha sinatura electrónica recoñecida, é se concorren os elementos constitutivos do devandito tipo de sinatura electrónica; é dicir, que se trata dunha sinatura electrónica avanzada baseada nun certificado recoñecido, que cumpre con todos os requisitos e condicións establecidos nesta Lei para este tipo de certificados electrónicos, e que a sinatura se xerou mediante un dispositivo seguro de creación de sinatura electrónica.

O artigo 6 inclúe un novo tipo de infracción no artigo 64 da Lei 7/1996, do 15 de xaneiro, de ordenación do comercio retalista, con obxecto de apoiar a nova obriga de dispoñer dun medio de interlocución

electrónica para a prestación de servizos ao público de especial transcendencia económica establecida no artigo 2 da presente Lei.

O artigo 7 da lei, introduce unha serie de modificacións na Lei 32/2003, do 3 de novembro, xeral de Telecomunicacións.

Co fin de reforzar os dereitos dos usuarios fronte aos provedores de redes e servizos de comunicacións electrónicas, modifícanse os artigos 53 e 54 da Lei xeral de telecomunicacións mediante a tipificación como infracción administrativa do incumprimento por parte dos operadores dos dereitos dos consumidores e usuarios no ámbito das telecomunicacións.

Así mesmo, restabléceselles a exención da antiga taxa por reserva de uso especial do espectro a radioaficionados e usuarios da Banda Cidadá CB-27, que figuraba na Lei 11/1998, do 24 de abril, xeral de telecomunicacións, para aqueles usuarios que á data de cobro cumprisen os 65 anos de idade.

O artigo 8 establece un novo réxime aplicable ás tarifas polas tarefas de asignación, renovación e outras operacións rexistradas pola entidade pública empresarial Rede.es en exercicio da súa función de Autoridade de Asignación dos nomes de dominio de Internet baixo o código de país correspondente a España, que pasarán a ter a consideración de prezo público. Con iso, permíteselle á entidade pública empresarial Rede.es comercializar os nomes de dominio «.es» nas mesmas condicións nas que se comercializan o resto de nomes de dominio xenéricos e territoriais.

## **8.2.- FACTURA ELECTRÓNICA**

Con carácter xeral pódese definir a factura como un documento que reflicte a entrega dun produto ou a provisión dun servizo, xunto á data de cobro, ademais de indicar a cantidade que se paga como contraprestación.

Na factura atópanse os datos do expedidor e do destinatario, o detalle dos produtos e servizos fornecidos, os prezos unitarios, os prezos totais, os descontos e os impostos.

A facturación electrónica consiste na transmisión das facturas ou documentos análogos entre emisor e receptor por medios electrónicos (ficheiros informáticos) e telemáticos (dun ordenador a outro), asinados dixitalmente con certificados recoñecidos (ou cualificados), coa mesma validez legal que as facturas emitidas en papel.

Se buscamos unha definición específica, podemos recorrer ao artigo 1 da Lei 56/2007: «A factura electrónica é un documento electrónico que cumpre cos requisitos legal e regulamentariamente esixibles ás facturas e que, ademais, garante a autenticidade da súa orixe e a integridade do seu contido».

Aínda que existen varios mecanismos para garantir a autenticidade da orixe, a integridade do contido e a lexibilidade dunha factura, xa sexa en papel ou en formato electrónico, desde o momento da súa expedición ata o final do período de conservación da factura, no caso da factura electrónica, o uso da sinatura electrónica é o máis xeneralizado en España.

Neste sentido, no texto consensuado da futura modificación da Directiva 112/2006, recóllese, no que se refire ao seu artigo 233:

*1. Garantirase a autenticidade da orixe, a integridade do contido e a lexibilidade dunha factura, xa sexa en papel ou en formato electrónico, desde o momento da súa expedición ata o final do período de conservación da factura. Cada suxeito pasivo determinará o modo de garantir a autenticidade da orixe, a integridade do contido e a lexibilidade das facturas. Poderá realizarse mediante controis de xestión que creen un*

*vínculo fiable de auditoría entre a factura e a entrega de bens ou a prestación de servizos.*

*Entenderase por «autenticidade da orixe», a garantía da identidade do provedor de bens ou prestador de servizos ou do emisor da factura.*

*Por «integridade do contido» entenderase que o contido requirido consonte o disposto na presente Directiva non foi modificado.*

*2. Ademais dos tipos de control da xestión contemplados polo segundo parágrafo do apartado 1, outros exemplos de tecnoloxías que garanten a autenticidade da orixe e a integridade do contido dunha factura electrónica son:*

- A sinatura electrónica avanzada no sentido do punto 2 do artigo 2 da Directiva 1999/93/CE do Parlamento Europeo e do Consello, do 13 de decembro de 1999, pola que se establece un marco comunitario para a sinatura electrónica, baseada nun certificado recoñecido e creada mediante un dispositivo seguro de creación de sinatura, no sentido dos puntos 6 e 10 da Directiva 1999/93/CE.*

- O intercambio electrónico de datos (IED), tal como se define no artigo 2 da Recomendación 1994/820/CE da Comisión, do 19 de outubro de 1994, relativa aos aspectos xurídicos do intercambio electrónico de datos, se o acordo relativo ao intercambio contempla o uso de procedementos que garantan a autenticidade da orixe e a integridade dos datos.*

Isto significa que, tras o período de transposición da Directiva (1 de xaneiro do 2013), a lexislación española reflectirá a posibilidade de que se poidan enviar facturas electrónicas entre empresas sen ningún requisito formal, aínda que probablemente se manteñan os mesmos requisitos que existen na actualidade cando o destinatario sexa unha administración pública.

En España, a adopción da sinatura electrónica como mecanismo xeneralizado para garantir a autenticidade e integridade das facturas electrónicas viuse favorecido pola extensión do DNI electrónico e a ampla dispoñibilidade de certificados electrónicos de múltiples prestadores de

servizos de certificación, así como pola dispoñibilidade de software gratuíto que permite a xeración e sinatura electrónica das facturas electrónicas que se envían, así como a súa verificación no caso da recepción de facturas.

O proceso de facturación é un proceso importante para calquera empresa e culmina o proceso de compra e venda. Aínda que, tradicionalmente, a relación entre empresas se baseou no intercambio de documentos en papel, isto entraña o emprego de grandes cantidades de recursos e a realización de moitas tarefas de forma manual. Nun contexto de universalización de Internet, cada vez máis as empresas estudan a optimización dos seus procesos para gañar eficiencia e aforrar custos.

E por iso avanza a adopción da facturación electrónica, que en España está regulada no Regulamento de facturación publicado en Real decreto 1496/2003 e modificado polo Real decreto 87/2005.

As denominacións factura electrónica, factura telemática e factura dixital son equivalentes, aínda que a denominación utilizada polo xera na normativa é remisión electrónica ou remisión por medios electrónicos de factura. Frecuentemente distínguese coa denominación factura dixital a modalidade de factura electrónica que utiliza a sinatura dixital para garantir a autenticidade e integridade da factura.

As facturas electrónicas pódense emitir en diferentes formatos (EDIFACT, XML, PDF, html, doc, xls, gif, jpeg ou txt, entre outros) sempre que se respecte o contido legal esixible a calquera factura e que se cumpran os requisitos de autenticidade e integridade; por exemplo, coa incorporación da sinatura electrónica recoñecida (qualified Electronic signature, en inglés).

Así e todo, tras a publicación da Orde PRE/2971/2007 definiuse o uso obrigatorio do formato XML de factura cando o destinatario sexa unha

administración da AXE (Administración Xeral do Estado) e os seus organismos públicos.

### **8.3. LEI DE SINATURA ELECTRÓNICA**

#### **8.3.1 Introducción**

Sen esquecer as referencias que sobre o tema de utilización de medios electrónicos establecía a Lei 30/92 do 20 de novembro (LRJPAC) é o Real decreto-lei 14/1999, do 17 de setembro, sobre sinatura electrónica, a norma pioneira á hora de fomentar a rápida incorporación das novas tecnoloxías de seguridade das comunicacións electrónicas á actividade das empresas, os cidadáns e as administracións públicas; actualmente, a Lei 59/2003 de sinatura electrónica, cuxa última modificación tivo lugar pola Lei 56/2007 de medidas de impulso da sociedade da información.

#### **8.3.2 Estrutura e análise.**

Desde o punto de vista da súa estrutura, a Lei 59/2003 de sinatura electrónica consta de 36 artigos agrupados en seis títulos, 11 disposicións adicionais, dúas disposicións transitorias, unha disposición derogatoria e tres disposicións finais.

O título I contén os principios xerais que delimitan os ámbitos subxectivo e obxectivo de aplicación da lei, os efectos da sinatura electrónica e o réxime de emprego ante as administracións públicas e de acceso á actividade de prestación de servizos de certificación.

O réxime aplicable aos certificados electrónicos contense no título II, que dedica o seu primeiro capítulo a determinar quen pode ser o seu titular e a regular as vicisitudes que afectan á súa vixencia. O capítulo II regula os

certificados recoñecidos e o terceiro o documento nacional de identidade electrónico.

O título III regula a actividade de prestación de servizos de certificación establecendo as obrigas a que están suxeitos os prestadores —distinguindo con nitidez as que soamente afectan aos que expiden certificados recoñecidos— e o réxime de responsabilidade aplicable.

O título IV establece os requisitos que deben reunir os dispositivos de verificación e creación de sinatura electrónica e o procedemento que debe seguirse para obter selos de calidade na actividade de prestación de servizos de certificación.

Os títulos V e VI dedican o seu contido, respectivamente, a fixar os réximes de supervisión e sanción dos prestadores de servizos de certificación.

Por último, pechan o texto as disposicións adicionais —que aluden aos réximes especiais que resultan de aplicación preferente—; as disposicións transitorias —que incorporan seguridade xurídica á actividade despregada ao abeiro da normativa anterior—; a disposición derogatoria e as disposicións finais relativas ao fundamento constitucional, á habilitación para o desenvolvemento regulamentario e á entrada en vigor.

Supón a incorporación ao ordenamento interno da regulación contida na Directiva 1999/93/ CE, do 13 de decembro de 1999, do Parlamento Europeo e do Consello. Esta lei parece ter presente na elaboración do seu contido a Lei modelo para as sinaturas electrónicas da Comisión das Nacións Unidas para o Dereito Mercantil Internacional (CNUDMI/ UNCITRAL), aprobada, xunto á súa Guía, o 5 de xullo de 2001.

Ten como principal finalidade reforzar o marco xurídico existente, incorporando ao seu texto «algunhas novidades respecto do Real Decreto 14/1999, que contribuirán a dinamizar o mercado da prestación de servizos de certificación, conferíndolles seguridade ás comunicacións a través de Internet, e configurando a sinatura electrónica como instrumento capaz de xerar confianza nas transaccións telemáticas, ademais de axilizar o comercio electrónico. Permitirase, en consecuencia, unha comprobación da procedencia e da integridade das mensaxes intercambiadas a través de redes de telecomunicacións, ofrecendo as bases para evitar o repudio, se se adoptan as medidas oportunas baseándose en datos electrónicos»

Constitúe o seu obxecto, conforme dispón o art. 1, tanto a regulación da sinatura electrónica, como elemento de seguridade das comunicacións nos seus diversos aspectos, e a súa eficacia xurídica, como a prestación de servizos de certificación nos seus diversos aspectos (obxectivo: certificados, e subxectivo: prestadores de servizo de certificación).

O apartado 1 do art. 3 da LFE define de forma xeral a sinatura electrónica como «o conxunto de datos en forma electrónica, consignados xunto a outros ou asociados a eles, que poden ser utilizados como medio de identificación do asinante».

É unha definición ampla que pode englobar a todo o conxunto de sinaturas electrónicas, desde aquelas máis complexas, coma a sinatura dixital baseada en sistemas biométricos coma o iris, a propia palma da man, a impresión dactilar, etc.; ata a máis simples, coma un nome ou outro elemento identificativo (por exemplo, a sinatura manual dixitalizada, ou un *password* ou contrasinal), incluído ao final da mensaxe electrónica, ou a existencia dunha pregunta-resposta, e un *pin* de acceso, o que se denomina tecnoloxía de segredo compartido, de tan escasa seguridade que se suscita a cuestión do seu valor probatorio para os efectos de autenticación ou identificación do autor.



Así mesmo, deste concepto amplo e tecnoloxicamente indefinido de sinatura que nos ofrece o citado precepto podemos salientar as seguintes características da sinatura electrónica:

- A sinatura electrónica é un conxunto de datos e non un símbolo, selo ou grafía electrónica que serve para identificar o asinante dunha mensaxe e para acreditar a identificación do mesmo, así como a integridade do contido da mensaxe.
- Trátase dunha técnica para identificar o asinante dun documento electrónico.
- Os datos de sinatura electrónica poden formar parte do documento ou ir asociados funcionalmente con eles ou, o que é o mesmo, poden aparecer como un conxunto independente. O modo concreto en que en cada momento se manifeste a sinatura electrónica dependerá do sistema técnico que se elixa e das aplicacións prácticas que ofrezca cada modalidade.

Define a lei qué se considera documento electrónico: este é a información de calquera natureza en forma electrónica, archivada nun soporte electrónico segundo un formato determinado e susceptible de identificación e tratamento diferenciado.

Para que un documento electrónico teña a natureza de documento público ou de documento administrativo deberá cumprirse, ou ben, estar asinado electronicamente por funcionarios que teñan legalmente atribuída a facultade de dar fe pública, xudicial, notarial ou administrativa, sempre que actúen no ámbito das súas competencias cos requisitos esixidos pola lei en cada caso, ou ben tratarse de documentos expedidos e asinados

electronicamente por funcionarios ou empregados públicos no exercicio das súas funcións públicas, conforme á súa lexislación específica.

Ao lado da sinatura electrónica atópase a sinatura electrónica avanzada, que segundo a lei, artigo 3.2 «A sinatura electrónica avanzada é a sinatura electrónica que permite identificar o asinante e detectar calquera cambio ulterior dos datos asinados, que está vinculada ao asinante de xeito único e aos datos a que se refire e que foi creada por medios que o asinante pode manter baixo o seu exclusivo control».

A lei de sinatura electrónica fronte á regulación contida tanto no RDL 14/99 coma na Directiva, introduce un terceiro tipo de sinatura, de maior calidade e seguridade, como é a sinatura electrónica recoñecida, definida no art. 3.3 como «a sinatura electrónica avanzada baseada nun certificado recoñecido e xerada mediante un dispositivo seguro de creación de sinatura».

Supón, como sinala a Exposición de motivos da lei, «a creación dun concepto novo demandado polo sector, sen que iso implique ningunha modificación dos requisitos substantivos que tanto a Directiva 1999/93/CE como o propio Real decreto lei 14/1999 viñan esixindo».

O art. 24 da LFE, baixo o título «Dispositivo de sinatura electrónica», define os datos de creación de sinatura como «os datos únicos, como códigos ou claves criptográficas privadas, que o asinante utiliza para crear a sinatura electrónica».

Como elemento característico destes establécese que estes deben ser únicos.

Pola súa banda, o art. 25 da LFE, baixo o título «Dispositivos de verificación de sinatura electrónica», define os «datos de verificación de

sinatura» como «os datos, códigos ou claves criptográficas públicas, que se utilizan para verificar a sinatura electrónica».

Xa que logo, baixo o Título «Dispositivos de sinatura electrónica» regúlase como nocións previas, tanto para a aplicación do dispositivo de creación como para o de verificación, os datos de creación e verificación de sinatura, respectivamente, que desde un punto de vista técnico constitúen ademais elementos que posibilitan a creación dunha sinatura ou a súa verificación.

### 8.3.3 Efectos xurídicos da sinatura electrónica

Á validez e eficacia da sinatura electrónica dedícalle a LFE os apartados 4, 8, 9 e 10 do art. 3, que coincide substancialmente co disposto no art. 5 da Directiva comunitaria, e nos que se equipara a sinatura electrónica recoñecida á sinatura manuscrita, se determina as consecuencias da impugnación da autenticidade da sinatura electrónica recoñecida pola outra parte non asinante, se lle recoñece valor xurídico á autonomía da vontade das partes para dotar de eficacia á sinatura electrónica e se especifica a admisibilidade dos datos asinados electronicamente como proba documental en xuízo;

O art. 3.4 da lei establece a regra do equivalente funcional entre a sinatura electrónica recoñecida e a sinatura manuscrita, ao dispoñer que «a sinatura electrónica recoñecida terá respecto dos datos consignados en forma electrónica o mesmo valor que a sinatura manuscrita en relación cos consignados en papel».

En consecuencia, sobre o exposto, para a plena operatividade da regra da equivalencia funcional da sinatura electrónica recoñecida coa sinatura manuscrita, que dispón o art. 3.4 da LFE, nunha interpretación conxunta co art. 3.3 desta mesma lei, é necesario o cumprimento dos seguintes requisitos:

1.º Debe tratarse dunha sinatura electrónica avanzada (art. 3.2 da LFE).

2.º A devandita sinatura electrónica avanzada debe estar baseada nun certificado recoñecido, é dicir, aquel que cumpre os requisitos dos arts. 11, 12 e 13 da LFE, e que fose expedido por un prestador de servizos de certificación que cumpra cos requisitos previstos no art. 20 da LFE.

3.º A devandita sinatura electrónica avanzada, ademais, debeu ser producida por un dispositivo seguro de creación de sinatura que cumpra cos requisitos do apartado 3 do art. 24 da LFE.

Regula tamén a lei a figura do DNI electrónico: este é o documento nacional de identidade que acredita electronicamente a identidade persoal do seu titular e permite a sinatura electrónica de documentos; imponse a obriga de que todas as persoas físicas ou xurídicas, públicas ou privadas, recoñecerán a eficacia do documento nacional de identidade electrónico para acreditar a identidade e os demais datos persoais do titular que consten no mesmo, e para acreditar a identidade do asinante e a integridade dos documentos asinados cos dispositivos de sinatura electrónica nel incluídos.

A lei regula a figura dos prestadores de servizos de certificación, sendo estes «a persoa física ou xurídica que expide certificados electrónicos ou presta outros servizos en relación coa sinatura electrónica».

Para a expedición de certificados electrónicos ao público, os prestadores de servizos de certificación unicamente poderán solicitar datos persoais directamente dos asinantes ou previo consentimento expreso destes, debendo cumprir, xa que logo, o disposto na Lei orgánica 15/1999, do 13 de decembro, de protección de datos de carácter persoal e nas súas normas de desenvolvemento.

Os prestadores de servizos de certificación que expidan certificados electrónicos deberán cumprir as seguintes obrigas:

- Non almacenar nin copiar os datos de creación de sinatura da persoa á que prestasen os seus servizos.
- Proporcionarlle ao solicitante antes da expedición do certificado a seguinte información mínima, que deberá transmitirse de forma gratuíta, por escrito ou por vía electrónica:
  - As obrigas do asinante, a forma en que deben custodiarse os datos de creación de sinatura, o procedemento que cumpra seguir para comunicar a perda ou posible utilización indebida dos devanditos datos e determinados dispositivos de creación e de verificación de sinatura electrónica que sexan compatibles cos datos de sinatura e co certificado expedido.
  - Os mecanismos para garantir a fiabilidade da sinatura electrónica dun documento ao longo do tempo.
  - O método utilizado polo prestador para comprobar a identidade do asinante ou outros datos que figuren no certificado.
  - As condicións precisas de utilización do certificado, os seus posibles límites de uso e a forma en que o prestador garante a súa responsabilidade patrimonial.
  - As certificacións que obtivese, de ser o caso, o prestador de servizos de certificación e os procedementos aplicables para a resolución extraxudicial dos conflitos que puideren xurdir polo exercicio da súa actividade.

- As demais informacións contidas na declaración de prácticas de certificación.
- A información citada anteriormente que sexa relevante para terceiros afectados polos certificados deberá estar dispoñible a instancia destes.
- Manter un directorio actualizado de certificados no que se indicarán os certificados expedidos e se están vixentes, ou se a súa vixencia foi suspendida ou extinguida. A integridade do directorio débese protexer mediante a utilización dos mecanismos de seguridade adecuados.
- Garantir a dispoñibilidade dun servizo de consulta sobre a vixencia dos certificados rápido e seguro.

Regula a lei aspectos relacionados coa supervisión e control da actividade dos prestadores de servizos e, así, o Ministerio de Ciencia e Tecnoloxía controlará o cumprimento polos prestadores de servizos de certificación que expidan ao público certificados electrónicos das obrigas establecidas nesta lei e nas súas disposicións de desenvolvemento. Así mesmo, supervisará o funcionamento do sistema e dos organismos de certificación de dispositivos seguros de creación de sinatura electrónica.

O Ministerio de Ciencia e Tecnoloxía realizará as actuacións inspectoras que sexan precisas para o exercicio da súa función de control; os funcionarios adscritos ao Ministerio de Ciencia e Tecnoloxía que realicen a inspección á que se refire o apartado anterior terán a consideración de autoridade pública no desempeño dos seus cometidos.

Os prestadores de servizos de certificación, a entidade independente de acreditación e os organismos de certificación teñen a obriga de facilitarlle ao Ministerio de Ciencia e Tecnoloxía toda a información e colaboración precisas para o exercicio das súas funcións.

## **8.4.- LEI DE SERVIZOS DE SOCIEDADE DE INFORMACIÓN E COMERCIO ELECTRÓNICO**

### 8.4.1 Introducción.

A Lei 34/2002, do 22 de xullo, ten como obxecto a incorporación ao ordenamento xurídico español da Directiva 2000/31/CE, do Parlamento Europeo e do Consello, do 8 de xuño, relativa a determinados aspectos dos servizos da sociedade da información; en particular, o comercio electrónico no mercado Interior (Directiva sobre o comercio electrónico). Así mesmo, incorpora parcialmente a Directiva 98/27/CE, do Parlamento Europeo e do Consello, do 19 de maio —relativa ás accións de cesación en materia de protección dos intereses dos consumidores— ao regular, de conformidade co establecido nela, unha acción de cesación contra as condutas que contraveñan o disposto nesta lei.

O que a Directiva 2000/31/CE denomina sociedade da información vén determinado pola extraordinaria expansión das redes de telecomunicacións e, en especial, de Internet como vehículo de transmisión e intercambio de todo tipo de información. A súa incorporación á vida económica e social ofrece innumerables vantaxes, como a mellora da eficiencia empresarial, o incremento das posibilidades de elección dos usuarios e a aparición de novas fontes de emprego. Pero a implantación de Internet e as novas tecnoloxías tropeza con algunhas incertezas xurídicas, que é preciso aclarar co establecemento dun marco xurídico adecuado, que

xere en todos os actores intervinientes a confianza necesaria para o emprego deste novo medio.

É obxecto da lei a regulación do réxime xurídico dos servizos da sociedade da información e da contratación por vía electrónica —no referente ás obrigas dos prestadores de servizos, incluídos os que actúen como intermediarios na transmisión de contidos polas redes de telecomunicacións—; as comunicacións comerciais por vía electrónica; a información previa e posterior á celebración de contratos electrónicos; as condicións relativas á súa validez e eficacia, e o réxime sancionador aplicable aos prestadores de servizos da sociedade da información.

#### 8.4.2 Ámbito de aplicación

Aplicaráselles aos prestadores de servizos da sociedade da información establecidos noutro Estado membro da Unión Europea ou do Espazo Económico Europeo cando o destinatario dos servizos radique en España e os servizos afecten ás materias seguintes:

- a. Dereitos de propiedade intelectual ou industrial.
- b. Emisión de publicidade por institucións de investimento colectivo.
- c. Actividade de seguro directo realizada en réxime de dereito de establecemento ou en réxime de libre prestación de servizos.
- d. Obrigas nadas dos contratos celebrados por persoas físicas que teñan a condición de consumidores.
- e. Réxime de elección polas partes contratantes da lexislación aplicable ao seu contrato.
- f. Licitude das comunicacións comerciais por correo electrónico ou outro medio de comunicación electrónica equivalente non solicitadas.

A prestación de servizos da sociedade da información non estará suxeita a autorización previa.





No caso de que un determinado servizo da sociedade da información atente ou poida atentar contra os principios que se expresan deseguido, os órganos competentes para a súa protección, en exercicio das funcións que teñan legalmente atribuídas, poderán adoptar as medidas necesarias para que se interrompa a súa prestación ou para retirar os datos que os vulneran.

#### 8.4.3 Principios e requisitos de actuación

Os principios de aplicación son os seguintes:

- a. A salvagarda da orde pública, a investigación penal, a seguridade pública e a defensa nacional.
- b. A protección da saúde pública ou das persoas físicas ou xurídicas que teñan a condición de consumidores ou usuarios, mesmo cando actúen como investidores.
- c. O respecto á dignidade da persoa e ao principio de non discriminación por motivos de raza, sexo, relixión, opinión, nacionalidade, discapacidade ou calquera outra circunstancia persoal ou social, e
- d. A protección da mocidade e da infancia.
- e. A salvagarda dos dereitos de propiedade intelectual.

O prestador de servizos da sociedade da información estará obrigado a dispoñer dos medios que lles permitan, tanto aos destinatarios do servizo como aos órganos competentes, accederen por medios electrónicos, de forma permanente, fácil, directa e gratuíta, á seguinte información:

- a. O seu nome ou denominación social; a súa residencia ou domicilio ou, na súa ausencia, o enderezo dun dos seus establecementos permanentes en España; o seu enderezo de correo electrónico e calquera outro dato que permita establecer con el unha comunicación directa e efectiva.

b. Os datos da súa inscrición no Rexistro Mercantil onde, se é o caso, se atopen inscritos, ou daqueloutro rexistro público onde o estivesen para a adquisición de personalidade xurídica ou unicamente para os efectos de publicidade.

c. No caso de que a súa actividade estivese suxeita a un réxime de autorización administrativa previa, os datos relativos á devandita autorización e os identificativos do órgano competente encargado da súa supervisión.

d. Se exerce unha profesión regulada deberá indicar:

1. Os datos do Colexio profesional ao que, de ser o caso, pertenza, e número de colexiado.

2. O título académico oficial ou profesional co que conte.

3. O Estado da Unión Europea ou do Espazo Económico Europeo no que se expediu o devandito título e, de ser o caso, a correspondente homologación ou recoñecemento.

4. As normas profesionais aplicables ao exercicio da súa profesión e os medios a través dos cales se poidan coñecer, incluídos os electrónicos.

e. O número de identificación fiscal que lle corresponda.

f. Cando o servizo da sociedade da información faga referencia a prezos, débese facilitar información clara e exacta sobre o prezo do produto ou servizo, indicando se inclúe ou non os impostos aplicables e, se procede, sobre os gastos de envío ou, se é o caso, daquilo que dispoñan as normas das Comunidades Autónomas con competencias na materia.

g. Os códigos de conduta aos que, de ser o caso, estea adherido e a maneira de consultalos electronicamente.

Os prestadores de servizos da sociedade da información están suxeitos á responsabilidade civil, penal e administrativa establecida con carácter xeral no ordenamento xurídico, sen prexuízo do disposto nesta lei.

Os prestadores de servizos da sociedade da información que faciliten ligazóns a outros contidos ou inclúan nos seus directorios ou instrumentos

de busca de contidos non serán responsables pola información á que dirixan aos destinatarios dos seus servizos, sempre que:

- a. Non teñan coñecemento efectivo de que a actividade ou a información á que remiten ou recomendan é ilícita ou de que lesiona bens ou dereitos dun terceiro susceptibles de indemnización, ou
- b. Se o teñen, actúen con dilixencia para suprimir ou inutilizar a ligazón correspondente.

As administracións públicas impulsarán, a través da coordinación e o asesoramento, a elaboración e aplicación de códigos de conduta voluntarios, por parte das corporacións, asociacións ou organizacións comerciais, profesionais e de consumidores, nas materias reguladas nesta lei. A Administración Xeral do Estado fomentará, en especial, a elaboración de códigos de conduta de ámbito comunitario ou internacional.

Os códigos de conduta poderán tratar, en particular, sobre os procedementos para a detección e retirada de contidos ilícitos e a protección dos destinatarios fronte ao envío por vía electrónica de comunicacións comerciais non solicitadas, así como sobre os procedementos extraxudiciais para a resolución dos conflitos que xurdan pola prestación dos servizos da sociedade da información.

Os contratos celebrados por vía electrónica producirán todos os efectos previstos polo ordenamento xurídico cando concorran o consentimento e os demais requisitos necesarios para a súa validez.

A proba da celebración dun contrato por vía electrónica e a das obrigas que teñen a súa orixe nel suxéitase ás regras xerais do ordenamento xurídico.

Cando os contratos celebrados por vía electrónica estean asinados electronicamente ateranse ao establecido no artigo 3 da Lei 59/2003, do 19 de decembro, de sinatura electrónica.

Os contratos celebrados por vía electrónica nos que interveña como parte un consumidor presumiranse celebrados no lugar en que este teña a súa residencia habitual.

O prestador e o destinatario de servizos da sociedade da información poderán someter os seus conflitos aos arbitraxes previstos na lexislación de arbitraje e de defensa dos consumidores e usuarios, e aos procedementos de resolución extraxudicial de conflitos que se instauren por medio de códigos de conduta ou outros instrumentos de autorregulación.

### **8.5.-ACCESIBILIDADE**

A disposición adicional quinta da Lei de servizos da sociedade da información e do comercio electrónico (Lei 34/2002, do 11 de xullo) establece unha norma relativa á accesibilidade para as persoas con discapacidade e de idade avanzada á información proporcionada por medios electrónicos e establece:

*As administracións públicas adoptarán as medidas necesarias para que a información dispoñible nas súas respectivas páxinas de internet poida ser accesible a persoas con discapacidade e de idade avanzada, de acordo cos criterios de accesibilidade ao contido xeralmente recoñecidos, antes do 31 de decembro do 2005.*

*A partir do 31 de decembro do 2008, as páxinas de internet das administracións públicas satisfarán, como mínimo, o nivel medio dos criterios de accesibilidade ao contido xeralmente recoñecidos. Excepcionalmente, esta obriga non será aplicable cando unha funcionalidade ou servizo non dispoña dunha solución tecnolóxica que permita a súa accesibilidade.*

*As administracións públicas esixirán que tanto as páxinas de internet cuxo deseño ou mantemento financien total ou parcialmente como as*

*páxinas de internet de entidades e empresas que se encarguen de xestionar servizos públicos apliquen os criterios de accesibilidade antes mencionados. En particular, será obrigatorio o expresado neste apartado para as páxinas de internet e os seus contidos dos centros públicos educativos, de formación e universitarios, así como dos centros privados que obteñan financiamento público.*

*As páxinas de internet das administracións públicas deberanlle ofrecer ao usuario información sobre o seu nivel de accesibilidade e facilitar un sistema de contacto para que poidan transmitir as dificultades de acceso ao contido das páxinas de internet ou formular calquera queixa, consulta ou suxestión de mellora.*

*Igualmente, promoverase a adopción de normas de accesibilidade polos prestadores de servizos e os fabricantes de equipos e software para facilitar o acceso das persoas con discapacidade ou de idade avanzada aos contidos dixitais.*

*As administracións públicas promoverán medidas de sensibilización, educación e formación sobre accesibilidade con obxecto de promover que os titulares doutras páxinas de internet incorporen progresivamente os criterios de accesibilidade.*

*Os incumprimentos das obrigas de accesibilidade establecidas nesta Disposición adicional estarán sometidos ao réxime de infraccións e sancións vixente en materia de igualdade de oportunidades, non discriminación e accesibilidade universal das persoas con discapacidade.*

*As páxinas de internet das empresas que presten servizos ao público en xeral de especial transcendencia económica, sometidas á obrigaón establecida no artigo 2 da Lei 56/2007, de medidas de impulso da sociedade da información, deberán satisfacer a partir do 31 de decembro do 2008, como mínimo, o nivel medio dos criterios de accesibilidade ao contido xeralmente recoñecidos. Excepcionalmente, esta obriga non será aplicable cando unha funcionalidade ou servizo non dispoña dunha solución tecnolóxica que permita a súa accesibilidade.*

O Deseño «Web Accesible» pretende establecer as técnicas e mecanismos para permitir que un sitio Web poida ser utilizado por calquera persoa, independentemente da súa discapacidade.

En decembro do 2007 aprobouse a Lei 56/2007, de medidas de impulso da sociedade da información (BOE 29-12-2008). Por unha banda, esta lei indica claramente que a accesibilidade das páxinas web da Administración Pública está suxeita ao réxime de infraccións e sancións (Lei 49/2007). Doutra banda, a obriga de facer sitios web accesibles amplíase ao sector privado, en concreto ás empresas que lle presten servizos ao público en xeral de especial transcendencia económica.

En decembro do 2007 aprobouse a Lei 49/2007, pola que se establece o réxime de infraccións e sancións en materia de igualdade de oportunidades, non discriminación e accesibilidade universal das persoas con discapacidade (BOE 27-12-2007). Nesta lei defínense sancións que poden chegar ata 1.000.000 de euros.

En novembro do 2007 aprobouse o Real decreto 1494/2007 polo que se aproba o Regulamento sobre as condicións básicas para o acceso das persoas con discapacidade ás tecnoloxías, produtos e servizos relacionados coa sociedade da información e medios de comunicación social (BOE 21-11-2007). Este Regulamento obriga as administracións públicas a que as súas páxinas web sexan accesibles de acordo co nivel 2 da norma española UNE 139803:2004 antes do 2009.

A Lei IONDAU (Lei 51/2003, do 2 de decembro, de igualdade de oportunidades, non discriminación e accesibilidade universal das persoas con discapacidade. BOE 3-12-2003), fixa varias fases: 1.º a primeiros do 2006 o Goberno deberá establecer os criterios básicos de accesibilidade para as Tecnoloxías da Sociedade da Información; 2.º no 2010 todos os novos produtos e servizos da Sociedade da Información deberán ser

accesibles; 3.º no 2014 todos os produtos e servizos da Sociedade da Información deberán ser accesibles.

A Lei SSICE (Lei 34/2002, do 11 de xullo, de servizos da sociedade da información e de comercio electrónico. BOE 12-7-2002), na súa disposición adicional 5.ª (que fai referencia á accesibilidade para as persoas con discapacidade e de idade avanzada á información proporcionada por medios electrónicos), obrigaba as administracións públicas a teren as súas Webs accesibles para todos antes do 2006.

No ámbito europeo existen numerosas normas e iniciativas neste sentido (como as iniciativas eEurope (an Information Society for All) 2002 e 2005 e a estratexia i2010), posto que se fala dun 20% da poboación europea afectada por algún tipo de discapacidade.

## **8.6.- DECRETO 3/2010 DO 8 DE XANEIRO POLO QUE SE REGULA O SISTEMA DE FACTURACIÓN ELECTRÓNICA DA XUNTA DE GALICIA**

### **8.6.1 Introducción**

A implantación dos medios electrónicos no ámbito da facturación e a contratación pública enmárcase nas políticas corporativas comúns do Goberno galego para o desenvolvemento da administración electrónica e integrárase harmónica e complementariamente co resto das aplicacións comúns para toda a Xunta de Galicia.

O Decreto regula, por unha banda, as liñas xerais de emprego dos medios electrónicos, informáticos e telemáticos nos procedementos de contratación e establece as condicións de utilización dos citados medios no marco do desenvolvemento da administración electrónica da Xunta de Galicia. Así mesmo, configura as bases dun sistema que se asenta sobre varios eixes que se complementan estruturando todas as relacións telemáticas entre os actores que interveñen nos procesos.

Así, polo que se refire ao servizos aos licitadores, ordena e estrutura novas canles de información e participación do empresariado nos procesos de contratación creando a Plataforma de Contratos Públicos de Galicia e un Portal de Contratación Pública da Comunidade Autónoma que potenciará os servizos en liña existentes e incorporará prestacións relacionadas coa licitación electrónica. Doutra banda, en canto aos servizos entre administracións prevense mecanismos de interoperatividade que, en primeiro lugar, reforzan a accesibilidade ás plataformas e sistemas e aplicacións existentes ou futuras e, en segundo lugar, facilitan a cooperación e colaboración intra e interadministrativas para os efectos de tráfico de información.

#### 8.6.2 Estrutura

Respecto da estrutura, o Decreto consta de 18 artigos, agrupados en 5 capítulos.

O capítulo I regula o obxecto do Decreto e o seu ámbito de aplicación.

O capítulo II regula a Plataforma de Contratos Públicos de Galicia, creada ao abeiro do disposto no artigo 309.5 da Lei 30/2007, do 30 de outubro, como servizo de información das licitacións do sector público galego a través de internet.

O capítulo III regula o Sistema de Licitación Electrónica que permitirá a presentación de ofertas e proposicións por vía telemática.

O capítulo IV regula determinados sistemas de tramitación e xestión electrónica de importante incidencia na contratación e a facturación electrónica.

Finalmente, no capítulo V créase un Portal de Contratación Pública da Comunidade Autónoma como punto central de acceso e entrada para os interesados a todas as aplicacións e servizos que, en materia de



contratación pública e por vía electrónica, se poidan realizar a través de internet.

O Decreto modifica tamén, na disposición final, o Decreto 262/2001, do 20 setembro, polo que se refunde a normativa reguladora do Rexistro Xeral de Contratistas da Comunidade Autónoma de Galicia ao introducir a tramitación por medios electrónicos, informáticos e telemáticos (EIT) dos procesos de alta, modificación e baixa do rexistro e un sistema de notificacións electrónicas coas empresas rexistradas.

Autor:

Alfonso García Magariños

Director Asesoría Xurídica Municipal Concello da Coruña

# **9. NORMATIVA NO ÁMBITO DA PROPIEDAD INTELECTUAL. A PROTECCIÓN XURÍDICA DOS PROGRAMAS DE ORDENADOR. TIPOS DE LICENZAS. SOFTWARE DE FONTES ABERTAS (FLOSS).**

## **Tema 9.- Normativa no ámbito da propiedade intelectual. A protección xurídica dos programas de ordenador. Tipos de licenzas: Software de fontes abertas ( FLOSS )**

### **INDICE**

#### 9.1 Normativa no ámbito da propiedade intelectual.

##### 9.1.1 Estatal

##### 9.1.2 Comunitaria

##### 9.1.3 Internacional

#### 9.2 Protección xurídica programas ordenador

##### 9.2.1 Introducción

##### 9.2.2 Normativa Estatal

#### 9.3 Tipos de licenzas

#### 9.4 Software de fontes abertas FLOSS

### **9.1- NORMATIVA NO ÁMBITO DA PROPIEDAD INTELECTUAL.**

Segundo a Organización Mundial da Propiedade Intelectual, a propiedade intelectual (P.I.) ten que ver coas creacións da mente: as invencións, as obras literarias e artísticas, os símbolos, os nomes, as imaxes e os debuxos e modelos utilizados no comercio.

A propiedade intelectual divídese en dúas categorías: a propiedade industrial, que inclúe as invencións, patentes, marcas, debuxos e modelos industriais e indicacións xeográficas de procedencia; e o dereito de autor, que abarca as obras literarias e artísticas, tales como as novelas, os poemas e as obras de teatro, as películas, as obras musicais, as obras de arte, tales como os debuxos, pinturas, fotografías e esculturas, e os deseños arquitectónicos. Os dereitos relacionados co dereito de autor son os dereitos dos artistas intérpretes e executantes sobre as súas interpretacións e execucións, os dereitos dos produtores de fonogramas sobre as súas gravacións e os dereitos dos organismos de radiodifusión sobre os seus programas de radio e de televisión

Polo que respecta aos dereitos que conforman a propiedade intelectual distínguense os dereitos morais e os dereitos patrimoniais:

Dereitos morais:

Fronte aos sistemas de corte anglosaxón, a lexislación española é claramente defensora dos dereitos morais, recoñecidos para os autores e para os artistas intérpretes ou executantes. Estes dereitos son irrenunciáveis e inalienables, acompañan ao autor ou ao artista intérprete ou executante durante toda a súa vida e aos seus herdeiros ou habentes-causa ao falecemento daqueles. Entre eles destaca o dereito ao recoñecemento da condición de autor da obra ou do recoñecemento do nome do artista sobre as súas interpretacións ou execucións, e o de esixir o

respecto á integridade da obra ou actuación e a non alteración das mesmas.

Dereitos de carácter patrimonial:

Hai que distinguir entre:

Dereitos relacionados coa explotación da obra ou prestación protexida que, á súa vez, se subdividen en dereitos exclusivos e en dereitos de remuneración:

1.-Os dereitos exclusivos son aqueles que permiten ao seu titular autorizar ou prohibir os actos de explotación da súa obra ou prestación protexida polo usuario, e a esixir deste unha retribución a cambio da autorización que lle conceda.

2.-Os dereitos de remuneración, a diferenza dos dereitos exclusivos, non facultan ao seu titular a autorizar ou prohibir os actos de explotación da súa obra ou prestación protexida polo usuario, aínda que si obrigan a este ao pagamento dunha cantidade de diñeiro polos actos de explotación que realice, cantidade esta que é determinada, ben pola lei ou na súa falta polas tarifas xerais das entidades de xestión.

3.-Dereitos compensatorios, como o dereito por copia privada que compensa os dereitos de propiedade intelectual deixados de percibir por razón das reproducións das obras ou prestacións protexidas para uso exclusivamente privado do copista

### **9.1.1 Normativa Estatal**

A propiedade intelectual é o conxunto de dereitos que corresponden aos autores e a outros titulares (artistas, produtores, organismos de radiodifusión...) respecto das obras e prestacións froito da súa creación.

A propiedade intelectual, tal e como establece o Código Civil nos seus artigos 428 e 429, forma parte das chamadas propiedades especiais, e vén constituír unha forma especial de exercer o dereito de propiedade sobre determinados obxectos xurídicos que, pola súa calidade, especializan o dominio.

Como propiedade especial, o Código Civil remite a súa regulación a unha lei especial, e declara a aplicación supletoria das regras xerais establecidas no mesmo sobre a propiedade para o non especificamente previsto na devandita lei especial. Esta lei é a Lei de Propiedade Intelectual (LPI), cuxo Texto Refundido foi aprobado polo Real Decreto Legislativo 1/1996, de 12 de abril.

O citado Texto foi obxecto de sucesivas modificacións entre as que debemos destacar a operada pola lei 5/1998, de 6 de marzo, e a lei 23/2006 de 7 de xullo, (responde esta á necesidade de incorporar ao dereito español unha das últimas directivas aprobadas en materia de propiedade intelectual, a Directiva 2001/29/CE do Parlamento Europeo e do Consello, do 22 de maio de 2001, relativa á harmonización de determinados aspectos dos dereitos de autor e dereitos afíns aos dereitos de autor na sociedade da información, coa que a Unión Europea, á súa vez, quixo cumprir os Tratados da Organización Mundial da Propiedade Intelectual (OMPI) de 1996 sobre Dereito de Autor e sobre Interpretación ou Execución e Fonogramas )

Cabe tamén destacar a lei 19/2006, do 5 de xuño, pola que se amplían os medios de tutela dos dereitos de propiedade intelectual e industrial e se establecen normas procesais para facilitar a aplicación de diversos regulamentos comunitarios.

### **9.1.2 Normativa comunitaria:**

1.-Directiva 92/100/CEE, de 19 de novembro de 1992, sobre dereitos de aluguer e préstamo e outros dereitos afíns aos dereitos de autor no ámbito da propiedade intelectual. Esta Directiva, entre outros aspectos, recoñece o dereito de autorizar ou prohibir o aluguer e préstamo de orixinais e copias de obras protexidas.

2.-Directiva 93/98/CEE, de 29 de outubro de 1993, relativa á harmonización do prazo de protección do dereito de autor e de determinados dereitos afíns. Nesta Directiva harmonízase o prazo de protección do dereito de autor, fixándoo nun período de setenta anos trala morte do autor ou desde o momento da primeira difusión lícita entre o público, e polo que se refire aos dereitos afíns, en cincuenta anos desde que se produce o feito xerador.

3.-Directiva 96/9/CE, de 11 de marzo de 1996, sobre a protección xurídica das bases de datos. Recoñece un dereito de autor ao creador da estrutura da base de datos, e un dereito *sui generis* ao fabricante da mesma, entendendo por tal a persoa física ou xurídica que realizou un investimento substancial para a fabricación das bases de datos.

4.-Directiva 2001/29/CE, de 22 de maio de 2001, relativa á harmonización de determinados aspectos dos dereitos de autor e dereitos afíns na sociedade da información, adecúa o sistema de dereitos de autor e conexos ao ámbito dixital, asumindo ao mesmo tempo as obrigacións contraídas pola Unión Europea e os seus Estados Membros no marco dos Tratados Dixitais OMPI (WCT e WPPT).

5.-Directiva 2000/31/CE do Parlamento Europeo e do Consello, de 8 de xuño de 2000 (DOCE do 17 de xullo) relativa a determinados aspectos xurídicos dos servizos da sociedade da información, en particular o comercio electrónico (Directiva sobre o comercio electrónico). Nesa

Directiva regúlase, entre outros aspectos e polo que interesa á materia de propiedade intelectual, a responsabilidade dos prestadores de servizos intermediarios (artigos 12 a 15 da Directiva).

### **9.1.3 Normativa internacional:**

1.-O Convenio de Berna, que protexe as obras literarias e artísticas, datando a súa acta orixinaria de 1886, sendo España socio fundador do mesmo. Entre os principios informadores do Convenio atópanse o de trato nacional (ou asimilación do estranxeiro ao nacional), o de protección automática, o de independencia da protección, e o de protección mínima (para lograr un conxunto dispositivo uniformemente aplicable).

2.-Tratado OMPI sobre Dereito de Autor (Tratado WCT, 1996): como resultado da Conferencia Diplomática da OMPI sobre certas cuestións de dereitos de autor e de dereitos conexos -celebrada en Xenebra en decembro de 1996-, adoptouse este tratado, orientado a ofrecer a necesaria resposta lexislativa aos problemas suscitados pola tecnoloxía dixital, e particularmente por Internet.

3.-ISO 12083. Marcaxe de documentos electrónicos

## **9.2.- PROTECCIÓN XURÍDICA DE PROGRAMAS DE ORDENADOR.**

### **9.2.1 Introducción**

Debemos partir, dada a súa importancia, da Directiva do Consello do 14 de maio de 1991 sobre a protección xurídica de programas de ordenador; alí indícasenos que a efectos da presente Directiva, o termo «programa de ordenador» inclúe programas en calquera forma, incluso os que están incorporados no «hardware»; que este termo designa tamén o traballo preparatorio de concepción que conduce ao desenvolvemento dun



programa de ordenador, sempre que a natureza do traballo preparatorio sexa tal que máis tarde poida orixinar un programa de ordenador

Dita directiva foi obxecto de transposición ao ordenamento español pola lei 16/1993 de 23 de decembro, sendo esta, á súa vez, derogada polo Real Decreto Legislativo 1/1996, do 12 de abril, polo que se aproba o Texto Refundido da Lei de Propiedade Intelectual, regularizando, aclarando e harmonizando as disposicións legais vixentes sobre a materia.

A Directiva establece que os Estados membros protexerán mediante dereitos de autor os programas de ordenador como obras literarias, tal e como se definen no Convenio de Berna para a protección das obras literarias e artísticas.

Para os fins da presente Directiva, a expresión «programas de ordenador» abranguerá a súa documentación preparatoria

Respecto da titularidade dos dereitos; considerarase autor do programa de ordenador a persoa física ou grupo de persoas físicas que o crearon ou, cando a lexislación dos Estados membros o permitan, a persoa xurídica que sexa considerada titular do dereito pola devandita lexislación. Cando a lexislación dun Estado membro recoñeza as obras colectivas, a persoa física ou xurídica que segundo a devandita lexislación cree o programa, será considerada o seu autor.

Cando un programa de ordenador se cree conxuntamente por varias persoas físicas, os dereitos exclusivos serán propiedade común.

Cando un traballador asalariado cree un programa de ordenador no exercicio das funcións que lle foron confiadas, ou seguindo as instrucións do seu empresario, a titularidade dos dereitos económicos correspondentes

ao programa de ordenador así creado corresponderán, exclusivamente, ao empresario, salvo pacto en contrario.

A protección concederase a todas as persoas físicas e xurídicas que cumpran os requisitos establecidos na lexislación nacional sobre dereitos de autor aplicable ás obras literarias

De conformidade coa Directiva, os dereitos exclusivos do titular incluírán o dereito de realizar ou de autorizar:

a) a reprodución total ou parcial dun programa de ordenador por calquera medio e baixo calquera forma, xa for permanente ou transitoria.

Cando a carga, presentación, execución, transmisión ou almacenamento dun programa necesitan tal reprodución do mesmo, estes actos estarán suxeitos á autorización do titular do dereito;

b) a tradución, adaptación, arranxo e calquera outra transformación dun programa de ordenador e a reprodución dos resultados de tales actos, sen prexuízo dos dereitos da persoa que transforme o programa de ordenador;

c) calquera forma de distribución pública, incluído o aluguer, do programa de ordenador orixinal ou das súas copias. A primeira venda na Comunidade dunha copia dun programa polo titular dos dereitos ou co seu consentimento, esgotará o dereito de distribución na Comunidade da devandita copia, salvo o dereito de controlar o subseguinte aluguer do programa ou dunha copia do mesmo.

Non obstante o anterior, salvo que existan disposicións contractuais específicas, non necesitarán a autorización do titular os actos indicados nas letras a) e b) anteriormente citadas cando os devanditos actos sexan necesarios para a utilización do programa de ordenador por parte do

adquirente lexítimo con arranxo á súa finalidade proposta, incluída a corrección de erros.

A realización dunha copia de salvagarda por parte dunha persoa con dereito a utilizar o programa non poderá impedirse por contrato sempre que resulte necesaria para dita utilización.

O usuario lexítimo da copia dun programa estará facultado para observar, estudar ou verificar o seu funcionamento, sen autorización previa do titular, co fin de determinar as ideas e principios implícitos en calquera elemento do programa, sempre que o faga durante calquera das operacións de carga, visualización, execución, transmisión ou almacenamento do programa, que ten dereito a facer.

#### 9.2.2 Normativa Estatal

Desde o punto de vista da normativa estatal regúlase no título VII do RD 1/1996, de 12 de abril, polo que se aproba o Texto Refundido da Lei de Propiedade Intelectual, que derogou a citada lei 16/1993 de 23 de decembro de transposición da Directiva 91/250/CEE

O dereito de autor sobre os programas de ordenador rexerase polos preceptos do presente Título VII e, no que non estea especificamente previsto no mesmo, polas disposicións que resulten aplicables da Lei.

Aos efectos da Lei entenderase por programa de ordenador toda secuencia de instrucións ou indicacións destinadas a ser utilizadas, directa ou indirectamente, nun sistema informático para realizar unha función ou unha tarefa ou para obter un resultado determinado, calquera que for a súa forma de expresión e fixación.

Aos mesmos efectos, a expresión programas de ordenador comprenderá tamén a súa documentación preparatoria. A documentación técnica e os manuais de uso dun programa gozarán da mesma protección que este Título dispensa aos programas de ordenador.

O programa de ordenador será protexido unicamente se fose orixinal, no sentido de ser unha creación intelectual propia do seu autor.

A protección prevista aplicarase a calquera forma de expresión dun programa de ordenador. Así mesmo, esta protección esténdese a calquera versión sucesiva do programa, así como aos programas derivados, salvo aquelas creadas co fin de ocasionar efectos nocivos a un sistema informático.

Cando os programas de ordenador formen parte dunha patente ou un modelo de utilidade gozarán da protección que puidese corresponderlles por aplicación do réxime xurídico da propiedade industrial.

Non estarán protexidos mediante os dereitos de autor as ideas e principios nos que se basean calquera dos elementos dun programa de ordenador incluídos os que serven de fundamento aos seus interfaces.

### 1.-Titularidade

Será considerado autor do programa de ordenador a persoa ou grupo de persoas naturais que o crearon, ou a persoa xurídica que sexa contemplada como titular dos dereitos de autor nos casos expresamente previstos pola lei. Cando se trate dunha obra colectiva terá a consideración de autor, salvo pacto en contrario, a persoa natural ou xurídica que a edite e divulgue baixo o seu nome.

Os dereitos de autor sobre un programa de ordenador que sexa resultado unitario da colaboración entre varios autores serán propiedade común e corresponderán a todos estes na proporción que determinen.

Cando un traballador asalariado cree un programa de ordenador, no exercicio das funcións que lle foron confiadas ou seguindo as instrucións do seu empresario, a titularidade dos dereitos de explotación correspondentes ao programa de ordenador así creado, tanto o programa fonte como o programa obxecto, corresponderán, exclusivamente, ao empresario, salvo pacto en contrario.

A protección concederase a todas as persoas naturais e xurídicas que cumpran os requisitos establecidos na lei para a protección dos dereitos de autor.

## 2.-Duración da protección.

Cando o autor sexa unha persoa natural a duración dos dereitos de explotación dun programa de ordenador será, segundo os distintos supostos que poden suscitarse, a prevista no Capítulo I do Título III do RD 1/1996, de 12 de abril, polo que se aproba o Texto Refundido da Lei de Propiedade Intelectual,

Cando o autor sexa unha persoa xurídica a duración dos dereitos á que se refire o parágrafo anterior será de setenta anos, computados desde o día 1 de xaneiro do ano seguinte ao da divulgación lícita do programa ou ao da súa creación se non se divulgou.

## 3.-Contido dos dereitos de explotación.

Os dereitos exclusivos da explotación dun programa de ordenador, por parte de quen sexa o seu titular, incluírán o dereito de realizar ou de autorizar:

- a) A reprodución total ou parcial, mesmo para uso persoal, dun programa de ordenador, por calquera medio e baixo calquera forma, xa for permanente ou transitoria. Cando a carga, presentación, execución, transmisión ou almacenamento dun programa necesiten tal reprodución deberá dispoñerse de autorización para iso, que outorgará o titular do dereito.
- b) A tradución, adaptación, arranxo ou calquera outra transformación dun programa de ordenador e a reprodución dos resultados de tales actos, sen prexuízo dos dereitos da persoa que transforme o programa de ordenador.
- c) Calquera forma de distribución pública, incluído o aluguer do programa de ordenador orixinal ou das súas copias.

A tales efectos, cando se produza cesión do dereito de uso dun programa de ordenador, entenderase, salvo proba en contrario, que dita cesión ten carácter non exclusivo e intransferible, presumíndose, así mesmo, que o é para satisfacer unicamente as necesidades do usuario. A primeira venda na Unión Europea dunha copia dun programa polo titular dos dereitos ou co seu consentimento, esgotará o dereito de distribución da devandita copia, salvo o dereito de controlar o subseguinte aluguer do programa ou dunha copia do mesmo.

#### 4.-Límites aos dereitos de explotación.

Non necesitarán autorización do titular, salvo disposición contractual en contrario,

a) A reprodución ou transformación dun programa de ordenador incluída a corrección de erros, cando os devanditos actos sexan necesarios para a utilización do mesmo por parte do usuario lexítimo, con arranxo á súa finalidade proposta.

b) A realización dunha copia de seguridade por parte de quen ten dereito a utilizar o programa non poderá impedirse por contrato en canto resulte necesaria para dita utilización.

c) O usuario lexítimo da copia dun programa estará facultado para observar, estudar ou verificar o seu funcionamento, sen autorización previa do titular, co fin de determinar as ideas e principios implícitos en calquera elemento do programa, sempre que o faga durante calquera das operacións de carga, visualización, execución, transmisión ou almacenamento do programa que ten dereito a facer.

O autor, salvo pacto en contrario, non poderá opoñerse a que o cesionario titular de dereitos de explotación realice ou autorice a realización de versións sucesivas do seu programa nin de programas derivados do mesmo.

Non será necesaria a autorización do titular do dereito cando a reprodución do código e a tradución da súa forma sexa indispensable para obter a información necesaria para a interoperabilidade dun programa creado de forma independente con outros programas, sempre que se cumpran os seguintes requisitos:

1.-Que tales actos sexan realizados polo usuario lexítimo ou por calquera outra persoa facultada para utilizar unha copia do programa, ou, no seu nome, por parte dunha persoa debidamente autorizada.

2.-Que a información necesaria para conseguir a interoperabilidade non sexa posta previamente e de xeito fácil e rápida, a disposición das persoas a que se refire o parágrafo anterior.

3.-Que ditos actos se limiten a aquelas partes do programa orixinal que resulten necesarias para conseguir a interoperabilidade.

#### 5.-Protección rexistral.

Os dereitos sobre os programas de ordenador, así como sobre as súas sucesivas versións e os programas derivados, poderán ser obxecto de inscrición no Rexistro da Propiedade Intelectual.

#### 6.-Infracción dos dereitos.

De acordo coa normativa vixente terán a consideración de infractores dos dereitos de autor quen, sen autorización do titular dos mesmos, realicen os actos seguintes previstos no artigo 99, ao indicar este que

«A reprodución total ou parcial, mesmo para uso persoal, dun programa de ordenador, por calquera medio e baixo calquera forma, xa for permanente ou transitoria. Cando a carga, presentación, execución, transmisión ou almacenamento dun programa necesiten tal reprodución deberá dispoñerse de autorización para iso, que outorgará o titular do dereito.

b. A tradución, adaptación, arranxo ou calquera outra transformación dun programa de ordenador e a reprodución dos resultados de tales actos, sen prexuízo dos dereitos da persoa que transforme o programa de ordenador.

c. Calquera forma de distribución pública incluído o aluguer do programa de ordenador orixinal ou das súas copias.»



Ademais en particular, considerarase infractor:

- 1.- Quen poña en circulación unha ou máis copias dun programa de ordenador coñecendo ou podendo presumir a súa natureza ilexítima.
- 2.- Quen teña con fins comerciais una ou máis copias dun programa de ordenador, coñecendo ou podendo presumir a súa natureza ilexítima.
- 3.- Quen poña en circulación ou teña con fins comerciais calquera instrumento cuxo único uso sexa facilitar a supresión ou neutralización non autorizadas de calquera dispositivo técnico utilizado para protexer un programa de ordenador.

#### 7.- Medidas de protección.

O titular dos dereitos recoñecidos sobre programas de ordenador que se dispoñen na lei, é dicir

- 1.- Poderá pedir o cesamento da actividade ilícita, que poderá comprender a suspensión da explotación ou actividade infractora,
- 2.-A prohibición ao infractor de renovar a explotación ou actividade infractora,
- 3.-A retirada do comercio dos exemplares ilícitos e a súa destrución,
- 4.-A retirada dos circuítos comerciais, a inutilización, e, en caso necesario, a destrución dos moldes, pranchas, matrices, negativos e demais elementos materiais, equipos ou instrumentos destinados principalmente á reprodución, á creación ou fabricación de exemplares ilícitos,
- 5.-A remoción ou o precinto dos aparellos utilizados na comunicación pública non autorizada de obras ou prestacións.
- 6.- A remoción ou o precinto dos instrumentos utilizados para facilitar a supresión ou a neutralización non autorizadas de calquera dispositivo

técnico utilizado para protexer obras ou prestacións, aínda que aquela non fose o seu único uso,

7.-A suspensión dos servizos prestados por intermediarios a terceiros que se vullan deles para infrinxir dereitos de propiedade intelectual

Ademais as medidas cautelares procedentes, conforme ao disposto na Lei de Axuizamento Civil.

### **9.3.-TIPOS DE LICENZAS**

Software Libre ou *Free Software* é un software dispoñible para calquera que desexe utilizalo, copialo e distribuílo, xa sexa na súa forma orixinal ou con modificacións. A posibilidade de modificacións implica que o código fonte está dispoñible. Se un programa é libre, pode ser potencialmente incluído nun sistema operativo tamén libre. É importante non confundir software libre con software gratis, porque a liberdade asociada ao software libre de copiar, modificar e redistribuír non significa gratuidade. Existen programas gratuítos que non poden ser modificados nin redistribuídos. E existen programas pagos.

#### Copyleft.

A maioría das licenzas usadas na publicación de software libre permite que os programas sexan modificados e redistribuídos. Estas prácticas están xeralmente prohibidas pola lexislación internacional de copyright, que intenta impedir que alteracións e copias sexan efectuadas sen a autorización do ou os autores. As licenzas que acompañan ao software libre fan uso da lexislación de copyright para impedir a utilización non autorizada, pero estas licenzas definen clara e explicitamente as condicións baixo as cales poden realizarse copias, modificacións e redistribucións, co fin de garantir as liberdades de modificar e redistribuír o software rexistrado. A esta versión de copyright dáselle o nome de copyleft.

### GPL.

A Licenza Pública Xeral GNU (GNU General Public License GPL) é a licenza que acompaña aos paquetes distribuídos polo Proxecto GNU, mais unha gran variedade de software que inclúe o núcleo do sistema operativo Linux. A formulación de GPL é tal que no canto de limitar a distribución do software que protexe, chega mesmo a impedir que este software sexa integrado en software propietario. A GPL baséase na lexislación internacional de copyright, o que debe garantir cobertura legal para o software licenciado con GPL.

### Debian.

A licenza Debian é parte do contrato realizado entre Debian e a comunidade de usuarios de software libre, e denomínase Debian Free Software Guidelines (DFSG). En esencia, esta licenza contén criterios para a distribución que inclúen, ademais da esixencia de publicación do código fonte: (a) a redistribución libre ; (b) o código fonte debe ser incluído e debe poder ser redistribuído; (c) todo traballo derivado debe poder ser redistribuído baixo a mesma licenza do orixinal; (d) pode haber restricións en canto á redistribución do código fonte, se o orixinal foi modificado; (e) a licenza non pode discriminar a ningunha persoa ou grupo de persoas, así como tampouco ningunha forma de utilización do software; (f) os dereitos outorgados non dependen do sitio no que o software se atope; e (g) a licenza non pode «contaminar» a outro software.

### BSD.

A licenza BSD cobre as distribucións de software de Berkeley Software Distribution, ademais doutros programas. Esta é unha licenza considerada «permisiva» , xa que impón poucas restricións sobre a forma de uso, alteracións e redistribución do software. O software pode ser vendido e non hai obrigacións de incluír o código fonte. Esta licenza garante o crédito aos autores do software pero non intenta garantir que as modificacións futuras permanezan sendo software libre.

### X.org.

O Consorcio X distribúe X Window System baixo unha licenza que o fai software libre, aínda que sen adherirse ao copyleft. Existen distribucións baixo a licenza da X.org que son software libre e outras distribucións que non o son. Existen algunhas versións non-libres do sistema de ventás X11 para estacións de traballo e certos dispositivos de IBM-PC que son as únicas funcións dispoñibles, sen outros similares que sexan distribuídos como software libre.

### Software con Dominio Público.

O Software con dominio público é software sen copyright. Algúns tipos de copia ou versións modificadas poden non ser libres se o autor impón restricións adicionais na redistribución do orixinal ou de traballos derivados.

### Software Semi-libre.

O Software semi-libre é un software que non é libre pero permite que outros individuos o usen, copien, distribúan e mesmo o modifiquen. Exemplos de software semi-libre son as primeiras versións de Internet Explorer de Microsoft, ou algunhas versións de browsers de Netscape, e StarOffice.

### Freeware.

O termo freeware non posúe unha definición amplamente aceptada, pero é utilizada para programas que permiten a redistribución, pero non a modificación, e que inclúen o seu código fonte. Estes programas non son software libre.

### Shareware.

Shareware é o software dispoñible co permiso para que sexa redistribuído, pero a súa utilización implica o pagamento. Xeralmente o código fonte non se atopa dispoñible e, xa que logo, é imposible realizar modificacións.

### Software Propietario.

O Software propietario é aquel cuxa copia, redistribución ou modificación están, nalgunha medida, prohibidos polo seu propietario. Para usar, copiar ou redistribuír, débese solicitar permiso ao propietario ou pagar.

### Software Comercial.

O Software comercial é o software desenvolvido por unha empresa co obxectivo de lucrarse coa súa utilización. Nótese que «comercial» e «propietario» non son o mesmo. A maior parte do software comercial é propietario, pero existe software libre que é comercial, e existe software non-libre que non é comercial.

## **9.4 .-SOFTWARE DE FONTES ABERTAS.**

O software libre e de código aberto (tamén coñecido como FOSS ou FLOSS, siglas de *free/libre and open source software*, en inglés) é o software que está licenciado de tal xeito que os usuarios poden estudar, modificar e mellorar o seu deseño mediante a dispoñibilidade do seu código fonte.

O termo «software libre e de código aberto» abarca os conceptos de software libre e software de código aberto e, aínda que comparten modelos de desenvolvemento similares, teñen diferenzas nos seus aspectos filosóficos. O software libre enfócase nas liberdades filosóficas que lles outorga aos usuarios, mentres que o software de código aberto enfócase nas vantaxes do seu modelo de desenvolvemento. «FOSS» é un termo imparcial con respecto a ambas filosofías.

O software gratis non necesariamente ten que ser libre ou de código aberto

Comparación entre software libre e de código aberto

Para que un software sexa definido como libre ou de código aberto, ou ambos, debe cumprir certas regras ou normas para posuír esta denominación:

As 4 liberdades do software libre

- 1.- Executar o programa con calquera propósito (liberdade 0)  
(privado, educativo, público, comercial, militar, etc.)
- 2.-Estudar e modificar o programa (liberdade 1)  
(para o que é necesario poder acceder ao código fonte)
- 3.-Distribuír o programa de maneira que se poida axudar aos demais (liberdade 2).
- 4.-Distribuír as versións modificadas propias (liberdade 3)

As 10 premisas do software de código aberto

- 1.-Libre redistribución: o software debe poder ser regalado ou vendido libremente.
- 2.-Código fonte: o código fonte debe estar incluído ou obterse libremente.
- 3.-Traballos derivados: a redistribución de modificacións debe estar permitida
- 4.-Integridade do código fonte do autor: as licenzas poden requirir que as modificacións sexan redistribuídas só como parches.
- 5.- Sen discriminación de persoas ou grupos: non se pode deixar fóra a ningún.
- 6.-Sen discriminación de áreas de iniciativa: os usuarios comerciais non poden ser excluídos.
- 7.-Distribución da licenza: deben aplicarse os mesmos dereitos a todo o que reciba o programa.
- 8.-A licenza non debe ser específica dun produto: o programa non pode licenciarse só como parte dunha distribución maior.

9.-A licenza non debe restrinxir outro software: a licenza non pode obrigir a que algún outro software que sexa distribuído co software aberto deba tamén ser de código aberto.

10.-A licenza debe ser tecnoloxicamente neutral: non debe requirirse a aceptación da licenza por medio dun acceso por clic de rato ou doutra forma específica do medio de soporte do software.

## Organizacións e licenzas tralo FOSS

Existen organizacións detrás de cada iniciativa de distinción do software.

Por parte do software libre, existe a Free Software Foundation (FSF); apoiando o concepto de software de código aberto existe a Open Source Initiative (OSI). Ambas enfócanse a diferentes aspectos do uso e distribución do software e á súa dispoñibilidade e responsabilidades que lle competen ter ao usuario. Por este motivo existen diferentes licenzas que as diferencian:

Licenzas de código aberto (para o software de código aberto), licenzas de software libre (para o software libre), entre outras, sen protección herdada e con protección herdada.

Autor:

Alfonso García Magariños

Director Asesoría Xurídica Municipal Concello da Coruña



# **10. LEI 32/2003, XERAL DE TELECOMUNICACIÓNS. REGULACIÓN DO MERCADO DAS TELECOMUNICACIÓNS.**



## **Tema 10.- Lei 32/2003 xeral de telecomunicacións. Regulación do mercado de telecomunicacións.**

### **ÍNDICE**

#### 10.1 Lei xeral de telecomunicacións.

##### 10.1.1 Introducción

##### 10.1.2 Aspectos Básicos

##### 10.1.3 Estrutura e Obxectivos

## **10.1.- LEI 32/2003 XERAL DE TELECOMUNICACIÓNS. REGULACIÓN DO MERCADO**

### 10.1.1 Introducción

Aínda que a Lei 11/1998, do 24 de abril, xeral de telecomunicacións, instaurou un réxime plenamente liberalizado na prestación de servizos e o establecemento e explotación de redes de telecomunicacións, abrindo o sector á libre competencia entre operadores, a devandita regulación quedara en certo xeito desfasada, en razón fundamentalmente da hiperactividade normativa da Unión Europea.

A lei incorpora ao ordenamento xurídico español o contido da normativa comunitaria citada, respectando plenamente os principios recollidos nela.

### 10.1.2 Aspectos Básicos

Como notas máis importantes da lei cómpre salientar as seguintes:

En primeiro lugar, diríxese a regular exclusivamente o sector das telecomunicacións, en exercicio da competencia exclusiva do Estado prevista no artigo 149.1.21ª da Constitución. A lei exclúe expresamente da súa regulación os contidos difundidos a través de medios audiovisuais, que constitúen parte do réxime dos medios de comunicación social e que se caracterizan por seren transmitidos nun só sentido de forma simultánea a unha multiplicidade de usuarios. Igualmente exclúese da súa regulación a prestación de servizos sobre as redes de telecomunicacións que non consistan principalmente no transporte de sinais a través das devanditas redes. Estes últimos son obxecto de regulación na Lei 34/2002, do 11 de xullo, de servizos da sociedade da información e de comercio electrónico. No entanto, as redes utilizadas como soporte dos servizos de radiodifusión sonora e televisiva, as redes de televisión

por cable e os recursos asociados, como parte integrante das comunicacións electrónicas, estarán suxeitos ao establecido na lei.

Toda a regulación das comunicacións electrónicas se entende incluída no concepto máis amplo de telecomunicacións e, polo tanto, ditada polo Estado en virtude da súa atribución competencial exclusiva do artigo 149.1.21ª da Constitución.

Avánzase na liberalización da prestación de servizos e na instalación e explotación de redes de comunicacións electrónicas. Neste sentido, cumprindo co principio de intervención mínima, enténdese que a habilitación para a devandita prestación e explotación a terceiros vén concedida con carácter xeral e inmediato pola lei. Unicamente será requisito previo a notificación á Comisión do Mercado das Telecomunicacións para iniciar a prestación do servizo. Desaparecen, pois, as figuras das autorizacións e licenzas previstas na Lei 11/1998, do 24 de abril, xeral de telecomunicacións, como títulos habilitantes individualizados de que era titular cada operador para a prestación de cada rede ou servizo.

Refórzanse as competencias e facultades da Comisión do Mercado das Telecomunicacións en relación coa supervisión e regulación dos mercados. Contémplase un sistema que gaña en flexibilidade, mediante o cal este organismo realizará análises periódicas dos distintos mercados de referencia, detectando aqueles que non se estean desenvolvendo nun contexto de competencia efectiva, e impoñéndolles, nese caso, obrigas específicas aos operadores con poder significativo no mercado. É innovador tamén o cambio na definición deste tipo de operadores, pasando dun concepto «formal», isto é, baseado na superación dunha determinada cota de mercado, a un «material», máis próximo ao tradicional dereito da competencia, é dicir, baseado na posición de forza do operador que lle permite actuar con independencia dos seus competidores ou dos consumidores, que sexan persoas físicas e usuarios.

En relación coa garantía dos dereitos dos usuarios, a lei recolle a ampliación das prestacións, que, como mínimo esencial, deben garantírselles a todos os cidadáns baixo a denominación de «servizo universal». Inclúese o acceso funcional a internet, xa incorporado anticipadamente pola Lei 34/2002, do 11 de xullo, de servizos da sociedade da información e de comercio electrónico, e a posibilidade de que se ofrezan opcións tarifarias especiais que permitan un maior control do gasto polos usuarios. Ademais, amplíase o catálogo de dereitos dos consumidores que sexan persoas físicas e usuarios recoñecidos con rango legal.

A regulación da ocupación do dominio público ou a propiedade privada para a instalación de redes pretende establecer uns criterios xerais, que deberán ser respectados polas administracións públicas titulares do dominio público. Deste xeito, recoñécenselles dereitos de ocupación a todos os operadores que practiquen a notificación á Comisión do Mercado das Telecomunicacións, na medida en que sexa necesario para a instalación das súas redes, á vez que se detallan os principios básicos que garantan o exercicio do devandito dereito en condicións de igualdade e transparencia, con independencia da administración ou o titular do dominio público ou a propiedade privada.

No referente ao dominio público radioelétrico, régúlase a garantía do uso eficiente do espectro radioelétrico como principio superior que debe guiar a planificación e a asignación de frecuencias pola Administración e o uso destas polos operadores. Así mesmo, ábrese a posibilidade da cesión de dereitos de uso do espectro radioelétrico nas condicións que se determinen regulamentariamente. Nos supostos en que as bandas de frecuencias asignadas a determinados servizos sexan insuficientes para atender a demanda dos operadores, prevese a celebración de procedementos de licitación. Como requisito esencial na prestación de servizos mediante tecnoloxías que usen o dominio público radioelétrico, establécese o respecto aos límites das emisións radioeléctricas fixadas na normativa vixente.

A lei tamén ten como obxectivo o establecemento dunha serie de criterios que guíen a actuación na imposición de taxas que afecten aos servizos de telecomunicacións. Distingue entre aquelas taxas que respondan á necesidade de compensar actuacións administrativas, onde a contía se fixará en función do seu custo, daquelas impostas sobre o uso de recursos asociados, como o dominio público, as frecuencias ou a numeración. Neste último caso perséguese garantir o seu uso óptimo, tendo en conta o valor do ben e a súa escaseza. Como principios básicos destas exaccións establécense a transparencia, a proporcionalidade e a súa xustificación obxectiva.

Na tipificación de infraccións e a imposición das correspondentes sancións reforzáronse as potestades administrativas como necesario contrapunto a unha maior simplificación nas condicións para obter a habilitación para prestar servizos. Con iso, o control «ex ante» que supoñía a obtención dunha autorización individualizada para cada operador coa Lei 11/1998, do 24 de abril, xeral de telecomunicacións, vén ser substituído por un «ex post» mediante a posibilidade de obter información dos operadores, de impoñer medidas cautelares no procedemento sancionador ou de inhabilitar as empresas que cometan infraccións moi graves.

### 10.1.3 Estrutura e Obxectivos

Contén a lei 7 títulos.

O título I contén as disposicións xerais da lei; así, declara que as telecomunicacións son servizos de interese xeral que se prestan en réxime de libre competencia.

Os obxectivos e principios desta lei son os seguintes:

Fomentar a competencia efectiva nos mercados de telecomunicacións e, en particular, na explotación das redes e na prestación dos servizos de comunicacións electrónicas e na subministración dos recursos asociados a eles. Todo iso promovendo un investimento eficiente en materia de infraestruturas e fomentando a innovación.

Garantir o cumprimento das referidas condicións e das obrigas de servizo público na explotación de redes e a prestación de servizos de comunicacións electrónicas, en especial as de servizo universal.

Promover o desenvolvemento do sector das telecomunicacións, así como a utilización dos novos servizos e o despregamento de redes, e o acceso a estes, en condicións de igualdade, e impulsar a cohesión territorial, económica e social.

Facer posible o uso eficaz dos recursos limitados de telecomunicacións, como a numeración e o espectro radioeléctrico, e a adecuada protección deste último, e o acceso aos dereitos de ocupación da propiedade pública e privada.

Defender os intereses dos usuarios

Fomentar, na medida do posible, a neutralidade tecnolóxica na regulación.

Promover o desenvolvemento da industria de produtos e servizos de telecomunicacións.

Contribuír ao desenvolvemento do mercado interior de servizos de comunicacións electrónicas na Unión Europea.

Recolle tamén que as redes, servizos, instalacións e equipos de telecomunicacións que desenvolvan actividades esenciais para a defensa nacional e integran os medios destinados a esta, resérvanse ao Estado e réxense pola súa normativa específica.

O título II regula a explotación de redes e prestación de servizos de comunicacións electrónicas en réxime de libre competencia.

A explotación das redes e a prestación dos servizos de comunicacións electrónicas realizaranse en réxime de libre competencia sen máis limitacións que as establecidas nesta lei e a súa normativa de desenvolvemento.

Poderán explotar redes e prestar servizos de comunicacións electrónicas a terceiros as persoas físicas ou xurídicas nacionais dun Estado membro da Unión Europea ou con outra nacionalidade, cando, no segundo caso, así estea previsto nos acordos internacionais que vinculen o Reino de España. Para o resto de persoas físicas ou

xurídicas, o Goberno poderá autorizar excepcións de carácter xeral ou particular á regra anterior.

En todo caso, as persoas físicas ou xurídicas que exploten redes ou presten servizos de comunicacións electrónicas a terceiros deberán designar unha persoa responsable para os efectos de notificacións domiciliada en España, sen prexuízo do que poidan prever os acordos internacionais.

Os interesados na explotación dunha determinada rede ou na prestación dun determinado servizo de comunicacións electrónicas deberán, con anterioridade ao comezo da actividade, notificalo de maneira indubidable á Comisión do Mercado das Telecomunicacións nos termos que se determinen mediante Real decreto, someténdose ás condicións previstas para o exercicio da actividade que pretendan realizar. Quedan exentos desta obriga aqueles que exploten redes e se presten servizos de comunicacións electrónicas en réxime de autoprestación.

Cando a Comisión do Mercado das Telecomunicacións constate que a notificación non reúne os requisitos establecidos no apartado anterior, ditará resolución motivada nun prazo máximo de 15 días, non tendo por realizada aquela.

Créase, dependente da Comisión do Mercado das Telecomunicacións, o Rexistro de operadores. O devandito rexistro será de carácter público e a súa regulación farase por Real decreto. Nel deberán inscribirse os datos relativos ás persoas físicas ou xurídicas que notifiquen a súa intención de explotar redes ou prestar servizos de comunicacións electrónicas, as condicións para desenvolver a actividade e as súas modificacións.

Os operadores de redes públicas de comunicacións electrónicas terán o dereito e, cando se solicite por outros operadores de redes públicas de comunicacións electrónicas, a obriga de negociar a interconexión mutua co fin de prestar servizos de

comunicacións electrónicas dispoñibles ao público, co obxecto de garantir así a prestación de servizos e a súa interoperabilidade.

Cando se lle impoñan obrigas a un operador de redes públicas de comunicacións electrónicas para que facilite acceso, a Comisión do Mercado das Telecomunicacións poderá establecerlles determinadas condicións técnicas ou operativas ao citado operador ou aos beneficiarios do devandito acceso cando sexa necesario para garantir o funcionamento normal da rede, conforme se estableza regulamentariamente.

A Comisión do Mercado das Telecomunicacións poderá impoñerlles aos operadores que, de conformidade co devandito artigo, fosen declarados con poder significativo no mercado, obrigas en materia de:

- 1.-Transparencia, en relación coa interconexión e o acceso, conforme á cal os operadores deberán facer público determinado tipo de información, como a relativa á contabilidade, especificacións técnicas, características das redes, condicións de subministración e utilización, e prezos. En particular, cando se impoñan obrigas de non discriminación a un operador, poderáselle esixir que publique unha oferta de referencia.
- 2.-Non discriminación, que garantirá, en particular, que o operador lles aplique condicións equivalentes en circunstancias semellantes a outros operadores que presten servizos equivalentes e lles proporcione a terceiros servizos e información da mesma calidade que os que proporcione para os seus propios servizos ou os das súas filiais ou asociados e nas mesmas condicións.
- 3.-Separación de contas, no formato e coa metodoloxía que, de ser o caso, se especifiquen.
- 4.-Acceso a recursos específicos das redes e á súa utilización.
- 5.-Control de prezos, tales como a orientación dos prezos en función dos custos, e contabilidade de custos, para evitar prezos excesivos ou a compresión dos prezos en detrimento dos usuarios finais.



Para os servizos de comunicacións electrónicas dispoñibles ao público débense proporcionar os números e enderezos que se precisen para permitir a súa efectiva prestación, tomándose esta circunstancia en consideración nos plans nacionais de numeración e enderezamento, respectivamente.

Os plans nacionais e as súas disposicións de desenvolvemento designarán os servizos para os que se poidan utilizar os números e, de ser o caso, enderezos e nomes correspondentes, incluído calquera requisito relacionado coa prestación de tales servizos.

O contido dos citados plans e o dos actos derivados do seu desenvolvemento e xestión serán públicos, salvo no relativo a materias que poidan afectar á seguridade nacional.

Regúlanse as obrigas de servizo público e dereitos e obrigas de carácter público na explotación de redes e na prestación de servizos de comunicacións electrónicas.

Os operadores están sometidos ás seguintes categorías de obrigas de servizo público:

O servizo universal nos termos seguintes:

Enténdese por servizo universal o conxunto definido de servizos cuxa prestación se garante para todos os usuarios finais con independencia da súa localización xeográfica, cunha calidade determinada e a un prezo accesible.

Débese garantir:

1.- Que todos os usuarios finais poidan obter unha conexión á rede telefónica pública desde unha localización fixa e acceder á prestación do servizo telefónico dispoñible ao público, sempre que as súas solicitudes se consideren razoables nos termos que regulamentariamente se determinen. A conexión débelle ofrecer ao usuario final a posibilidade de efectuar e recibir chamadas telefónicas e permitir comunicacións de fax e datos a velocidade suficiente para acceder de forma funcional a internet. No entanto, a conexión deberá permitir comunicacións en banda ancha, nos termos que se definan pola normativa vixente.

2.- Que se poña a disposición dos abonados ao servizo telefónico dispoñible ao público unha guía xeral de números de abonados, xa sexa impresa ou electrónica, ou

ambas, e se actualice, como mínimo, unha vez ao ano. Así mesmo, que se poña a disposición de todos os usuarios finais do devandito servizo, incluídos os usuarios de teléfonos públicos de pago, polo menos un servizo de información xeral sobre números de abonados. Todos os abonados ao servizo telefónico dispoñible ao público terán dereito a figurar na mencionada guía xeral, sen prexuízo, en todo caso, do respecto ás normas que regulen a protección dos datos persoais e o dereito á intimidade.

3.- Que exista unha oferta suficiente de teléfonos públicos de pago en todo o territorio nacional que satisfaga razoablemente as necesidades dos usuarios finais en cobertura xeográfica, en número de aparatos, accesibilidade destes teléfonos polos usuarios con discapacidades e calidade dos servizos, e que sexa posible efectuar gratuitamente chamadas de urxencia desde os teléfonos públicos de pago sen ter que utilizar ningunha forma de pagamento, utilizando o número único de chamadas de urxencia 112 e outros números de urxencia españois. Así mesmo, nos termos que se definan pola normativa vixente para o servizo universal, que exista unha oferta suficiente de equipos terminais de acceso a internet de banda ancha.

4.- Que os usuarios finais con discapacidade teñan acceso ao servizo telefónico dispoñible ao público desde unha localización fixa e aos demais elementos do servizo universal citados neste artigo en condicións equiparables ás que se lles ofrecen ao resto de usuarios finais.

5.- Que, cando así se estableza regulamentariamente, se lles ofrezan aos consumidores que sexan persoas físicas, de acordo con condicións transparentes, públicas e non discriminatorias, opcións ou paquetes de tarifas que difiran das aplicadas en condicións normais de explotación comercial, con obxecto de garantir, en particular, que as persoas con necesidades sociais especiais poidan ter acceso ao servizo telefónico dispoñible ao público ou facer uso deste.

6.- Que se apliquen, cando cumpra, opcións tarifarias especiais ou limitacións de prezos, tarifas comúns, equiparación xeográfica ou outros réximes similares, de acordo con condicións transparentes, públicas e non discriminatorias.

O Goberno poderá, por necesidades da defensa nacional, da seguridade pública ou dos servizos que afecten á seguridade das persoas ou á protección civil, impoñerlles outras obrigas de servizo público distintas das de servizo universal aos operadores.

O Goberno poderá, así mesmo, impoñer outras obrigas de servizo público, tras informe da Comisión do Mercado das Telecomunicacións, motivadas por:

- 1.-Razóns de cohesión territorial.
- 2.-Razóns de extensión do uso de novos servizos e tecnoloxías, en especial á sanidade, á educación, á acción social e á cultura.
- 3.-Razóns de facilitar a comunicación entre determinados colectivos que se atopen en circunstancias especiais e estean insuficientemente atendidos coa finalidade de garantir a suficiencia da súa oferta.
- 4.-Por necesidade de facilitar a dispoñibilidade de servizos que impliquen a acreditación de poder dar fe do contido da mensaxe remitida ou da súa remisión ou recepción.

Os operadores terán dereito á ocupación do dominio público na medida en que sexa necesario para o establecemento da rede pública de comunicacións electrónicas de que se trate.

Os operadores tamén terán dereito á ocupación da propiedade privada cando resulte estritamente necesario para a instalación da rede na medida prevista no proxecto técnico presentado e sempre que non existan outras alternativas economicamente viables, xa sexa a través da súa expropiación forzosa ou mediante a declaración de serventía forzosa de paso para a instalación de infraestruturas de redes públicas de comunicacións electrónicas. En ambos os casos terán a condición de beneficiarios nos expedientes que se tramiten, conforme ao disposto na lexislación sobre expropiación forzosa.

As administracións públicas fomentarán a celebración de acordos voluntarios entre operadores para a localización compartida e o uso compartido de infraestruturas situadas en bens de titularidade pública ou privada.

### Segredo das comunicacións

Os operadores que exploten redes públicas de comunicacións electrónicas ou que presten servizos de comunicacións electrónicas dispoñibles ao público deberán garantir o segredo das comunicacións de conformidade cos artigos 18.3 e 55.2 da Constitución, debendo adoptar as medidas técnicas necesarias.

1.- Os operadores están obrigados a realizar as interceptacións que se autoricen de acordo co establecido na lei.

Os suxeitos obrigados deberán facilitarlle ao axente facultado, agás que polas características do servizo non estean á súa disposición e sen prexuízo doutros datos que poidan ser establecidos mediante Real decreto, os datos indicados na orde de interceptación legal, de entre os que se relacionan deseguido:

- a) Identidade ou identidades do suxeito obxecto da medida da interceptación.
- b) Identidade ou identidades das outras partes implicadas na comunicación electrónica.
- c) Servizos básicos utilizados.
- d) Servizos suplementarios utilizados.
- e) Dirección da comunicación.
- f) Indicación de resposta.
- g) Causa de finalización.
- h) Marcas temporais.
- i) Información de localización.
- j) Información intercambiada a través da canle de control ou sinalización.

O título IV regula a conformidade de aparatos.

O Ministerio de Ciencia e Tecnoloxía velará por que os operadores de redes públicas de comunicacións electrónicas publiquen as especificacións técnicas precisas e adecuadas das interfaces de rede ofrecidas en España, con anterioridade á posibilidade de acceso público aos servizos prestados a través das tales interfaces, e por que publiquen as especificacións técnicas actualizadas cando se produza algunha modificación naquelas.

Os aparatos de telecomunicación, entendendo por tales calquera dispositivo non excluído expresamente do regulamento que desenvolva este título que sexa equipo radioeléctrico ou equipo terminal de telecomunicación, ou ambas as cousas á vez, deberán avaliar a súa conformidade cos requisitos esenciais recollidos nas disposicións que o determinen, ser conformes con todas as disposicións que se establezan e incorporar o marcado correspondente como consecuencia da avaliación realizada. Poderá exceptuarse da aplicación do disposto neste título o uso de determinados equipos de radioaficionados construídos polo propio usuario e non dispoñibles para venda no mercado, conforme ao disposto na súa regulación específica.

Os aparatos de telecomunicación que avaliasen a súa conformidade cos requisitos esenciais noutro Estado membro da Unión Europea ou en virtude dos acordos de recoñecemento mutuo celebrados por ela con terceiros países, e cumpran coas demais disposicións aplicables na materia, terán a mesma consideración.

O Ministerio de Ciencia e Tecnoloxía establecerá os procedementos para o recoñecemento da conformidade dos aparatos de telecomunicación afectos aos acordos de recoñecemento mutuo que estableza a Unión Europea con terceiros países.

A prestación a terceiros de servizos de instalación ou mantemento de equipos ou sistemas de telecomunicación realizarase en réxime de libre competencia sen máis limitacións que as establecidas nesta lei e a súa normativa de desenvolvemento.

Regula o título V o dominio público radioeléctrico.

O espectro radioeléctrico é un ben de dominio público, cuxa titularidade, xestión, planificación, administración e control lle corresponden ao Estado. Esta xestión exerceuse de conformidade co disposto neste título e nos tratados e acordos internacionais nos que España sexa parte, atendendo á normativa aplicable na Unión Europea e ás resolucións e recomendacións da Unión Internacional de Telecomunicacións e doutros organismos internacionais.

A administración, xestión, planificación e control do espectro radioeléctrico inclúen, entre outras funcións, a elaboración e aprobación dos plans xerais de utilización, o establecemento das condicións para o outorgamento do dereito ao seu uso, a atribución dese dereito e a comprobación técnica das emisións radioeléctricas. Así mesmo, intégrase dentro da administración, xestión, planificación e control do referido espectro a inspección, detección, localización, identificación e eliminación das interferencias prexudiciais, irregularidades e perturbacións nos sistemas de telecomunicacións, iniciándose, de ser o caso, o oportuno procedemento sancionador.

A utilización do dominio público radioeléctrico mediante redes de satélites inclúese dentro da xestión, administración e control do espectro de frecuencias.

A xestión do dominio público radioeléctrico ten por obxectivo o establecemento dun marco xurídico que asegure unhas condicións harmonizadas para o seu uso e que permita a súa dispoñibilidade e uso eficiente. Para os tales efectos:

Os dereitos de uso privativo do dominio público radioeléctrico outórganse por prazos que se fixarán regulamentariamente, renovables en función das dispoñibilidades e previsións da planificación do devandito dominio público. Os dereitos de uso privativo sen limitación de número outórganse por un período que finalizará o 31 de decembro do ano natural en que cumbran o seu quinto ano de vixencia, prorrogable por períodos de cinco anos. Pola súa banda, os dereitos de uso privativo con limitación de

número terán a duración prevista nos correspondentes procedementos de licitación que, en todo caso, será dun máximo de vinte anos renovables.

Facultades do Goberno para a xestión do dominio público radioelétrico.

O Goberno desenvolverá regulamentariamente as condicións de xestión do dominio público radioelétrico, a elaboración dos plans para a súa utilización e os procedementos de outorgamento dos dereitos de uso do devandito dominio. No mencionado regulamento débese regular, como mínimo, o seguinte:

O procedemento de determinación, control e inspección dos niveis de emisión radioelétrica tolerable e que non supoñan un perigo para a saúde pública, en concordancia co disposto polas recomendacións da Comisión Europea. Os devanditos límites deberán ser respectados, en todo caso, polo resto das administracións públicas, tanto autonómicas como locais.

O procedemento para a elaboración dos plans de utilización do espectro radioelétrico, que inclúen o cadro nacional de atribución de frecuencias, os plans técnicos nacionais de radiodifusión e televisión, cuxa aprobación lle corresponderá ao Goberno, e as necesidades de espectro radioelétrico para a defensa nacional. Os datos relativos a esta última materia terán o carácter de reservados.

Os procedementos de outorgamento de dereitos de uso do dominio público radioelétrico. Os procedementos de outorgamento de dereitos de uso do dominio público radioelétrico terán en conta, entre outras circunstancias, a tecnoloxía utilizada, o interese dos servizos, as bandas e o seu grao de aproveitamento. Tamén terán en consideración a valoración económica, para o interesado, do uso do dominio público, que este é un recurso escaso e, se procede, as ofertas presentadas polos licitadores.

A habilitación para o exercicio dos dereitos de uso do dominio público radioelétrico revestirá a forma de afectación, concesión ou autorización administrativa. O prazo para o outorgamento das autorizacións e concesións de dominio público radioelétrico será de seis semanas desde a entrada da solicitude en calquera dos rexistros do órgano administrativo competente, sen prexuízo do disposto no apartado seguinte. O devandito prazo non será de aplicación cando sexa necesaria a coordinación internacional de frecuencias ou afecte a reservas de posicións orbitais.

A axeitada utilización do espectro radioelétrico mediante o emprego de equipos e aparatos.

Cando sexa preciso para garantir o uso eficaz do espectro radioelétrico, o Ministerio de Ciencia e Tecnoloxía poderá, tras audiencia ás partes interesadas, incluídas as asociacións de consumidores e usuarios, limitar o número de concesións demaniais a outorgar sobre o devandito dominio para a explotación de redes públicas e a prestación de servizos de comunicacións electrónicas. Esta limitación será revisable polo propio ministerio, de oficio ou a instancia de parte, na medida en que desaparezan as causas que a motivaron.

O dereito de uso do dominio público radioelétrico outorgarase pola Axencia Estatal de Radiocomunicacións a través da afectación demanial ou da concesión ou autorización administrativa; o uso común do dominio público radioelétrico será libre.

O outorgamento do dereito ao uso do dominio público radioelétrico revestirá a forma de autorización administrativa nos seguintes supostos:

Se se trata dunha reserva do dereito de uso especial non privativo do dominio público. Terán a consideración de uso especial do dominio público o do espectro radioelétrico por radioaficionados e outros sen contido económico, como os de banda cidadá, establecéndose mediante regulamento o prazo da súa duración e as condicións asociadas esixibles.



Se se outorga o dereito de uso privativo para autoprestación polo solicitante, salvo no caso de administracións públicas que requirirán de afectación demanial. Non se outorgarán dereitos de uso privativo do dominio público radioelétrico para o seu uso en autoprestación nos supostos en que a demanda supere a oferta. Nos restantes supostos, o dereito ao uso privativo do dominio público radioelétrico requirirá concesión administrativa. Para o outorgamento da devandita concesión demanial, será requisito previo que os solicitantes acrediten a súa condición de operador. As resolucións mediante as cales se outorguen as concesións de dominio público radioelétrico se ditarán e publicarán na forma e prazos que se establezan mediante Real decreto.

O título VI regula a administración das telecomunicacións.

Terán a consideración de Autoridade Nacional de Regulamentación de Telecomunicacións:

O Goberno.

Os órganos superiores e directivos do Ministerio de Ciencia e Tecnoloxía que, de conformidade coa estrutura orgánica do departamento, asuman as competencias desta lei.

Os órganos superiores e directivos do Ministerio de Economía en materia de regulación de prezos.

A Comisión do Mercado das Telecomunicacións.

A Axencia Estatal de Radiocomunicacións.

. Créase, coa denominación de Axencia Estatal de Radiocomunicacións, un organismo público con carácter de organismo autónomo, de acordo co previsto no artigo 43.1.a) da Lei 6/1997, do 14 de abril, de organización e funcionamento da administración xeral do estado, con personalidade xurídico-pública diferenciada e plena capacidade de obrar.

A devandita Axencia adscíbese, a través da Secretaría de Estado de Telecomunicacións e para a Sociedade da Información, ao Ministerio de Ciencia e Tecnoloxía.

Á Axencia, dentro da esfera das súas competencias, correspóndenlle as potestades administrativas para o cumprimento dos seus fins, nos termos que prevea o seu Estatuto e de acordo coa lexislación aplicable.

A Axencia terá por obxecto a execución da xestión do dominio público radioeléctrico no marco das directrices fixadas polo Goberno, o Ministerio de Ciencia e Tecnoloxía e a Secretaría de Estado de Telecomunicacións e para a Sociedade da Información, así como na normativa correspondente.

A Axencia desenvolverá as seguintes funcións :

- a) A proposta de planificación, a xestión e a administración do dominio público radioeléctrico, así como a tramitación e o outorgamento dos títulos habilitantes para a súa utilización, salvo cando se limite o seu número de acordo co previsto no apartado 2 do artigo 44 .
- b) O exercicio das funcións atribuídas á Administración Xeral do Estado en materia de autorización e inspección de instalacións radioeléctricas en relación cos niveis de emisión radioeléctrica permitidos, no ámbito da competencia exclusiva que lle corresponde ao Estado sobre as telecomunicacións, de acordo co artigo 149.1.21ª da Constitución.
- c) A xestión dun rexistro público de radiofrecuencias, accesible a través de internet, no que constarán os titulares de concesións administrativas para o uso privativo do dominio público radioeléctrico.
- d) A elaboración de proxectos e desenvolvemento dos plans técnicos nacionais de radiodifusión e televisión.
- e) A comprobación técnica de emisións radioeléctricas para a identificación, localización e eliminación de interferencias prexudiciais, infraccións, irregularidades e perturbacións dos sistemas de radiocomunicación.

- f) O control e a inspección das telecomunicacións, así como a proposta de incoación de expedientes sancionadores na materia. En materias de competencia do Ministerio de Ciencia e Tecnoloxía ou da Comisión do Mercado de Telecomunicacións, e á súa solicitude, a Axencia Estatal de Radiocomunicacións realizará as funcións de inspección que lle sexan requiridas.
- g) A xestión da asignación dos recursos órbita-espectro para comunicacións por satélite.
- h) A xestión en período voluntario da taxa por reserva do dominio público radioeléctrico establecida na lei.
- i) A elaboración de estudos e informes e, en xeral, o asesoramento da Administración Xeral do Estado en todo o relativo á xestión do dominio público radioeléctrico.
- j) A colaboración coa Secretaría de Estado de Telecomunicacións e para a Sociedade da Información na participación nos organismos internacionais relacionados coa planificación do espectro radioeléctrico.
- k) A elaboración e elevación ao Ministerio de Ciencia e Tecnoloxía dun informe anual sobre a súa actuación.

A Comisión do Mercado das Telecomunicacións é un organismo regulador dos previstos polo artigo 8 da Lei 2/2011, do 4 de marzo, de economía sustentable, dotado de personalidade xurídica propia e plena capacidade pública e privada.

A Comisión do Mercado das Telecomunicacións terá por obxecto o establecemento e supervisión das obrigas específicas que deban cumprir os operadores nos mercados de telecomunicacións e o fomento da competencia nos mercados dos servizos audiovisuais, conforme ao previsto pola súa normativa reguladora, e no apartado 1 do artigo 10 da Lei 2/2011, do 4 de marzo, de economía sustentable, a resolución dos conflitos entre os operadores e, de ser o caso, o exercicio como órgano arbitral das controversias entre os mesmos.

A Comisión do Mercado das Telecomunicacións exercerá as seguintes funcións:

- 1.-Arbitrar nos conflitos que poidan xurdir entre os operadores do sector das comunicacións electrónicas, así como naqueles outros casos que se poidan establecer por vía regulamentaria, cando os interesados o acorden.
- 2.-O exercicio desta función arbitral non terá carácter público. O procedemento arbitral axustarase aos principios esenciais de audiencia, liberdade de proba, contradición e igualdade, e será indispoñible para as partes.
- 3.-Asignar a numeración aos operadores, para o que ditará as resolucións oportunas, en condicións obxectivas, transparentes e non discriminatorias, de acordo co que regulamentariamente se determine. A Comisión velará pola correcta utilización dos recursos públicos de numeración asignados. Así mesmo, autorizará a transmisión dos devanditos recursos, establecendo, mediante resolución, as condicións daquela.
- 4.-Exercer as funcións que en relación co servizo universal e o seu financiamento lle encomende a lei.
- 5.- A resolución vinculante dos conflitos que se susciten entre os operadores en materia de acceso e interconexión de redes, así como en materias relacionadas coas guías telefónicas, o financiamento do servizo universal e o uso compartido de infraestruturas.
- 6.- Adoptar as medidas necesarias para salvagardar a pluralidade de oferta do servizo, o acceso ás redes de comunicacións electrónicas polos operadores, a interconexión das redes e a explotación de rede en condicións de rede aberta, e a política de prezos e comercialización polos prestadores dos servizos.

#### Inspección e réxime sancionador

A función inspectora en materia de telecomunicacións corresponde a:

A Axencia Estatal de Radiocomunicacións.

A Comisión do Mercado das Telecomunicacións.

O Ministerio de Ciencia e Tecnoloxía.

## Responsabilidade polas infraccións en materia de telecomunicacións

A responsabilidade administrativa polas infraccións das normas reguladoras das telecomunicacións será esixible:

- 1.-No caso de incumprimento das condicións establecidas para a explotación de redes ou a prestación de servizos de comunicacións electrónicas, á persoa física ou xurídica que desenvolva a actividade.
- 2.-Nas cometidas con motivo da explotación de redes ou a prestación de servizos sen efectuar a notificación á que se refire o artigo 6 desta lei, á persoa física ou xurídica que realice a actividade ou, subsidiariamente, á que teña a dispoñibilidade dos equipos e instalacións por calquera título xurídico válido en dereito ou carecendo deste.
- 3.-Nas cometidas polos usuarios ou por outras persoas que, sen estaren comprendidas nos parágrafos anteriores, realicen actividades reguladas na normativa sobre telecomunicacións, á persoa física ou xurídica cuxa actuación se atope tipificada polo precepto infrinxido ou á que as normas correspondentes atribúen especificamente a responsabilidade.

Considéranse infraccións moi graves:

- a) A realización de actividades sen título habilitante cando sexa legalmente necesario ou utilizando parámetros técnicos diferentes dos propios do título, e a utilización de potencias de emisión notoriamente superiores ás permitidas ou de frecuencias radioeléctricas sen autorización ou distintas das autorizadas, sempre que, nestes dous últimos casos, se produzan danos graves ás redes ou á prestación dos servizos de comunicacións electrónicas.
- b) O uso, en condicións distintas ás autorizadas, do espectro radioeléctrico que provoque alteracións que impidan a correcta prestación doutros servizos por outros operadores.
- c) O incumprimento grave ou reiterado polos titulares de concesións, afectacións demaniais ou autorizacións para o uso do dominio público radioeléctrico das condicións esenciais que se lles impoñan polo Ministerio de Ciencia e Tecnoloxía.

d) A transmisión total ou parcial de concesións ou autorizacións para o uso privativo do dominio público radioeléctrico, sen cumprir cos requisitos establecidos para ese efecto pola normativa.

e) A produción deliberada de interferencias definidas como prexudiciais segundo a Lei de telecomunicacións, incluídas as causadas por estacións radioeléctricas que estean instaladas ou en funcionamento a bordo dun buque, dunha aeronave ou de calquera outro obxecto flotante ou aerotransportado que transmita emisións desde fóra do territorio español para a súa posible recepción total ou parcial neste.

Considéranse infraccións graves:

a) A realización de actividades sen título habilitante cando sexa legalmente necesario ou utilizando parámetros técnicos diferentes dos propios do título e a utilización de potencias de emisión notoriamente superiores ás permitidas ou de frecuencias radioeléctricas sen autorización ou distintas das autorizadas, sempre que as referidas condutas non constitúan infracción moi grave.

b) A instalación de estacións radioeléctricas sen autorización, cando, de acordo co disposto na normativa reguladora das telecomunicacións, sexa necesaria, ou de estacións radioeléctricas a bordo dun buque, dunha aeronave ou de calquera outro obxecto flotante ou aerotransportado, que, no mar ou fóra del, posibilita a transmisión de emisións desde o exterior para a súa posible recepción total ou parcial en territorio nacional.

c) A mera produción de interferencias definidas como prexudiciais nesta lei que non sexan moi graves.

d) A emisión de sinais de identificación falsas ou enganosas.

e) O uso, en condicións distintas das autorizadas, do espectro radioeléctrico que provoque alteracións que dificulten a correcta prestación doutros servizos por outros operadores.

f) Non atender o requirimento feito pola autoridade competente para o cesamento das emisións radioeléctricas, nos supostos de produción de interferencias.

Considéranse infraccións leves:

A produción de calquera tipo de emisión radioelétrica non autorizada, agás que deba ser considerada como infracción grave ou moi grave.

A mera produción de interferencias cando non deba ser considerada como infracción grave ou moi grave.

Carecer dos preceptivos cadros de tarifas ou de prezos cando a súa exhibición se esixa pola normativa vixente.

Non facilitar os datos requiridos pola Administración ou atrasar inxustificadamente a súa presentación cando resulte esixible conforme ao previsto pola normativa reguladora das comunicacións electrónicas.

Calquera outro incumprimento das obrigas impostas a operadores de redes ou de servizos de comunicacións electrónicas ou dos seus usuarios, previsto nas leis vixentes, salvo que deba ser considerado como infracción grave ou moi grave, conforme ao disposto nos artigos anteriores.

As infraccións reguladas na Lei de telecomunicacións prescribirán, as moi graves, aos tres anos; as graves, aos dous anos, e as leves, aos seis meses.

Autor:

Alfonso García Magariños

Director Asesoría Xurídica Municipal Concello da Coruña

**11. LEXISLACIÓN SOBRE  
PROTECCIÓN DE DATOS.  
NORMATIVA COMUNITARIA. LEI  
ORGÁNICA 15/1999, DE  
PROTECCIÓN DE DATOS DE  
CARÁCTER PERSOAL, REAL  
DECRETO 1720/2007, DO 21 DE  
DECEMBRO, POLO QUE SE  
APROBA O REGULAMENTO DE  
DESENVOLVEMENTO DA DA LEI  
ORGÁNICA 15/1999, DO 13 DE  
DECEMBRO, DE PROTECCIÓN  
DE DATOS DE CARÁCTER  
PERSOAL.**



**Tema 11.- Lexislación sobre protección de datos. Normativa Comunitaria.  
Lei orgánica 15/1999, do 13 de decembro, de protección de datos de  
carácter persoal. Real decreto 1720/2007 polo que se aproba o  
Regulamento de desenvolvemento da Lei orgánica 15/1999, do 13 de  
decembro, de protección de datos de carácter persoal**

**ÍNDICE**

- 11.1 Lexislación sobre protección de datos
- 11.2 Normativa Comunitaria
  - 11.2.1 Xeral
  - 11.2.2 Regulamentos
  - 11.2.3 Directivas
  - 11.2.4 Decisións
  - 11.2.5 Convenios:
- 11.3.- Lei orgánica 15/1999, do 13 de decembro, de protección de datos de carácter persoal
  - 11.3.1 Introducción
  - 11.3.2 Principios
  - 11.3.3 Dereitos
  - 11.3.4 Ficheiros Públicos e Privados
  - 11.3.5 Axencia Protección Datos
- 11.4.- Real decreto 1720/2007 polo que se aproba o Regulamento de desenvolvemento da Lei orgánica 15/1999, do 13 de decembro, de protección de datos de carácter persoal.
  - 11.4.1 Introducción
  - 11.4.2 Análise

## **10.1 LEXISLACION SOBRE PROTECCION DE DATOS.**

Sen prexuízo do desenvolvemento ao longo do tema das normas máis importantes, cómpre destacar:

1.-Constitución Española de 1978.

2.-Lei orgánica 15/1999, do 13 de decembro, de protección de datos de carácter persoal.

3.-Lei 2/2011, do 4 de marzo, de economía sustentable. Modificación da LOPD. Disposición final quincuaxésima sexta.

4.-Real decreto 1720/2007, do 21 de decembro, polo que se aproba o Regulamento de desenvolvemento da Lei orgánica 15/1999, do 13 de decembro, de protección de datos de carácter persoal.

5.-Real decreto 3/2010, do 8 de xaneiro, polo que se regula o Esquema Nacional de Seguridade no ámbito da Administración electrónica (DA.4.<sup>a</sup>)

6.-Real decreto 1665/2008, do 17 de outubro, polo que se modifica o Estatuto da Axencia Española de Protección de Datos, aprobado polo Real decreto 428/1993, do 26 de marzo.

7.-Real decreto 156/1996, do 2 de febreiro, polo que se modifica o Estatuto da Axencia Española de Protección de Datos.

8.-Real Decreto 428/1993, do 26 de marzo, polo que se aproba o Estatuto da Axencia Española de Protección de Datos.

## **11.2 NORMATIVA COMUNITARIA**

### **11.2.1 Xeral**

Na Carta dos dereitos fundamentais da Unión Europea, do 7 de decembro do 2000, o artigo 8 dispón:

*Toda persoa ten dereito á protección dos datos de carácter persoal que lle concirnan.*

*Estes datos trátanse de modo leal, para fins concretos e sobre a base do consentimento da persoa afectada ou en virtude doutro fundamento lexítimo previsto pola lei. Toda persoa ten dereito a acceder aos datos recollidos que lle concirnan e á súa rectificación.*

*O respecto destas normas quedará suxeito ao control dunha autoridade independente.*

Nas versións consolidadas do Tratado da Unión Europea e do Tratado de Funcionamento da Unión Europea, publicadas no Diario Oficial da Unión Europea o 30 de marzo do 2010, recóllense aspectos relacionados coa protección de datos; así no artigo 16 do Tratado de Funcionamento da UE dispónse:

*Toda persoa ten dereito á protección dos datos de carácter persoal que lle concirnan.*

*2. O Parlamento Europeo e o Consello establecerán, conforme ao procedemento legislativo ordinario, as normas sobre protección das persoas físicas respecto do tratamento de datos de carácter persoal polas institucións, órganos e organismos da Unión, así como polos Estados membros no exercicio das actividades comprendidas no ámbito de aplicación do dereito da Unión, e sobre a libre circulación destes datos.*

*O respecto das devanditas normas estará sometido ao control de autoridades independentes.*

*As normas que se adopten en virtude do presente artigo entenderanse sen prexuízo das normas específicas previstas no artigo 39 do Tratado da Unión Europea.*

O artigo 39 do Tratado da Unión Europea establece:

*De conformidade co artigo 16 do Tratado de Funcionamento da Unión Europea, e malia o disposto no seu apartado 2, o Consello adoptará unha decisión que fixe as normas sobre protección das persoas físicas respecto do tratamento de datos de carácter persoal polos Estados membros, no exercicio das actividades comprendidas no ámbito de aplicación do presente capítulo e sobre a libre circulación dos devanditos datos. O respecto das devanditas normas estará sometido ao control de autoridades independentes.*

#### 11.2.2 Regulamentos:

1.- Regulamento do Eurodac, N.º 2725/2000 do Consello do 11 de decembro do 2000 relativo á creación do sistema «Eurodac» para a comparación das impresións dactilares para a aplicación efectiva do Convenio de Dublín; alí créase un sistema denominado «Eurodac» que ten como finalidade axudar a determinar o Estado membro responsable, conforme ao Convenio de Dublín, do exame das solicitudes de asilo presentadas nos Estados membros e, ademais, facilitar a aplicación do Convenio de Dublín nas condicións establecidas no presente regulamento; considérase que as impresións dactilares constitúen un elemento importante para determinar a identidade exacta das devanditas persoas. É necesario crear un sistema para comparar os seus datos dactiloscópicos, considerando estes como datos de carácter persoal.

2.- Regulamento (CE) N.º 45/2001 do Parlamento Europeo e do Consello do 18 de decembro do 2000 relativo á protección das persoas físicas no que respecta ao tratamento de datos persoais; alí establécese que as institucións e os organismos

creados polos Tratados constitutivos das Comunidades comunitarias, “garantirán, de conformidade co presente regulamento, a protección dos dereitos e as liberdades fundamentais das persoas físicas, e en particular o seu dereito á intimidade, no que respecta ao tratamento dos datos persoais, e non limitarán nin prohibirán a libre circulación de datos persoais entre eles ou entre eles e destinatarios suxeitos ao dereito nacional dos Estados membros adoptado en aplicación da Directiva 95/46/CE”.

A autoridade de control independente establecida polo presente regulamento, denominada «Supervisor Europeo de Protección de Datos», supervisará a aplicación das disposicións do presente regulamento a todas as operacións de tratamento realizadas polas institucións e organismos comunitarios.

Enténdese por «datos persoais» toda información sobre unha persoa física identificada ou identificable; considerarase identificable toda persoa cuxa identidade poida determinarse, directa ou indirectamente, en particular, mediante un número de identificación ou un ou varios elementos específicos, característicos da súa identidade física, fisiolóxica, psíquica, económica, cultural ou social;

“tratamento de datos persoais”: calquera operación ou conxunto de operacións, efectuadas ou non mediante procedementos automatizados, aplicadas a datos persoais, como a recollida, rexistro, organización, conservación, adaptación ou modificación, extracción, consulta, utilización, comunicación por transmisión, difusión ou calquera outra forma que permita o acceso aos mesmos, así como a aliñación ou interconexión, e o bloqueo, supresión ou destrución.

As disposicións do regulamento aplicaranse ao tratamento de datos persoais por parte de todas as institucións e organismos comunitarios na medida en que o mencionado tratamento se leve a cabo para o exercicio de actividades que pertencen ao ámbito de aplicación do Dereito comunitario.

Os datos persoais deberán ser:

- a) tratados de maneira leal e lícita;
- b) recollidos con fins determinados, explícitos e lexítimos, e non ser tratados posteriormente de modo incompatible cos devanditos fins; non se considerará incompatible o tratamento posterior de datos con fins históricos, estatísticos ou científicos, a condición de que o responsable do tratamento estableza as garantías oportunas, en particular para asegurar que os datos non serán tratados con outros fins e que non se utilizarán en favor de medidas ou decisións que afecten a persoas concretas;
- c) adecuados, pertinentes e non excesivos con relación aos fins para os que se soliciten e para os que se traten posteriormente;
- d) exactos e, se fose necesario, actualizados; débense tomar todas as medidas razoables para a supresión ou rectificación dos datos inexactos ou incompletos en relación cos fins para os que foron recollidos ou para os que se traten posteriormente;
- e) conservados nunha forma que permita a identificación dos interesados durante un período non superior ao necesario para a consecución dos fins para os que foron recollidos ou para os que se traten posteriormente. A institución ou o organismo comunitario establecerá para os datos persoais que deban ser arquivados por un período máis longo do mencionado para fins históricos, estatísticos ou científicos, que os devanditos datos se arquiven ben unicamente en forma anónima, ou ben, cando iso non sexa posible, só coa identidade codificada do interesado. En calquera caso, deberá imposibilitarse o uso dos datos salvo para fins históricos, estatísticos ou científicos.

3.- Decisión do Consello do 13 de setembro do 2004 pola que se adoptan as normas de desenvolvemento do Regulamento (CE) n.º 45/2001 do Parlamento Europeo e do Consello relativo á protección das persoas físicas no que respecta ao tratamento de

datos persoais polas institucións e os organismos comunitarios e á libre circulación destes datos.

### 11.2.3 Directivas:

1.-Directiva 2009/136/CE do Parlamento Europeo e do Consello, do 25 de novembro do 2009, pola que se modifican a Directiva 2002/22/CE, relativa ao servizo universal e aos dereitos dos usuarios en relación coas redes e os servizos de comunicacións electrónicas; a Directiva 2002/58/CE, relativa ao tratamento dos datos persoais e á protección da intimidade no sector das comunicacións electrónicas, e o Regulamento (CE) n.º 2006/2004 sobre a cooperación en materia de protección dos consumidores.

2.-Directiva 2006/24/CE, do Parlamento Europeo e do Consello do 15 de marzo do 2006, sobre a conservación de datos xerados ou tratados en relación coa prestación de servizos de comunicacións electrónicas de acceso público ou de redes públicas de comunicacións, e pola que se modifica a Directiva 2002/58/CE.

3.-Directiva 2004/82/CE, do Consello do 29 de abril do 2004, sobre a obriga dos transportistas de comunicaren os datos das persoas transportadas.

4.-Directiva 2002/58/CE do Parlamento Europeo e do Consello do 12 de xullo do 2002, relativa ao tratamento dos datos persoais e á protección da intimidade no sector das comunicacións electrónicas (Directiva sobre privacidade e as comunicacións electrónicas).

5.-Directiva 2002/22/CE do Parlamento Europeo e do Consello, do 7 de marzo do 2002, relativa ao servizo universal e aos dereitos dos usuarios en relación coas redes e os servizos de comunicacións electrónicas (Directiva servizo universal).

6.-Directiva 2002/21/CE, do Parlamento Europeo e do Consello do 29 de abril do 2004, sobre a obriga dos transportistas de comunicaren os datos das persoas transportadas.

7.-Directiva 2002/20/CE, do Parlamento Europeo e do Consello, do 7 de marzo do 2002, relativa á autorización de redes e servizos de comunicacións electrónicas (Directiva de autorización).

8.-Directiva 2002/19/CE, do Parlamento Europeo e do Consello, do 7 de marzo do 2002, relativa ao acceso ás redes de comunicacións electrónicas e recursos asociados, e á súa interconexión (Directiva de acceso).

9.-Directiva 2000/31/CE, do Parlamento Europeo e do Consello, do 8 de xuño do 2000, relativa a determinados aspectos xurídicos dos servizos da sociedade da información, en particular o comercio electrónico no mercado interior (Directiva sobre o comercio electrónico).

10.-Directiva 1999/93/CE, do Parlamento Europeo e do Consello, do 13 de decembro de 1999, pola que se establece un marco comunitario para a sinatura electrónica.

11.-Directiva 97/66/CE do Parlamento Europeo e do Consello do 15 de decembro de 1997 relativa ao tratamento dos datos persoais e á protección da intimidade no sector das telecomunicacións. (Derrogada pola Directiva 2002/58/CE).

12.-Directiva 95/46/CE do Parlamento Europeo e do Consello do 24 de outubro de 1995 relativa á protección das persoas físicas no que respecta ao tratamento de datos persoais e á libre circulación destes datos.

#### 11.2.4 Decisións:



1.-Decisión da Comisión do 31 de xaneiro do 2011, de conformidade coa Directiva 95/46/CE do Parlamento Europeo e do Consello, relativa á protección adecuada dos datos persoais polo Estado de Israel no que respecta ao tratamento automatizado dos datos persoais.

2.-Decisión da Comisión do 19 de outubro do 2010, de conformidade coa Directiva 95/46/CE do Parlamento Europeo e do Consello, relativa á adecuada protección dos datos persoais en Andorra.

3.-Decisión da Comisión do 5 de marzo do 2010, conforme á Directiva 95/46/CE do Parlamento Europeo e do Consello, relativa á protección adecuada dada na Lei das Illas Feroe sobre o tratamento de datos persoais.

4.-Decisión da Comisión (2010/87/UE), do 5 de febreiro do 2010, relativa ás cláusulas contractuais tipo para a transferencia de datos persoais aos encargados do tratamento establecidos en terceiros países, de conformidade coa Directiva 95/46/CE do Parlamento Europeo e do Consello.

5.-Decisión da Comisión do 8 de maio do 2008, de conformidade coa Directiva 95/46/CE do Parlamento Europeo e do Consello, relativa á protección adecuada dos datos persoais en Jersey.

6.-Decisión da Comisión do 6 de setembro do 2005, relativa ao carácter adecuado da protección dos datos persoais incluídos nos rexistros de nomes dos pasaxeiros (PNR) que se transfiren á Axencia de Servizos de Fronteiras de Canadá.

7.-Decisión da Comisión do 27 de decembro do 2004, pola que se modifica a Decisión 2001/497/CE no relativo á introdución dun conxunto alternativo de cláusulas contractuais tipo para a transferencia de datos persoais a terceiros países.

8.-Decisión da Comisión do 14 de maio do 2004 relativa ao carácter adecuado da protección dos datos persoais incluídos nos rexistros de nomes dos pasaxeiros que se transfiren ao Servizo de aduanas e protección de fronteiras dos Estados Unidos (Bureau of Customs and Border Protection).

9.-Decisión da Comisión do 29 de abril do 2004 pola que se establece unha lista de organismos cuxos investigadores poden acceder, con fins científicos, a datos confidenciais.

10.-Decisión da Comisión do 28 de abril do 2004 relativa ao carácter adecuado da protección de datos persoais na Illa de Man.

11.-Decisión da Comisión de novembro do 2003, relativa ao carácter adecuado da protección de datos persoais en Guernsey.

12.-Decisión da Comisión do 30 de xuño do 2003, conforme á Directiva 95/46/CE do Parlamento Europeo e do Consello, sobre a adecuación da protección dos datos persoais en Arxentina.

13.-Decisión reguladora da Unidade de Cooperación Xudicial Eurojust.

14.-Decisión 2002/16/CE da Comisión, do 27 de decembro do 2001, relativa a Cláusulas contractuais tipo para a transferencia de datos persoais aos encargados do tratamento establecidos en terceiros países, de conformidade coa Directiva 95/46/CE. (Queda derogada a partir do 15 de maio de 2010).

15.-Decisión da Comisión, do 20 de decembro do 2001, conforme á Directiva 95/46/CE do Parlamento Europeo e do Consello, sobre a adecuación da protección dos datos persoais conferida pola lei canadense Personal Information and Electronic Documents Act.

16.-Decisión 2001/497/CE da Comisión, do 15 de xuño do 2001, relativa a Cláusulas contractuais tipo para a transferencia de datos persoais a un terceiro país previstas na Directiva 95/46/CE.

17.-Decisión da Comisión, do 26 de xullo do 2000, conforme á Directiva 95/46/CE do Parlamento Europeo e do Consello, relativa ao nivel de protección adecuado dos datos persoais en Suíza.

18.-Decisión da Comisión, do 26 de xullo de 2000, conforme á Directiva 95/46/CE do Parlamento Europeo e do Consello, relativa á protección adecuada dos datos persoais en Hungría.

19.-Decisión da Comisión, do 26 de Xullo do 2000, conforme á Directiva 95/46/CE do Parlamento Europeo e do Consello, sobre a adecuación conferida polos principios de porto seguro para a protección da vida privada e as correspondentes preguntas máis frecuentes publicadas polo Departamento de Comercio de Estados Unidos de América.

#### 11.2.5 Convenios:

1.-Convenio de Europol.

2.-Convenio de Schengen.

3.-Convenio do Sistema de Información de Aduanas.

### **11.3 LEI ORGÁNICA 15/1999, DO 13 DE DECEMBRO, DE PROTECCIÓN DE DATOS DE CARÁCTER PERSOAL**

### 11.3.1 Introducción

A lei ten por obxecto garantir e protexer, no que atinxe ao tratamento dos datos persoais, as liberdades públicas e os dereitos fundamentais das persoas físicas, e especialmente o seu honor e intimidade persoal e familiar.

Será de aplicación aos datos de carácter persoal rexistrados en soporte físico que os faga susceptibles de tratamento, e a toda modalidade de uso posterior destes datos polos sectores público e privado.

Para os efectos da Lei orgánica entenderase por:

- a) Datos de carácter persoal: Calquera información relativa a persoas físicas identificadas ou identificables.
- b) Ficheiro: Todo conxunto organizado de datos de carácter persoal, calquera que sexa a forma ou modalidade da súa creación, almacenamento, organización e acceso.
- c) Tratamento de datos: Operacións e procedementos técnicos, de carácter automatizado ou non, que permitan a recollida, gravación, conservación, elaboración, modificación, bloqueo e cancelación, así como as cesións de datos que resulten de comunicacións, consultas, interconexións e transferencias.
- d) Responsable do ficheiro ou tratamento: Persoa física ou xurídica, de natureza pública ou privada, ou órgano administrativo, que decida sobre a finalidade, contido e uso do tratamento.
- e) Afectado ou interesado: Persoa física titular dos datos que sexan obxecto do tratamento a que se refire o apartado c) do presente artigo.
- f) Procedemento de disociación: Todo tratamento de datos persoais, de modo que a información que se obteña non se poida asociar á persoa identificada ou identificable.

- g) Encargado do tratamento: A persoa física ou xurídica, autoridade pública, servizo ou calquera outro organismo que, só ou conxuntamente con outros, trate datos persoais por conta do responsable do tratamento.
- h) Consentimento do interesado: Toda manifestación de vontade, libre, inequívoca, específica e informada, mediante a cal o interesado consinta o tratamento de datos persoais que lle atinxan.
- i) Cesión ou comunicación de datos: Toda revelación de datos realizada a unha persoa distinta do interesado.
- j) Fontes accesibles ao público: Aqueles ficheiros que poden ser consultados por calquera persoa, non impedida por unha norma limitativa, ou sen máis esixencia que, se é o caso, o aboamento dunha contraprestación. Teñen a consideración de fontes de acceso público, exclusivamente, o censo promocional, os repertorios telefónicos nos termos previstos pola súa normativa específica e as listas de persoas pertencentes a grupos de profesionais que conteñan unicamente os datos de nome, título, profesión, actividade, grao académico, enderezo e indicación da súa pertenza ao grupo. Así mesmo, teñen o carácter de fontes de acceso público, os diarios e boletíns oficiais e os medios de comunicación.

### 11.3.2 Principios.

- 1.- Calidade dos datos: os datos de carácter persoal só se poderán recoller para o seu tratamento, así como para sometelos ao devandito tratamento, cando sexan adecuados, pertinentes e non excesivos en relación co ámbito e as finalidades determinadas, explícitas e lexítimas para as que se obtiveron.
- 2.- Dereito de información na recollida de datos: os interesados aos que se lle soliciten datos persoais deberán ser previamente informados de modo expreso, preciso e inequívoco:
  - a) Da existencia dun ficheiro ou tratamento de datos de carácter persoal, da finalidade da recollida destes e dos destinatarios da información.

b) Do carácter obrigatorio ou facultativo da súa resposta ás preguntas que lles sexan formuladas.

c) Das consecuencias da obtención dos datos ou da negativa a subministralos.

d) Da posibilidade de exercitar os dereitos de acceso, rectificación, cancelación e oposición.

e) Da identidade e dirección do responsable do tratamento ou, se é o caso, do seu representante.

3.- Principio do consentimento do afectado: o tratamento dos datos de carácter persoal requirirá o consentimento inequívoco do afectado, agás que a lei dispoña outra cousa.

4.- Comunicación de datos: os datos de carácter persoal obxecto do tratamento só lle poderán ser comunicados a un terceiro para o cumprimento de fins directamente relacionados coas funcións lexítimas do cedente e do cesionario co previo consentimento do interesado.

5.- Deber de segredo: o responsable do ficheiro e quen interveñan en calquera fase do tratamento dos datos de carácter persoal están obrigados ao segredo profesional respecto deles e ao deber de os gardar, obrigas que subsistirán mesmo despois de finalizaren as súas relacións co titular do ficheiro ou, se é o caso, co seu responsable.

6.- Especial protección a determinados datos: ninguén poderá ser obrigado a declarar sobre a súa ideoloxía, relixión ou crenzas.

7.- Seguridade dos datos: O responsable do ficheiro, e, se é o caso, o encargado do tratamento, deberán adoptar as medidas de índole técnica e organizativas necesarias que garantan a seguridade dos datos de carácter persoal e eviten a súa alteración, perda, tratamento ou acceso non autorizado, tendo en conta do estado da tecnoloxía, a natureza dos datos almacenados e os riscos a que están expostos, xa proveñan da acción humana ou do medio físico ou natural.

### 11.3.3 Dereitos das persoas

Os cidadáns teñen dereito a non se veren sometidos a unha decisión con efectos xurídicos, sobre eles ou que o afecte de maneira significativa, que se basee unicamente nun tratamento de datos destinados a avaliar determinados aspectos da súa personalidade.

Cómpre salientar:

1.-Dereito de consulta ao Rexistro Xeral de Protección de Datos: calquera persoa poderá coñecer, recadando para tal fin a información oportuna do Rexistro Xeral de Protección de Datos, a existencia de tratamentos de datos de carácter persoal, as súas finalidades e a identidade do responsable do tratamento. O Rexistro Xeral será de consulta pública e gratuíta.

2.-Dereito de acceso: o interesado terá dereito a solicitar e obter gratuitamente información dos seus datos de carácter persoal sometidos a tratamento, a orixe dos devanditos datos, así como as comunicacións realizadas ou que se prevén facer dos mesmos.

3.-Dereito de rectificación e cancelación. O responsable do tratamento terá a obriga de facer efectivo o dereito de rectificación ou cancelación do interesado no prazo de dez días.

4.-Dereito de tutela: as actuacións contrarias ao disposto nesta lei poden ser obxecto de reclamación polos interesados ante a Axencia Española de Protección de Datos.

5.- Dereito a indemnización. Os interesados que, como consecuencia do incumprimento do disposto na presente lei polo responsable ou o encargado do

tratamento, sufran dano ou lesión nos seus bens ou dereitos terán dereito a ser indemnizados.

#### 11.3.4 Ficheiros Públicos e Privados.

A creación, modificación ou supresión dos ficheiros das administracións públicas só se poderán facer por medio de disposición xeral publicada no «Boletín Oficial do Estado» ou diario oficial correspondente.

As disposicións de creación ou de modificación de ficheiros deberán indicar:

- a. A finalidade do ficheiro e os usos previstos para o el.
- b.- As persoas ou colectivos sobre os que se pretenda obter datos de carácter persoal ou que resulten obrigados a subministralos.
- b. O procedemento de recollida dos datos de carácter persoal.
- c. A estrutura básica do ficheiro e a descrición dos tipos de datos de carácter persoal incluídos nel.
- d. As cesións de datos de carácter persoal e, se é o caso, as transferencias de datos que se prevexan a países terceiros.
- e. Os órganos das administracións responsables do ficheiro.
- f. Os servizos ou unidades ante os que se puidesen exercer os dereitos de acceso, rectificación, cancelación e oposición.



g. As medidas de seguridade con indicación do nivel básico, medio ou alto exixible.

Poderán crearse ficheiros de titularidade privada que conteñan datos de carácter persoal cando resulte necesario para o logro da actividade ou obxecto lexítimos da persoa, empresa ou entidade titular e se respecten as garantías que esta lei establece para a protección das persoas.

Toda persoa ou entidade que proceda á creación de ficheiros de datos de carácter persoal notificarallo previamente á Axencia Española de Protección de Datos.

Entre os extremos que debe conter a notificación, figurarán necesariamente o responsable do ficheiro, a súa finalidade mesmo, a súa localización, o tipo de datos de carácter persoal que contén, as medidas de seguridade, con indicación do nivel básico, medio ou alto exixible e as cesións de datos de carácter persoal que se prevexan realizar e, se é o caso, as transferencias de datos que se prevexan a países terceiros.

Deberánselle comunicar á Axencia Española de Protección de Datos os cambios que se produzan na finalidade do ficheiro automatizado, no seu responsable e na dirección da súa localización.

O Rexistro Xeral de Protección de Datos inscribirá o ficheiro se a notificación se axusta aos requisitos esixibles.

En caso contrario poderá pedir que se completen os datos que falten ou se proceda á súa emenda.

Transcorrido un mes desde a presentación da solicitude de inscrición sen que a Axencia Española de Protección de Datos resolverse sobre ela, entenderase inscrito o ficheiro automatizado para todos os efectos.

#### 11.3.5 Axencia Protección Datos

A Axencia Española de Protección de Datos é un ente de dereito público, con personalidade xurídica propia e plena capacidade pública e privada, que actúa con plena independencia das administracións públicas no exercicio das súas funcións.

Son funcións da Axencia Española de Protección de Datos:

1.-Velar polo cumprimento da lexislación sobre protección de datos e controlar a súa aplicación, en especial no relativo aos dereitos de información, acceso, rectificación, oposición e cancelación de datos.

2.-Emitir as autorizacións previstas na lei ou nas súas disposicións regulamentarias.

3.-Ditar, se é o caso, e sen prexuízo das competencias doutros órganos, as instrucións precisas para adecuar os tratamentos aos principios da lei.

4.-Atender as peticións e reclamacións formuladas polas persoas afectadas.

5.-Proporcionar información ás persoas sobre os seus dereitos en materia de tratamento dos datos de carácter persoal.

6.-Requirir os responsables e os encargados dos tratamentos, logo de audiencia destes, para adoptaren as medidas necesarias para a adecuación do tratamento de datos ás disposicións desta lei e, se é o caso, ordenar a cesación dos tratamentos e a cancelación dos ficheiros, cando non se axuste ás súas disposicións.

7.-Exercer a potestade sancionadora nos termos previstos pola Lei orgánica de protección de datos.

8.-Informar, con carácter preceptivo, dos proxectos de disposicións xerais que desenvolvan esta lei.

9.-Solicitar dos responsables dos ficheiros tanta axuda e información estime necesaria para o desempeño das súas funcións.

10.-Velar pola publicidade da existencia dos ficheiros de datos con carácter persoal, a cuxo efecto publicará periodicamente unha relación dos devanditos ficheiros coa información adicional que o director da Axencia determine.

11.-Redactar unha memoria anual e remitirla ao Ministerio de Xustiza.

12.-Exercer o control e adoptar as autorizacións que procedan en relación cos movementos internacionais de datos, así como desempeñar as funcións de cooperación internacional en materia de protección de datos persoais.

13.-Velar polo cumprimento das disposicións que a Lei da función estatística pública establece respecto da recollida de datos estatísticos e do segredo estatístico, así como ditar as instrucións precisas, ditaminar sobre as condicións de seguridade dos ficheiros constituídos con fins exclusivamente estatísticos.

As resolucións da Axencia Española de Protección de Datos faranse públicas unha vez sexan notificadas aos interesados. A publicación realizarase preferentemente a través de medios informáticos ou telemáticos.

#### 11.3.6 Infraccións e Sancións.

Os responsables dos ficheiros e os encargados dos tratamentos estarán suxeitos ao réxime sancionador establecido na presente lei.

As infraccións cualificaranse como leves, graves ou moi graves.

Son infraccións leves:

- 1.-Non remitirles á Axencia Española de Protección de Datos as notificacións previstas nesta lei ou nas súas disposicións de desenvolvemento.
- 2.-Non solicitar a inscrición do ficheiro de datos de carácter persoal no Rexistro Xeral de Protección de Datos.
- 3.-O incumprimento do deber de información ao afectado sobre o tratamento dos seus datos de carácter persoal cando os datos sexan solicitados polo propio interesado.
- 4.-A transmisión dos datos a un encargado do tratamento sen dar cumprimento aos deberes formais establecidos na lei.

Son infraccións graves:

- 1.-Proceder á creación de ficheiros de titularidade pública ou iniciar a recollida de datos de carácter persoal para eles, sen autorización de disposición xeral, publicada no «Boletín Oficial do Estado» ou no diario oficial correspondente.
- 2.-Tratar datos de carácter persoal sen solicitar o consentimento das persoas afectadas, cando este sexa necesario conforme ao disposto na lei e nas súas disposicións de desenvolvemento.

3.-Tratar datos de carácter persoal ou usalos posteriormente con conculcación dos principios e garantías establecidos nesta lei e nas disposicións que a desenvolven, agás cando sexa constitutivo de infracción moi grave.

4.-A vulneración do deber de gardar segredo sobre o tratamento dos datos de carácter persoal.

5.-O impedimento ou a obstaculización do exercicio dos dereitos de acceso, rectificación, cancelación e oposición.

6.-O incumprimento do deber de información ao afectado sobre o tratamento dos seus datos de carácter persoal cando os datos sexan solicitados polo propio interesado.

7.-O incumprimento dos restantes deberes de notificación ou requirimento ao afectado.

8.-Manter os ficheiros, locais, programas ou equipos que conteñan datos de carácter persoal sen as debidas condicións de seguridade que por vía regulamentaria se determinen.

9.-Non atender aos requirimentos ou apercibimentos da Axencia Española de Protección de Datos ou non lle proporcionar a aquela cantos documentos e informacións sexan solicitados por ela.

10.-A obstrución ao exercicio da función inspectora.

11.-A comunicación ou cesión dos datos de carácter persoal sen contar con lexitimación para isto, agás que a mesma sexa constitutiva de infracción moi grave.

Son infraccións moi graves:

- 1.-A recollida de datos en forma enganosa ou fraudulenta.
- 2.-Tratar ou ceder os datos de carácter persoal especialmente protexidos (ideoloxía, afiliación sindical, relixión e crenzas, orixe racial, a saúde e a vida sexual, comisión de infraccións penais ou administrativas).
- 3.-Non cesar no tratamento ilícito de datos de carácter persoal cando existise un previo requirimento para iso do director da Axencia Española de Protección de Datos.
- 4.-A transferencia internacional de datos de carácter persoal con destino a países que non proporcionen un nivel de protección equiparable sen autorización do director da Axencia Española de Protección de Datos, salvo nos supostos nos que a devandita autorización non resulta necesaria.

Tipo de sancións.

As infraccións leves serán sancionadas con multa de 900 a 40.000 euros.

As infraccións graves serán sancionadas con multa de 40.001 a 300.000 euros.

As infraccións moi graves serán sancionadas con multa de 300.001 a 600.000 euros.

A contía das sancións graduarase atendendo aos seguintes criterios:

- a.-O carácter continuado da infracción.
- b.-O volume dos tratamentos efectuados.

c.-A vinculación da actividade do infractor coa realización de tratamentos de datos de carácter persoal.

d.-O volume de negocio ou actividade do infractor.

e.-Os beneficios obtidos como consecuencia da comisión da infracción.

f.-O grao de intencionalidade.

g.-A reincidencia por comisión de infraccións da mesma natureza.

h.-A natureza dos prexuízos causados ás persoas interesadas ou a terceiras persoas.

i.-A acreditación de que con anterioridade aos feitos constitutivos de infracción a entidade imputada tiña implantados procedementos adecuados de actuación na recollida e tratamento dos datos de carácter persoal, sendo a infracción consecuencia dunha anomalía no funcionamento dos devanditos procedementos non debida a unha falta de dilixencia esixible ao infractor.

j.-Calquera outra circunstancia que sexa relevante para determinar o grao de antixuridicidade e de culpabilidade presentes na concreta actuación infractora.

## **11.4 Real Decreto 1720/2007 polo que se aproba o Regulamento de desenvolvemento da Lei orgánica 15/1999, do 13 de decembro, de Protección de Datos de Carácter Persoal**

### **11.4.1 Introducción**

A Lei Orgánica 15/1999, do 13 de decembro, de protección de datos de carácter persoal adaptou o noso ordenamento ao disposto pola Directiva 95/46/CE do Parlamento Europeo e do Consello, do 24 de outubro de 1995, relativa á protección das persoas físicas no que respecta ao tratamento de datos persoais e á libre circulación destes datos, e derogou, pola súa vez, a ata entón vixente Lei orgánica 5/1992, do 29 de outubro, de regulación do tratamento automatizado de datos de carácter persoal.

O regulamento comparte coa lei orgánica a finalidade de facer fronte aos riscos que para os dereitos da personalidade poden supoñer a captación e tratamento de datos persoais. Por iso, cómpre destacar que esta norma regulamentaria nace coa vocación de non reiterar os contidos da norma superior e de desenvolver non só os mandatos contidos na lei orgánica de acordo cos principios que emanan da directiva, senón tamén aqueles que nestes anos de vixencia da lei se demostrou que precisan dun maior desenvolvemento normativo.

O regulamento parte da necesidade de dotar de coherencia á regulación regulamentaria en todo o relacionado coa transposición da directiva e de desenvolver os novos aspectos da Lei orgánica 15/1999, xunto con aqueles en que a experiencia aconsellou un certo de grao de precisión que dote de seguridade xurídica ao sistema.

#### 11.4.2 Análise

O título I contempla o obxecto e ámbito de aplicación do regulamento. Ao longo da vixencia da Lei orgánica 15/1999, advertiuse a conveniencia de aclarar qué se entende por ficheiros e tratamentos relacionados con actividades persoais ou domésticas, aspecto moi relevante, dado que está excluído da normativa sobre protección de datos de carácter persoal.



Achégase un conxunto de definicións que axudan ao correcto entendemento da norma, o que resulta particularmente necesario nun ámbito tan tecnificado como o da protección de datos persoais. Por outra banda, fixa o criterio a seguir en materia de cómputo de prazos co fin de homoxeneizar esta cuestión evitando distincións que supoñen diferenzas de trato dos ficheiros públicos respecto dos privados.

O título II refírese aos principios da protección de datos. Reviste particular importancia a regulación do modo de captación do consentimento atendendo a aspectos moi específicos, como o caso dos servizos de comunicacións electrónicas e, moi particularmente, a captación de datos dos menores. Así mesmo, ofrécese o que non se pode definir senón como un estatuto do encargado do tratamento, que, sen dúbida contribuirá a clarificar todo o relacionado con esta figura. As previsións neste ámbito complétanse co disposto no título VIII en materia de seguridade, dotando dun marco coherente a actuación do encargado.

O título III ocúpase dunha cuestión tan esencial como os dereitos das persoas neste ámbito. Estes dereitos de acceso, rectificación, cancelación e oposición ao tratamento, segundo afirmou o Tribunal Constitucional na súa Sentenza número 292/2000, constitúen o grupo de facultades que emanan do dereito fundamental á protección de datos e serven á capital función que desempeña este dereito fundamental: garantirle á persoa un poder de control sobre os seus datos persoais, o que só é posible e efectivo impoñéndolles a terceiros os mencionados deberes de facer.

A continuación, os títulos IV a VII permiten clarificar aspectos importantes para o tráfico ordinario, como a aplicación de criterios específicos a determinado tipo de ficheiros de titularidade privada que pola súa transcendencia o requirían —os relativos á solvencia patrimonial e crédito e os utilizados en actividades de publicidade e prospección comercial—, o conxunto de obrigas materiais e formais que deben conducir aos responsables á creación e inscrición dos ficheiros, os

criterios e procedementos para a realización das transferencias internacionais de datos, e, finalmente, a regulación dun instrumento, o código tipo, chamado a representar cada vez un papel máis relevante como elemento dinamizador do dereito fundamental á protección de datos.

O título VIII regula un aspecto esencial para a tutela do dereito fundamental á protección de datos, a seguranza, que repercute sobre múltiples aspectos organizativos, de xestión e mesmo de investimento, en todas as organizacións que traten datos persoais. A repercusión do deber de seguranza obrigaba a un particular rigor, xa que nesta materia teñen confluído distintos elementos moi relevantes. Por unha parte, a experiencia dimanante da aplicación do Real decreto 994/1999 permitía coñecer as dificultades que enfrontaran os responsables e identificar os puntos débiles e fortes da regulación. Por outra, reclamábase a adaptación da regulación en distintos aspectos. Neste sentido, o regulamento trata de ser particularmente rigoroso na atribución dos niveis de seguridade, na fixación das medidas que corresponda adoptar en cada caso e na revisión destas cando iso resulte necesario. Por outra banda, ordena con maior precisión o contido e as obrigas vinculadas ao mantemento do documento de seguridade. Ademais, pretendeuse regular a materia de modo que prevexa as múltiples formas de organización material e persoal da seguranza que se dan na práctica. Por último, régúlase un conxunto de medidas destinadas aos ficheiros e tratamentos estruturados e non automatizados que lles ofrezca aos responsables un marco claro de actuación.

Finalmente, no título IX, dedicado aos procedementos tramitados pola Axencia Española de Protección de Datos, optouse por normativizar exclusivamente aquelas especialidades que diferencian os distintos procedementos tramitados pola Axencia das normas xerais previstas para os procedementos na Lei 30/1992, do 26 de novembro, de réxime xurídico das administracións públicas e do procedemento

administrativo común, cuxa aplicación se declara supletoria deste presente regulamento.

Autor:

Alfonso García Magariños

Director Asesoría Xurídica Municipal Concello da Coruña

**12. PLAN DIRECTOR DE  
SEGURIDADE DE  
INFORMACIÓN DA XUNTA DE  
GALICIA. DECRETO 230/2008,  
POLO QUE SE ESTABLECEN AS  
NORMAS DE BOAS PRÁCTICAS  
NA UTILIZACIÓN DOS  
SISTEMAS DE INFORMACIÓN  
DA ADMINISTRACIÓN DA  
COMUNIDADE AUTÓNOMA DE  
GALICIA. ADMINISTRACIÓN  
ELECTRÓNICA E SOCIEDADE  
DA INFORMACIÓN.**

**Tema 12.- Plan Director de Seguridade e Información da Xunta de Galicia.  
Decreto 230/2008 polo que se establecen as normas de boas practicas na  
utilización de sistemas de información na Administración da CCAA de  
Galicia.**

**ÍNDICE**

12.1 Plan Director de Seguridade e Información da Xunta de Galicia

- 12.1.1. Introducción
- 12.1.2 Responsabilidades
- 12.1.3 Obxectivos
- 12.1.4 Axentes implicados

12.2 Decreto 230/2008 polo que se establecen as normas de boas practicas na  
utilización de sistemas de información na Administración da CCAA de Galicia.

- 12.2.1 Obxecto e ámbito de aplicación
- 12.2.2 Órganos responsables e de coordinación
- 12.2.3 Acceso a información, redes de comunicacións e Internet
- 12.2.4 Servizo de mensaxería corporativo
- 12.2.5 Deber das persoas usuarias
- 12.2.6 Inspección
- 12.2.7 Responsabilidade das persoas usuarias que teñan a condición de  
empregados públicos

## **12.1 PLAN DIRECTOR DE SEGURIDADE E INFORMACION DA XUNTA DE GALICIA**

### 12.1.1 Introducción

O Plan Director de Seguridade da Información establece as actuacións que debe levar a cabo a Administración da Comunidade Autónoma de Galicia en materia de seguridade da información así como os axentes implicados e as súas respectivas responsabilidades. Ademais, define as directrices necesarias para xestionar de maneira segura os sistemas de información da Administración e manifesta o recoñecemento da importancia que ten a seguridade da información sobre a confianza que os cidadáns depositan na Administración.

As tecnoloxías da información e as comunicacións (TIC) constitúen un instrumento de alto nivel estratéxico polo seu potencial para impulsar a modernización da Administración da Comunidade Autónoma Galega, así como pola súa capacidade para estimular e sustentar o desenvolvemento social e económico de Galicia.

Este plan prevé todos os sistemas de información da Xunta de Galicia. Nace coa vontade de ser aplicado progresivamente ao conxunto das consellerías da Administración autonómica, aos seus organismos autónomos, sociedades públicas, fundacións do sector público autonómico e demais entidades de dereito público vinculadas ou dependentes da Comunidade Autónoma de Galicia. Sen prexuízo do anterior, está directamente destinado a garantir a seguridade dos sistemas corporativos.

Dentro deste plan, correspóndelle á Secretaría Xeral de Modernización e Innovación Tecnolóxica a análise de necesidades, planificación, deseño, xestión e implantación dos sistemas de información e elementos tecnolóxicos nos órganos da Administración de Xustiza en Galicia, en coordinación coas administracións e órganos competentes na materia de sistemas de información de xustiza.

Neste plan tamén se perfilan unha serie de iniciativas orientadas a asesorar e sensibilizar ao persoal da Administración local en materia de protección de datos, de seguridade informática e de acceso electrónico dos cidadáns aos servizos públicos.

O alcance temporal do presente plan abrangue o período 2010-2014. No plan efectúase unha priorización das distintas actuacións no tocante á súa urxencia e impacto. A seguridade da información precisa unha visión global que recolla unha mellora pragmática e accesible a curto prazo e, á vez, un modelo obxectivo ambicioso e de longo prazo.

#### 12.1.2 Responsabilidades

Á Secretaría Xeral de Modernización e Innovación Tecnolóxica, segundo o Decreto 325/2009, do 18 de xuño, de estrutura orgánica dos órganos superiores dependentes da Presidencia da Xunta de Galicia, correspóndelle establecer a política de seguridade informática corporativa da Xunta de Galicia e a promoción de boas prácticas no relativo ao tratamento de datos de carácter persoal. A través do Centro de Seguridade da Información (CSI), elaborará os plans, medidas e directrices de seguridade informática, supervisará o cumprimento de todas as medidas de seguridade informática nos diferentes ámbitos e departamentos e deseñará e realizará as accións encamiñadas a garantir o cumprimento da normativa vixente en materia de Protección de Datos de Carácter Persoal na Administración da Comunidade Autónoma.

As consellerías da Administración da Comunidade Autónoma de Galicia, segundo o Decreto 230/2008, do 18 de setembro, polo que se establecen as normas de boas prácticas na utilización dos sistemas de información da Administración da Comunidade Autónoma de Galicia designarán o órgano que será responsable dos sistemas de información da súa propiedade e de establecer os medios tecnolóxicos que necesitan as persoas ao seu servizo, así como de velar polo correcto funcionamento das infraestruturas e do equipamento informático e de comunicacións de que dispoñan. Cando estas atribucións non estean asignadas regulamentariamente a un órgano, a designación farase polas secretarías xerais de cada departamento. Así mesmo, cada departamento da Xunta de Galicia deberá designar unha persoa como responsable de seguridade.

O Comité de Seguridade dos Sistemas de Información (CSSI), creado no Decreto de boas prácticas, é un órgano colexiado formado polas persoas responsables de seguridade dos distintos departamentos da Xunta de Galicia que ten como obxectivo definir a política de seguridade corporativa. Este comité estará coordinado e asesorado polo órgano competente en materia de seguridade corporativa a través do Centro de seguridade da Información.

As persoas que prestan servizos á Administración da Comunidade Autónoma de Galicia, ademais de cumpriren coas medidas indicadas no Decreto de boas prácticas, teñen o deber de sigilo e confidencialidade respecto da información á que poidan ter acceso por razón das súas funcións, limitándose a empregala para o estrito cumprimento das tarefas encomendadas.

A Xunta de Galicia expresa o seu compromiso coa seguridade, de forma que dará a coñecer este Plan Director de Seguridade entre todo o persoal que preste os seus servizos na Administración da Comunidade Autónoma, velará polo seu cumprimento e impulsará a implantación e difusión da xestión da seguridade da información nas persoas e empresas de Galicia.



### 12.1.3 Obxectivos

O presente plan trata de mellorar o nivel de seguridade existente na Administración da Comunidade Autónoma de Galicia. Isto significa xestionar a seguridade da información de tal forma que as medidas de seguridade implantadas acaden un alto grao de efectividade que reduza ao máximo o impacto das incidencias de seguridade.

Con este fin, a Xunta de Galicia fíxase, en materia de seguridade da información, os seguintes obxectivos:

- . Concienciar e implicar na xestión da seguridade a toda a dirección e persoal da Administración autonómica, aos seus organismos autónomos, sociedades públicas, fundacións do sector público autonómico e demais entidades de dereito público vinculadas ou dependentes da Comunidade Autónoma de Galicia, contando coa colaboración de provedores e especialistas.
- . Promover o máximo aproveitamento das tecnoloxías da información e as comunicacións na actividade administrativa e asegurar asemade o respecto das garantías e dereitos dos cidadáns nas súas relacións coa Administración, establecendo que a seguridade nos sistemas sexa atendida, revisada e auditada por persoal cualificado e que a súa configuración e deseño garantan a seguridade por defecto.
- . Xestionar os riscos que poidan afectar aos compoñentes dos sistemas de información para poder identificalos e avalialos e tomar as medidas de seguridade informática axeitadas (físicas, lóxicas, técnicas, normativas e organizativas).
- . Garantir a dispoñibilidade dos sistemas de información de acordo cos requisitos establecidos para os servizos prestados, xestionando e controlando o acceso físico e lóxico; certificando que os produtos de seguridade usados para lle dar servizo ao cidadán cumpren cos estándares establecidos; revisando o nivel de actualización;

asegurando a confidencialidade da información xestionada pola Administración e evitando accesos ou alteracións indebidas e perdas de información; implantando a seguridade perimetral necesaria ante os posibles riscos de interconexión con outros sistemas de redes externas, e rexistrando toda actividade dos usuarios que accedan ao sistema.

- . Xestionar a continuidade dos servizos TIC proporcionados pola Administración establecendo os sistemas de protección a nivel organizativo, lóxico e físico que permitan reducir a probabilidade de que se produza un incidente e, no caso de que se produza, acurtar o tempo de volta á normalidade e minimizar o seu impacto.

- . Avaliar periodicamente o sistema de xestión de seguridade baseándose no rexistro e tratamento de incidencias, garantindo que as medidas implantadas alcancen un nivel de madurez optimizado con políticas, normas, procedementos e estruturas organizacionais que promovan a concienciación e formación continua dos usuarios en temas de seguridade da información.

- . Proporcionar un ambiente de seguridade que garanta o cumprimento dos requisitos legais para a validez e eficacia dos procedementos administrativos que utilicen os medios electrónicos, informáticos e telemáticos, establecendo para cada sistema de información responsables diferenciados da información, do servizo e da seguridade.

- . A Xunta de Galicia actuará como elemento xerador de e-confianza que promova un tecido empresarial sólido en seguridade da información e incremente a confianza e a protección dos dereitos da cidadanía galega na Sociedade da información.

#### 12.1.4 Axentes implicados

1.- Subdirección Xeral de Calidade, interoperabilidade e seguridade (SXCIS).  
A Subdirección Xeral de Calidade, Interoperabilidade e Seguridade (SXCIS) da SXMIT

ten, entre as súas funcións, a de establecer a política de seguridade informática corporativa da Xunta de Galicia e a de promover as boas prácticas no relativo ao tratamento de datos de carácter persoal.

Para iso, creouse, dentro da SXCIS, o Servizo de Calidade e Seguridade Informática coas seguintes competencias en materia de seguridade da información:

- . Dirección das políticas corporativas de seguridade informática da Xunta de Galicia a través do Centro de Seguridade da Información.
- . Elaboración dos plans, medidas e directrices de seguridade informática para o conxunto de órganos e unidades da Xunta.
- . Supervisión do cumprimento de todas as medidas de seguridade informática nos distintos ámbitos e departamentos da Xunta.
- . Deseño e realización de accións encamiñadas a garantir o cumprimento da normativa vixente en materia de protección de datos de carácter persoal na Administración da Comunidade Autónoma de Galicia.

## 2.- Centro de Seguridade da Información (CSI)

O Centro de Seguridade da Información ten unha función transversal dentro da Xunta. Entre as súas atribucións están a resolución de incidencias de seguridade e o asesoramento ás distintas consellerías en materia de seguridade da información, tanto en materia de protección de datos coma na avaliación de solucións de seguridade.

O CSI supervisará a seguridade dos sistemas corporativos da Administración da Comunidade Autónoma de Galicia e será o centro de resolución de incidentes de

seguridade (ataques activos e pasivos, perda de información, falta de dispoñibilidade, etc.).

Dentro dos servizos de apoio e asesoramento ás distintas consellerías no seu cometido de adecuación dos seus sistemas de información ás esixencias da lexislación vixente en materia de protección de datos, o Centro de Seguridade da Información será o interlocutor coa Axencia Española de Protección de Datos.

O Centro de Seguridade da Información encargárase de avaliar, analizar e probar nun contorno controlado as distintas solucións de seguridade existentes no mercado e de aplicación e interese para a Administración da Comunidade Autónoma de Galicia. Os resultados destas avaliacións reflectiránse nunha serie de informes de análises e de estudos comparativos. Así mesmo, poderán realizarse demostracións ás consellerías, xa sexa a través do contorno de probas ou mediante charlas divulgativas. Estas avaliacións poderán realizarse en función das necesidades detectadas polo propio Centro de Seguridade da Información ou en función da valoración de peticións dos distintos departamentos e poderán referirse á seguridade perimetral, de centros de proceso de datos, de aplicacións, de posto informático, etc.

Co fin de promover o desenvolvemento do presente Plan nas diferentes consellerías, incluíranse dentro das funcións do CSI, as seguintes tarefas:

- . Realizar o seguimento e revisar o presente Plan Director de forma periódica.
- . Apoiar e asesorar ás consellerías para que alcancen os obxectivos fixados no presente plan.
- . Impulsar e apoiar o Comité de Seguridade dos Sistemas de Información da Xunta.
- . Velar pola mellora do nivel de seguridade da información da Administración da Comunidade Autónoma de Galicia.

Para o desenvolvemento destas funcións o Centro de Seguridade da Información

dispón dun amplo coñecemento no campo da seguridade da información e poderá contar co asesoramento de expertos externos.

### 3.- Consellerías da Xunta

As consellerías son as máximas responsables do estado de seguridade dos seus sistemas de información. Deberán velar pola súa seguridade garantindo a confidencialidade, integridade e dispoñibilidade da información. Son tamén as responsables de acometeren as actuacións recomendadas no presente Plan Director e acadar os obxectivos marcados.

Dentro de cada consellería, o persoal de soporte técnico desempeñará funcións de asesoría técnica, execución, proposta, coordinación e supervisión dos plans de informatización.

Así mesmo, os órganos responsables dos sistemas de información de cada departamento da Xunta de Galicia, co apoio do persoal de soporte técnico, serán os competentes para velar polo cumprimento dos obxectivos deste plan. Correspóndelles a eles asegurarse de que os equipos se utilizan adecuadamente e atendendo á finalidade á que están destinados.

### 4.- Comité de seguridade dos sistemas de información (CSSI).

O Comité de Seguridade dos Sistemas de Información ten como obxectivo establecer o marco de traballo que impulse a implantación e difusión da xestión da seguridade da información no ámbito da Administración da Comunidade Autónoma de Galicia.

Os membros do Comité reúnense para revisar o estado da seguridade da información na Administración da Comunidade Autónoma de Galicia, aprobar as políticas de seguridade, revisar e aprobar os proxectos de seguridade, revisar os procesos de

monitorización das incidencias de seguridade e realizar outras tarefas de xestión da seguridade de alto nivel que sexan necesarias.

As principais funcións asumidas por este Comité son as que se presentan a continuación:

.Identificar, revisar e propoñer obxectivos estratéxicos en materia de seguridade da información.

. Establecer roles e responsabilidades en materia de seguridade da información.

. Propoñer e aprobar políticas, normas e directrices de seguridade da información para a Xunta de Galicia e velar polo seu cumprimento.

. Proporcionar apoio ao esforzo de seguridade da información, dando unha visión máis transversal para a análise e toma de decisións, a fin de lograr a mellor relación custo-efectividade na súa xestión.

. Constituír a canle primaria de discusión de aspectos de seguridade da información que se deban abordar na Administración da Comunidade Autónoma de Galicia.

. Apoiar os coordinadores de seguridade no desenvolvemento de estratexias de mitigación de riscos, baseándose no coñecemento que os seus integrantes teñen das súas respectivas áreas.

. Impulsar a implantación e difusión da xestión da seguridade da información.

. Revisar e aprobar anualmente a Política de Seguridade.

. Realizar outras tarefas de xestión da seguridade de alto nivel que sexan necesarias.

. Revisar periodicamente o presente Plan Director.

Para o desenvolvemento destas funcións, o CSSI poderá contar co apoio, en materia de actualización normativa, da Asesoría Xurídica Xeral. Puntualmente, poderá solicitar a colaboración da Xunta Consultiva de Contratación Administrativa da Xunta de Galicia e do equipo de auditores e analistas de xestión do rendemento e calidade formal da Dirección Xeral de Avaliación e Reforma Administrativa da Consellería de Presidencia, Administracións Públicas e Xustiza.

## 5.- Asesoría Xurídica Xeral

O papel do dereito nas tecnoloxías da información é amplo e abarca varios campos, como poden ser os que enunciámos deseguido:

- . Protección de datos de carácter persoal.
- . Propiedade intelectual.
- . Servizos da sociedade da información.
- . Sinatura electrónica.
- . Constitución de proba por medios informáticos.
- . Uso de ferramentas informáticas polo persoal.

A Asesoría Xurídica Xeral ofrecerá ao Comité de Seguridade dos Sistemas de Información o seu coñecemento no ámbito legal como apoio á actualización normativa mediante a emisión de ditames ou informes en dereito, a formulación de criterios xerais de asesoramento xurídico e o estudo dos proxectos de regulamentos con exame da súa adecuación ao ordenamento constitucional, estatutario e legal.

Polo seu coñecemento en materias xurídicas vinculadas ao dereito das tecnoloxías da información, asegurará que as iniciativas do Comité de Seguridade dos Sistemas de Información e da Secretaría Xeral competente sexan acordes á lexislación vixente aplicable. Por outra banda, a Asesoría Xurídica de cada consellería ha prestarlle un servizo de apoio nas materias anteriormente mencionadas.

## 6.- Xunta Consultiva de Contratación Administrativa

A Xunta Consultiva de Contratación Administrativa da Comunidade Autónoma de Galicia está adscrita á consellería responsable dos asuntos tributarios como un órgano consultivo específico en materia de contratación administrativa.

Dentro das funcións e competencias da Xunta, están:

:. Elaborar e propoñer as normas, instrucións e medidas que considere precisas para a mellora e eficacia da contratación da Administración autonómica, os seus organismos e sociedades, fundacións do sector público e demais entidades de dereito público dela dependentes.

. Realizar estudos e investigacións sobre contratación administrativa, trasladándolles aos órganos de contratación as recomendacións que se deriven daquela.

A Xunta de Galicia recorre a provedores para a prestación de servizos como poden ser o desenvolvemento de novas aplicacións, infraestruturas, ou a externalización dunha actividade.

É importante para garantir a seguridade da información xestionar a actuación dos provedores. Por iso é necesario identificar os requisitos de seguridade vinculados á prestación do servizo e incluílos nos contratos.

Xa que logo, a Xunta Consultiva de Contratación Administrativa trasladará aos órganos de contratación todas as recomendacións que considere oportunas para que se inclúan cláusulas sobre dispoñibilidade, confidencialidade, integridade e autenticidade da información manexada polos sistemas de información.

Coa finalidade de asegurar este aspecto, exercerá unha función de análise e proposta de inclusión nos pregos de contratación de cláusulas ambientais, sociais, de comercio xusto e de protección de datos que os adxudicatarios deberán cumprir en función do servizo contratado.

## 7. Equipo de auditores e analistas de xestión do rendemento e calidade



O equipo de auditores e analistas de xestión do rendemento e calidade formal da Dirección Xeral de Avaliación e Reforma Administrativa da Consellería de Presidencia, Administracións Públicas e Xustiza.

Esta Dirección ten, entre outras, as seguintes competencias:

. En materia de avaliación do rendemento e xestión da calidade:

1.-O desenvolvemento e a xestión das medidas para a implantación de sistemas de mellora da calidade tendendo a promover a mellora continua dos servizos da Administración autonómica, tanto dos que se lle prestan directamente ao cidadán coma dos servizos internos.

. En materia de racionalización e simplificación de procedementos administrativos:

1.-Coordinar a aplicación da normativa europea e estatal sobre simplificación e mellora da xestión administrativa.

. En materia de información administrativa e atención ao cidadán:

1.-Avaliar periodicamente a calidade do sistema de información administrativa, propoñendo as medidas de melloras convenientes co fin de lles facilitar aos cidadáns e usuarios os servizos que solicitan.

2.- Tramitar, sen prexuízo das competencias que lles corresponden ás secretarías xerais e en colaboración con estas, as queixas e as propostas que formulen os cidadáns e usuarios sobre o funcionamento dos servizos prestados pola Administración autonómica de acordo co establecido nos artigos 25 e seguintes do Decreto 164/2005, do 16 de xuño.

Entre os principios de protección de datos están o principio de información e o principio de consentimento. O principio de información, que se regula no artigo 5 da LOPD, establece que o interesado debe estar informado no momento da recollida de datos. Tocante ao principio de consentimento esixe que se obteña o consentimento do afectado para o tratamento dos datos, agás excepcións recollidas na LOPD. Estes

dereitos fundamentais deben garantirse non só para cumprir coa lexislación vixente senón tamén para garantir a calidade do servizo prestado ao cidadán.

Os procedementos administrativos son uns dos puntos nos que é necesario prestar atención, tendo en conta que recollen, a miúdo, datos de carácter persoal.

Cando a recollida de datos se realiza mediante formulario, ben sexa en formato papel ou en formato electrónico, introducirase unha cláusula informativa no formulario que cubra as esixencias do artigo 5 da Lei orgánica de protección datos. Con respecto ao consentimento recollerase mediante a sinatura do formulario papel e a aprobación do formulario electrónico.

O equipo revisa os procedementos administrativos antes da súa publicación no DOG.

## 12.2 DECRETO 230/2008 DO 18 DE SETEMBRO POLO QUE SE ESTABLECEN BOAS PRACTICAS

### 12.2.1 Obxecto e ámbito de aplicación

Este decreto ten por obxecto regular as normas de utilización dos sistemas de información e de comunicacións, fixos e móbiles, dos que dispón a Administración da Comunidade Autónoma de Galicia, establecendo os dereitos e os deberes das persoas usuarias destes sistemas no relativo á súa seguridade e bo uso.

A finalidade da presente norma é conseguir o mellor aproveitamento das tecnoloxías da información e as comunicacións na actividade administrativa, así como garantir a protección da información das persoas e das empresas nas súas relacións coa Administración da Comunidade Autónoma de Galicia.

Será de aplicación a todas as persoas que presten servizos para a Administración da Comunidade Autónoma de Galicia e utilicen para o desempeño das súas funcións os sistemas de información ou as redes de comunicacións propiedade da Administración autonómica.

O contido deste decreto será de aplicación na utilización do equipamento informático e de comunicacións, fixo e móbil, incluíndo calquera dispositivo posto a disposición das persoas que prestan servizos para a Administración autonómica.

### 12.2.2 Órganos responsables e de coordinación

#### 1.- Órganos responsables

As secretarías xerais designarán, dentro de cada departamento da Xunta de Galicia, o órgano que será responsable dos sistemas da súa propiedade e de establecer os medios tecnolóxicos que necesitan as persoas ao seu servizo, así como de velar polo correcto funcionamento das infraestruturas e do equipamento informático e de comunicacións de que dispoñan. Naqueles casos en que as ditas atribucións xa estean asignadas regulamentariamente a un órgano, non será precisa esta designación.

Estes órganos, co apoio do persoal de soporte técnico, son os competentes para velar polo cumprimento das normas contidas neste decreto. Corresponderalles a eles asegurarse de que os equipos se utilizan axeitadamente e atendendo á finalidade á que están destinados.

Para o mellor cumprimento destas atribucións sobre os sistemas, cada departamento da Xunta de Galicia deberá designar unha persoa como responsable de seguridade. As persoas designadas deberán comunicar, dentro do seu ámbito, as normas, procedementos e políticas de seguridade para o seu coñecemento polo persoal, así como impulsar a súa implantación.

## 2.- Órganos de coordinación

Son órganos de coordinación:

a) A Comisión de Informática da Xunta de Galicia, regulada polo Decreto 290/1992, do 8 de outubro.

b) A Dirección Xeral de Calidade e Avaliación das Políticas Públicas da Consellería de Presidencia, Administracións Públicas e Xustiza.

c) O Comité de Seguridade dos Sistemas de Información da Xunta de Galicia. É un órgano colexiado, adscrito á Consellería de Presidencia, Administracións Públicas e Xustiza, formado polas persoas responsables de seguridade dos distintos departamentos da Xunta de Galicia, que ten como obxectivo definir a política de seguridade corporativa. Este comité estará coordinado e asesorado pola dirección xeral competente a través do Centro de Seguridade Informática. O seu réxime básico de funcionamento regularase por orde da Consellería de Presidencia, Administracións Públicas e Xustiza.

### 12.2.3 Acceso á información, redes de comunicacións e Internet.

#### 1.- Acceso á información

As persoas usuarias terán autorizado o acceso unicamente a aquela información e recursos que precisen para o desenvolvemento das súas funcións. O acceso á información contida nos sistemas da Administración da Comunidade Autónoma de Galicia estará restrinxido a aquelas persoas posuidoras da correspondente autorización, que será persoal e intransferible e composta polo menos dun identificador e dun contrasinal.

Os órganos responsables dos sistemas establecerán os mecanismos axeitados para evitar que as persoas poidan acceder ou modificar datos sen autorización. Exclusivamente o persoal de soporte técnico, conforme os criterios establecidos polo responsable de cada un dos sistemas de información, poderá conceder, alterar ou anular a autorización de acceso aos datos e recursos.

Non se poderán obter dereitos de acceso á información distintos aos autorizados, nin se utilizará o identificador doutra persoa, aínda que se dispoña do permiso desta, salvo indicación expresa e puntual do órgano responsable da devandita información ou recurso. Con este fin, as unidades de persoal dos distintos departamentos da Xunta de Galicia comunicarán ao servizo de informática todos os cambios que se produzan nos postos de traballo.

As persoas ao servizo da Administración da Comunidade Autónoma de Galicia deberán velar pola seguridade dos datos aos que teñan acceso polas tarefas do seu posto de traballo, especialmente os confidenciais ou de carácter persoal.

Por motivos de seguridade, a Administración da Comunidade Autónoma de Galicia poderá monitorar os accesos á información contida nos seus sistemas, cumprindo os requisitos que para o efecto estableza a normativa vixente.

## 2 Redes de comunicacións

. A conexión á rede corporativa da Xunta de Galicia será facilitada pola Dirección Xeral de Calidade e Avaliación das Políticas Públicas en uso das competencias atribuídas no decreto de estrutura orgánica da Consellería de Presidencia, Administracións Públicas e Xustiza.

Non se poderá conectar a esta rede de comunicacións ningún dispositivo por medios distintos aos definidos e autorizados polo Centro de Xestión de Rede da devandita dirección xeral.

No caso daquelas redes de comunicacións da Administración da Comunidade Autónoma de Galicia xa xestionadas por outras consellerías, a conexión a estas será facilitada polo órgano responsable de cada unha delas.

### 3 Internet

A Administración da Comunidade Autónoma de Galicia proverá de conexión a Internet ás persoas ao seu servizo cunha finalidade exclusivamente profesional.

O equipo que teña acceso a Internet, a través das redes de comunicación xestionadas pola Administración da Comunidade Autónoma de Galicia, deberá dispoñer de software de protección fronte a virus e demais códigos maliciosos.

Os datos de conexión e tráfico serán monitorados e gardarase un rexistro durante o tempo que establece a normativa vixente en cada suposto. En ningún caso esta retención de datos afectará ao segredo das comunicacións.

As conexións a sitios web que conteñan material ofensivo ou software malicioso serán bloqueadas, salvo excepcións debidamente autorizadas.

#### 12.2.4 Servizo de mensaxería corporativo

A Administración da Comunidade Autónoma de Galicia proverá de servizo de mensaxería ás persoas ao seu servizo cunha finalidade exclusivamente profesional.

Por razóns de seguridade e rendemento, os órganos responsables do servizo poderán monitorar o servizo de mensaxería corporativa. Esta monitorización non será nunca selectiva ou discriminatoria senón que será realizada de forma sistemática ou aleatoria e sen vulneración da intimidade persoal nin do segredo das comunicacións.

Aquelas contas en que se detecte un uso inadecuado, que se definirá no documento de política de seguridade corporativa, poderán ser bloqueadas ou suspendidas temporalmente. En ningún caso, poderá utilizarse o servizo de mensaxería para:

- a) A difusión de mensaxes ofensivas ou discriminatorias.
- b) O uso da conta de correo corporativo para expresar opinións persoais en foros temáticos fóra do ámbito das administracións.
- c) A difusión masiva non autorizada; subscrición indiscriminada a listas de correo ou calquera ataque co obxecto de impedir ou dificultar o servizo de correo.

#### 12.2.5 Deber das persoas usuarias

As persoas que prestan servizos á Administración da Comunidade Autónoma de Galicia, ademais de cumpriren coas medidas indicadas neste decreto relativas ao equipamento informático e de comunicacións, ás aplicacións informáticas, á información e ao uso dos servizos corporativos, son responsables do bo uso dos medios electrónicos, informáticos, telemáticos e de comunicacións, fixos e móbiles, postos á súa disposición para as actividades propias das funcións que desenvolven.

Non se poderá acceder aos recursos informáticos e telemáticos para desenvolver actividades que persigan ou teñan como consecuencia:

- a) A degradación dos servizos.

- b) A destrución ou modificación non autorizada da información de modo premeditado.
- c) A violación da intimidade, do segredo das comunicacións e do dereito á protección de datos persoais.
- d) A deterioración intencionada do traballo doutras persoas.
- e) O uso dos sistemas de información para fins alleos aos da Administración.
- f) Incorrer en actividades ilícitas de calquera tipo.
- g) Danar intencionadamente os recursos informáticos da Administración da Comunidade Autónoma de Galicia ou doutras institucións.
- h) Instalar ou utilizar «software» que non dispoña da licenza correspondente.

3. Para garantir uns mínimos de seguridade no equipamento asignado, deberase:

- a) Utilizar e gardar en segredo o contrasinal que protexe a conta de acceso, responsabilidade directa da persoa usuaria. Esta debe pechar a súa conta ao final de cada sesión ou cando deixe desatendido o equipo, co fin de que non poida ser utilizado por terceiras persoas.
- b) Revisar de forma periódica os seus ordenadores, eliminando calquera virus, programa ou ficheiro que poida causar danos a outros equipos da rede ou outras actuacións que contraveñan a lexislación vixente.



c) No caso de que o seu equipo conteña información importante que non estea gardada nun servidor, realizar copias de seguridade periódicas para garantir a súa dispoñibilidade.

As persoas usuarias, no exercicio das súas funcións, deberán colaborar co órgano competente en materia de seguridade dos sistemas de información e seguir as súas recomendacións e, en particular, as do Centro de Seguridade Informática, en aplicación da política de seguridade corporativa definida polo Comité de Seguridade dos Sistemas de Información da Xunta de Galicia.

Tamén estarán obrigadas ao cumprimento daquelas outras medidas adicionais que especifiquen os órganos responsables dos sistemas.

#### 12.2.6 Inspección

A Administración da Comunidade Autónoma de Galicia, mediante os medios tecnolóxicos e persoais que estime oportunos, revisará periódica e puntualmente, por razóns de seguridade e de calidade do servizo, o estado dos equipos, dispositivos e redes de comunicacións da súa responsabilidade, así como a súa correcta utilización, co obxecto de verificar o seu correcto funcionamento, eficiencia e o cumprimento das medidas e protocolos de seguridade establecidos na lexislación vixente.

A dirección xeral competente en materia de seguridade corporativa velará polo cumprimento da presente normativa e informará o Comité de Seguridade dos Sistemas de Información da Xunta de Galicia sobre os incumprimentos ou deficiencias de seguridade observados co obxecto de que se tomen as medidas oportunas.

Os servizos para os que se detecte un uso inadecuado ou que non cumpran os requisitos de seguridade, que se definirán no documento de política de seguridade corporativa, poderán ser bloqueados ou suspendidos temporalmente para aquelas

contas nas que se detecte un dano para os sistemas de información e de comunicacións. O servizo restablecerase cando a causa da súa degradación desapareza.

#### 12.2.7 Responsabilidade das persoas usuarias que teñan a condición de empregados públicos

A Administración da Comunidade Autónoma de Galicia esixirá dos empregados públicos a responsabilidade na que incorresen por dolo, culpa ou negligencia graves das que se deriven danos e prexuízos nos seus bens ou dereitos ou indemnizacións para particulares, logo da instrución do procedemento correspondente nos termos previstos na normativa de aplicación.

O incumprimento dos deberes e obrigas impostos polo presente decreto, que sexan constitutivos de infracción disciplinaria, segundo a tipificación efectuada na normativa aplicable, dará lugar á incoación do correspondente procedemento disciplinario que se tramitará conforme ao establecido na normativa aplicable aos empregados públicos en función da natureza xurídica do seu vínculo coa Administración. Non obstante o anterior, a incoación dos expedientes e a imposición das sancións requirirá informe previo da Dirección Xeral de Calidade e Avaliación das Políticas Públicas.

Autor:

Alfonso García Magariños

Director Asesoría Xurídica Municipal Concello da Coruña



**13. IMPLANTACIÓN DA  
ADMINISTRACIÓN  
ELECTRÓNICA. SEDE  
ELECTRÓNICA E SERVIZOS DE  
SEDE. REXISTRO  
ELECTRÓNICO. EXPEDIENTE  
ELECTRÓNICO. ARQUIVO  
ELECTRÓNICO DE  
DOCUMENTOS.  
DIXITALIZACIÓN, COMPULSA  
ELECTRÓNICA. FACTURA E  
LICITACIÓN ELECTRÓNICAS.**

## **BLOQUE: ADMINISTRACIÓN ELECTRÓNICA E SOCIEDADE DA INFORMACIÓN**

**TEMA 13. IMPLANTACIÓN DA ADMINISTRACIÓN ELECTRÓNICA. SEDE ELECTRÓNICA E SERVIZOS DE SEDE. REXISTRO ELECTRÓNICO. EXPEDIENTE ELECTRÓNICO. ARQUIVO ELECTRÓNICO DE DOCUMENTOS. DIXITALIZACIÓN, COMPULSA ELECTRÓNICA. FACTURA E LICITACIÓN ELECTRÓNICAS.**

### **13.1. IMPLANTACIÓN DA ADMINISTRACIÓN ELECTRÓNICA**

### **13.2. SEDE ELECTRÓNICA E SERVIZOS DA SEDE**

### **13.3. REXISTRO ELECTRÓNICO**

### **13.4. EXPEDIENTE ELECTRÓNICO**

### **13.5. ARQUIVO ELECTRÓNICO DE DOCUMENTOS**

### **13.6. DIXITALIZACIÓN, COMPULSA ELECTRÓNICA.**

### **13.7. FACTURA E LICITACIÓN ELECTRÓNICAS**

### **13.8. REFERENCIAS**

### **13.1. IMPLANTACIÓN DA ADMINISTRACIÓN ELECTRÓNICA**

Segundo establece a Comisión Europea, a Administración electrónica defínese como o uso das Tecnoloxías da Información e as Comunicacions nas Administracións Públicas, combinada con cambios organizativos e novas aptitudes, co fin de mellorar os servizos públicos e os procesos democráticos e reforzar o apoio ás políticas públicas.

A e-Administración ou Administración electrónica fai referencia á incorporación das tecnoloxías da información e as comunicacións en dúas vertentes:

- Desde un punto de vista organizativo, transformando as oficinas tradicionais, convertendo os procesos en papel en procesos electrónicos.

- Desde unha perspectiva das relacións externas, habilitando a vía electrónica como un novo medio para a relación co cidadán, empresas e outras institucións.

A idea clave sobre a administración electrónica é que non se trata simplemente de levar as TIC á actividade administrativa, senón que constitúe un elemento fundamental nos procesos de modernización administrativa dentro dos cales se enmarca que debe levar á mellora e simplificación dos servizos.

A Administración electrónica ten o seu maior impulso na última década, motivado en parte por un marco legal que permitiu levar as garantías xurídicas que existen no mundo real ao mundo virtual e noutra parte pola evolución das tecnoloxías relacionadas e o desenvolvemento de proxectos emblemáticos, como o DNI electrónico.

Pode mencionarse como antecedente o RD 263/1996, do 16 de febreiro, polo que se regula a utilización de técnicas electrónicas, informáticas e telemáticas pola Administración Xeral do Estado (ampliado posteriormente por RD 209/2003).

Neste proceso salienta especialmente a Lei 59/2003, do 19 de decembro, de firma electrónica, que establece, entre moitas outras cuestións, o concepto de firma electrónica recoñecida e a equipara xuridicamente á firma manuscrita ou en papel, dotándoa así de plena validez legal para as transaccións electrónicas públicas e privadas. A primeira regulación da firma electrónica en España producira mediante o Real Decreto 14/1999, transposición da directiva europea 1999/93/CE sobre firma electrónica.

Por outra banda, coa Lei Orgánica 15/1999, do 13 de decembro, de Protección de Datos de Carácter Persoal e o seu regulamento de desenvolvemento (mediante Real Decreto 1720/2007), establécense as garantías de confidencialidade dos datos proporcionados polas persoas físicas nestas transaccións.

Pero sobre todo é necesario facer mención á Lei 11/2007, do 22 de xuño, de acceso electrónico dos cidadáns aos Servizos Públicos, moitas veces denominada simplemente "Lei de Administración Electrónica" ou mencionada por siglas LAECSPC<sup>1</sup>, que consagra o concepto de Administración electrónica no marco xurídico español e a eleva á categoría de dereito dos cidadáns.

A LAECSPC é a primeira norma legal con rango de lei que se centra enteiramente na problemática propia da Administración Electrónica, é xa que logo a norma legal de referencia nesta materia e establece un marco homoxéneo para as tres administracións na materia.

O seu principal obxectivo é recoñecer e garantir o dereito do cidadán a relacionarse por medios electrónicos coas Administracións Públicas. Por outra banda preténdese impulsar o uso dos servizos electrónicos na Administración creando as condicións necesarias, e de xeito indirecto exercer con iso un efecto arrastre sobre a sociedade da información en xeral.

As Administracións Públicas teñen a obriga de posibilitar o acceso a todos os seus servizos electrónicos, incluíndo rexistro, pagamento, notificacións e a consulta do estado de tramitación dos seus procedementos desde o 31 de decembro de 2009. Neste sentido é especialmente esixente coa Administración do Estado, condicionando a obrigatoriedade para as Comunidades Autónomas e Administración Local á dispoñibilidade de financiamento suficiente para a implantación destes servizos.

A LAECSPC ademais supuxo o punto de partida para un desenvolvemento normativo que permite avanzar en aspectos concretos, e que tamén se mencionarán nestes capítulos e aparecen no apartado de referencias.

---

<sup>1</sup> Dadas as múltiples referencias que se fan neste texto á devandita Lei, optaremos habitualmente por utilizar esta expresión ou ben simplemente Lei 11/2007.

En particular, e con respecto aos aspectos técnicos, destacan o Esquema Nacional de Seguridade e o Esquema Nacional de Interoperabilidade, e con respecto a este último, as recentes Normas Técnicas de Interoperabilidade, que fan referencia aos distintos apartados estudados neste bloque. Todos están mencionados no apartado de referencias.

Ademais de recoñecer o dereito dos cidadáns a relacionarse coas Administracións Públicas por medios electrónicos, regula os aspectos básicos da utilización das tecnoloxías da información na actividade administrativa, nas relacións entre as Administracións Públicas, así como nas relacións dos cidadáns coas mesmas coa finalidade de garantir os seus dereitos, un tratamento común ante elas e a validez e eficacia da actividade administrativa en condicións de seguridade xurídica.

A LAECSPC obriga ás Administracións a asegurar a dispoñibilidade, o acceso, a integridade, a autenticidade, a confidencialidade e a conservación dos datos, informacións e servizos que xestionen no exercicio das súas competencias.

Tamén establece unha serie de fins, que definen con claridade qué debe perseguir todo proxecto de Administración Electrónica:

1. Facilitar o exercicio de dereitos e o cumprimento de deberes por medios electrónicos.
2. Facilitar o acceso por medios electrónicos dos cidadáns á información e ao procedemento administrativo, con especial atención á eliminación das barreiras que limiten o devandito acceso.
3. Crear as condicións de confianza no uso dos medios electrónicos, establecendo as medidas necesarias para a preservación da integridade dos dereitos fundamentais, e en especial os relacionados coa intimidade e a protección de datos de carácter persoal, por medio da garantía da seguridade dos sistemas, os datos, as comunicacións, e os servizos electrónicos.

4. Promover a proximidade co cidadán e a transparencia administrativa, así como a mellora continuada na consecución do interese xeral.
5. Contribuír á mellora do funcionamento interno das Administracións Públicas, incrementando a eficacia e a eficiencia das mesmas mediante o uso das tecnoloxías da información, coas debidas garantías legais na realización das súas funcións.
6. Simplificar os procedementos administrativos e proporcionar oportunidades de participación e maior transparencia, coas debidas garantías legais.
7. Contribuír ao desenvolvemento da sociedade da información no ámbito das Administracións Públicas e na sociedade en xeral.

A utilización das tecnoloxías da información terá as limitacións establecidas pola Constitución e o resto do ordenamento xurídico, respectando o pleno exercicio polos cidadáns dos dereitos que teñen recoñecidos, e axustándose aos seguintes principios:

- a. O respecto ao dereito á protección de datos de carácter persoal nos termos establecidos pola Lei Orgánica 15/1999, de Protección dos Datos de Carácter Persoal, nas demais leis específicas que regulan o tratamento da información e nas súas normas de desenvolvemento, así como aos dereitos ao honor e á intimidade persoal e familiar.
- b. Principio de igualdade con obxecto de que en ningún caso o uso de medios electrónicos poida implicar a existencia de restricións ou discriminacións para os cidadáns que se relacionen coas Administracións Públicas por medios non electrónicos, tanto respecto ao acceso á prestación de servizos públicos como respecto de calquera actuación ou procedemento administrativo sen prexuízo das medidas dirixidas a incentivar a utilización dos medios electrónicos.
- c. Principio de accesibilidade á información e aos servizos por medios electrónicos nos termos establecidos pola normativa vixente nesta materia, a través de sistemas que permitan obtelos de xeito seguro e comprensible, garantindo especialmente a accesibilidade universal e o deseño para todos os soportes,





canles e contornas con obxecto de que todas as persoas poidan exercer os seus dereitos en igualdade de condicións, incorporando as características necesarias para garantir a accesibilidade daqueles colectivos que o requiran.

- d. Principio de legalidade en canto ao mantemento da integridade das garantías xurídicas dos cidadáns ante as Administracións Públicas establecidas na Lei 30/1992, de Réxime Xurídico das Administracións Públicas e do Procedemento Administrativo Común.
- e. Principio de cooperación na utilización de medios electrónicos polas Administracións Públicas ao obxecto de garantir tanto a interoperabilidade dos sistemas e solucións adoptados por cada unha delas como, no seu caso, a prestación conxunta de servizos aos cidadáns. En particular, garantirase o recoñecemento mutuo dos documentos electrónicos e dos medios de identificación e autenticación que se axusten ao disposto na presente Lei.
- f. Principio de seguridade na implantación e utilización dos medios electrónicos polas Administracións Públicas, en cuxa virtude esixir polo menos o mesmo nivel de garantías e seguridade que se require para a utilización de medios non electrónicos na actividade administrativa.
- g. Principio de proporcionalidade en cuxa virtude só se esixirán as garantías e medidas de seguridade axeitadas á natureza e circunstancias dos distintos trámites e actuacións. Así mesmo só se requirirán aos cidadáns aqueles datos que sexan estritamente necesarios en atención á finalidade para a que se soliciten.
- h. Principio de responsabilidade e calidade na veracidade e autenticidade das informacións e servizos ofrecidos polas Administracións Públicas a través de medios electrónicos.
- i. Principio de neutralidade tecnolóxica e de adaptabilidade ao progreso das técnicas e sistemas de comunicacións electrónicas garantindo a independencia na elección das alternativas tecnolóxicas polos cidadáns e polas Administracións Públicas, así como a liberdade de desenvolver e implantar os avances tecnolóxicos nun ámbito de libre mercado. A estes efectos as

Administracións Públicas utilizarán estándares abertos así como, no seu caso e de forma complementaria, estándares que sexan de uso xeneralizado polos cidadáns.

- j. Principio de simplificación administrativa, polo cal se reduzan de xeito substancial os tempos e prazos dos procedementos administrativos, logrando unha maior eficacia e eficiencia na actividade administrativa.
- k. Principio de transparencia e publicidade do procedemento, polo cal o uso de medios electrónicos debe facilitar a máxima difusión, publicidade e transparencia das actuacións administrativas.

A nivel técnico, pódese destacar o principio de neutralidade tecnolóxica e uso de estándares abertos na utilización das TIC.

Recoñécese aos cidadáns o dereito a relacionarse coas Administracións Públicas utilizando medios electrónicos (a LAECSPC, como a maioría da normativa que garda relación, utiliza normalmente este termo en lugar doutros como “telemáticos”) para o exercicio dos dereitos previstos no artigo 35 da Lei 30/1992, do 26 de novembro, de Réxime Xurídico das Administracións Públicas e do Procedemento Administrativo Común, así como para obter informacións, realizar consultas e alegacións, formular solicitudes, manifestar consentimento, entaboar pretensións, efectuar pagamentos, realizar transaccións e opoñerse ás resolucións e actos administrativos.

Ademais, os cidadáns teñen en relación coa utilización dos medios electrónicos na actividade administrativa, e nos termos previstos na presente Lei, os seguintes dereitos:

- a. A elixir, entre aqueles que en cada momento se atopen dispoñibles, a canle a través da cal relacionarse por medios electrónicos coas Administracións Públicas.

- b. A non achegar os datos e documentos que obren en poder das Administracións Públicas, as cales utilizarán medios electrónicos para solicitar dita información sempre que, no caso de datos de carácter persoal, se conte co consentimento dos interesados nos termos establecidos pola Lei Orgánica 15/1999, de Protección de Datos de Carácter Persoal, ou unha norma con rango de Lei así o determine, salvo que existan restricións conforme á normativa de aplicación aos datos e documentos solicitados. O citado consentimento poderá emitirse e solicitarse por medios electrónicos.
- c. Á igualdade no acceso electrónico aos servizos das Administracións Públicas (entendida como non discriminación de persoas que non teña un acceso fácil aos medios electrónicos).
- d. A coñecer por medios electrónicos o estado de tramitación dos procedementos nos que sexan interesados, salvo nos supostos en que a normativa de aplicación estableza restricións ao acceso á información sobre aqueles.
- e. A obter copias electrónicas dos documentos electrónicos que formen parte de procedementos nos que teñan a condición de interesado.
- f. Á conservación en formato electrónico polas Administracións Públicas dos documentos electrónicos que formen parte dun expediente.
- g. A obter os medios de identificación electrónica necesarios, podendo as persoas físicas utilizar en todo caso os sistemas de firma electrónica do Documento Nacional de Identidade para calquera trámite electrónico con calquera Administración Pública.
- h. Á utilización doutros sistemas de firma electrónica admitidos no ámbito das Administracións Públicas.
- i. Á garantía da seguridade e confidencialidade dos datos que figuren nos ficheiros, sistemas e aplicacións das Administracións Públicas.
- j. Á calidade dos servizos públicos prestados por medios electrónicos.
- k. A elixir as aplicacións ou sistemas para relacionarse coas Administracións Públicas a condición de que utilicen estándares abertos ou, no seu caso, aqueloutros que sexan de uso xeneralizado polos cidadáns.

En particular, nos procedementos relativos ao acceso a unha actividade de servizos e o seu exercicio, os cidadáns teñen dereito á realización da tramitación a través dun portelo único, por vía electrónica e a distancia, e á obtención da seguinte información a través de medios electrónicos, que deberá ser clara e inequívoca:

- a. Os requisitos aplicables aos prestadores establecidos en territorio español, en especial os relativos aos procedementos e trámites necesarios para acceder ás actividades de servizo e para o seu exercicio.
- b. Os datos das autoridades competentes nas materias relacionadas coas actividades de servizos, así como os datos das asociacións e organizacións distintas das autoridades competentes ás que os prestadores ou destinatarios poidan dirixirse para obter asistencia ou axuda.
- c. Os medios e condicións de acceso aos rexistros e bases de datos públicos relativos a prestadores de actividades de servizos.
- d. As vías de reclamación e recurso en caso de litixio entre as autoridades competentes e o prestador ou o destinatario, ou entre un prestador e un destinatario, ou entre prestadores.

As Administracións Públicas deberán habilitar diferentes canles ou medios para a prestación dos servizos electrónicos, garantindo en todo caso o acceso aos mesmos a todos os cidadáns, con independencia das súas circunstancias persoais, medios ou coñecementos, na forma que estimen adecuada.

A Administración Xeral do Estado garantirá o acceso de todos os cidadáns aos servizos electrónicos proporcionados no seu ámbito a través dun sistema de varias canles que conte, polo menos, cos seguintes medios:

- a. As oficinas de atención presencial que se determinen, as cales poñerán a disposición dos cidadáns de forma libre e gratuíta os medios e instrumentos

precisos para exercer os dereitos recoñecidos no artigo 6 da LAECSPC, debendo contar con asistencia e orientación sobre a súa utilización, ben a cargo do persoal das oficinas en que se sitúen ou ben por sistemas incorporados ao propio medio ou instrumento.

- b. Puntos de acceso electrónico, consistentes en sedes electrónicas creadas e xestionadas polos departamentos e organismos públicos e dispoñibles para os cidadáns a través de redes de comunicación. En particular crearase un Punto de acceso xeral a través do cal os cidadáns poidan, nas súas relacións coa Administración Xeral do Estado e os seus Organismos Públicos, acceder a toda a información e aos servizos dispoñibles. Este Punto de acceso xeral conterá a relación de servizos a disposición dos cidadáns e o acceso aos mesmos, debendo manterse coordinado, polo menos, cos restantes puntos de acceso electrónico da Administración Xeral do Estado e os seus Organismos Públicos.
- c. Servizos de atención telefónica que, na medida en que os criterios de seguridade e as posibilidades técnicas o permitan, faciliten aos cidadáns o acceso ás informacións e servizos electrónicos aos que se refiren os apartados anteriores.

Co fin de que os cidadáns poidan exercer o seu dereito a non achegar datos que xa obren en poder da Administración Pública, cada Administración deberá facilitar o acceso das restantes Administracións Públicas aos datos relativos aos interesados que obren no seu poder e se achen en soporte electrónico, especificando as condicións, protocolos e criterios funcionais ou técnicos necesarios para acceder aos devanditos datos coas máximas garantías de seguridade, integridade e dispoñibilidade, de conformidade co disposto na Lei Orgánica 15/1999, do 13 de decembro, de Protección de Datos de Carácter Persoal e a súa normativa de desenvolvemento.

A dispoñibilidade de tales datos estará limitada estritamente a aqueles que son requiridos aos cidadáns polas restantes Administracións para a tramitación e

resolución dos procedementos e actuacións da súa competencia de acordo coa normativa reguladora dos mesmos.

### **13.2. SEDE ELECTRÓNICA E SERVIZOS DA SEDE**

A LAECSPC define a sede electrónica como aquela dirección electrónica dispoñible para os cidadáns a través de redes de telecomunicacións cuxa titularidade, xestión e administración corresponde a unha Administración Pública, órgano ou entidade administrativa no exercicio das súas competencias.

O establecemento dunha sede electrónica implica a responsabilidade do titular respecto da integridade, veracidade e actualización da información e os servizos aos que poida accederse a través da mesma.

Cada Administración Pública determinará as condicións e instrumentos de creación das sedes electrónicas, con suxeición aos principios de publicidade oficial, responsabilidade, calidade, seguridade, dispoñibilidade, accesibilidade, neutralidade e interoperabilidade. En todo caso deberá garantirse a identificación do titular da sede, así como os medios dispoñibles para a formulación de suxestións e queixas.

As sedes electrónicas dispoñerán de sistemas que permitan o establecemento de comunicacións seguras sempre que sexan necesarias. Este apartado cobra especial importancia cando se ofrecen servizos de tramitación.

A publicación nas sedes electrónicas de informacións, servizos e transaccións respectará os principios de accesibilidade e usabilidade de acordo coas normas establecidas respecto diso, estándares abertos e, no seu caso, aqueloutros que sexan de uso xeneralizado polos cidadáns.

A publicación dos diarios ou boletíns oficiais nas sedes electrónicas da Administración, Órgano ou Entidade competente terá, nas condicións e garantías que cada Administración Pública determine, os mesmos efectos que os atribuídos á súa edición impresa. A publicación do “*Boletín Oficial do Estado*” na sede electrónica do organismo competente terá carácter oficial e auténtico nas condicións e coas garantías que se determinen regulamentariamente, derivándose da devandita publicación os efectos previstos no título preliminar do Código Civil e nas restantes normas aplicables.

A publicación de actos e comunicacións que, por disposición legal ou regulamentaria deban publicarse en taboleiro de anuncios ou edictos poderá ser substituída ou complementada pola súa publicación na sede electrónica do organismo correspondente.

Polo tanto, a sede electrónica diferénciase de calquera sede institucional tradicional en medio telemático pola responsabilidade do titular, o feito de que a publicación de diarios ou boletíns oficiais reviste os mesmos efectos que a publicación impresa e que pode actuar como substituta ou complemento ao taboleiro de anuncios ou edictos. Ademais, cómpre ter en conta as condicións que teñen que cumprir as sedes electrónicas da Administración Xeral do Estado no marco do Real Decreto 1671/2009. Para o resto das Administracións Públicas, aínda que están fóra do seu ámbito, é indubidable a súa validez como elemento de referencia.

En todo caso, a través do seu articulado, a LAECSP establece os seguintes requisitos para as sedes electrónicas:

- Debe permitir o acceso dos cidadáns para a realización de calquera tipo de trámite ou interacción coa Administración.
- Debe permitir aos cidadáns realizar consultas sobre o estado de tramitación de expedientes nos que teñan a condición de interesado.



- Tanto a sede como os elementos e contidos da mesma deben basearse en aplicacións e sistemas que utilicen estándares abertos ou sexan de uso xeneralizado polos cidadáns.
- Debe conter a información sobre os pasos a seguir para cada un dos trámites e procedementos das Administracións Públicas.
- Debe conter a información sobre as autoridades competentes para cada actividade dos servizos ofrecidos polas Administracións Públicas.
- A AGE deberá dispoñer dunha sede electrónica que sirva como Punto de acceso xeral único aos servizos que presta a AGE e os seus Organismos.
- O Punto de acceso xeral creado pola AGE deberá estar integrado co resto de sedes da AGE e Organismos Públicos para a prestación dos distintos servizos.
- Debe garantir a identificación do seu titular.
- Debe permitir establecer as conexións seguras cando sexan necesarias.
- Debe cumprir os principios de accesibilidade e usabilidade de acordo coas normas establecidas respecto diso (Segundo o BOE n. 141 do 13/6/2003 na disposición 7, artigo 2: débense cumprir os requisitos AA).
- Permitirá a publicación de actos e comunicacións que, por disposición legal ou regulamentaria deban publicarse en taboleiro de anuncios ou edictos.
- Debe conter a lista de sistemas de firma electrónica avanzada admitidos.
- Debe conter a lista de selos electrónicos utilizados por cada Administración.
- Debe conter as disposicións de creación de rexistros electrónicos.
- A sede permitirá a publicación electrónica do boletín oficial da Administración, órgano ou Entidade competente.
- Debe conter os distintos tipos de escritos, comunicacións, solicitudes, etc. que poden presentarse.
- Deberá publicar os medios electrónicos dispoñibles para que o cidadán se relacione coas Administracións Públicas.
- Deberá mostrar de xeito visible a data e hora garantindo a súa integridade.
- Deberá publicar unha lista cos días considerados inhábiles.



- Naquelas administracións que teñan linguas cooficiais, débese garantir o acceso en ambas linguas.

Desde o punto de vista técnico, a sede electrónica non presenta características tecnolóxicas distintas ás de calquera sitio web tradicional, aínda que é necesario establecer as medidas de seguridade que permitan garantir a responsabilidade establecida pola LAECSP.

En particular, é importante a identificación segura da sede electrónica. Neste sentido, a Lei establece a posibilidade de creación de certificados de sede electrónica con este propósito.

A Fábrica Nacional de Moneda y Timbre – Real Casa de la Moneda (FNMT-RCM), que xa ofrecía certificados de identificación segura, dispón xa da versión actualizada para o cumprimento da LAECSP (son os chamados xenericamente certificados APE). Os "Certificados de identificación de sede electrónica" son aqueles certificados expedidos pola FNMT-RCM baixo a Declaración de Prácticas de Certificación da Administración Pública do Estado e que vinculan uns datos de verificación de firma aos datos identificativos dunha sede electrónica na que existe unha persoa física que actúa como asinante ou custodio da clave e titular do certificado, xunto coa entidade da administración á que pertence e que é titular da dirección electrónica a través da que se accede a sede electrónica (só a titularidade é compartida, non sendo así a custodia). Esta persoa física é a que ten o control sobre o devandito certificado e os datos de creación e verificación de firma e é responsable da súa custodia de forma dilixente.

Constitúen os límites de uso deste tipo de certificados a identificación de sedes electrónicas da Administración Pública, Organismos e entidades públicas vinculadas ou dependentes así como o establecemento de comunicacións seguras con estas.

Ademais, as sedes electrónicas poden contar con requisitos técnicos adicionais segundo os servizos que presten, podendo por exemplo, ser necesario garantir a integridade e contido das súas páxinas a unha data e hora determinada mediante a firma con selado de tempo do devandito contido, e o mesmo pódese dicir dos documentos emitidos ou recibidos.

### **13.3. REXISTRO ELECTRÓNICO**

As tarefas fundamentais do rexistro electrónico son tomar unha referencia de tempo, anotar o asento da entrada/saída, gardar os datos da presentación de información, e devolver un acuse de recibo co número de rexistro e momento da presentación.

O rexistro poderá así mesmo incluír funcionalidades adicionais, por exemplo, o selado de tempo para obter a referencia temporal, o cotexo/compulsa electrónica de documentos presentados fisicamente ou o funcionamento como rexistro único para toda a Administración.

Con respecto aos rexistros electrónicos, a LAECSP establece que as Administracións Públicas crearán rexistros electrónicos para a recepción e remisión de solicitudes, escritos e comunicacións. Os rexistros electrónicos poderán admitir:

- a. Documentos electrónicos normalizados correspondentes aos servizos, procedementos e trámites que se especifiquen conforme ao disposto na norma de creación do rexistro, cumprimentados de acordo con formatos preestablecidos.
- b. Calquera solicitude, escrito ou comunicación distinta dos mencionados no apartado anterior dirixido a calquera órgano ou entidade do ámbito da administración titular do rexistro.

En cada Administración Pública existirá, polo menos, un sistema de rexistros electrónicos suficiente para recibir todo tipo de solicitudes, escritos e comunicacións

dirixidos á devandita Administración Pública. As Administracións Públicas poderán, mediante convenios de colaboración, habilitar aos seus respectivos rexistros para a recepción das solicitudes, escritos e comunicacións da competencia doutra Administración que se determinen no correspondente convenio.

No ámbito da Administración Xeral do Estado se automatizarán as oficinas de rexistro físicas ás que se refire o artigo 38 da Lei 30/1992, de Réxime Xurídico das Administracións Públicas e do Procedemento Administrativo Común, a fin de garantir a interconexión de todas as súas oficinas e posibilitar o acceso por medios electrónicos aos asentos rexistrais e ás copias electrónicas dos documentos presentados.

As disposicións de creación de rexistros electrónicos publicaranse no Diario Oficial correspondente e o seu texto íntegro deberá estar dispoñible para consulta na sede electrónica de acceso ao rexistro. En todo caso, as disposicións de creación de rexistros electrónicos especificarán o órgano ou unidade responsable da súa xestión, así como a data e hora oficial e os días declarados como inhábiles aos efectos previstos no artigo seguinte.

Na sede electrónica de acceso ao rexistro figurará a relación actualizada das solicitudes, escritos e comunicacións que poden presentarse no mesmo.

Os rexistros electrónicos emitirán automaticamente un recibo consistente nunha copia autenticada do escrito, solicitude ou comunicación de que se trate, incluíndo a data e hora de presentación e o número de entrada de rexistro.

Poderán aportarse documentos que acompañen á correspondente solicitude, escrito ou comunicación, sempre que cumpran os estándares de formato e requisitos de seguridade que se determinen nos Esquemas Nacionais de Interoperabilidade e de Seguridade.

Os rexistros electrónicos xerarán recibos acreditativos da entrega destes documentos que garantan a integridade e o non repudio dos documentos achegados.

Os rexistros electrónicos rexeranse a efectos de cómputo dos prazos imputables tanto aos interesados como ás Administracións Públicas pola data e hora oficial da sede electrónica de acceso, que deberá contar coas medidas de seguridade necesarias para garantir a súa integridade e figurar visible.

Os rexistros electrónicos permitirán a presentación de solicitudes, escritos e comunicacións todos os días do ano durante as vinte e catro horas.

Aos efectos do cómputo de prazo fixado en días hábiles ou naturais, e no que se refire a cumprimento de prazos polos interesados, a presentación nun día inhábil entenderase realizada na primeira hora do primeiro día hábil seguinte, salvo que unha norma permita expresamente a recepción en día inhábil.

O inicio do cómputo dos prazos que teñan que cumprir os órganos administrativos e entidades de dereito público virá determinado pola data e hora de presentación no propio rexistro ou, no caso previsto no apartado 2.b do artigo 24 da LAECSP, pola data e hora de entrada no rexistro do destinatario. En todo caso, a data efectiva de inicio do cómputo de prazos deberá ser comunicada a quen presentou o escrito, solicitude ou comunicación.

Cada sede electrónica na que estea dispoñible un rexistro electrónico determinará, atendendo ao ámbito territorial no que exerce as súas competencias o titular daquela, os días que se considerarán inhábiles aos efectos dos apartados anteriores. En todo caso, non será de aplicación aos rexistros electrónicos o disposto no artigo 48.5 da Lei 30/1992, de Réxime Xurídico das Administracións Públicas e do Procedemento Administrativo Común, que establece que cando un día fose hábil no municipio ou

Comunidade Autónoma en que residise o interesado, e inhábil na sede do órgano administrativo, ou á inversa, considerarase inhábil en todo caso.

Desde o punto de vista técnico, o rexistro electrónico debe permitir a presentación de documentación en formato electrónico e a xeración do correspondente asento no rexistro de entrada e saída da Administración. Iso implica probablemente a necesidade de integración cun sistema de xestión de rexistro de entrada e saída xeral, que permita a introdución de asentos manuais desde os distintos departamentos.

Ademais, para poder realizar esta función coas suficientes garantías, debe permitir o seguinte:

- a) Presentar a documentación en formato electrónico e asinada polo cidadán mediante o correspondente certificado electrónico que garanta a súa autenticidade, integridade e non repudio.
- b) Rexistrar de modo fidedigno o proceso de rexistro da devandita documentación. Para ese efecto pódese utilizar algún tipo de resgardo asinado mediante o uso dun certificado da Administración Pública (previsiblemente un certificado de selo electrónico) que inclúa selado de tempo para garantir a data e hora de entrega.
- c) Entregar ao cidadán o resgardo do devandito rexistro en formato electrónico, convenientemente asinado pola Administración, no que constará a data e hora de entrada e os documentos entregados, e podendo incorporar un *checksum* ou sistema equivalente que permita verificar que os contidos presentados son os que constan no devandito resgardo.

Os documentos deberían entrar a formar parte do sistema de xestión de documentos electrónicos, recibindo polo tanto unha identificación única dentro do sistema e o tratamento que corresponda en cada caso. Así por exemplo, de ser necesario entrarían a formar parte do correspondente expediente electrónico.

#### **13.4. EXPEDIENTE ELECTRÓNICO**

A LAECSP define expediente electrónico como o conxunto de documentos electrónicos correspondentes a un procedemento administrativo, calquera que sexa o tipo de información que conteñan.

O foliado dos expedientes electrónicos levarase a cabo mediante un índice electrónico, asinado pola Administración, órgano ou entidade actuante, segundo proceda.

Este índice garantirá a integridade do expediente electrónico e permitirá a súa recuperación sempre que sexa preciso, sendo admisible que un mesmo documento forme parte de distintos expedientes electrónicos.

A remisión de expedientes poderá ser substituída para todos os efectos legais pola posta a disposición do expediente electrónico, tendo o interesado dereito a obter copia do mesmo.

Desde o punto de vista técnico, o expediente vén definido polo índice ordenado de documentos que foi asinado electronicamente, polo que non pode ser modificado sen a perda de validez da devandita firma. Os documentos como tal poden ser almacenados de forma independente, previsiblemente estarán á súa vez asinados para garantir a súa integridade e non repudio, e deben contar cun código que os identifique de forma unívoca dentro da organización e non só dentro do ámbito do expediente. Deste xeito, un mesmo documento pode ser referenciado desde varios índices, ou o que é o mesmo, formar parte de distintos expedientes.

#### **13.5. ARQUIVO ELECTRÓNICO DE DOCUMENTOS**

As Administracións Públicas poderán emitir validamente por medios electrónicos os documentos administrativos aos que se refire o artigo 46 da Lei 30/1992, de Réxime Xurídico das Administracións Públicas e do Procedemento Administrativo Común, sempre que incorporen unha ou varias firmas electrónicas conforme ao establecido na Sección III do Capítulo II da LAECSP.

Os documentos administrativos incluírán referencia temporal, que se garantirá a través de medios electrónicos cando a natureza do documento así o requira.

A Administración Xeral do Estado, na súa relación de prestadores de servizos de certificación electrónica, especificará aqueles que con carácter xeral estean admitidos para prestar servizos de selado de tempo.

Poderán almacenarse por medios electrónicos todos os documentos utilizados nas actuacións administrativas.

Os documentos electrónicos que conteñan actos administrativos que afecten a dereitos ou intereses dos particulares deberán conservarse en soportes desta natureza, xa sexa no mesmo formato a partir do que se orixinou o documento ou noutro calquera que asegure a identidade e integridade da información necesaria para reproducilo. Asegurarase en todo caso a posibilidade de trasladar os datos a outros formatos e soportes que garantan o acceso desde diferentes aplicacións.

Os medios ou soportes en que se almacenen documentos, deberán contar con medidas de seguridade que garantan a integridade, autenticidade, confidencialidade, calidade, protección e conservación dos documentos almacenados. En particular, asegurarán a identificación dos usuarios e o control de accesos, así como o cumprimento das garantías previstas na lexislación de protección de datos.

Desde o punto de vista técnico, o almacenamento e tratamento de documentos en formato electrónico implica a utilización dunha firma avanzada que permita garantir a súa integridade e o non repudio. En caso de tratarse de documentos noutro formato, como o papel, pode ser necesaria a súa conversión previa a algún formato electrónico mediante técnicas como a do escaneado.

Ademais, o sistema informático de soporte debe garantir a seguridade dos documentos tanto desde o punto de vista da dispoñibilidade como do control de acceso. Para rematar, implica tamén a implantación dun sistema de custodia de documentos electrónicos con mecanismos que permitan garantir a súa validez ao longo do tempo, mediante o uso, por exemplo, de firmas lonxevas ou da actualización periódica de formatos para evitar a súa obsolescencia.

### 13.6. **DIXITALIZACIÓN, COMPULSA ELECTRÓNICA.**

En primeiro lugar, debemos distinguir entre cotexo ou copia compulsada e copia auténtica:

- O cotexo e a compulsa de documentos é a técnica consistente na comprobación de que unha copia coincide co seu orixinal, que leva a poder afirmar que a mesma é exacta. A copia cotexada ou compulsada en ningún caso acredita a autenticidade do documento orixinal.
- A copia auténtica dun documento acredita a autenticidade dos datos contidos na mesma, non só desde a perspectiva da súa identidade co documento orixinal, senón polos seus efectos certificativos, despois de que garante, igualmente, a autenticidade dos datos contidos neste último.

Por conseguinte, a copia auténtica goza da mesma validez e eficacia que o documento orixinal, non limitando os seus efectos a un procedemento administrativo concreto.



As copias realizadas por medios electrónicos de documentos electrónicos emitidos polo propio interesado ou polas Administracións Públicas, manténdose ou non o formato orixinal, terán inmediatamente a consideración de copias auténticas coa eficacia prevista no artigo 46 da Lei 30/1992, de Réxime Xurídico das Administracións Públicas e do Procedemento Administrativo Común, sempre que o documento electrónico orixinal estea en poder da Administración, e que a información de firma electrónica e, no seu caso, de selado de tempo permitan comprobar a coincidencia co devandito documento.

As copias realizadas polas Administracións Públicas, utilizando medios electrónicos, de documentos emitidos orixinalmente polas Administracións Públicas en soporte papel terán a consideración de copias auténticas sempre que se cumpran os requirimentos e actuacións previstos no artigo 46 da Lei 30/1992, de Réxime Xurídico das Administracións Públicas e do Procedemento Administrativo Común.

As Administracións Públicas poderán obter imaxes electrónicas dos documentos privados achegados polos cidadáns, coa súa mesma validez e eficacia, a través de procesos de dixitalización que garantan a súa autenticidade, integridade e a conservación do documento imaxe, do que se deixará constancia. Esta obtención poderá facerse de forma automatizada, mediante o correspondente selo electrónico.

Nos supostos de documentos emitidos orixinalmente en soporte papel dos que se efectuaron copias electrónicas de acordo co disposto neste artigo, poderá procederse á destrución dos orixinais nos termos e coas condicións que por cada Administración Pública se establezan.

As copias realizadas en soporte papel de documentos públicos administrativos emitidos por medios electrónicos e asinados electronicamente terán a consideración de copias auténticas sempre que inclúan a impresión dun código xerado

electronicamente ou outros sistemas de verificación que permitan contrastar a súa autenticidade mediante o acceso aos arquivos electrónicos da Administración Pública, órgano ou entidade emisora.

Desde o punto de vista técnico, a compulsa e creación de copias auténticas implica a firma dun documento electrónico mediante o uso dun certificado electrónico. No caso de que o devandito documento estea en formato papel, debe ser previamente dixitalizado mediante un procedemento establecido e seguro.

O proceso tecnolóxico de conversión a formato electrónico denomínase “dixitalización certificada”, entendendo como tal a definición dada compatible co termo “dixitalización” que se pode atopar no Anexo do Esquema Nacional de Interoperabilidade (RD 4/2010).

Ao ser necesario que a copia sexa fiel e íntegra, o proceso de dixitalización debe cumprir unha serie de características:

- a) Debe ser completamente automático e realizarse de forma atómica, obtendo como entrada o documento orixinal e devolvendo como resultado a copia electrónica. Así, non será posible a intervención humana en ningunha fase do proceso que poida alterar por erro ou de forma deliberada o contido previsto.
- b) O proceso tecnolóxico debe ser deseñado de tal forma que non produza alteración con respecto ao documento orixinal. Neste aspecto hai que ter en conta que a obtención da copia implica a realización de distintas operacións. Así por exemplo, será necesario nun primeiro momento obter a partir do contido en papel unha representación en formato electrónico, posiblemente mediante unha operación de escaneado ou similar. Nesta fase será importante definir as características técnicas dos dispositivos a utilizar, e parámetros do proceso como pode ser o nivel de resolución (termo definido no Anexo do RD

4/2010) mínima. A partir desta información, xa en formato electrónico, moi probablemente será necesario ademais realizar conversións entre formatos ou aplicar algoritmos de compresión con ou sen perda de información, para os que será necesario establecer uns límites de tolerancia.

Para a firma, a LAECSP establece a posibilidade de utilizar certificados de persoal adscrito á Administración ou funcionario.

A Fábrica Nacional de Moneda y Timbre – Real Casa de la Moneda (FNMT-RCM), que xa ofrecía certificados de identificación segura, dispón xa da versión actualizada para o cumprimento da LAECSP. Os Certificados emitidos pola FNMT-RCM para o persoal ao servizo das administracións públicas cuxa política e Declaración Particular se define na DPC da APE , son certificados recoñecidos segundo o definido na Lei de Firma Electrónica 59/2003 e a norma ETSI 101 456 e válidos para a realización de firma electrónica por parte do persoal ao servizo das administracións públicas e segundo o definido na Lei 11/2007, do 22 de xuño, de acceso electrónico dos cidadáns aos Servizos Públicos (LAECSP).

O certificado para o persoal da Administración Pública, é a certificación electrónica emitida pola FNMT-RCM que vincula ao seu titular cuns datos de verificación de firma e confirma, de forma conxunta:

- a identidade do seu titular, número de identificación persoal, cargo, posto de traballo e/ou condición de autorizado.
- ao órgano, organismo ou entidade da Administración Pública, ben sexa esta Xeral, autonómica, Local ou institucional, onde exerce as súas competencias, presta os seus servizos, ou desenvolve a súa actividade.

O ámbito de uso deste tipo de Certificados compóñeno as diferentes competencias e funcións propias dos titulares de acordo co seu cargo, emprego e, no seu caso, condicións de autorización.

### **13.7. FACTURA E LICITACIÓN ELECTRÓNICAS**

#### **13.7.1. FACTURA ELECTRÓNICA**

A facturación electrónica é un equivalente funcional da factura en papel e consiste na transmisión das facturas ou documentos análogos entre emisor e receptor por medios electrónicos (ficheiros informáticos) e telemáticos (dun ordenador a outro), asinados dixitalmente con certificados recoñecidos.

A Lei 57/2007, de Medidas de Impulso da Sociedade da Información, define a factura electrónica como “un documento electrónico que cumpre cos requisitos legal e regulamentariamente exixibles ás facturas e que, ademais, garante a autenticidade da súa orixe e a integridade do seu contido, o que permite atribuír a factura ao seu obrigado tributario emisor”.

Desta definición estendida en todo o mercado, transmítese tres condicionantes para a realización de e-Factura:

- Necesítase un formato electrónico de factura de maior ou menor complexidade (EDIFACT, XML, PDF, html, doc, xls, gif, jpeg ou txt, entre outros).
- É necesario unha transmisión telemática (ten que partir dun ordenador, e ser recollida por outro ordenador).
- Este formato electrónico e transmisión telemática, deben garantir a súa integridade e autenticidade a través dunha firma electrónica recoñecida. O artigo 3.3 da Lei 59/2003 do 19 de decembro define a firma electrónica

recoñecida como: “a firma electrónica avanzada baseada nun certificado recoñecido e xerada mediante un dispositivo seguro de creación de firma”.

O certificado que se usa é o do expedidor real da factura. Xa sexa este o obrigado tributario, un terceiro que actúe no seu nome ou o destinatario da factura, se se acordou auto-facturación.

Para rematar e para que tivese a facturación electrónica a mesma validez legal que unha factura en papel, necesítase o consentimento de ambas partes (emisor e receptor).

Adicionalmente, e como requisito de todas as facturas independentemente de como se transmitan, en papel ou en formato electrónico, o artigo 6 do RD 1496/2003 que regula o contido dunha factura establece que os campos obrigatorios dunha factura son:

- Número de factura
- Data expedición
- Razón Social emisor e receptor
- NIF emisor e “receptor”
- Enderezo emisor e receptor
- Descrición das operacións (base impositiva)
- Tipo impositivo
- Cota tributaria
- Data prestación do servizo (se distinta a expedición)

Para cumprir coa norma e que unha factura electrónica teña a mesma validez legal que unha emitida en papel, o documento electrónico que a representa debe conter os campos obrigatorios exibibles a toda factura, estar asinado mediante unha firma electrónica avanzada baseado en certificado recoñecido e ser transmitido dun ordenador a outro recollendo o consentimento de ambas partes.

Para homoxeneizar estes aspectos técnicos desenvolveuse a Orde PRE/2971/2007, sobre a expedición de facturas por medios electrónicos cando o destinatario das mesmas sexa a Administración Xeral do Estado ou organismos públicos vinculados ou dependentes daquela e sobre a presentación ante a Administración Xeral do Estado ou os seus organismos públicos vinculados ou dependentes de facturas expedidas entre particulares.

Nesta orde créase o formato de factura electrónica Facturae, xunto coa previsión de compatibilidade en futuras con normas como UBL (Universal Business Language). Facturae define fundamentalmente as tecnoloxías de firma a utilizar nas facturas e unha estrutura en XML que estas deben cumprir. Pódese atopar ampla información sobre este formato no sitio web <http://www.facturae.es/>.

Tamén é posible crear extensións do formato. Unha extensión é unha definición estruturada de información específica, dun sector determinado, que non está contemplada no núcleo do formato Facturae e que é de interese para emisores e receptores. Facturae permite a inclusión de extensións a nivel de liña, de factura ou de lote de facturas.

Facilítase a divulgación das extensións a través da publicación de enlaces a repositorios de extensións relevantes. Estas extensións constituiranse nun modelo de uso común susceptible de utilización maioritaria polos usuarios de Facturae do sector correspondente.

Para que unha extensión figure na táboa de enlaces, é necesario cumprir unha serie de requisitos. Para a creación da extensión, aínda que é responsabilidade da asociación encargada, facilítase un documento de recomendacións xerais:

Obrigas legais do expedidor:

1. Regulamento sobre Facturación Electrónica. A Orde 962/2007, do 10 de abril, desenvolve determinadas disposicións sobre facturación telemática e conservación electrónica de facturas, contidas no Real Decreto 1496/2003, que é o regulamento de facturación. Respecto do consentimento do destinatario, áchase recollido no Artigo 2 da citada Orde, onde di que o consentimento poderá formularse de forma expresa por calquera medio, verbal ou escrito.
2. Creación da factura. Mediante unha aplicación informática, cos contidos obrigatorios mínimos requiridos.
3. Uso de firma electrónica recoñecida
4. Remisión telemática
5. Conservación de copia ou matriz da factura. Esta obrigação regúlase no artigo 1 do RD 1496/2003, onde se especifica a obrigação de expedir, entregar e conservar facturas.

Tamén existiron dúbidas sobre se as facturas electrónicas poden emitirse en copia ou só se debe gardar a matriz. Respecto diso a Axencia Tributaria aclarouno no borrador antes citado (Art. 5) coa seguinte definición:

“Enténdese por Matriz dunha factura (...) un conxunto de datos, táboas, base de datos ou sistemas de ficheiros que conteñen todos os datos reflectidos nas facturas xunto aos programas que permitiron a xeración das facturas....

6. Contabilización e anotación en rexistros de IVE
7. Conservación durante o período de prescrición
8. Garantía de accesibilidade completa. Deber de xestionar as facturas de modo que se garanta unha accesibilidade completa: visualización, busca selectiva, copia ou descarga en liña e impresión. Esta é unha obrigação inherente á conservación das facturas por medios electrónicos que o lexislador denomina acceso completo a datos, tratando de facilitar a auditoría e inspección das facturas electrónicas. (Artigo 9 do RD 1496/2003)



9. Subcontratación a un terceiro. Todas as fases anteriores poden ser subcontratadas a un terceiro, sen perder a súa responsabilidade. Regulado no artigo 5.1 do RD 1496/2003 o lexislador deixa claro nese mesmo parágrafo que, aínda que se permite a subfacturación a terceiros, é o obrigado tributario o responsable de cumprir todas estas obrigacións.

#### Obrigas legais do destinatario:

1. Recepción da factura por medio electrónico

- Verificación dos contidos mínimos exixibles
- Verificación segura da firma electrónica. Regulado no artigo 21 e inherente ás obrigacións da conservación das facturas electrónicas indícase que: “o destinatario débese asegurar da lexibilidade no formato orixinal no que se recibiu, así como, no seu caso, dos datos asociados e mecanismo de verificación de firma”.

A diferenza do emisor, ao que se permite construír a factura desde a matriz, o destinatario debe conservar os orixinais asinados.

2. Contabilización e anotación en rexistros de IVE

3. Conservación durante o período de prescrición. Deber de xestionar as facturas de modo que se garanta unha accesibilidade completa.

4. Todas as fases anteriores pode subcontratalas a un terceiro, sen perder a súa responsabilidade.

A obrigación do uso de facturas electrónicas nace das previsións da Lei 30/2007, de Contratos do Sector Público, a cal regula, entre outras moitas materias, o establecemento dunha plataforma de contratación electrónica do Estado e a utilización de medios electrónicos, informáticos ou telemáticos por parte das empresas do sector privado para a contratación con Administracións Públicas.

Por outra banda, establece un calendario de implantación progresiva do uso obrigatorio da facturación electrónica por parte das empresas do sector privado que



accedan a contratos do sector público como provedores do mesmo. Neste calendario pódense salientar principalmente dous fitos: un período de transición que finalizou o 1 de agosto do ano 2009 e implica que as sociedades que non presenten conta de perdas e ganancias abreviada xa están obrigadas a presentar facturas electrónicas aos seus clientes que sexan entidades pertencentes ao sector público estatal.

### 13.7.2. LICITACIÓN ELECTRÓNICA

A Lei 30/2007, de Contratos do Sector Público, na súa disposición final novena, dedicada á habilitación normativa en materia de uso de medios electrónicos, informáticos ou telemáticos, e uso de factura electrónica, di o seguinte:

1. Autorízase ao Ministro de Economía e Facenda para aprobar, previo ditame do Consello de Estado, as normas de desenvolvemento da disposición adicional decimonovena que poidan ser necesarias para facer plenamente efectivo o uso de medios electrónicos, informáticos ou telemáticos nos procedementos regulados nesta Lei.
2. Igualmente, o Ministro de Economía e Facenda, mediante Orde, definirá as especificacións técnicas das comunicacións de datos que deban efectuarse en cumprimento da presente Lei e establecerá os modelos que deban utilizarse.
3. No prazo máximo dun ano desde a entrada en vigor da Lei, o Ministro de Economía e Facenda aprobará as normas de desenvolvemento necesarias para facer posible o uso das facturas electrónicas nos contratos que se celebren polas entidades do sector público estatal.
4. Transcorridos tres meses desde a entrada en vigor das normas a que se refire o apartado anterior a presentación de facturas electrónicas será obrigatoria na

contratación co sector público estatal para as sociedades que non poidan presentar conta de perdas e ganancias abreviada.

Por Orde conxunta dos Ministros de Economía e Facenda e de Industria, Turismo e Comercio, estenderase progresivamente a obrigatoriedade do uso das facturas electrónicas para outras persoas físicas e xurídicas en función das súas características e o volume da súa cifra de negocios. En todo caso, transcorridos dezaoito meses desde a entrada en vigor das normas a que se refire o apartado anterior, o uso da factura electrónica será obrigatorio en todos os contratos do sector público estatal; no entanto, nos contratos menores, a utilización da factura electrónica será obligatoria cando así se estableza expresamente nestas Ordes de extensión.

5. O Consello de Ministros, a proposta dos Ministros de Economía e Facenda e de Industria, Turismo e Comercio, adoptará as medidas necesarias para facilitar a emisión de facturas electrónicas polas persoas e entidades que contraten co sector público estatal, garantindo a gratuidade dos servizos de apoio que se establezan para as empresas cuxa cifra de negocios no ano inmediatamente anterior e para o conxunto das súas actividades sexa inferior ao limiar que se fixe na Orde a que se refire o parágrafo anterior.

Na práctica, un sistema de licitación electrónica debe permitir:

- Consultar en Internet as convocatorias dos contratos e obter os pregos. Para iso créase a figura do Perfil do contratante, onde é posible consultar toda a información relativa a expedientes de contratación. O perfil do contratante debe garantir tecnicamente a data e hora da publicación, así como a integridade do contido. Isto lévase á práctica mediante un sistema polo cal o contido que vai ser publicado é primeiro asinado electronicamente, incluíndo a firma un selado de tempo.
- Presentar por medios electrónicos solicitudes de participación, ofertas e documentos. Os licitantes deben poder presentar durante o prazo previsto

ofertas de modo telemático. Para iso poderán facer uso do correspondente rexistro electrónico. Tal e como se explicou no devandito apartado, os licitantes poderán obter o correspondente resgardo.

- Obter información sobre o desenvolvemento do procedemento mediante a consulta dun taboleiro de anuncios electrónico. Novamente a través do perfil do contratante.
- Recibir notificacións telematicamente. Para a emisión de notificacións telemáticas de modo fidedigno (de non ser así, en ocasións denomínanse simplemente comunicacións), dispónse de servizos como o Sistema de Notificacións Telemáticas Seguras creado pola Sociedade Estatal de Correos e Telégrafos. Neste sistema, o cidadán dispón dunha caixa de correos ao que son enviadas as notificacións. O cidadán ten a posibilidade de ignorar, aceptar ou rexeitar as notificacións, coas mesmas garantías que pola canle tradicional, e o servizo informa á Administración da situación en cada caso.

Un sistema de licitación electrónica debe ademais garantir que, en función do procedemento de contratación establecido, só se poderá acceder ás ofertas na fase de tramitación prevista. Permitirá polo tanto definir as mesas de contratación, se é o caso, e establecerá os mecanismos necesarios para que as ofertas non poidan ser abertas ata que estas se constituíron formalmente.

Tecnicamente, isto resólvese mediante a creación de sobres electrónicos, seguindo os pasos que se detallan a continuación:

#### PREPARACIÓN DA LICITACIÓN

- Identifícase aos membros da mesa. O sistema debe ter acceso á clave pública de cada un dos membros.

#### PRESENTACIÓN DE OFERTAS:

- No momento da presentación das ofertas, xérase un par de claves pública e privada para cada unha, e a oferta é cifrada coa clave pública, creando o sobre electrónico.

- Dito sobre só pode ser aberto mediante a correspondente clave privada. Con todo, a clave privada non se almacena no sistema. No seu lugar, aplícaselle un algoritmo que a divide en varias partes.
- Cada parte é asignada a un membro da mesa e cifrada coa súa clave pública, de tal modo que é a única persoa que pode acceder a ela coa súa clave privada.

#### APERTURA DE OFERTAS:

- No día e hora de constitución da mesa de contratación, o sistema considera aberta a mesa de contratación e os membros poden acceder ao sistema.
- Cada un dos membros poden acceder á parte da clave privada do sobre que lle corresponde. Para iso, posto que está cifrada coa súa clave pública, deben utilizar a súa clave privada, identificándoos fidedignamente.
- Unha vez o sistema dispón de suficientes partes da clave privada (non é necesario que participen todos os membros da mesa, senón que é posible establecer previamente un quórum), recompón a clave privada do sobre.
- Coa clave privada do sobre, o sistema xa pode extraer e mostrar a oferta.

Para rematar, o sistema de licitación electrónica debe contar cun compoñente de xestión de expedientes que permita levar a cabo todos os trámites na secuencia correcta, así como garantir o acceso á documentación xerada (actas, informes, etc.) e almacenada.

#### **13.8. REFERENCIAS**

- Lei 30/1992, do 26 de novembro, de Réxime Xurídico das Administracións Públicas e do Procedemento Administrativo Común.
- Lei 15/1999, do 13 de decembro, de Protección de datos de carácter persoal
- Lei 53/1999, do 19 de decembro, de Firma electrónica.
- Lei 34/2002, do 11 de xullo, de Servizos da sociedade da información e de comercio electrónico.
- Lei 11/2007, do 22 de xuño, de Acceso electrónico dos cidadáns aos servizos públicos.

- Lei 30/2007, do 30 de outubro, de Contratos do Sector Público.
- Lei 37/2007, do 16 de novembro, sobre Reutilización da información do sector público.
- Real Decreto 1720/2007, do 21 de decembro, polo que se aproba o Regulamento de desenvolvemento da Lei 15/1999, do 13 de decembro, de protección de datos de carácter persoal.
- Lei 56/2007, do 28 de decembro, de Medidas de impulso da sociedade da Información.
- Real Decreto 1494/2007, do 12 de novembro, polo que se aproba o Regulamento sobre as condicións básicas para o acceso das persoas con discapacidade ás tecnoloxías, produtos e servizos relacionados coa sociedade da información e medios de comunicación social.
- Lei 17/2009, do 23 de novembro, sobre o Libre acceso ás actividades de servizos e o seu exercicio.
- Lei 25/2009, do 22 de decembro, de Modificación de diversas leis para a súa adaptación á Lei 17/2009, do 23 de novembro, sobre o Libre acceso ás actividades de servizos e o seu exercicio.
- Real Decreto 3/2010, de 8 de xaneiro, polo que se regula o Esquema Nacional de Seguridade no ámbito da Administración Electrónica.
- Real Decreto 4/2010, de 8 de xaneiro, polo que se regula o Esquema Nacional de Interoperabilidade no ámbito da Administración Electrónica.
- Decreto 198/2010, do 2 de decembro, polo que se regula o Desenvolvemento da Administración Electrónica na Xunta de Galicia e nas entidades dependentes.
- Resolucións da Secretaría de Estado para a Función Pública pola que se aproban distintas normas técnicas de interoperabilidade.
  
- *Manual práctico de supervivencia de la Administración Electrónica*, de Alberto López Tallón, publicado baixo licenza 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.



**XUNTA  
DE GALICIA**



*ESCOLA GALEGA  
DE ADMINISTRACIÓN  
PÚBLICA*

Autor: Jesús Rodríguez Castro

Xefe do Servizo de Informática do Concello de Santiago de Compostela

Colexiado do CPEIG

**14. INTEROPERABILIDADE.  
COORDINACIÓN  
INTERADMINISTRATIVA E  
INTEROPERABILIDADE NO  
MARCO DA ADMINISTRACIÓN  
ELECTRÓNICA. INICIATIVAS DE  
DESENVOLVEMENTO DA  
ADMINISTRACIÓN  
ELECTRÓNICA: @FIRMA, DNI  
ELECTRÓNICO.**



## **TEMA 14. INTEROPERABILIDADE. COORDINACIÓN ADMINISTRATIVA E INTEROPERABILIDADE NO MARCO DA ADMINISTRACIÓN ELECTRÓNICA. INICIATIVAS DE DESENVOLVEMENTO DA ADMINISTRACIÓN ELECTRÓNICA: @FIRMA, DNI ELECTRÓNICO**

### **14.1. INTEROPERABILIDADE.**

### **14.2. COORDINACIÓN INTERADMINISTRATIVA E INTEROPERABILIDADE NO MARCO DA ADMINISTRACIÓN ELECTRÓNICA.**

### **14.3. INICIATIVAS DE DESENVOLVEMENTO DA ADMINISTRACIÓN ELECTRÓNICA: @FIRMA, DNI ELECTRÓNICO.**

#### **14.3.1. @FIRMA**

#### **14.3.2. DNI ELECTRÓNICO**

### **14.4. REFERENCIAS**

### **14.1. INTEROPERABILIDADE.**

A interoperabilidade é a capacidade dos sistemas de información e dos procedementos aos que estes dan soporte, de compartir datos e posibilitar o intercambio de información e coñecemento entre eles.

Resulta necesaria para a cooperación, o desenvolvemento, a integración e a prestación de servizos conxuntos polas Administracións públicas; para a execución das diversas políticas públicas; para a realización de diferentes principios e dereitos; para a transferencia de tecnoloxía e a reutilización de aplicacións en beneficio dunha mellor eficiencia; para a cooperación entre diferentes aplicacións que habiliten novos servizos; todo iso facilitando o desenvolvemento da administración electrónica e da sociedade da información.

No ámbito das Administracións públicas, a consagración do dereito dos cidadáns a comunicarse con elas a través de medios electrónicos comporta unha obrigaón correlativa das mesmas. Esta obrigaón ten, como premisas, a promoción das condicións para que a liberdade e a igualdade sexan reais e efectivas, así como a eliminación dos obstáculos que impidan ou dificulten o exercicio pleno do principio de neutralidade tecnolóxica e de adaptabilidade ao progreso das tecnoloxías da información e as comunicacións, garantindo con iso a independencia na elección das alternativas tecnolóxicas polos cidadáns, así como a liberdade de desenvolver e implantar os avances tecnolóxicos nun ámbito de libre mercado.

A Lei 11/2007, do 22 de xuño, de acceso electrónico dos cidadáns aos servizos públicos (LAECSP), recoñece o protagonismo da interoperabilidade e refírese a ela como un dos aspectos nos que é obrigado que as previsións normativas sexan comúns e debe ser, xa que logo, abordado pola regulación do Estado.

O Real Decreto 4/2010, do 8 de xaneiro (BOE do 29 de xaneiro. Publicada o 10 de marzo unha corrección de erros), polo que se regula o Esquema Nacional de Interoperabilidade no ámbito da administración electrónica, regula o citado Esquema previsto no artigo 42 da LAECSP, do 22 de xuño, de acceso electrónico dos cidadáns aos Servizos Públicos. O seu obxecto é comprender o conxunto de criterios e recomendacións en materia de seguridade, conservación e normalización da información, dos formatos e das aplicacións que se deberán ter en conta por parte das Administracións Públicas para a toma de decisións tecnolóxicas que garantan a interoperabilidade. En materia de seguridade, véxase o Esquema Nacional de Seguridade regulado no Real Decreto 3/2010, do 8 de xaneiro.

O Esquema Nacional de Interoperabilidade persegue a creación das condicións necesarias para garantir o adecuado nivel de interoperabilidade técnica, semántica e organizativa dos sistemas e aplicacións empregados polas Administracións Públicas, que permita o exercicio de dereitos e o cumprimento de deberes a través do acceso

electrónico aos servizos públicos, á vez que redunda en beneficio da eficacia e a eficiencia.

Ao obxecto de crear estas condicións, o Esquema Nacional de Interoperabilidade introduce os elementos comúns que han de guiar a actuación das Administracións Públicas en materia de interoperabilidade. En particular, introduce os seguintes elementos principais:

- Enúncianse os principios específicos da interoperabilidade.
- Contémplanse as dimensións da interoperabilidade organizativa, semántica e técnica ás que se refire o artigo 41 da LAECSP.
- Trátanse as infraestruturas e os servizos comúns, elementos recoñecidos de dinamización, simplificación e propagación da interoperabilidade, á vez que facilitadores da relación multilateral.
- Trátase a reutilización, aplicada ás aplicacións das administracións públicas, da documentación asociada e doutros obxectos de información, dado que a voz 'compartir' se atopa presente na definición de interoperabilidade recollida na LAECSP, e xunto coa voz 'reutilizar', ambas son relevantes para a interoperabilidade e atópanse entroncadas coas políticas da Unión Europea en relación coa idea de compartir, reutilizar e colaborar.
- Trátase a interoperabilidade da sinatura electrónica e dos certificados.
- Aténdese á recuperación e conservación do documento electrónico, segundo o establecido na citada LAECSP como manifestación da interoperabilidade ao longo do tempo, e que afecta de forma singular ao documento electrónico.
- Para rematar, créanse as normas técnicas de interoperabilidade e os instrumentos para a interoperabilidade, co fin de facilitar a aplicación do Esquema.
- Ten en conta as recomendacións da Unión Europea, a situación tecnolóxica das diferentes Administracións Públicas, así como os servizos electrónicos xa existentes e a utilización de estándares abertos así como, no seu caso e de

forma complementaria, estándares que sexan de uso xeneralizado por parte dos cidadáns.

- Na súa elaboración manexáronse, entre outros, referentes en materia de desenvolvemento da administración electrónica e, en particular, de interoperabilidade provenientes do ámbito da Unión Europea, de actuacións similares noutros países, da normalización nacional e internacional; así como a normativa sobre administración electrónica, protección de datos de carácter persoal, sinatura electrónica e Documento Nacional de Identidade Electrónico, entre outros.

Realizouse nun proceso coordinado polo Ministerio da Presidencia, coa participación de todas as Administracións Públicas.

Os seus obxectivos son os seguintes:

- Comprender os criterios e recomendacións que se deberán ter en conta por parte das administracións públicas para a toma de decisións tecnolóxicas que garantan a interoperabilidade e que eviten a discriminación aos cidadáns por razón da súa elección tecnolóxica.
- Introducir os elementos comúns que deberán guiar a actuación das administracións públicas en materia de interoperabilidade.
- Achegar unha linguaxe común para facilitar a interacción das administracións públicas, así como a comunicación dos requisitos de interoperabilidade á industria.

A interoperabilidade concíbese, en consecuencia, desde unha perspectiva integral, de maneira que non caben actuacións puntuais ou tratamentos conxunturais, debido a que a debilidade dun sistema a determina o seu punto máis fráxil e, a miúdo, este punto é a coordinación entre medidas individualmente adecuadas pero deficientemente ensambladas.

Dada a natureza da interoperabilidade, a consecución destes obxectivos require un desenvolvemento que teña en conta a complexidade técnica, a obsolescencia da tecnoloxía subxacente e o importante cambio que supón na operativa da administración a aplicación da LAECSP.

O Esquema Nacional de Interoperabilidade no ámbito da Administración Electrónica establece, na súa disposición adicional primeira, o desenvolvemento da serie de Normas Técnicas de Interoperabilidade que son de obrigado cumprimento por parte das Administracións públicas.

As Normas Técnicas de Interoperabilidade desenvolven aspectos concretos de diversas cuestións necesarios para asegurar os aspectos máis prácticos e operativos da interoperabilidade entre as Administracións públicas e co cidadán. A relación de normas incluída na citada disposición adicional primeira é a seguinte<sup>1</sup>:

- Catálogo de estándares.
- Documento electrónico (\*).
- Dixitalización de documentos (\*).
- Expediente electrónico (\*).
- Política de sinatura electrónica e de certificados da Administración (\*).
- Protocolos de intermediación de datos.
- Relación de modelos de datos que teñan o carácter de comúns na Administración e aqueles que se refiran a materias suxeitas a intercambio de información cos cidadáns e outras administracións.
- Política de xestión de documentos electrónicos.
- Requisitos de conexión á Rede de comunicacións das Administracións Públicas españolas (\*).

---

<sup>1</sup> As Normas Técnicas marcadas co símbolo (\*) foron xa desenvolvidas e publicadas no Boletín Oficial do Estado número 182 do 30 de xullo de 2011.

- Procedementos de copiado auténtico e conversión entre documentos electrónicos, así como desde papel ou outros medios físicos a formatos electrónicos (\*).
- Modelo de Datos para o intercambio de asentos entre as Entidades Rexistras (\*).

Estanse elaborando coa participación de todas as Administracións públicas, Administración Xeral do Estado, Comunidades Autónomas, Corporacións Locais a través da FEMP e Universidades Públicas a través da CRUE.

Os Ministerios de Política Territorial e Administración Pública e de Industria, Turismo e Comercio lanzaron en 2009 o Proxecto Aporta (<http://www.aporta.es>), co obxectivo de impulsar o sector da reutilización da información do sector público (RISP) no noso país.

#### **14.2. COORDINACIÓN INTERADMINISTRATIVA E INTEROPERABILIDADE NO MARCO DA ADMINISTRACIÓN ELECTRÓNICA.**

A LAECSP determina que o Comité Sectorial de administración electrónica, dependente da Conferencia Sectorial de Administración Pública, é o órgano técnico de cooperación da Administración Xeral do Estado, das administracións das Comunidades Autónomas e das entidades que integran a Administración Local en materia de administración electrónica.

O Comité Sectorial da administración electrónica velará polo cumprimento dos fins e principios establecidos na LAECSP, e en particular desenvolverá as seguintes funcións:

- Asegurar a compatibilidade e interoperabilidade dos sistemas e aplicacións empregados polas Administracións Públicas.

- Preparar plans programas conxuntos de actuación para impulsar o desenvolvemento da administración electrónica en España.
- Asegurar a cooperación entre as administracións públicas para proporcionarlle ao cidadán información administrativa clara, actualizada e inequívoca.

Cando por razón das materias tratadas resulte de interese, poderá invitarse ás organizacións, corporacións ou axentes sociais que se estime conveniente en cada caso a participar nas deliberacións do comité sectorial.

Os grupos de traballo que ten definidos actualmente son os seguintes:

- Rede SARA, a través da cal se interconectan todas as Administracións Públicas: Unión Europea, Administración Xeral do Estado, Comunidades Autónomas e Concellos.
- Identificación e sinatura electrónica, traballa en servizos e aspectos relacionados coa harmonización da sinatura electrónica e a expansión do DNI electrónico.
- Mellora de Procesos Software: pretende elaborar unhas directrices que permitan mellorar o desenvolvemento do software e os procedementos para a súa adquisición por parte das administracións públicas.
- Observatorio Administración Electrónica (OBSAE): Permite coñecer o estado da Administración electrónica nas administracións públicas e cuxo principal produto é o informe CAE.
- Programas Libres e reutilización dos sistemas de información: Traballa na coordinación entre as diversas distribucións GNU/Linux autonómicas; a promoción dos estándares abertos; a consolidación do apoio ás actuacións de normalización en curso en materia do Formato Aberto de Documentos (Proxecto ISO/IEC DIS 26300) e en materia de compatibilidade do hardware con GNU/Linux (Grupo Técnico de AENOR AEN GT22). Para reutilización realizouse un sistema automatizado que trata a información do inventario de

aplicacións de todas as CCAA e preténdese obter un marco de reutilización de obxectos.

As Administracións Públicas utilizarán as tecnoloxías da información nas súas relacións coas demais administracións e cos cidadáns, aplicando medidas informáticas, tecnolóxicas, organizativas e de seguridade, que garantan un adecuado nivel de interoperabilidade técnica, semántica e organizativa e eviten discriminación dos cidadáns por razón da súa elección tecnolóxica.

- O Esquema Nacional de Interoperabilidade comprende o conxunto de criterios e recomendacións en materia de seguridade, conservación e normalización da información, dos formatos e das aplicacións que se deberán ter en conta por parte das Administracións Públicas para a toma de decisións tecnolóxicas que garantan a interoperabilidade.
- O Esquema Nacional de Seguridade ten por obxecto establecer a política de seguridade na utilización de medios electrónicos no ámbito da presente Lei, e está constituído polos principios básicos e requisitos mínimos que permitan unha protección adecuada da información.

Ambos Esquemas elaboráronse coa participación de todas as Administracións e foron aprobados por Real Decreto do Goberno, a proposta da Conferencia Sectorial de Administración Pública e previo informe da Comisión Nacional de Administración Local, debendo manterse actualizados de xeito permanente.

Na elaboración de ambos Esquemas teranse en conta as recomendacións da Unión Europea, a situación tecnolóxica das diferentes Administracións Públicas, así como os servizos electrónicos xa existentes. A estes efectos considerarán a utilización de estándares abertos así como, no seu caso e de forma complementaria, estándares que sexan de uso xeneralizado polos cidadáns.



A Administración Xeral do Estado, as Administracións Autonómicas e as entidades que integran a Administración Local, así como os consorcios ou outras entidades de cooperación constituídos a tales efectos por estas, adoptarán as medidas necesarias e incorporarán nos seus respectivos ámbitos as tecnoloxías precisas para posibilitar a interconexión das súas redes co fin de crear unha rede de comunicacións que interconecte os sistemas de información das Administracións Públicas españolas e permita o intercambio de información e servizos entre as mesmas, así como a interconexión coas redes das Institucións da Unión Europea e doutros Estados Membros.

As Administracións Públicas poderán subscribir convenios de colaboración co obxecto de articular medidas e instrumentos de colaboración para a implantación coordinada e normalizada dunha rede de espazos comúns ou portelos únicos.

En particular, e de conformidade co disposto no apartado anterior, hanse implantar espazos comúns ou portelos únicos para obter a información prevista no artigo 6.3 da LAECSP e para realizar os trámites e procedementos aos que fai referencia o apartado a do devandito artigo.

## REUTILIZACIÓN DE APLICACIÓNS E TRANSFERENCIA DE TECNOLOXÍA

A este respecto, a LAECSP establece que as administracións titulares dos dereitos de propiedade intelectual de aplicacións, desenvolvidas polos seus servizos ou cuxo desenvolvemento sexa obxecto de contratación, poderán poñelas a disposición de calquera Administración sen contraprestación e sen necesidade de convenio.

As aplicacións ás que se refire o apartado anterior poderán ser declaradas como de fontes abertas, cando diso se derive unha maior transparencia no funcionamento da

Administración Pública ou se fomenta a incorporación dos cidadáns á Sociedade da información

As Administracións Públicas manterán directorios actualizados de aplicacións para a súa libre reutilización, especialmente naqueles campos de especial interese para o desenvolvemento da administración electrónica e de conformidade co que respecto diso se estableza no Esquema Nacional de Interoperabilidade.

A Administración Xeral do Estado, a través dun centro para a transferencia da tecnoloxía, manterá un directorio xeral de aplicacións para a súa reutilización, prestará asistencia técnica para a libre reutilización de aplicacións e impulsará o desenvolvemento de aplicacións, formatos e estándares comúns de especial interese para o desenvolvemento da administración electrónica no marco dos esquemas nacionais de interoperabilidade e seguridade.

No sitio web do Consello Superior de Administración Electrónica ou CSAE, cuxa dirección é <http://www.csae.map.es/>, ou a través do Portal de Administración Electrónica ou PAE, cuxa dirección é <http://administracionelectronica.gob.es/>, é posible acceder ao Centro de Transferencia de Tecnoloxía (CTT).

O Centro de Transferencia de Tecnoloxía (CTT) publica un directorio xeral de aplicacións e/ou iniciativas cuxo obxectivo é favorecer a reutilización de solucións por todas as Administracións Públicas. Este portal informa de proxectos, iniciativas, servizos, normativa e solucións que se están desenvolvendo en materia de Administración electrónica. Ademais, desde a forxa do CTT permítese o desenvolvemento colaborativo de aplicacións das administracións públicas.

O CTT conta con dous ámbitos tecnolóxicos nos que traballar en función de diferentes necesidades.

- O ámbito CTT-PAe ou directorio de iniciativas do CTT é o lugar indicado para atopar unha iniciativa, proxecto ou/e servizo para reutilizar na túa administración. Neste ámbito está dispoñible a información divulgativa de todas as iniciativas recollidas no CTT e ofrécense diferentes opcións de descarga e de colaboración nelas.
- O ámbito da forxa-CTT, é unha contorna de desenvolvemento colaborativo para aplicacións das administracións públicas na que poden participar activamente administracións, empresas e particulares. Conta con funcionalidades de descargas, documentos, novidades, foros, rexistros de incidencias, bugs, suxestións, enquisas, distribución de tarefas, listas de distribución de correo e xestión do código fonte.

A Lei 37/2007, do 16 de novembro, sobre reutilización da información do sector público ten por obxecto a regulación básica do réxime xurídico aplicable á reutilización dos documentos elaborados ou custodiados polas Administracións e organismos do sector público.

CENATIC é o Centro Nacional de Referencia de Aplicación das Tecnoloxías da Información e a Comunicación (TIC) baseadas en fontes abertas.

CENATIC é unha Fundación Pública Estatal, promovida polo Ministerio de Industria, Turismo e Comercio (a través da Secretaría de Telecomunicacións e para a Sociedade da Información e a entidade pública Red.es) e a Junta de Extremadura, que ademais conta no seu Padroado coas comunidades autónomas de Andalucía, Asturias, Aragón, Cantabria, Cataluña, Illes Balears, País Vasco e Xunta de Galicia. Tamén forma parte do Padroado de CENATIC a empresa Telefónica.

CENATIC é o único proxecto estratéxico do Goberno de España para impulsar o coñecemento e uso do software de fontes abertas en todos os ámbitos da sociedade.

A vocación da Fundación é situarse como centro de excelencia nacional, con proxección internacional, tanto no ámbito europeo coma iberoamericano.

### **14.3. INICIATIVAS DE DESENVOLVEMENTO DA ADMINISTRACIÓN ELECTRÓNICA: @FIRMA, DNI ELECTRÓNICO.**

A comunicación a través de medios telemáticos e a administración electrónica require o uso da sinatura electrónica na administración. A sinatura electrónica constitúe un instrumento capaz de permitir unha comprobación da procedencia e da integridade das mensaxes intercambiadas a través de redes de telecomunicacións, ofrecendo as bases para evitar o repudio, se se adoptan as medidas oportunas baseándose en datos electrónicos.

A utilización da sinatura electrónica na administración pública está regulada na seguinte normativa, entre outra:

- Directiva 1999/93/CE do Parlamento Europeo e do Consello, do 13 de decembro de 1999, pola que se establece un marco comunitario para a sinatura electrónica
- Lei 59/2003, do 19 de decembro, de sinatura electrónica
- LEI 11/2007, do 22 de xuño, de acceso electrónico dos cidadáns aos Servizos Públicos.
- Real Decreto 1671/2009, do 6 de novembro, polo que se desenvolve parcialmente a Lei 11/2007, do 22 de xuño, de acceso electrónico dos cidadáns aos servizos público.
- Real Decreto 3/2010, do 8 de xaneiro, polo que se regula o Esquema Nacional de Seguridade no ámbito da Administración Electrónica
- Real Decreto 4/2010, do 8 de xaneiro, polo que se regula o Esquema Nacional de Interoperabilidade no ámbito da Administración Electrónica

### **14.3.1. @FIRMA**

@FIRMA é unha plataforma de validación e sinatura electrónica multi-PKI, que se pon a disposición das Administracións Públicas, proporcionando servizos para implantar a autenticación e sinatura electrónica avanzada dunha forma rápida e efectiva.

Trátase dun proxecto da Dirección Xeral para o Impulso da Administración Electrónica, dependente do Ministerio de Política Territorial e Administración Pública.

As Administracións Públicas ofrecen aos cidadáns servizos públicos electrónicos nos que se necesita sinatura electrónica e métodos avanzados de identificación ou autenticación baseados en certificados dixitais. Debido aos múltiples certificados que poden utilizarse para a identificación e a sinatura, implantar sistemas que soporten todas as funcionalidades e relacións coas CA pode resultar complexo e custoso.

Este proxecto céntrase en facilitar ás aplicacións os complementos de seguridade necesarios para implantar a autenticación e sinatura electrónica avanzada baseada en certificados dixitais dunha forma eficaz e efectiva. Ofrécense así servizos que impulsan o uso da certificación e sinatura electrónica nos sistemas de información das diferentes Administracións públicas que así o requiran.

É unha solución de referencia para cumprir coas medidas de identificación e autenticación descritas no Capítulo II da LAECSP.

Desde o punto de vista tecnolóxico, constrúe unha capa de abstracción de seguridade a nivel de aplicación que desacopla a lóxica de negocio das aplicacións da introdución de mecanismos de seguridade no ámbito de control de accesos, sinatura, cifrado, control do non repudio e validez dos certificados, etc.

Facilita a creación de redes de confianza e de recoñecemento mutuo de servizos de

validación entre autoridades de validación e os prestadores de certificación acreditados así como primeira base para cumprir co plan de acción i2010 en materia de interoperatividade do IDM (xestión de identidades electrónicas) da Unión Europea.

O obxectivo desta plataforma de validación é comprobar que o certificado utilizado polo cidadán é un certificado válido e que non foi revogado e que, xa que logo, segue tendo plena validez para identificar ao seu propietario.

Os servizos da plataforma son aplicables a todos os certificados electrónicos cualificados publicados por calquera proveedor de servizo de certificación acreditado en España, incluídos os certificados da tarxeta do DNIe do cidadán.

A través do conxunto de aplicacións da suite @firma proporciónanse uns servizos horizontais de sinatura e uns compoñentes informáticos. Estes servizos e aplicacións póñense a disposición das administracións públicas que o desexen:

- @firma: Plataforma de validación de certificados e sinaturas do Ministerio de Política Territorial e Administración Pública
- CLIENTE de @firma: Applet de xeración de sinaturas en diferentes formatos
- Autoridade de selado de tempo do Ministerio de Política Territorial e Administración Pública
- Valide: Aplicación web para o usuario final de validación de sinaturas e certificados. Demostrador de @firma
- Portafirmas: Compoñente para a integración da sinatura nos fluxos de traballo organizativos
- Stork: Proxecto para conseguir o recoñecemento paneuropeo das identidades electrónicas, e en concreto a aceptación do DNI electrónico e identificadores similares en Servizos de Administración Electrónica doutras administracións europeas

- Política de sinatura e certificados: directrices e normas técnicas aplicables á utilización de certificados e sinatura electrónica na Administración Xeral do Estado

Cando o cidadán interacciona coa Administración, para realizar un trámite persoal, é necesario coñecer a súa identidade, que telematicamente se realiza a través do DNI electrónico ou un certificado electrónico. A Administración comproba o estado do certificado ou o DNIE co que o cidadán estase identificando ou asinando a solicitude. Para esta comprobación utilízase a plataforma de validación @firma, delegando nela a verificación das credenciais do certificado ou DNIE utilizado.

Ademais, dispón de múltiples utilidades de valor engadido, entre as que se atopan a xeración e validación de sinaturas electrónicas en múltiples formatos, auditoría das transaccións e documentos asinados, selado de tempos ou a compatibilidade con certificados dixitais xerados por múltiples prestadores de servizos de certificación.

A plataforma de validación do Ministerio da Política Territorial e Administración Pública funciona como un servizo non intrusivo ou pechado, que pode ser utilizado por todos os servizos telemáticos ofrecidos polas distintas Administracións Públicas.

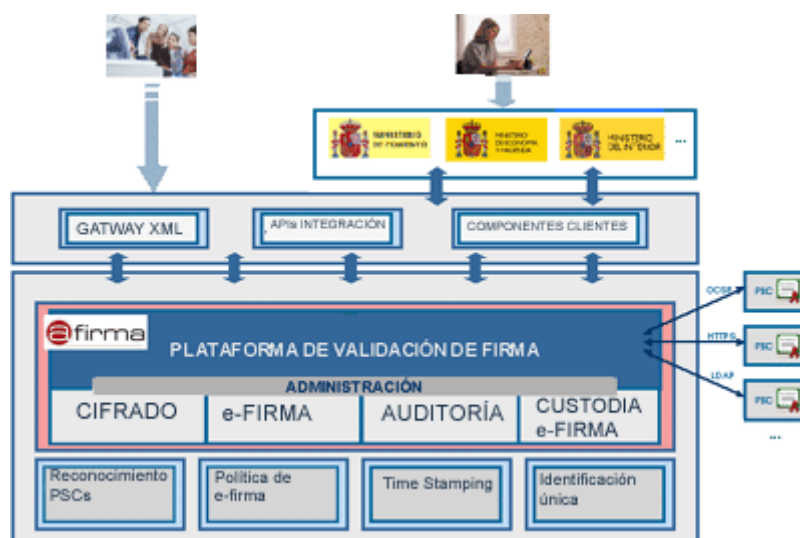
Os servizos ofrecidos aos organismos pódense catalogar en catro bloques, baseándose a maioría na publicación dun catálogo amplo de servizos web compatible coas tecnoloxías java e Microsoft. Todos os servizos web atópanse dispoñibles tanto en castelán como en inglés, facilitando así a integración e interoperabilidade con solucións existentes nas implantacións dos organismos usuarios.

1. Servizos de validación: servizos web de validación de sinaturas dixitais en múltiples formatos e certificados electrónicos de diferentes perfís e prestadores.
2. Servizos de sinatura electrónica: sinatura electrónica de servidor simple, en paralelo (cosign), en cadoiro (countersign) ou en bloque. Nestes momentos estes

servizos non se están mantendo e actualizando, por iso proporciónase un compoñente de sinatura electrónica para contorna de usuario final. Actualización de sinaturas electrónicas a un formato máis avanzado, para iso é posible especificar o formato ao que se desexa estender a sinatura. Os distintos valores poden ser: BES, EPES, T, C, X, X-1, X-2, X-L, X-L-1, X-L-2 e A. Soporta os algoritmos de hash SHA1 e SHA2 e os algoritmos de sinatura RSA e curvas elípticas. Validación lonxeva de sinaturas.

3. Servizos de soporte á Operación: a través de servizos de soporte á integración, apoio á evolución cara a novos estándares de sinatura electrónica, etc.

Esquema de funcionamento da plataforma de validación.



A plataforma de validación @firma na súa versión 5.5 proporciona servizos de validación de certificados e de sinatura electrónica dos principais Prestadores de Servizos de Certificación recoñecidos do noso país, entre eles a Dirección Xeral de Policía.

Os servizos que ofrece son:



1. Funcionalidades de verificación: Validación de certificados X.509 segundo a RFC 3280, das Autoridades de Certificación incluídas na plataforma. Entre as funcionalidades de validación pódense destacar:

- Recoñecemento e validación do DNI electrónico emitido pola Dirección Xeral da Policía, e de múltiples prestadores.
- Validación de certificados X.509 segundo a RFC 3280, de todas as Autoridades de Certificación recoñecidas no país polo Ministerio de Industria
- Validación Multinivel de certificados (no caso de estrutura de certificación de máis de dous niveis).
- Obtención mediante unha análise en XML, da información correspondente aos campos do certificado, segundo a Política de Confianza definida para o tipo de certificado de que se trate.
- Caché de validación configurable en tempo, para evitar ter que acceder ao Proveedor de Servizos de Certificación ante validacións dun mesmo certificado nun curto período de tempo.

2. Funcionalidades de Sinatura: A plataforma permite varias modalidades de sinatura como de servidor, de bloque, en dúas fases e en tres fases (Nestes momentos os servizos de sinatura en servidor non se están mantendo e actualizando). Ademais:

- Fai transparente para as aplicacións o uso de diferentes formatos de sinatura electrónica como PKCS#7, CMS, XML signature, PDF, ODF, XAdES e CAdES
- Ofrécese un Cliente de sinatura que permite a asinar electrónica de documentos por parte dos cidadáns que accedan aos servizos de Administración Electrónica. Para iso empréganse os certificados dixitais de usuario que se atopan instalados no navegador ou dispoñibles a través dun módulo PKCS#11 instalado no navegador. O devandito cliente é compatible cos S.Ou. Windows XP, 2000 e Linux; e con navegadores Mozilla Firefox e Internet Explorer.

- Validación de sinatura vía servizos web (WS) dun elemento asinado, indicando se a sinatura é correcta e a validez, datado de tempo, etc. Tamén se realiza a interpretación dos campos dos certificados a un XML homoxéneo.
  - Permite a actualización de sinaturas electrónicas a un formato máis avanzado, para iso é posible especificar o formato ao que se desexa estender a sinatura. Os distintos valores poden ser: BES, EPES, T, C, X, X-1, X-2, X-L, X-L-1, X-L-2 e A.
  - Nestes momentos os algoritmos de hash soportados son SHA1 e SHA2 (o resto atópanse obsoletos).
  - Nestes momentos os algoritmos de sinatura dixital soportados son RSA e curvas elípticas.
3. Selado de Tempo (TSA) Inclúese un servizo de selado de tempo segundo o estándar RFC 3161 para certificar temporalmente todas as operacións de validación e sinatura que se realizan a través da plataforma.
4. Xestión e administración: A plataforma realiza a xestión e administración dos Prestadores de Servizos de Certificación adheridos. Todas as operacións realizadas na plataforma son rexistradas para a auditoría e trazabilidade do sistema.

Os beneficios que a plataforma facilita aos organismos son:

1. O recoñecemento de múltiples certificados.
2. Independencia do prestadores de servizos de certificación xa que soporta de varios protocolos de validación de certificados (OCSP, HTTP, LDAP).
3. O uso de Políticas de Seguridade para garantir a confidencialidade, autenticidade e integridade de todas as transaccións realizadas.
4. Maior eficiencia e menor custo na utilización da sinatura electrónica nos servizos telemáticos prestados.
5. Fai transparente para as aplicacións o uso de diferentes formatos de sinatura electrónica como PKCS#7, CMS, XML signature, XAdES e CAdES

6. A interoperabilidade cos servizos proporcionados polas Administracións Públicas. Faise extensible a interoperabilidade ao ámbito Europeo e ao dos seus organismos e institucións ao ser contempladas as especificacións de compatibilidade coa Unión Europea.
7. Redución de custos: o servizo permite optimizar o custo dos servizos de validación de certificados por cada aplicación.
8. Innovación: a plataforma da validación multi-PKI converteuse no primeiro servizo centralizado principal que proporciona servizos electrónicos horizontais a todas as Administracións Públicas do país gratuitamente.
9. Boas prácticas: trasladar o modelo español a foros europeos e aos grupos de traballo de e-signature de IDABC.

Pódese atopar no Portal PAE-CTT a documentación necesaria sobre cada actualización nos servizos, así como os recursos actualizados (esquemas e descritores de servizo).

Ademais, na dirección <https://valide.redsara.es/valide/> pódese acceder a VALIDe, o servizo de validación e demostrador de sinatura electrónica.

### **14.3.2. DNI ELECTRÓNICO**

Ademais de toda a lexislación relativa á utilización de certificados electrónicos, o DNIe electrónico atópase regulado no Real Decreto 1553/2005, do 23 de decembro, polo que se regula a expedición do Documento Nacional de Identidade e os seus certificados de sinatura electrónica (BOE núm. 307, do 24 de decembro de 2005). Transcríbense a continuación os principais artigos, especialmente os relativos á incorporación e utilización de certificados electrónicos.

O Documento Nacional de Identidade é un documento persoal e intransferible emitido polo Ministerio do Interior que goza da protección que aos documentos públicos e

oficiais outorgan as leis. O seu titular estará obrigado á custodia e conservación do mesmo.

O devandito Documento ten suficiente valor, por si só, para acreditar a identidade e os datos persoais do seu titular que nel se consignen, así como a nacionalidade española do mesmo.

A cada Documento Nacional de Identidade, asignaráselle un número persoal que terá a consideración de identificador numérico persoal de carácter xeral.

Igualmente, o Documento Nacional de Identidade permite aos españois maiores de idade e que gocen de plena capacidade de obrar a identificación electrónica do seu titular, así como realizar a sinatura electrónica de documentos, nos termos previstos na Lei 59/2003, do 19 de decembro, de sinatura electrónica.

A sinatura electrónica realizada a través do Documento Nacional de Identidade terá respecto dos datos consignados en forma electrónica o mesmo valor que a sinatura manuscrita en relación cos consignados en papel.

Será competencia do Ministerio do Interior o exercicio das funcións relativas á xestión, dirección, organización, desenvolvemento e administración de todos aqueles aspectos referentes á expedición e confección do Documento Nacional de Identidade, conforme ao previsto na lexislación en materia de seguridade cidadá e de sinatura electrónica.

O exercicio das competencias a que se refire o apartado anterior, incluída a emisión dos certificados de sinatura electrónica recoñecidos, será realizado pola Dirección Xeral da Policía, a quen corresponderá tamén a custodia e responsabilidade dos arquivos e ficheiros, automatizados ou non, relacionados co Documento Nacional de Identidade. Para ese efecto, a Dirección Xeral da Policía quedará sometida ás

obligacións impostas ao responsable do ficheiro pola Lei Orgánica 15/1999, do 13 de setembro, de Protección de Datos de Carácter Persoal.

O Documento Nacional de Identidade expedirase a solicitude do interesado na forma e lugares que para tal efecto se determinen, para o que deberá achegar os documentos que se establecen no artigo 5.1 deste Real Decreto.

Para solicitar a expedición do Documento Nacional de Identidade será imprescindible a presenza física da persoa a quen se lle deba expedir, o aboamento da taxa legalmente establecida en cada momento e a presentación da correspondente documentación.

Con carácter xeral o Documento Nacional de Identidade terá un período de validez, a contar desde a data da expedición ou de cada unha das súas renovacións, de:

- a) Cinco anos, cando o titular non cumpra os trinta no momento da expedición ou renovación
- b) Dez anos, cando o titular cumpra os trinta e non alcance os setenta.
- c) Permanente cando o titular cumpra os setenta anos.

De forma excepcional poderase outorgar validez distinta ao Documento Nacional de Identidade nos seguintes supostos de expedición e renovación:

- a) Permanente, a persoas maiores de trinta anos que acrediten a condición de grande inválido.
- b) Por un ano, nos supostos do apartado segundo do artigo 5 e do mesmo apartado do artigo 7.

Transcorrido o período de validez que para cada suposto se contempla no artigo anterior, o Documento Nacional de Identidade considerarase caducado e quedarán sen efecto as atribucións e efectos que lle recoñece o ordenamento xurídico, estando

o seu titular obrigado a proceder á renovación do mesmo. Dita renovación levarase a cabo mediante a presenza física do titular do Documento.

Independentemente dos supostos do apartado anterior deberase proceder á renovación do Documento Nacional de Identidade nos supostos de variación dos datos que se recollen no mesmo; nese caso será preciso achegar, ademais do establecido no apartado anterior, os documentos xustificativos que acrediten dita variación.

O extravío, subtracción, destrución ou deterioro do Documento Nacional de Identidade, implicará a obrigaón do seu titular de proverse inmediatamente dun duplicado, que será expedido na forma e cos requisitos indicados para a renovación prevista no apartado primeiro do artigo anterior. A validez destes duplicados será a mesma que tiñan os documentos aos que substitúen, salvo que estes se atopen dentro dos últimos 90 días da súa vixencia; nese caso expediranse coa mesma validez que se se tratase dunha renovación.

A entrega do Documento Nacional de Identidade deberá realizarse persoalmente ao seu titular, e cando este sexa menor de 14 anos ou incapaz levarase a cabo en presenza da persoa que teña encomendada a patria potestade ou tutela, ou persoa apoderada por estas últimas. No momento da entrega do Documento Nacional de Identidade proporcionarase a información á que se refire o artigo 18. b) da Lei 59/2003, do 19 de decembro.

A activación da utilidade informática a que se refire o artigo 1.4, que terá carácter voluntario, levarase a cabo mediante unha clave persoal secreta, que o titular do Documento Nacional de Identidade poderá introducir reservadamente no sistema.

Ao entregar o Documento renovado, procederase á retirada do anterior para a súa inutilización física. Unha vez inutilizado poderá ser devolto ao seu titular se este o solicita.

O material, formato e deseño da tarxeta soporte do Documento Nacional de Identidade determinarase por parte do Ministerio do Interior, tendo en conta na súa elaboración a utilización de procedementos e produtos conducentes á consecución de condicións de calidade e inalterabilidade e máximas garantías para impedir a súa falsificación. Levará incorporado un chip electrónico co obxecto de posibilitar a utilidade informática á que se refire o artigo 1.4 deste Real Decreto.

O Documento Nacional de Identidade recollerá graficamente os seguintes datos do seu titular:

- No anverso: Apelidos e nome, data de nacemento, sexo, nacionalidade, Número persoal do Documento Nacional de Identidade e carácter de verificación correspondente ao Número de Identificación Fiscal, fotografía, sinatura manuscrita.
- No reverso: Lugar de nacemento, provincia-nación, nome dos pais, enderezo, lugar de enderezo, provincia, nación, Carácteres OCR-B de lectura mecánica.

Os datos de filiación reflectiranse nos mesmos termos en que consten na certificación á que se alude no artigo 5.1.a) deste Real Decreto, excepto no campo de carácteres OCR-B de lectura mecánica, en que por aplicación de acordos ou convenios internacionais a transcripción literal daqueles datos impida ou dificulte a lectura mecánica e finalidade daqueles carácteres.

Igualmente constarán os seguintes datos referentes ao propio Documento e á tarxeta soporte: Data de caducidade e número de soporte.

O chip incorporado á tarxeta soporte conterá:

- Datos de filiación do titular.
- Imaxe dixitalizada da fotografía.
- Imaxe dixitalizada da sinatura manuscrita.
- Plantilla da impresión dactilar do dedo índice da man dereita ou, no seu caso, do que corresponda segundo o indicado no artigo 5.3 deste Real Decreto.
- Certificados recoñecidos de autenticación e de sinatura, e certificado electrónico da autoridade emisora, que conterán os seus respectivos períodos de validez.
- Claves privadas necesarias para a activación dos certificados mencionados anteriormente.

Con independencia do que establece o artigo 6.1 sobre a validez do Documento Nacional de Identidade, os certificados electrónicos recoñecidos incorporados ao mesmo terán un período de vixencia de trinta meses.

Á extinción da vixencia do certificado electrónico poderá solicitarse a expedición de novos certificados recoñecidos, mantendo a mesma tarxeta do Documento Nacional de Identidade mentres o devandito Documento continúe vixente. Para a solicitude dun novo certificado deberá mediar a presenza física do titular na forma e cos requisitos que se determinen polo Ministerio do Interior, de acordo co previsto na Lei 59/2003, do 19 de decembro.

O cumprimento do período establecido no apartado anterior implicará a inclusión dos certificados na lista de certificados revogados que será mantida pola Dirección Xeral da Policía, ben directamente ou a través das entidades ás que encomende a súa xestión.

A perda de validez do Documento Nacional de Identidade levará aparellada a perda de validez dos certificados recoñecidos incorporados ao mesmo. A renovación do



Documento Nacional de Identidade ou a expedición de duplicados do mesmo implicará, á súa vez, a expedición de novos certificados electrónicos.

Tamén serán causas de extinción da vixencia do certificado recoñecido as establecidas na Lei 59/2003, do 19 de decembro, que resulten de aplicación, e, entre outras, o falecemento do titular do Documento Nacional de Identidade electrónico.

De acordo e en cumprimento do artigo 19 da Lei 59/2003, do 19 de decembro, o Ministerio do Interior formulará unha Declaración de Prácticas e Políticas de Certificación. Dita Declaración de Prácticas e Políticas de Certificación estará dispoñible para o público de xeito permanente e facilmente accesible na páxina de internet do Ministerio do Interior.

A documentación requirida para a expedición do Documento Nacional de Identidade no artigo 5.1 deste Real Decreto non será esixible cando sexa posible remitir esta desde os órganos competentes por medios telemáticos á Dirección Xeral da Policía, de conformidade co que se estableza mediante Convenio.

Nestes casos, por Orde do Ministro do Interior establecerase o réxime de achega dos devanditos documentos.

Coa chegada da Sociedade da Información e a xeneralización do uso de Internet faise necesario adecuar os mecanismos de acreditación da personalidade á nova realidade e dispoñer dun instrumento eficaz que traslade ao mundo dixital as mesmas certezaas coas que operamos cada día no mundo físico e que, esencialmente, son:

- Acreditar electronicamente e de forma certa a identidade da persoa
- Asinar dixitalmente documentos electrónicos, outorgándolles unha validez xurídica equivalente á que lles proporciona a sinatura manuscrita

Para responder a estas novas necesidades nace o Documento Nacional de Identidade electrónico (DNIe), similar ao tradicional e cuxa principal novidade é que incorpora un pequeno circuíto integrado (chip), capaz de gardar de forma segura información e de procesala internamente.

Para poder incorporar este chip, o Documento Nacional de Identidade cambia o seu soporte tradicional (cartolina plastificada) por unha tarxeta de material plástico, dotada de novas e maiores medidas de seguridade. A esta nova versión do Documento Nacional de Identidade ao que nos referimos como DNI electrónico permitíranos, ademais do seu uso tradicional, acceder aos novos servizos da Sociedade da Información, que ampliarán as nosas posibilidades de actuar a distancia coas Administracións Públicas, coas empresas e con outros cidadáns.

A Autoridade de Validación é o compoñente que ten como tarefa fornecer información sobre a vixencia dos certificados electrónicos que, á súa vez, sexan rexistrados por unha Autoridade de Rexistro e certificados pola Autoridade de Certificación.

A información sobre os certificados electrónicos revogados (non vixentes) almacénase nas denominadas listas de revogación de certificados (CRL).

Na Infraestrutura de Clave Pública (PKI) adoptada para o DNI electrónico, optouse por asignar as funcións de Autoridade de Validación a entidades diferentes da Autoridade de Certificación, coa fin de illar a comprobación da vixencia dun certificado electrónico dos datos de identidade do seu titular.

Así, a Autoridade de Certificación (Ministerio do Interior – Dirección Xeral da Policía) non ten de ningún xeito acceso aos datos das transaccións que se realicen cos certificados que ela emite, mentres que as Autoridades de Validación non teñen acceso á identidade dos titulares dos certificados electrónico que manexan, reforzando a transparencia do sistema.

Para a validación do DNI electrónico existen dous prestadores de Servizos de Validación:

- Fábrica Nacional de Moeda e Timbre – Real Casa da Moeda, que prestará os seus servizos de validación con carácter universal: cidadáns, empresas e Administracións Públicas.
- Ministerio da Presidencia, que prestará os servizos de validación ao conxunto das Administracións Públicas.

A prestación destes servizos de validación realízase tomando como base o protocolo Online Certificate Status Protocol (OCSP), o que, en esencia, supón que un cliente OCSP lle envía unha petición sobre o estado do certificado á Autoridade de Validación, a cal, tras consultar a súa base de datos, ofrece vía HTTP unha resposta sobre o estado do certificado. O servizo de validación está dispoñible de forma ininterrompida todos os días do ano.

O DNI electrónico inclúe dous certificados electrónicos, que son o conxunto de datos incluídos no chip, que permiten a identificación do seu titular (Certificado de Autenticación) e a sinatura electrónica de documentos (Certificado de Sinatura).

Os datos alóxanse en dúas partes do chip da tarxeta: pública e privada. A primeira contén os datos básicos dos certificados e unha clave pública, mentres que a parte privada contén a clave privada da tarxeta, só coñecida polo seu titular. A xeración de claves realízase dentro da tarxeta criptográfica e en presenza do seu titular.

Para poder realizar transaccións electrónicas co DNI electrónico é necesario:

- Un lector de tarxetas intelixentes (con chip), cos seus correspondente drivers.
- A librería para facer uso do DNIE: CSP (para S.Ou. Microsoft) ou PKCS#11
- Unha conexión a Internet para realizar as transaccións telemáticas.

O lector de DNIE debe cumprir as características técnicas seguintes:

- Debe cumprir o estándar ISO 7816 (1, 2 e 3)
- Debe soportar tarxetas asíncronas baseadas en protocolos T=0 (e T=1)
- Debe soportar velocidades de comunicación mínimas de 9.600 bps.
- Debe soportar os estándares seguintes:
  - API PC/SC (Personal Computer/Smart Card)
  - CSP (Cryptographic Service Provider, Microsoft)
  - API PKCS#11

Na estrutura das tarxetas intelixentes que cumpren co estándar PKCS#15 existe un ficheiro elemental denominado CDF (Certificate Directory File). A finalidade deste ficheiro é conter certificados ou índices a certificados. No caso do DNIE o CDF contén unha estrutura con codificación ASN.1 que incorpora a referencia interna aos certificados de cidadán e os atributos countryName, serialNumber, surname, givenName e commonName que aparecen no certificado x509 v3 de autenticación do cidadán. Tamén se incorporaron á estrutura os atributos organizationName, organizationalUnitName e o commonName da autoridade de certificación subordinada que expediou o certificado do cidadán. O EF implicado ten como identificador 6004.

Co fin de facilitar e fomentar o uso do DNIE, púxose a disposición dos cidadáns un sitio web co seu enderezo <http://www.dnielectronico.es/>.

#### **14.4. REFERENCIAS**

- Lei 30/1992, do 26 de novembro, de Réxime Xurídico das Administracións Públicas e do Procedemento Administrativo Común.
- Lei 15/1999, do 13 de decembro, de Protección de datos de carácter persoal
- Lei 53/1999, do 19 de decembro, de Sinatura electrónica.
- Lei 34/2002, do 11 de xullo, de Servizos da sociedade da información e de comercio electrónico.
- Real Decreto 1553/2005, do 23 de decembro, polo que se regula a expedición do Documento Nacional de Identidade e os seus certificados de sinatura electrónica (BOE núm. 307, do 24 de decembro de 2005).
- Lei 11/2007, do 22 de xuño, de Acceso electrónico dous cidadáns aos servizos públicos.
- Lei 37/2007, do 16 de novembro, sobre reutilización da información do sector público.
- Real Decreto 1720/2007, do 21 de decembro, polo que se aproba o Regulamento de desenvolvemento da Lei 15/1999, do 13 de decembro, de protección de datos de carácter persoal.
- Lei 56/2007, do 28 de decembro, de Medidas de impulso da sociedade da Información.
- Real Decreto 1494/2007, do 12 de novembro, polo que se aproba o Regulamento sobre as condicións básicas para o acceso das persoas con discapacidade ás tecnoloxías, produtos e servizos relacionados coa sociedade da información e medios de comunicación social.
- Real Decreto 3/2010, do 8 de xaneiro, polo que se regula o Esquema Nacional de Seguridade no ámbito da Administración Electrónica.
- Real Decreto 4/2010, do 8 de xaneiro, polo que se regula o Esquema Nacional de Interoperabilidade no ámbito da Administración Electrónica.
- Decreto 198/2010, do 2 de decembro, polo que se regula o Desenvolvemento da Administración Electrónica na Xunta de Galicia e nas entidades dependentes.

- Resolucións da Secretaría de Estado para a Función Pública pola que se aproban distintas normas técnicas de interoperabilidade.
- *Manual práctico de supervivencia de la Administración Electrónica* de Alberto López Tallón, publicado baixo 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

Xefe do Servizo de Informática do Concello de Santiago de Compostela

Colexiado do CPEIG

**15. SERVIZOS HORIZONTAIS DE  
ADMINISTRACIÓN  
ELECTRÓNICA.  
IDENTIFICACIÓN E  
AUTENTICACIÓN DOS  
FUNCIONARIOS, DOS  
CIDADÁNS E DAS  
ADMINISTRACIÓN PÚBLICAS.  
ACREDITACIÓN E  
REPRESENTACIÓN DOS  
CIDADÁNS. SINATURA  
ELECTRÓNICA, INTERCAMBIO  
DE CERTIFICADOS, SELAXE DE  
TEMPO (TIME-STAMPING).  
PAGAMENTO ELECTRÓNICO E  
NOTIFICACIÓNS TELEMÁTICAS.**



## **BLOQUE: ADMINISTRACIÓN ELECTRÓNICA E SOCIEDADE DA INFORMACIÓN**

**TEMA 15. SERVIZOS HORIZONTAIS DA ADMINISTRACIÓN ELECTRÓNICA. IDENTIFICACIÓN E AUTENTICACIÓN DOS FUNCIONARIOS, DOS CIDADÁNS, E DAS ADMINISTRACIÓNS PÚBLICAS. ACREDITACIÓN E REPRESENTACIÓN DOS CIDADÁNS. SINATURA ELECTRÓNICA, INTERCAMBIO DE CERTIFICADOS, SELADO DE TEMPO (TIME-STAMPING). PAGAMENTO ELECTRÓNICO E NOTIFICACIÓNS TELEMÁTICAS.**

**15.1. SERVIZOS HORIZONTAIS DA ADMINISTRACIÓN ELECTRÓNICA.**

**15.2. IDENTIFICACIÓN E AUTENTICACIÓN DOS FUNCIONARIOS, DOS CIDADÁNS, E DAS ADMINISTRACIÓNS PÚBLICAS.**

**15.3. ACREDITACIÓN E REPRESENTACIÓN DOS CIDADÁNS.**

**15.4. SINATURA ELECTRÓNICA, INTERCAMBIO DE CERTIFICADOS, SELADO DE TEMPO (TIME-STAMPING).**

**15.4.1. SINATURA ELECTRÓNICA**

**15.4.2. INTERCAMBIO DE CERTIFICADOS**

**15.4.3. SELADO DE TEMPO (TIME-STAMPING)**

**15.5. PAGAMENTO ELECTRÓNICO E NOTIFICACIÓNS TELEMÁTICAS.**

**15.5.1. PAGAMENTO ELECTRÓNICO**

**15.5.2. NOTIFICACIÓNS TELEMÁTICAS**

**15.6. REFERENCIAS**

**15.1. SERVIZOS HORIZONTAIS DA ADMINISTRACIÓN ELECTRÓNICA.**

Un dos obxectivos da Administración Electrónica é ofrecer servizos públicos electrónicos que contribúan a mellorar a vida dos cidadáns. Para iso desenvolvéronse un conxunto de servizos horizontais, utilizables por calquera Administración, que axudan a acelerar o proceso de implantación da Administración Electrónica.

Devanditos servizos comúns agrúpanse nas seguintes materias:

- Interconexión entre Administracións.
- Sinatura electrónica
- Tramitación electrónica
- Normativa, Regulación e Recomendacións
- Servizos integrais
- Información e difusión
- Ferramentas de apoio
- Xestión de Recursos Humanos na Administración Xeral do Estado

## REDE SARA

O artigo 43 da lei 11/2007 establece a obriga de crear unha rede de comunicacións que interconecte as Administracións Públicas españolas entre si e con outras redes das Institucións Europeas e doutros Estados membros, para o intercambio de información e servizos entre elas.

A Rede SARA permite a interconexión das Administracións Públicas, facilitando o intercambio de información e servizos entre elas. A través da Rede SARA os Ministerios, as Comunidades Autónomas, os Entes Locais e outros organismos públicos poden interconectar as súas redes dun xeito fiable, segura, capaz e flexible.

Ademais, a través do enlace da Rede SARA coa rede transeuropea sTESTA as Administracións Públicas españolas pódense interconectar con redes de institucións europeas e de administracións doutros Estados membros da UE, para o despregamento e acceso aos servizos paneuropeos de Administración electrónica.

## Características de SARA



- **Fiabilidade:** A rede SARA está deseñada con tecnoloxía de última xeración VPLS (Virtual Private LAN Services) que a dota de gran capacidade de transmisión de datos e moi alta dispoñibilidade.
- **Seguridade:** A rede SARA implanta medidas de seguridade entre as que destaca o establecemento de VPNs. É unha rede extremadamente segura na que todo o tráfico circula cifrado pola Troncal.
- **Capacidade:** A rede SARA conta cun ancho de banda de 1 Gbps en Ministerios e CPDs, e 100 Mbps en cada Comunidade Autónoma.
- **Calidade de Servizo (QoS):** A tecnoloxía VPLS permite dotar á rede de mecanismos de calidade de servizo para todo tipo de tráfico.
- **Punto-Multipunto:** A rede SARA está deseñada cun modelo de conexión punto-multipunto mediante o cal non existe un nodo central no que converxen todas as conexións e, dese xeito, elimínanse posibles puntos únicos de fallo. Os mecanismos de seguridade están distribuídos en cada nodo, aínda que a política é homoxénea e con xestión centralizada.
- **Flexibilidade:** A rede SARA está deseñada para poder evolucionar e crecer na medida en que o fagan as necesidades da Administración.

A rede SARA permite que as administracións compartan entre elas todos os servizos que estimen necesarios. Ademais existen servizos comúns que facilitan o despregamento da oferta de Administración electrónica, e aos que as diferentes administracións poden acceder, tales coma os seguintes:

- Verificación dos datos de identidade e residencia.
- Plataforma de validación de sinatura electrónica (@firma).
- Solicitud de cambio de domicilio.
- Notificación electrónica certa.
- Pasarela de pago.
- Rexistro electrónico común.
- Consultas do estado de expedientes.

- Catálogos de procedementos das AAPP.
- Videoconferencia.
- Voz IP.
- Contornas de traballo en colaboración.

## PLAN DE DIRECCIONAMENTO E INTERCONEXIÓN DE REDES

O Plan de direccionamento e interconexión de redes na Administración define un espazo de direccionamento privado común para os Centros da Administración. Este Plan permite que cada entidade ou organismo poida establecer de xeito independente os seus plans de numeración IP, en función da súa infraestrutura de rede, ou distribución orgánica ou departamental, pero mantendo unha coordinación co resto das Administracións Públicas que evite o uso de direccións duplicadas.

## SUITE DE PRODUCTOS RELACIONADOS COA SINATURA ELECTRÓNICA

Creouse unha suite de produtos relacionados coa sinatura electrónica para impulsar e facilitar a implantación de sistemas de sinatura e autenticación na Administración Pública, que son obxecto de estudo noutros apartados desta documentación.

## SERVIZOS COMÚNS PARA O INTERCAMBIO DE DATOS

Desenvolvéronse unha serie de produtos para impulsar e facilitar a verificación e consulta de datos na Administración Pública, fomentando a reutilización de solucións coa finalidade primordial de ofrecer un punto centralizado de servizos de verificación de datos como é a Plataforma de Intermediación, facilitando a interoperabilidade entre as Administracións Públicas.

É unha solución de referencia para cumprir o artigo 6.2b da LAECSP.

Proporcionanse uns servizos horizontais de consulta e verificación de datos, así como compoñentes e aplicacións informáticas que os desenvolven, e póñense a disposición das Administracións Públicas que o desexen de xeito gratuíto:

- Plataforma de Intermediación: Ofrece un conxunto de servizos de verificación e consulta de datos que permite a calquera organismo público verificar, en tempo real, os datos relativos a un cidadán que iniciou un trámite cunha entidade e que sexan necesarios para a resolución do trámite.
- SCSP: É un protocolo que facilita a interoperabilidade e intercambio de datos entre as AAPP co obxectivo de evitar que o cidadán teña que presentar certificados en papel, de datos que a Administración xa ten. Estes certificados substitúense por un intercambio de datos entre Administracións Públicas.
- Broker SCCD: Servizo web para permitir a comunicación do cambio de domicilio desde os Concellos (e Comunidades Autónomas) cara aos organismos tramitadores da Administración Xeral do Estado (AEAT, DGP, TGSS, INSS, MUFACE, etc...)

#### SUITE DE PRODUCTOS RELACIONADOS COA XESTIÓN DE RECURSOS HUMANOS NA ADMINISTRACIÓN XERAL DO ESTADO.

Dentro dos servizos comúns proporcionados pola Dirección Xeral para o Impulso da Administración Electrónica creouse unha suite de produtos relacionados coa xestión de RRHH na Administración Xeral do Estado para fomentar a reutilización de solucións coa finalidade primordial de ofrecer servizos para a confección de nóminas, xestión dos procedementos de RRHH departamentais e interdepartamentais, xestión do Plan de Pensións da AGE, consulta de información para a toma de decisións no ámbito dos RRHH das Administracións Públicas e do Rexistro Central de Persoal, e presentación de propostas de modificación de Relacións de Postos de Traballo á Comisión Executiva da Comisión Interministerial de Retribucións CECIR.

A través do conxunto de aplicacións de xestión de RRHH da AGE proporciónanse uns servizos horizontais de xestión e uns compoñentes informáticos. Estes servizos e aplicacións póñense a disposición da Administración Xeral do Estado:

- Portal do empregado Funciona: Portal de información e servizos que proporciona un espazo virtual de relación, colaboración e xestión do coñecemento para o persoal da Administración Xeral do Estado.
- Sistema de Nómina Estándar da Administración do Estado: Xestión completa de nómina de centros, entidades e organismos da Administración do Estado.
- Sistema de Información do Rexistro Central de Persoal (RCP): O RCP inscribe ao persoal ao servizo da Administración Xeral do Estado e anota os actos relevantes da súa vida administrativa. Os sistemas de información son:
  - Sistema de Información do Rexistro Central de Persoal (RCP): Anotacións rexistrais, relacións de postos de traballo e estrutura orgánica da AGE.
  - Sistema de información á Dirección e minería de datos SID – eSIR.
  - Sistema de arquivo electrónico de imaxes de documentos rexistrais.
  - Sistema de Xestión BADARAL: Sistema de información integrado co Rexistro Central de Persoal e o Portal CECIR para apoio aos xestores de RRHH da AGE. Xestión de Concursos, Plan de Pensións AGE, permisos e licenzas, Situacións de Incapacidade Temporal, entre outros.
  - Sistema Integrado de Xestión de Persoal SIGP: Sistema para a xestión electrónica de procedementos de xestión de RRHH da AGE.
- Portal CECIR: Espazo de traballo para os xestores de Recursos Humanos dos Departamentos Ministeriais e a CECIR.

## **15.2. IDENTIFICACIÓN E AUTENTICACIÓN DOS FUNCIONARIOS, DOS CIDADÁNS, E DAS ADMINISTRACIÓN PÚBLICAS.**

A LAECSP establece que as Administracións Públicas admitirán, nas súas relacións por medios electrónicos, sistemas de sinatura electrónica que sexan conformes ao

establecido na Lei 59/2003, do 19 de decembro, de Sinatura electrónica e resulten adecuados para garantir a identificación dos participantes e, no seu caso, a autenticidade e integridade dos documentos electrónicos.

Os cidadáns poderán utilizar os seguintes sistemas de sinatura electrónica para relacionarse coas Administracións Públicas, de acordo co que cada Administración determine:

- a) En todo caso, os sistemas de sinatura electrónica incorporados ao Documento Nacional de Identidade, para persoas físicas.
- b) Sistemas de sinatura electrónica avanzada, incluíndo os baseados en certificado electrónico recoñecido, admitidos polas Administracións Públicas.
- c) Outros sistemas de sinatura electrónica, como a utilización de claves concertadas nun rexistro previo como usuario, a achega de información coñecida por ambas partes ou outros sistemas non criptográficos, nos termos e condicións que en cada caso se determinen.

Doutra banda, as Administracións Públicas poderán utilizar os seguintes sistemas para a súa identificación electrónica e para a autenticación dos documentos electrónicos que produzan:

- a) Sistemas de sinatura electrónica baseados na utilización de certificados de dispositivo seguro ou medio equivalente que permita identificar a sede electrónica e o establecemento con ela de comunicacións seguras.
- b) Sistemas de sinatura electrónica para a actuación administrativa automatizada.
- c) Sinatura electrónica do persoal ao servizo das Administracións Públicas.
- d) Intercambio electrónico de datos en contornas pechadas de comunicación, conforme ao especificamente acordado entre as partes.

As persoas físicas poderán, en todo caso e con carácter universal, utilizar os sistemas de sinatura electrónica incorporados ao Documento Nacional de Identidade na súa relación por medios electrónicos coas Administracións Públicas.

Os cidadáns, ademais dos sistemas de sinatura electrónica incorporados ao Documento Nacional de Identidade, poderán utilizar sistemas de sinatura electrónica avanzada para se identificaren e autenticaren os seus documentos.

A relación de sistemas de sinatura electrónica avanzada admitidos, con carácter xeral, no ámbito de cada Administración Pública, deberá ser pública e accesible por medios electrónicos. Dita relación incluírá, polo menos, información sobre os elementos de identificación utilizados así coma, no seu caso, as características dos certificados electrónicos admitidos, os prestadores que os expiden e as especificacións da sinatura electrónica que pode realizarse con ditos certificados.

Os certificados electrónicos expedidos a Entidades sen personalidade xurídica, previstos na Lei 59/2003, do 19 de decembro, de Sinatura electrónica poderán ser admitidos polas Administracións Públicas nos termos que estas determinen.

As Administracións Públicas poderán determinar, tendo en conta os datos e intereses afectados, e sempre de forma xustificada, os supostos e condicións de utilización polos cidadáns doutros sistemas de sinatura electrónica, tales como claves concertadas nun rexistro previo, achega de información coñecida por ambas partes ou outros sistemas non criptográficos.

Naqueles supostos nos que se utilicen estes sistemas para confirmar información, propostas ou borradores remitidos ou exhibidos por unha Administración Pública, esta deberá garantir a integridade e o non repudio por ambas partes dos documentos electrónicos concernidos.



Cando resulte preciso, as Administracións Públicas certificarán a existencia e contido das actuacións dos cidadáns nas que se usaron formas de identificación e autenticación ás que se refire este artigo.

As sedes electrónicas utilizarán, para identificarse e garantir unha comunicación segura coas mesmas, sistemas de sinatura electrónica baseados en certificados de dispositivo seguro ou medio equivalente.

Para a identificación e a autenticación do exercicio da competencia na actuación administrativa automatizada, cada Administración Pública poderá determinar os supostos de utilización dos seguintes sistemas de sinatura electrónica:

- a) Selo electrónico de Administración Pública, órgano ou entidade de dereito público, baseado en certificado electrónico que reúna os requisitos esixidos pola lexislación de sinatura electrónica.

Os certificados de selo electrónico vinculan uns datos de verificación de sinatura (clave pública) aos datos identificativos dunha unidade organizativa (unidade que se realiza a actuación administrativa automatizada: área, sección, departamento, etc.) dunha entidade da Administración Pública e a persoa física que ten a máxima responsabilidade sobre a devandita unidade organizativa. Un exemplo son os certificados APE da FNMT-RCM, do cal se pode obter información en <http://cert.fntm.es/>. Poden ser utilizados para o intercambio de información entre sistemas informáticos ou a xeración automática de documentos.

- b) Código seguro de verificación vinculado á Administración Pública, órgano ou entidade e, no seu caso, á persoa asinante do documento, permitíndose en todo caso a comprobación da integridade do documento mediante o acceso á sede electrónica correspondente.

Desde o punto de vista técnico, este sistema funciona mediante a asignación dun código único a cada documento emitido pola Administración, e o almacenamento dunha copia nunha base de datos documental. Na sede electrónica está dispoñible un servizo que, previa introdución do código de documento, mostra o contido almacenado. Deste xeito, calquera cidadán pode verificar a validez dun documento impreso ou en formato electrónico comparándoo coa copia que obra en poder da Administración.

A relación de selos electrónicos utilizados por cada Administración Pública, incluíndo as características dos certificados electrónicos e os prestadores que os expiden, deberá ser pública e accesible por medios electrónicos. Ademais, cada Administración Pública adoptará as medidas adecuadas para facilitar a verificación dos seus selos electrónicos.

Sen prexuízo do previsto nos artigos 17 e 18 da LAECSP, a identificación e autenticación do exercicio da competencia da Administración Pública, órgano ou entidade actuante, cando utilice medios electrónicos, realizarase mediante sinatura electrónica do persoal ao seu servizo.

Cada Administración Pública poderá prover ao seu persoal de sistemas de sinatura electrónica, os cales poderán identificar de forma conxunta ao titular do posto de traballo ou cargo e á Administración ou órgano na que presta os seus servizos. A sinatura electrónica baseada no Documento Nacional de Identidade poderá utilizarse estes efectos.

Os documentos electrónicos transmitidos en contornas pechadas de comunicacións establecidos entre Administracións Públicas, órganos e entidades de dereito público, serán considerados válidos a efectos de autenticación e identificación dos emisores e receptores nas condicións establecidas no presente artigo. Cando os participantes nas

comunicacións pertencen a unha mesma Administración Pública, esta determinará as condicións e garantías polas que se rexerá que, cando menos, comprenderá a relación de emisores e receptores autorizados e a natureza dos datos a intercambiar. Cando os participantes pertencen a distintas administracións, as condicións e garantías citadas no apartado anterior estableceranse mediante convenio. En todo caso deberá garantirse a seguridade da contorna pechada de comunicacións e a protección dos datos que se transmitan.

A comunicación a través de medios telemáticos e a Administración Electrónica require o uso da sinatura electrónica na Administración. A sinatura electrónica constitúe un instrumento capaz de permitir unha comprobación da procedencia e da integridade das mensaxes intercambiadas a través de redes de telecomunicacións, ofrecendo as bases para evitar o repudio, se se adoptan as medidas oportunas baseándose en datos electrónicos.

A utilización da sinatura electrónica na Administración pública está regulada na seguinte normativa, entre outra:

- Directiva 1999/93/CE do Parlamento Europeo e do Consello, do 13 de decembro de 1999, pola que se establece un marco comunitario para a sinatura electrónica.
- Lei 59/2003, do 19 de decembro, de sinatura electrónica.
- Lei 11/2007, do 22 de xuño, de acceso electrónico dos cidadáns aos Servizos Públicos.
- Real Decreto 1671/2009, do 6 de novembro, polo que se desenvolve parcialmente a Lei 11/2007, do 22 de xuño, de acceso electrónico dos cidadáns aos Servizos Públicos.
- Real Decreto 3/2010, do 8 de xaneiro, polo que se regula o Esquema Nacional de Seguridade no ámbito da Administración Electrónica.

- Real Decreto 4/2010, de 8 de xaneiro, polo que se regula o Esquema Nacional de Interoperabilidade no ámbito da Administración Electrónica

No caso concreto da Xunta de Galicia, e en aplicación do estipulado na LAECSP, foi aprobada a ORDE do 25 de maio de 2011, pola que se regula a tarxeta do persoal ao servizo do sector público autonómico.

Tal e como se establece na orde, o artigo 35.b) da Lei 30/1992, do 26 de novembro, de réxime xurídico das Administracións Públicas e do procedemento administrativo común, establece que os cidadáns, nas súas relacións coas Administracións Públicas, teñen dereito a identificar ás autoridades e o persoal ao servizo das Administracións Públicas, baixo cuxa responsabilidade se tramiten os procedementos.

O avance das novas tecnoloxías e os sistemas de comunicacións ten o seu reflexo no ámbito da Comunidade Autónoma de Galicia no Decreto 198/2010, do 2 de decembro, polo que se regula o desenvolvemento da Administración Electrónica da Xunta de Galicia e nas entidades dela dependentes, que recolle como a primeira das súas finalidades de carácter xeral no seu artigo 2.1.A) "a) Ordenar e impulsar a Administración Electrónica, a fin de mellorar a eficiencia interna, as relacións intra e interadministrativas e as relacións cos cidadáns", regulando a identificación electrónica dos empregados públicos no seu artigo 18 mediante sistemas de sinatura electrónica, e podendo determinarse a súa aplicación para outros usos.

É necesario así, e para o conxunto do sector público autonómico, regulado na Lei 16/2010, do 17 de decembro, establecer unha tarxeta que sirva tanto para a identificación presencial do empregado/a ante os cidadáns como para permitir ao persoal e á Administración acceder ás prestacións e servizos derivados do avance das novas tecnoloxías e a implantación da Administración Electrónica.

A tarxeta acreditativa do persoal ao servizo do sector público autonómico será de utilización obrigatoria para o seguinte persoal:

- a) Os altos cargos incluídos no ámbito de aplicación da Lei 9/1996, do 18 de outubro, de incompatibilidades dos membros da Xunta de Galicia e altos cargos da Administración autonómica, modificada pola Lei 4/2006, de 30 de xuño, de transparencia e de boas prácticas da Administración pública galega.
- b) Persoal funcionario, laboral e estatutario ao servizo da Administración xeral da Comunidade Autónoma de Galicia.
- c) Persoal das entidades instrumentais do sector público autonómico, segundo o define e regula a Lei 16/2010, do 17 de decembro, de organización e funcionamento da Administración xeral e do sector público autonómico de Galicia.
- d) O persoal eventual que non estea incluído no ámbito de aplicación das leis ás que fai referencia o apartado a) deste artigo.
- e) A tarxeta non será de aplicación ao persoal que preste servizos en centros sanitarios e centros educativos.

A tarxeta terá as seguintes finalidades:

- a) Identificar e acreditar o seu titular como persoal ao servizo do sector público autonómico, nos ámbitos da Administración xeral da comunidade autónoma, e das entidades instrumentais.
- b) O persoal que desempeñe funcións de atención presencial ao cidadán deberá levar, nun lugar visible, a tarxeta.
- c) A identificación electrónica dos empregados públicos, de conformidade co disposto no artigo 18 do Decreto 198/2010, do 2 de decembro, polo que se regula o desenvolvemento da Administración Electrónica na Xunta de Galicia e nas entidades dela dependentes.
- d) Permitir o acceso a sistemas de información e áreas restrinxidas.

- e) Mellorar o control do acceso aos edificios e instalacións.
- f) O seguimento do cumprimento do horario e xornada laboral polos empregados públicos, facilitando o control dos supostos de diminución e redución de xornada, e a implantación do horario flexible e o teletraballo.

As tarxetas deberán levar a fotografía do seu titular, o seu nome e apelidos e o número do DNI co formato que se recolle no anexo da presente orde.

A nivel tecnolóxico dispoñerá das seguintes capacidades:

- a) Chip criptográfico que permitirá o almacenamento de varios certificados dixitais (entre eles, o certificado para persoal ao servizo das Administracións Públicas e o certificado de persoa física).
- b) Identificación por radiofrecuencia (chip RFID de proximidade) que permitirá o control de acceso a lugares de acceso restrinxido e a instalacións con acceso controlado mediante elementos de impedimento de paso.
- c) Banda magnética como contedor de datos do profesional para a súa utilización en sistemas de información que requiran destes datos.

### **15.3. ACREDITACIÓN E REPRESENTACIÓN DOS CIDADÁNS.**

Os certificados electrónicos recoñecidos emitidos por prestadores de servizos de certificación serán admitidos polas Administracións Públicas como válidos para relacionarse coas mesmas, a condición de que o prestador de servizos de certificación poña a disposición das Administracións Públicas a información que sexa precisa en condicións que resulten tecnoloxicamente viables e sen que supoña custo algún para aquelas.

Os sistemas de sinatura electrónica utilizados ou admitidos por algunha Administración Pública distintos dos baseados nos certificados aos que se refire o

apartado anterior poderán ser así mesmo admitidos por outras Administracións, conforme a principios de recoñecemento mutuo e reciprocidade.

A Administración Xeral do Estado dispoñerá, polo menos, dunha plataforma de verificación do estado de revogación de todos os certificados admitidos no ámbito das Administracións Públicas que será de libre acceso por parte de todos os Departamentos e Administracións. Cada Administración Pública poderá dispoñer dos mecanismos necesarios para a verificación do estado de revogación e a sinatura cos certificados electrónicos admitidos no seu ámbito de competencia.

Nos supostos en que para a realización de calquera operación por medios electrónicos se requira a identificación ou autenticación do cidadán mediante algún instrumento dos previstos dos que aquel non dispoña, tal identificación ou autenticación poderá ser validamente realizada por funcionarios públicos mediante o uso do sistema de sinatura electrónica do que estean dotados.

Para a eficacia do disposto no apartado anterior, o cidadán deberá identificarse e prestar o seu consentimento expreso, debendo quedar constancia diso para os casos de discrepancia ou litixio.

Cada Administración Pública manterá actualizado un rexistro dos funcionarios habilitados para a identificación ou autenticación.

Sen prexuízo do disposto no [artigo 13.2](#) da LAECSP, onde se determinan os posibles medios de identificación dos cidadáns, as Administracións Públicas poderán habilitar con carácter xeral ou específico a persoas físicas ou xurídicas autorizadas para a realización de determinadas transaccións electrónicas en representación dos interesados. Dita habilitación deberá especificar as condicións e obrigas ás que se comprometen os que así adquiren a condición de representantes, e determinará a presunción de validez da representación, salvo que a normativa de aplicación prevexa

outra cousa. As Administracións Públicas poderán requirir, en calquera momento, a acreditación da devandita representación.

#### **15.4. SINATURA ELECTRÓNICA, INTERCAMBIO DE CERTIFICADOS, SELADO DE TEMPO (TIME-STAMPING).**

##### **15.4.1. SINATURA ELECTRÓNICA**

A política de sinatura electrónica e certificados no ámbito da Administración Xeral do Estado e dos seus organismos públicos, segundo se establece no artigo 24 do Real Decreto 1671/2009, polo que se desenvolve parcialmente a LAECSP, está constituída polas directrices e normas técnicas aplicables á utilización de certificados e sinatura electrónica dentro do seu ámbito de aplicación.

O artigo 18 do Real Decreto 4/2010 polo que se regula o Esquema Nacional de Interoperabilidade, establece que a política de sinatura electrónica e de certificados da Administración Xeral do Estado servirá de marco xeral de interoperabilidade para a autenticación e o recoñecemento mutuo de sinaturas electrónicas dentro do seu ámbito de actuación. Tamén establece que dita política poderá ser utilizada como referencia por outras Administracións públicas para definir as políticas de certificados e sinaturas a recoñecer dentro dos seus ámbitos competenciais.

En termos xerais, unha política de sinatura electrónica contén unha serie de normas relativas á sinatura electrónica, organizadas ao redor dos conceptos de xeración e validación de sinatura, nun contexto particular (contractual, xurídico, legal,...), definindo as regras e obrigas de todos os actores involucrados en dito proceso. O obxectivo deste proceso é determinar a validez da sinatura electrónica para unha transacción en particular, especificando a información que deba incluír o asinante no proceso de xeración da sinatura, e a información que debese comprobar o verificador no proceso de validación da mesma.



## Obxectivo

A política de sinatura da Administración Xeral do Estado representa o conxunto de criterios comúns asumidos por esta Administración e os seus organismos públicos vinculados ou dependentes, en relación coa sinatura electrónica.

- inclúe as normas relativas á sinatura electrónica, organizadas ao redor dos conceptos de xeración e validación de sinatura asociada a un contexto dado.
- permite reforzar a confianza nas transaccións electrónicas.
- define as regras e obrigas de todos os actores involucrados nun proceso de sinatura.
- permite determinar a validez da sinatura electrónica para unha transacción en particular.

No Boletín Oficial do Estado con data 31 de xullo de 2011 foi publicada a Resolución do 19 de xullo de 2011, da Secretaría de Estado para a Función Pública, pola que se aproba a Norma Técnica de Interoperabilidade de Política de Sinatura electrónica e de certificados da Administración.

### **15.4.2. INTERCAMBIO DE CERTIFICADOS**

Un dos servizos horizontais da Administración Electrónica mencionados anteriormente é o SCSP, cuxa finalidade é substituír a presentación de certificados en papel ante unha Administración por unha transmisión de datos entre o organismo que require os datos e o organismo que os custodia e proporciona, coas garantías xurídicas descritas no RD 263/1996 (redacción do RD 209/2003) por transmisións de datos. O sistema ten en conta a normativa referente á protección de datos.

Actualmente están dispoñibles os seguintes datos que cumpren coa especificación de SCSP: Identidade, residencia, situación de desemprego, títulos universitarios, títulos non universitarios, datos catastrais, certificación catastral, importes de prestación de

desemprego percibidos, estar ao corrente de pago das obrigas tributarias, consulta de débeda coa Seguridade Social, alta na Tesourería Xeral da Seguridade Social, certificado de Renda, domicilio fiscal, imposto de actividades económicas.

As vantaxes deste sistema: Aforro de tempo e custo ao diminuír o número de trámites que debe realizar, axilidade de resolución nos trámites ao non ter que esperar por datos que a Administración pode obter en liña, e todos os trámites do procedemento que poden realizarse de forma electrónica..

O funcionamento do servizo é o seguinte:

- Petición de datos: o organismo peticionario identifica a solicitude, xera e envía asinado a mensaxe de petición completo.
- Autorización de organismos: para cada petición o organismo emisor comproba que o organismo tramitador está autorizado para pedir eses datos.
- Validación do esquema de petición: o organismo emisor analiza o esquema XML da mensaxe de petición.
- Transmisións emitidas: cada petición é gardada e tramitada no organismo emisor. Xera, sinatura, e almacena as respostas a cada petición co mesmo identificador da petición. O tempo de almacenamento da transmisión será o que marque a Lei en cada caso.
- Transmisións recibidas: o organismo peticionario valida, tramita e almacena cada unha das respostas recibidas.
- Conexión co *backoffice*: inclúe un módulo de conexión co backoffice configurable a medida do organismo.

Ademais deste proxecto, diferentes organismos como a AEAT, a DGT, ou a DGP desenvolveron ou están desenvolvendo os seus propios sistemas de intercambio telemático de información, e asinando convenios de colaboración que permiten o seu uso con outras Administracións.

### **15.4.3. SELADO DE TEMPO**

No artigo 29.2 da LAEPD indícase que: "Os documentos administrativos incluírán referencia temporal, que se garantirá a través de medios electrónicos cando a natureza do documento así o requira."

Nesta lei fálase de referencia "temporal", sen especificar o tipo. As posibles referencias temporais que se poden asociar a un documento electrónico establécense no Real Decreto 1671/2009, de 6 de novembro, polo que se desenvolve parcialmente a LAECSP, fai a seguinte distinción no seu artigo 47:

- a) Marca de tempo: Asignación por medios electrónicos da data e, no seu caso, a hora a un documento electrónico. A marca de tempo será utilizada en todos aqueles casos nos que as normas reguladoras non establezan a utilización dun selo de tempo.
- b) Selo de tempo: Asignación por medios electrónicos dunha data e hora a un documento electrónico coa intervención dun prestador de servizos de certificación que asegure a exactitude e integridade da marca de tempo do documento.

Xa que logo, os dous tipos de referencias posibles son marca de tempo e selo de tempo, sendo a norma que regula o procedemento onde residirán os documentos electrónicos a que dicta a conveniencia da utilización dun ou outro tipo.

**AUTORIDADE DE SELADO DE TEMPO TSA@**

A Autoridade de Selados de Tempo (TSA) integrada na plataforma de Validación e sinatura electrónica (@firma) é unha solución tecnolóxica que se centra en proporcionar servizos de selado de tempo: emisión de selos de tempo, validación de selos de tempo e reselado.

Os servizos da TSA están dispoñibles para todo Organismo ou Entidade Pública pertencente ás diferentes Administracións Públicas. Desde o Ministerio de Política Territorial e Administración Pública ofrécese a axuda e o soporte necesario para que os organismos integren estes servizos de selado de tempo sincronizados coa hora oficial do Estado, nos sistemas de información de Administración Electrónica. Para iso desenvolveuse un cliente a integrar dentro das aplicacións daqueles Organismos que desexen dotar dunha referencia válida de tempo.

A plataforma de selado de tempo cobre os seguintes obxectivos:

- Trala aprobación da LAECSP, coa plataforma TS@ promóvense e facilítanse servizos cuxo obxectivo é o cumprimento das obrigas das Administracións para cos cidadáns no referente a garantir a acreditación a cargo dun terceiro de confianza da data e hora de realización de calquera operación ou transacción por medios electrónicos
- Os servizos son ofrecidos a calquera organismo ou Entidade Pública pertencente ás diferentes Administracións Públicas sexa cal for o seu ámbito.

A posibilidade de emitir validamente por medios electrónicos os documentos administrativos vén descrita no Artigo 29 da LAECSP, o cal nos seus apartados 2 e 3 indica que, ademais da sinatura electrónica, deben incluír unha referencia temporal cando a natureza do documento así o requira. Dita referencia temporal debe de ser realizada por medios electrónicos a través de calquera prestador de servizos de selado de tempo admitidos pola Administración Xeral do Estado.

A TS@ é unha plataforma de selado de tempo, sincronizada coa hora legal provista polo Real Observatorio da Armada, coas funcionalidades de selado, validación e reselado de selos de tempo. Mediante a emisión dun selo de tempo sobre un

documento xerárase unha evidencia que determinará a existencia dese documento nun instante determinado.

A través da interface de validación poderán validarse selos de tempo emitidos previamente, podendo incluír unha data de xeito opcional para saber se nesa data dada o selo de tempo era válido. Se non se indica a data validarase coa data actual. Mediante a interface de reselado poderá volver selar selos previamente emitidos.

Os protocolos de selado de tempo nos cales se basea a plataforma atópanse especificados nas seguintes normas:

- RFC 3161 "Internet X.509 Public Key Infrastructure Time Stamp Protocols", estándar definido pola Internet Engineering Task Force (IETF) para o 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.

É unha solución baseada en software libre, estándares abertos e en Java: servidor web Apache Tomcat, Sistema Operativo Solaris/Linux, AXIS, JGROUPS, etc.

Desde o punto de vista técnico, o funcionamento habitual á hora de utilizar os servizos de selado de tempo adoita ser o seguinte:

- a) A Administración asina o documento ao que pretende achegar un selo de tempo.
- b) A Administración envía á TS@ o devandito documento.

- c) A TS@ recibe o documento, incorpora a data e hora e asínoa coa súa clave privada, xerando deste xeito un certificado ou selo de tempo.

## **15.5. PAGAMENTO ELECTRÓNICO E NOTIFICACIÓNS TELEMÁTICAS.**

### **15.5.1. PAGAMENTO ELECTRÓNICO**

O pagamento electrónico é un servizo indispensable para que a tramitación completamente electrónica sexa posible. Na Administración moitos servizos levan asociado o pago de taxas, impostos ou prezos públicos, polo que se fai necesario dispoñer de servizos de pago de distinto tipo. O procedemento máis habitual é o de utilización de pasarelas de pago específicas de cada entidade bancaria, ou preferiblemente pasarelas de pago desenvolvidas pola Administración para a centralización do devandito proceso.

#### **PASARELA DE PAGO DE REDE.ES**

A Entidade Pública Rede.es ofrece o Servizo de Pago Telemático (SPT), que lles proporciona aos administrados, organismos públicos e entidades financeiras un mecanismo común, normalizado e seguro que permite o pagamento electrónico de conceptos de débeda administrativa (tributos, prezos públicos, etc.) con todas as garantías xurídicas, e que soporta os seguintes procesos:

- Pagos en liña e consultas: Para trámites administrativos que implican o pago individual de tributos e taxas que realizan tanto os cidadáns como os profesionais que actúan en representación e con autorización dos mesmos.
- Pagos por lotes: Para pagos en lotes ou remesas, de forma que faciliten as tarefas repetitivas dos profesionais que actúan en representación e con autorización dos cidadáns.

- Administración: Procesos orientados a que os Organismos poidan aproveitar as características do SPT: Consultas de pagos, estatísticas, personalización

As Administracións Públicas que poden optar a diferentes modalidades de prestación do SPT, dependendo do modo da súa utilización: Modalidade web, Modalidade Servizo web con validación de sinatura por Rede.es, modalidade servizo web con validación de sinatura pola Administración adherida.

Os medios de pago que permite o servizo son tres: Cargo en conta, pago por tarxeta de crédito e domiciliación.

Desde o punto de vista tecnolóxico, como principal característica destaca o seu deseño modular e escalable, baseado nos paradigmas de seguridade (autenticidade, integridade, confidencialidade, dispoñibilidade, non repudio e flexibilidade)

Tecnoloxía: Integración vía WEB e servizos web, protocolo de acceso seguro HTTPS, estándar de sinatura electrónica XMLdsig, e soporte de certificados de sinatura electrónica emitidos por diversos Prestadores de Servizos de Certificación (PSC)

Pódese atopar máis información na dirección <http://pago.rede.es/>.

## PASARELA DE PAGOS DO MINISTERIO DE POLÍTICA TERRITORIAL E ADMINISTRACIÓN PÚBLICAS - AEAT

A pasarela de pagos pretende mellorar a disposición da Administración do Estado para adoptar o pago telemático nos seus trámites.

### Obxectivo:

- Impulsar o pagamento electrónico na Administración Xeral do Estado.
- Facilitar a implantación do pagamento electrónico nos trámites que o queiran.
- Aproveitar a experiencia e boas prácticas da AEAT, así como a súa infraestrutura de pago.

O proxecto ten dous modelos de servizo claramente diferenciados. O Organismo colaborador pode solicitar o que máis se axuste ás súas necesidades:

- a) Servizo “Mis pagos” centralizado na web 060. Servizo de pago centralizado. O organismo non necesita implantar nada na súa infraestrutura. O cidadán pode realizar o pago no servizo centralizado e presentar o xustificante correspondente co NRC no Organismo tramitador.

O pago poderá ser verificado polo Organismo a través dunha páxina Web habilitada para iso ou utilizar un modelo de integración co servizo no que poida actualizar o seu backoffice e redirixir o cidadán ao pago sen perder o contacto co mesmo.

O servizo incorpora, facilidades adicionais para os cidadáns, como poder planificar pagos coa Administración, de tal forma que teña un recordatorio dos mesmos para iniciar o pago no momento correspondente ou manter un histórico dos mesmos independentemente do Organismo onde realice o trámite.

- b) Librerías de pago: Servizo no que se proporcionan unhas librerías que se implantan no Organismo e que son utilizadas polas aplicacións de xestión que o requiren. Estas librerías intégranse coas aplicacións, ben como un servizo web ou coma unha librería java propiamente dita.

A seguridade para a autenticación e integridade dos datos baséase no uso de sinatura dixital avanzada e comunicación HTTPS entre o Organismo e a AEAT, con certificado de servidor e cliente.

Ademais, o cidadán ten que asinar co seu certificado dixital os datos do pago que se envían á Entidade Financeira, cotexándose posteriormente esta sinatura no banco co



propietario da conta ou a tarxeta. Isto permite garantir todo o ciclo de pago e manter informados a todos os actores do resultado do mesmo no instante.

Permite o pago mediante cargo en conta ou tarxeta, aínda que o cidadán ten que ter conta no banco que expide a tarxeta.

Permite o pago a terceiros, é dicir, a persoa que asina con certificado dixital a petición de pago e está autorizado a unha conta no banco, pode pagar por outra persoa, que sexa a obrigada ao pago.

A plataforma de sinatura electrónica utilizada é @Firma, que proporciona a librería de sinatura do cliente, así como aqueles servizos de seguridade que requira a aplicación de pago do organismo ou a propia pasarela, como pode ser a verificación de que o certificado non está revogado.

O servizo de pago é proporcionado gratuitamente polas Entidades Financeiras colaboradoras en función dos seus acordos de colaboración coa AEAT.

#### 15.5.2. **NOTIFICACIÓNS TELEMÁTICAS**

A LAECSP establece que os cidadáns poderán elixir en todo momento o xeito de comunicarse coas Administracións Públicas, sexa ou non por medios electrónicos, excepto naqueles casos nos que dunha norma con rango de Lei se estableza ou infira a utilización dun medio non electrónico. A opción de comunicarse por uns ou outros medios non vincula ao cidadán, que poderá, en calquera momento, optar por un medio distinto do inicialmente elixido.

As Administracións Públicas utilizarán medios electrónicos nas súas comunicacións cos cidadáns sempre que así o solicitaran ou consentiran expresamente. A solicitude e o consentimento poderán, en todo caso, emitirse e solicitarse por medios electrónicos.

As comunicacións a través de medios electrónicos serán válidas sempre que exista constancia da transmisión e recepción das súas datas, do contido íntegro das comunicacións e se identifique fielmente o remitente e o destinatario das mesmas.

As Administracións publicarán, no correspondente Diario Oficial e na propia sede electrónica, aqueles medios electrónicos que os cidadáns poden utilizar en cada suposto no exercicio do seu dereito a comunicarse con elas.

Os requisitos de seguridade e integridade das comunicacións estableceranse en cada caso de forma apropiada ao carácter dos datos obxecto daquelas, de acordo con criterios de proporcionalidade, conforme ao disposto na lexislación vixente en materia de protección de datos de carácter persoal.

Reglamentariamente, as Administracións Públicas poderán establecer a obrigatoriedade de comunicarse con elas utilizando só medios electrónicos, cando os interesados se correspondan con persoas xurídicas ou colectivos de persoas físicas que por razón da súa capacidade económica ou técnica, dedicación profesional ou outros motivos acreditados teñan garantido o acceso e dispoñibilidade dos medios tecnolóxicos precisos.

As Administracións Públicas utilizarán preferentemente medios electrónicos nas súas comunicacións con outras Administracións Públicas. As condicións que rexerán estas comunicacións determinaranse entre as Administracións Públicas participantes.

Para que a notificación se practique utilizando algún medio electrónico requirirase que o interesado sinale dito medio como preferente ou consinta a súa utilización, sen prexuízo do disposto no artigo 27.6 da LAECSP. Tanto a indicación da preferencia no uso de medios electrónicos como o consentimento citados anteriormente poderán emitirse e solicitarse, en todo caso, por medios electrónicos.

O sistema de notificación permitirá acreditar a data e hora en que se produza a posta a disposición do interesado do acto obxecto de notificación, así como a de acceso ao seu contido, momento a partir do cal a notificación entenderase practicada para todos os efectos legais.

Cando, existindo constancia da posta a disposición, transcorresen dez días naturais sen que se acceda ao seu contido, entenderase que a notificación foi rexeitada cos efectos previstos no artigo 59.4 da Lei 30/1992 de Réxime Xurídico e do Procedemento Administrativo Común e normas concordantes, salvo que de oficio ou a instancia do destinatario se comprobe a imposibilidade técnica ou material do acceso.

Durante a tramitación do procedemento o interesado poderá requirirle ao órgano correspondente que as notificacións sucesivas non se practiquen por medios electrónicos, utilizándose os demais medios admitidos no artigo 59 da Lei 30/1992, de Réxime Xurídico e do Procedemento Administrativo Común, excepto nos casos previstos no artigo 27.6 da LAECSP.

Producirá os efectos propios da notificación por comparecencia o acceso electrónico por parte dos interesados ao contido das actuacións administrativas correspondentes, sempre que quede constancia do devandito acceso.

En resposta a estas esixencias da LAECSP está dispoñible unha plataforma desenvolvida e mantida pola Sociedade Estatal de Correos e Telégrafos, denominada Sistema de Notificacións Telemáticas Seguras. A Administración pode facer uso deste servizo integrándoo nos seus sistemas informáticos a través do módulo SISNOT.

O Servizo de Notificacións Electrónicas proporcionalles a cada cidadán ou empresa unha Dirección Electrónica Habilitada na que recibir todas as notificacións e comunicacións das administracións públicas. O servizo é gratuíto para os cidadáns e

empresas. Nunha única caixa de correos poderá recibir todas as notificacións e comunicacións da Administración.

Os axentes que interveñen no Servizo son:

- O Cidadán ou empresa que teña o control da súa dirección electrónica e que pode solicitar a calquera Administración que lle notifique electronicamente por este sistema, xa que o cidadán ten o dereito a elixir o lugar de notificación.
- O Ministerio de Política Territorial e Administración Pública, responsable da Dirección Electrónica Habilitada e do servizo.
- Correos, o prestador que xestiona a entrega das notificacións ao interesado
- O emisor, organismo responsable do trámite e competente de emitir a notificación ao interesado.

O funcionamento do servizo consiste en:

- O cidadán solicita unha caixa de correos identificada mediante unha Dirección Electrónica Habilitada.
- O cidadán selecciona, do Catálogo de procedementos, aqueles que para os que quere ser notificado electronicamente con total seguridade e confidencialidade.
- O organismo emisor consulta o censo do procedemento (aqueles cidadáns que solicitaron a notificación telemática dese procedemento).
- O organismo envía a notificación ao prestador. O prestador verifica os datos e distribúe as notificacións na caixa de correos correspondente, poñendo esta a disposición do cidadán. Ao mesmo tempo emite un aviso á dirección de correo electrónico que facilitou ou mediante unha mensaxe curta a móbil SMS.
- O cidadán consulta a súa caixa de correos e acepta ou rexeita a notificación telemática, asinando a aceptación ou o rexeitamento da notificación. A notificación descárgase no ordenador do interesado.

- O prestador almacena a aceptación, o rexeitamento asinada por interesar ou o vencemento de prazo asinado polo prestador e entrégalle esta información de retorno ao emisor.

O único requisito para o interesado é que se identifique a través dun certificado electrónico ou DNIE.

Para facilitar a integración ao servizo, existe un paquete denominado SISNOT, que é un sistema intermedio que xestiona o ciclo de vida das notificacións emitidas por aplicacións cliente e a comunicación co Servizo de Notificacións Electrónicas; encargado de facerllas chegar ao cidadán. Tamén xestiona a actualización do censo de cidadáns e empresas dados de alta para a notificación telemática segundo normativa, para o que se comunica cos sistemas de censo do portal do cidadán.

SISNOT ofrece un interface de servizo web abstraendo á aplicación xestora do procedemento da labores de comunicación co SNE.

Pódese atopar máis información na dirección <https://notificacións.060.es/>

### **15.6. REFERENCIAS**

- Lei 30/1992, do 26 de novembro, de Réxime Xurídico das Administracións Públicas e do Procedemento Administrativo Común.
- Lei 15/1999, do 13 de decembro, de Protección de datos de carácter persoal
- Lei 53/1999, do 19 de decembro, de Sinatura electrónica.
- Lei 34/2002, do 11 de xullo, de Servizos da sociedade da información e de comercio electrónico.
- Lei 11/2007, do 22 de xuño, de Acceso electrónico dos cidadáns aos servizos públicos.
- Lei 37/2007, do 16 de novembro, sobre Reutilización da información do sector público.
- Real Decreto 1720/2007, do 21 de decembro, polo que se aproba o Regulamento de desenvolvemento da Lei 15/1999, do 13 de decembro, de protección de datos de carácter persoal.
- Lei 56/2007, do 28 de decembro, de Medidas de impulso da sociedade da Información.
- Real Decreto 3/2010, do 8 de xaneiro, polo que se regula o Esquema Nacional de Seguridade no ámbito da Administración Electrónica.
- Real Decreto 4/2010, do 8 de xaneiro, polo que se regula o Esquema Nacional de Interoperabilidade no ámbito da Administración Electrónica.
- Decreto 198/2010, do 2 de decembro, polo que se regula o Desenvolvemento da Administración Electrónica na Xunta de Galicia e nas entidades dependentes.
- Resolucións da Secretaría de Estado para a Función Pública pola que se aproban distintas normas técnicas de interoperabilidade.
  
- *Manual práctico de supervivencia de la Administración Electrónica*, de Alberto López Tallón, publicado baixo licenza Creative Commons.
- *Anotaciones y comentarios al Decreto de Administración Electrónica de la 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

Xefe do Servizo de Informática do Concello de Santiago de Compostela

Colexiado do CPEIG



# **16. DESENVOLVEMENTO DA SOCIEDADE DA INFORMACIÓN: MARCO DE ACTUACIÓN. EUROPA 2020 AXENDA DIXITAL EUROPEA. PLAN AVANZA 2.**

## **TEMA 16. DESENVOLVEMENTO DA SOCIEDADE DA INFORMACIÓN: MARCO DE ACTUACIÓN. EUROPA 2020. AXENDA DIXITAL EUROPEA. PLAN AVANZA 2.**

### **16.1. DESENVOLVEMENTO DA SOCIEDADE DA INFORMACIÓN. MARCO DE ACTUACIÓN.**

#### **16.1.1. EUROPA 2020.**

#### **16.1.2. AXENDA DIXITAL EUROPEA.**

#### **16.1.3. PLAN AVANZA 2.**

### **16.2. REFERENCIAS**

### **16.1. DESENVOLVO DA SOCIEDADE DA INFORMACIÓN. MARCO DE ACTUACIÓN.**

#### **16.1.1. EUROPA 2020.**

A Estratexia 2020 é o plan de crecemento sustentable e intelixente deseñado pola Comisión Europea para a próxima década, e posto en marcha en mazo de 2010. Nel establécense as liñas de actuación básicas e os obxectivos que se pretenden lograr nos próximos dez anos para conseguir un desenvolvemento integral que volva situar a Unión Europea nunha posición de liderado mundial a nivel económico e social. Nas seguintes liñas faise un resumo das principais medidas, actuacións e obxectivos fixados para a próxima década.

1. Emprego: Aumentar a taxa de emprego da poboación activa ata o 75%. Reforzar a flexibilidade e a seguridade laboral dos traballadores a través de plans nacionais. Incrementar a colaboración entre as institucións privadas do mercado laboral e as institucións públicas. Asegurar as competencias necesarias para unha aprendizaxe permanente. Fomentar o movemento do capital humano. Levar a cabo unha reforma no sistema de pensións.

2. Educación: Incrementar a calidade de todos os niveis de educación xeral da UE. Integrar e incrementar os programas de mobilidade e investigación dentro da UE. Explorar as formas de promover o espírito emprendedor, a creatividade e a excelencia. Realizar unha avaliación comparativa dos resultados das universidades e dos sistemas educativos nun contexto xeral. Reducir a % de abandono escolar ao 10%. Consolidar o atractivo internacional da educación superior europea. Mellorar a entrada da xente nova ao mercado laboral mediante orientación, asesoramento e prácticas. Conseguiar incrementar a % de poboación de entre 30 e 34 anos que finaliza o ensino superior do 31% a polo menos o 40% en 2020.
3. Innovación: Impulsar os niveis de investimento en I+D en toda a UE ata chegar ao 3% do PIB da UE. Utilizar incentivos fiscais que promovan o investimento en I+D. Mellorar as condicións de investimento e o acceso ao financiamento do sector privado centrándose nas PEME (promoción do espírito emprendedor). Poñer en marcha cooperación de innovación europea entre universidades e empresas. Acelerar a implantación de redes da internet de alta velocidade. Revisar e consolidar o papel dos instrumentos da UE destinados a apoiar a innovación. Crear unha axenda de investigación europea centrada nos grandes retos do futuro: transporte, seguridade enerxética, cambio climático... Crear as condicións para que a PEME de rápido crecemento ocupe os mercados emerxentes. Utilizar incentivos fiscais para promover os gastos en coñecemento e os investimentos en I+D.
4. Enerxía e industria: Lograr unha Europa que aproveite máis eficazmente os seus recursos. Reducir as emisións de carbono nun 20% respecto dos niveis de 1990. Incrementar o uso das enerxías renovables. Promover unha maior seguridade enerxética. Eliminar obstáculos a un mercado único da enerxía renovable. Mellorar as redes europeas e transeuropeas. Desenvolver un marco



de normas comúns na promoción de novas tecnoloxías. Modernizar o sector transporte. Utilizar instrumentos regulamentarios e normativos para reducir o consumo de enerxía, e así, incentivar o aforro. Eliminar os obstáculos a un mercado único da enerxía renovable. Manter o liderado mundial no campo das enerxías verdes. Eliminar as subvencións a enerxías que producen un deterioro medioambiental. Desenvolver un enfoque horizontal da política industrial. Promover a internacionalización da PEME. Revisar e mellorar a normativa europea co fin de mellorar a competitividade europea. Desenvolver unha política espacial efectiva e líder no mundo. Reforzar a competitividade do sector turístico europeo. Promover a responsabilidade social das empresas. Promover o cambio en sectores en crise.

5. Economía e finanzas: Evitar os proteccionismos nacionais. Levar a cabo reformas no sector financeiro que melloren a supervisión, a estabilidade e a rendición de contas. Fortalecer o goberno das institucións financeiras. Impulsar un saneamento das finanzas públicas dos estados que contribúa a un crecemento sostido a longo prazo. Buscar unha maior integración e interconexión dos mercados para que a competencia e o acceso dos consumidores estimulen o crecemento e a innovación. Facilitar e abaratar a execución de contratos para as empresas e os consumidores. Facer realidade un mercado europeo de capital risco. Desenvolver unha estratexia comercial para Europa centrada nas negociacións multilaterais e bilaterais con socios estratéxicos. Reducir as cargas administrativas que pesan sobre as empresas e mellorar a calidade da lexislación.
6. Plataforma contra a pobreza: Reducir o número de europeos que viven por baixo dos limiares de pobreza nun 25%. Promover a cohesión e a inclusión social dos máis pobres permitíndolles vivir con dignidade e facéndoos partícipes da vida en sociedade. Promover a responsabilidade colectiva. Garantirlles a estas persoas o acceso universal á asistencia sanitaria.

As prioridades que se establecen en Europa 2020 son as seguintes:

- a) **Crecemento intelixente:** Significa mellorar o rendemento da UE en materia de: educación (estimular as persoas a aprender, estudar e actualizar os seus coñecementos, investigación e innovación (crear novos produtos e servizos que xeren crecemento e emprego e axuden a afrontar os desafíos sociais) e sociedade dixital (utilizar as tecnoloxías da información e a comunicación).
- b) **Crecemento sustentable:** É crecemento sustentable crear unha economía con baixas emisións de carbono máis competitiva, que faga un uso eficiente e sustentable dos recursos, protexer o medio ambiente, reducir as emisións e evitar a perda de biodiversidade, aproveitar o liderado europeo no desenvolvemento de novas tecnoloxías e métodos de produción ecolóxicos, introducir redes eléctricas intelixentes e eficaces, aproveitar as redes que xa existen a escala da UE para lles dar unha vantaxe competitiva máis ás nosas empresas, sobre todo as pequenas do sector fabril, mellorar o contorno empresarial, particularmente para as PEME, e axudarlles aos consumidores a elixir con coñecemento de causa.
- c) **Crecemento integrador:** É crecemento integrador: aumentar o nivel de emprego en Europa: máis e mellores postos de traballo, sobre todo para as mulleres, os mozos e os traballadores de máis idade, axudarlles ás persoas de todas as idades a prever e xestionar o cambio a través do investimento nas cualificacións e a formación, modernizar os mercados de traballo e os sistemas de benestar, garantir que os beneficios do crecemento cheguen a todos os recunchos da UE.
- d) **Gobernanza económica:** A crise deixou ao descuberto en moitos países europeos problemas fundamentais e tendencias insoportables. Tamén puxo de manifesto ata que punto son interdependentes as economías dos países da UE. Unha maior coordinación de políticas económicas na UE contribuirá a resolver

os problemas e a impulsar o crecemento e a creación de emprego no futuro. A gobernanza económica baséase en tres elementos principais: Reforzar a axenda económica cunha supervisión máis estreita da UE, salvagardar a estabilidade da zona euro, e restauración do sector financeiro

Europa descubriu novos motores do crecemento e o emprego. A estes ámbitos destínanse sete iniciativas emblemáticas. Dentro de cada iniciativa, tanto a administración europea como as nacionais deben coordinar os seus esforzos co fin de axudarse mutuamente. A Comisión presentou a maioría destas iniciativas en 2010.

Actuacións emblemáticas na área do crecemento intelixente:

1. Unha axenda dixital para Europa
2. Unión pola innovación
3. Mocidade en movemento

Actuacións emblemáticas na área do crecemento sustentable:

4. Unha Europa que utilice eficazmente os recursos
5. Unha política industrial para a era da mundialización

Actuacións emblemáticas na área do crecemento integrador:

6. Unha axenda de novas cualificacións e empregos
7. Plataforma europea contra a pobreza

Coa publicación, o 7 de xuño de 2011, das recomendacións específicas para cada un dos 27 países da UE, a Comisión tomou outra medida para axudar aos Estados membros a xerar crecemento e emprego e volver encarrilar así a economía da Unión.

As recomendacións baséanse nunha avaliación exhaustiva (documentos de traballo) dos plans dos Estados membros para sanear as finanzas públicas (Programas de Estabilidade ou Converxencia) e das medidas para impulsar o crecemento e o emprego (Programas Nacionais de Reforma).

#### 16.1.2. **A AXENDA DIXITAL EUROPEA.**

A finalidade xenérica da Axenda Dixital é obter os beneficios económicos e sociais sustentables que poden derivar dun mercado único dixital baseado nunha internet rápida e ultrarrápida e nunhas aplicacións interoperables.

A crise destruíu anos de progreso económico e social e deixou ao descuberto os puntos débiles estruturais da economía de Europa. O obxectivo principal de Europa debe ser hoxe volver á boa senda. Para conseguir un futuro sustentable, hai que ver máis aló do curto prazo. Enfrontados a unha situación de envellecemento demográfico e competencia mundial, dispoñemos de tres opcións: traballar máis, traballar durante máis tempo ou traballar con máis intelixencia. O máis probable é que teñamos que facer as tres cousas, pero a última é a única que garantirá un incremento do nivel de vida dos europeos. Para ese efecto, a Axenda Dixital propón medidas que é preciso adoptar urxentemente para poñer a Europa na senda cara a un crecemento intelixente, sustentable e incluínte. As súas propostas establecerán o marco para as transformacións a longo prazo que traerán consigo unha sociedade e unha economía crecentemente dixitais.

A Comisión Europea puxo en marcha en marzo de 2010 a estratexia Europa 2020, co obxectivo de saír da crise e preparar a economía da UE para os retos da próxima década. Europa 2020 expón unha estratexia para conseguir uns niveis elevados de emprego, unha economía de baixa emisión de carbono, produtividade e cohesión social, que debe aplicarse a través de medidas concretas a nivel nacional e da UE.

Esta batalla polo crecemento e o emprego esixe unha toma de conciencia nas altas esferas políticas e a mobilización en toda Europa da totalidade dos axentes.

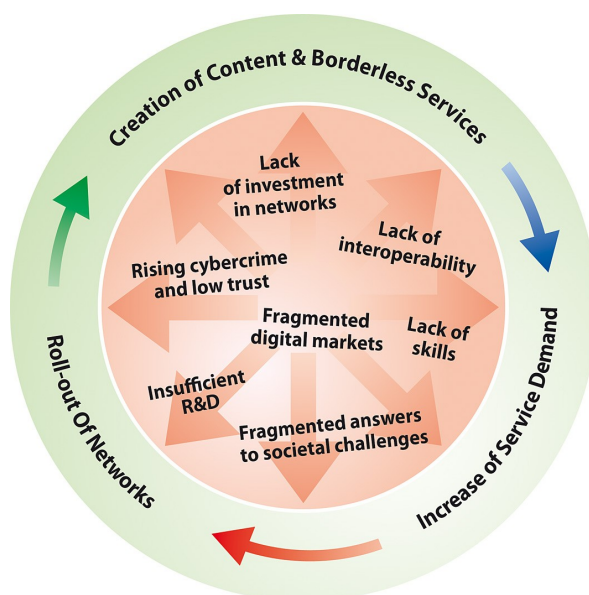
A Axenda Dixital para Europa é unha das sete iniciativas emblemáticas da estratexia Europa 2020, e o seu propósito é definir a función capacitadora esencial que deberá desempeñar o uso das tecnoloxías da información e a comunicación (TIC) se Europa quere facer realidade as súas ambicións para 2020.

O obxectivo desta Axenda é trazar un rumbo que permita maximizar o potencial económico e social das TIC, e en particular da internet, como soporte esencial da actividade económica e social: para facer negocios, traballar, xogar, comunicarse e expresarse en liberdade. De conseguir levala a bo fin, a Axenda fomentará a innovación, o crecemento económico e a mellora da vida cotiá tanto para os cidadáns como para as empresas. Deste xeito, o despregue xeneralizado e a utilización máis eficaz das tecnoloxías dixitais permitirán a Europa afrontar os retos esenciais que ten suscitados e proporcionaralles aos europeos unha mellor calidade de vida manifestada, por exemplo, nunha mellor atención sanitaria, unhas solucións de transporte máis seguras e eficientes, un medio ambiente máis limpo, novas oportunidades en materia de medios de comunicación e un acceso máis fácil aos servizos públicos e aos contidos culturais.

O enorme potencial das TIC pode mobilizarse a través dun ciclo virtuoso de actividade que funcione adecuadamente. É preciso ofrecer uns contidos e servizos atractivos nun contorno da internet interoperable e sen fronteiras. Con iso estímúlase a demanda de velocidades e capacidades máis elevadas, o que á súa vez xustifica o investimento en redes máis rápidas. O despregue e a adopción dunhas redes máis rápidas, pola súa banda, abre o camiño cara a uns servizos innovadores que exploten as velocidades máis elevadas.



Figura 1: Ciclo virtuoso da economía dixital



Este fluxo de actividade pode, en boa medida, autoalimentarse. Esixe un contorno empresarial que fomente o investimento e o espírito emprendedor. Pero, aínda cando o poder de transformación asociado ás TIC sexa evidente, non é menos certo que para explotalo hai que facer fronte a retos importantes.

Sobre a base dunha consulta coas partes interesadas e dos elementos contidos tanto na Declaración de Granada como na Resolución do Parlamento Europeo, a Comisión confeccionou a lista dos sete obstáculos máis importantes. Son os situados no anel interior da Figura 1, e descríbense brevemente a continuación.

Por si sos, ou combinadamente, estes obstáculos socavan gravemente os esforzos realizados para explotar as TIC, evidenciando a necesidade dunha resposta política global e unificada a nivel europeo.

#### 1. Fragmentación dos mercados dixitais.

Europa segue sendo un mosaico de mercados nacionais en liña, e problemas que poderían resolverse perfectamente impídenlles aos europeos gozar dos beneficios dun mercado único dixital. É necesario que os servizos e contidos comerciais e culturais flúan a través das fronteiras; para ese efecto, hai que eliminar os obstáculos regulamentarios e facilitar os pagamentos e a

facturación electrónicas, así como a solución de controversias, e suscitar a confianza dos consumidores. Pódese e débese facer máis dentro do marco regulador actual para tecer un mercado único no sector das telecomunicacións.

## 2. Falta de interoperabilidade

Europa non obtén aínda o máximo beneficio da interoperabilidade. Os puntos débiles en materia de fixación de normas, contratación pública e coordinación entre autoridades públicas impiden que os servizos e dispositivos dixitais que utilizan os europeos traballan conxuntamente todo o ben que deben.

## 3. Incremento da ciberdelincuencia e risco de escasa confianza nas redes

Europa debe combater o auxo das novas formas de delincuencia (a «ciberdelincuencia») que van desde a explotación infantil ao roubo da identidade e os ciberataques, e elaborar mecanismos de resposta.

## 4. Ausencia de investimento en redes

É preciso facer máis para garantir o despregue e a adopción da banda larga para todos, a velocidades crecentes, a través de tecnoloxías tanto fixas como de redes sen fíos.

## 5. Insuficiencia dos esforzos de investigación e innovación

Europa segue investindo pouco, fragmentando os seus esforzos, infrautilizando a creatividade das PEME e fracasando no seu empeño por transformar a vantaxe intelectual da investigación na vantaxe competitiva dunhas innovacións baseadas no mercado.

## 6. Carencias na alfabetización e a capacitación dixitais

Europa padece unha crecente penuria de cualificación profesional nas TIC e un déficit na alfabetización dixital.

## 7. Perda de oportunidade para afrontar os retos sociais.

Se aproveitase plenamente o potencial das TIC, Europa podería facer fronte con moita máis eficacia a algúns dos retos sociais máis agudos: o cambio

climático e outras presións sobre o noso medio ambiente, o envellecemento da poboación e os custos sanitarios crecentes, o desenvolvemento duns servizos públicos máis eficientes e a integración das persoas con discapacidade, a dixitalización do patrimonio cultural de Europa e a súa posta a disposición das xeracións presentes e futuras, etc.

A Axenda Dixital para Europa estrutura as súas accións clave en torno á necesidade de abordar sistematicamente estes sete aspectos problemáticos, que como iniciativa horizontal abarca as tres dimensións de crecemento establecidas en Europa 2020.

A Axenda Dixital esixirá un nivel sostido de compromiso tanto a nivel da UE como dos Estados membros (incluído o nivel rexional). Non poderá ter éxito sen unha importante contribución das demais partes interesadas, incluídos os mozos «nativos dixitais».

Na Axenda Dixital establécense oito campos de actuación para dar resposta a estes problemas, dentro dos cales se definen apartados máis específicos e accións clave.

## 1. UN MERCADO ÚNICO DIXITAL DINÁMICO

A creación de contidos e servizos en liña atractivos e a súa libre circulación dentro da UE e a través das súas fronteiras resultan fundamentais para estimular o círculo virtuoso da demanda. A lexislación relativa ao mercado único en materia de comercio electrónico, facturación electrónica e firma electrónica, as transaccións no contorno dixital seguen sendo demasiado complexas, dadas a incoherencias na aplicación da normativa nos Estados membros. Os consumidores e as empresas seguen enfrontándose a unha incerteza considerable en relación cos seus dereitos e a súa protección xurídica cando fan negocios en liña. Europa está lonxe de contar cun mercado único de servizos de telecomunicacións.

Afrontar estes problemas esixe actuacións nos campos que a continuación se enumeran:

- a) Apertura de acceso aos contidos
- b) Simplificación das transaccións en liña e transfronteirizas
- c) Crear confianza no mundo dixital
- d) Reforzar o mercado único de servizos de telecomunicación.

## 2. INTEROPERABILIDADE E NORMAS

A internet constitúe o mellor exemplo do potencial da interoperabilidade técnica. A súa arquitectura aberta achega dispositivos e aplicacións interoperables a miles de millóns de persoas en todo o mundo. Pero para beneficiarse plenamente do despregue das TIC, é preciso potenciar aínda máis a interoperabilidade entre dispositivos, aplicacións, repositorios de datos, servizos e redes.

Afrontar estes problemas esixe actuacións nos campos que a continuación se enumeran:

- a) Mellorar o establecemento de normas de TIC
- b) Promover un mellor uso das normas
- c) Mellorar a interoperabilidade a través da coordinación.

## 3. CONFIANZA E SEGURIDADE

Os usuarios teñen que estar seguros e protexidos cando se conecten en liña. Do mesmo xeito que a súa contrapartida física, a ciberdelincuencia non se pode tolerar. Ademais, se as novas tecnoloxías non resultan plenamente fiables, será simplemente imposible que existan algúns dos servizos en liña máis innovadores e avanzados, tales como os bancarios ou de asistencia sanitaria.

Afrontar estas ameazas e reforzar a seguridade na sociedade dixital é unha responsabilidade compartida, tanto dos particulares como das entidades privadas e públicas, tanto no fogar como a nivel mundial. Por exemplo, para combater a explotación sexual e a pornografía infantil, poden constituírse plataformas de alerta a nivel nacional e da UE, xunto con medidas encamiñadas a suprimir os contidos nocivos e evitar a súa visualización. Tamén resultan esenciais as actividades educativas e as campañas de sensibilización para o público en xeral. Tamén poderían instarse as industrias a seguir desenvolvendo e aplicar réximes de autorregulación, en particular no que se refire á protección dos menores que utilizan os seus servizos.

O dereito á intimidade e á protección dos datos persoais constitúe un dereito fundamental na UE que é preciso facer aplicar eficazmente utilizando un amplo abanico de métodos: desde a aplicación xeneralizada do principio de «privacidade a través do deseño» nas tecnoloxías de TIC pertinentes, ata as sancións disuasorias cando resulte necesario. O marco das comunicacións electrónicas revisado da UE clarifica as responsabilidades dos operadores de redes e provedores de servizos, incluíndo a súa obriga de notificar as violacións da seguridade dos datos persoais. A revisión do marco xeral de protección de datos recentemente posta en marcha incluírá unha posible ampliación da obriga de notificar as violacións da seguridade dos datos. A aplicación da prohibición do correo non solicitado reforzarase utilizando a rede de cooperación en materia de protección dos consumidores (CPC).

Unha aplicación rápida e efectiva do plan de acción da UE para a protección das infraestruturas críticas de información e do Programa de Estocolmo xerará unha ampla gama de medidas no ámbito da seguridade das redes e da información, así como no da loita contra a ciberdelincuencia. Por exemplo, para reaccionar en tempo real, debería establecerse en Europa unha rede, ampla e cun bo funcionamento, de equipos de resposta a urxencias informáticas (CERT), e tamén para as institucións europeas. A cooperación entre os CERT e os organismos policiais e xudiciais é algo esencial, e debe promoverse un sistema de puntos de contacto que axude a previr a ciberdelincuencia e a reaccionar en caso de urxencias tales como os ciberataques.

Europa necesita tamén unha estratexia de xestión de identidades, en particular para que os servizos de administración electrónica sexan seguros e eficaces.

Para rematar a cooperación entre os axentes pertinentes debe organizarse a nivel mundial, para que sexa efectivamente capaz de loitar contra as ameazas á seguridade e reducilas. Esta posibilidade podería dirixirse dentro dos debates sobre a gobernanza da internet. A nivel máis operativo, deberían proseguir as accións sobre seguridade da información coordinadas internacionalmente e deberían emprenderse accións conxuntas para loitar contra a delincuencia informática, co apoio dunha Axencia Europea de Seguridade das Redes e da Información (ENISA) renovada.

#### 4. ACCESO RÁPIDO E ULTRARRÁPIDO Á INTERNET

Necesitamos unha internet moi rápida para que a economía creza e xere postos de traballo e prosperidade, así como para garantir que os cidadáns poidan acceder aos contidos e servizos que desexan.

A economía do futuro será unha economía do coñecemento baseada en redes nas que o centro será a internet. Europa necesita un acceso á internet rápido e ultrarrápido xeneralizado e a un prezo competitivo. A estratexia Europa 2020 subliñou a importancia do despregue da banda larga para fomentar a inclusión social e a competitividade na UE, reafirmou o obxectivo de poñer a banda larga básica a disposición de todos os europeos como moi tarde en 2013 e propónse que, para 2020, i) todos os europeos teñan acceso a unhas velocidades da internet moi superiores, por encima dos 30 Mbps, e que ii) o 50 % ou máis dos fogares europeos estean abonados a conexións da internet por riba dos 100 Mbps.

Para alcanzar estas ambiciosas metas é necesario elaborar unha política global, baseada nunha combinación de tecnoloxías, que se centre en dous obxectivos paralelos: por unha banda, garantir a cobertura universal da banda larga (combinando a fixa e sen fíos) con velocidades da internet que vaian aumentando gradualmente ata os 30 Mbps e máis, e, co tempo, fomentar o despregue e a adopción das redes de acceso de nova xeración (NGA) nunha gran parte do territorio da UE, para facer posibles conexións ultrarrápidas da internet por riba dos 100 Mbps.

Afrontar estes problemas esixe actuacións nos campos que a continuación se enumeran:

- a) Garantir a cobertura universal da banda larga con velocidades crecentes
- b) Fomentar o despregue das redes NGA
- c) Unha internet aberta e neutral

## 5. INVESTIGACIÓN E INNOVACIÓN

Europa segue investindo pouco na investigación e o desenvolvemento relacionados coas TIC. En comparación cos nosos principais socios comerciais, tales como os Estados Unidos, o I+D sobre TIC en Europa non só representa unha proporción moito menor do gasto total en I+D (17 % fronte ao 29 %), senón que, en termos absolutos, supón ao redor do 40 % do gasto de Estados Unidos.

Afrontar estes problemas esixe actuacións nos campos que a continuación se enumeran:

- a) Incrementar os esforzos e a eficiencia
- b) Explotar o mercado único para impulsar a innovación en TIC
- c) Iniciativas a favor da innovación aberta lideradas pola industria

## 6. FOMENTAR A ALFABETIZACIÓN, A CAPACITACIÓN E A INCLUSIÓN DIXITAIS

A internet converteuse en parte integrante da vida cotiá de moitos europeos. Con todo, 150 millóns de europeos —o 30 % aproximadamente— nunca utilizaron aínda a internet. Adoitan dicir que non o necesitan, ou que resulta demasiado caro. Este grupo está composto principalmente polas persoas de 65 a 74 anos, as persoas de renda baixa, os desempregados e os de nivel cultural máis baixo.

En moitos casos, esta situación débese á falta de capacitación do usuario, por exemplo alfabetización dixital e mediática, non só para a empregabilidade, senón tamén para aprender, crear, participar e abordar con confianza e discernimento o uso

dos medios de comunicación dixitais. A accesibilidade e a utilizabilidade constitúen tamén senllos problemas para os europeos con discapacidade. Salvar esta fenda dixital pode axudar aos membros dos grupos sociais desfavorecidos a participar máis en pé de igualdade na sociedade dixital (incluídos os servizos de interese directo para eles, por exemplo nos ámbitos da aprendizaxe, a administración pública ou a saúde en liña) e a saír da súa condición desfavorecida incrementando a súa empregabilidade. A competencia dixital é, pois, unha das oito competencias clave que resultan fundamentais para as persoas nunha sociedade baseada no coñecemento. Tamén é esencial para que todos saiban como garantir a propia seguridade cando se está en liña.

Ademais, as TIC non poden funcionar con eficacia como sector europeo en crecemento e como motor da mellora da competencia e a produtividade na economía europea se non se dispón de persoal capacitado. E a economía da UE padece unha penuria deste tipo de persoal: Para 2015, Europa podería carecer da capacitación necesaria para cubrir ata 700.000 postos de traballo nas TI.

Afrontar estes problemas esixe actuacións nos campos que a continuación se enumeran:

- a) Alfabetización e capacitación dixitais
- b) Servizos dixitais incluíntes

## 7. BENEFICIOS QUE FAN POSIBLES AS TIC PARA A SOCIEDADE DA UE

A sociedade dixital debe entenderse como unha sociedade que supoñerá vantaxes para todos. O despregue das TIC estase convertendo nun elemento crítico para a consecución de obxectivos políticos tales como o apoio a unha sociedade que envellece, o cambio climático, a redución do consumo enerxético, a mellora da eficiencia do transporte e da mobilidade, a autonomización dos pacientes e a inclusión das persoas con discapacidade.



Afrontar estes problemas esixe actuacións nos campos que a continuación se enumeran:

- a) As TIC ao servizo do medio
- b) Atención sanitaria sustentable e apoio baseado nas TIC para unha vida digna e autónoma
- c) Promoción da diversidade cultural e os contidos creativos
- d) Administración electrónica
- e) Sistemas de transporte intelixentes a favor dun transporte eficiente e unha mobilidade mellor

## 8. ASPECTOS INTERNACIONAIS DA AXENDA DIXITAL

A Axenda Dixital europea propónse facer de Europa un centro neurálxico do crecemento intelixente, sustentable e incluínte na escena mundial. Os sete alicerces da Axenda Dixital teñen, todos eles, dimensións internacionais. O mercado único dixital, en particular, necesita dunha faceta externa, porque só a nivel internacional se pode progresar en moitas das cuestións políticas. Unha interoperabilidade e unhas normas recoñecidas a escala mundial poden contribuír a promover unha innovación máis rápida ao diminuír os riscos e os custos das novas tecnoloxías. Tamén a loita contra as crecentes ameazas á ciberseguridade debe desenvolverse nun contexto internacional. Así mesmo, as solucións regulamentarias europeas, que se basean na igualdade de oportunidades, a transparencia dos poderes públicos e a gobernanza e a apertura dos mercados á competencia, están servindo de inspiración noutros lugares do mundo. Para rematar, tamén é importante comparar os progresos europeos na Axenda Dixital coas mellores prestacións internacionais.

Por conseguinte, resulta crucial unha dimensión internacional na Axenda Dixital a fin de completar as accións antes mencionadas, sobre todo á vista da importancia estratéxica da internet. Europa debe seguir desempeñando un papel de liderado, en consonancia coa Axenda de Tunicia, na promoción dunha gobernanza da internet o

máis aberta e incluínte posible. Actualmente a internet inclúe unha ampla gama de dispositivos e aplicacións que penetran en todos os aspectos da vida, con independencia da xeografía, e no futuro esta tendencia mesmo se acentuará. Constitúe un instrumento formidable para a liberdade de expresión en todo o mundo.

Para fomentar a innovación tamén a nivel internacional, a Comisión traballará por conseguir unhas condicións favorables para os bens e servizos dixitais no comercio exterior, p. ex., crear unha asociación máis sólida para obter acceso ao mercado e oportunidades de investimento, reducir as barreiras arancelarias e non arancelarias a nivel mundial, mellorar a protección dos dereitos de propiedade intelectual e evitar o falseamento do mercado.

O Acordo sobre Tecnoloxías da Información (ATI) de 1997 produciu resultados tanxibles á hora de promover a adopción da tecnoloxía da información en Europa e no mundo. Con todo, hoxe en día é preciso actualizar ese acordo para ter en conta as últimas novidades, e en especial a converxencia das tecnoloxías e os produtos.

Tamén será necesario que o progreso tecnolóxico quede mellor reflectido nos acordos comerciais internacionais no que se refire ao ámbito dos servizos dixitais e a propiedade intelectual.

## APLICACIÓN E GOBERNANZA

O éxito da Axenda Dixital depende de que as diferentes medidas do conxunto se executen de forma precisa e de acordo coa estrutura de gobernanza prevista en Europa 2020. A Comisión propónse:

1. Instituír un mecanismo de coordinación interno
2. Cooperar estreitamente cos Estados membros, co Parlamento Europeo e con todas as partes interesadas.
3. Levar un seguimento dos avances da Axenda Dixital mediante a publicación anual, no mes de maio, dun cadro de indicadores.

4. Organizar un amplo debate entre as partes interesadas sobre os avances rexistrados, segundo figuren nos cadros de indicadores dixitais, que adoptará a forma de Asemblea Dixital anual que se celebrará en xuño e reunirá os Estados membros, as institucións da UE e os representantes dos cidadáns e do sector, para avaliar os progresos e os desafíos que xurdan.
5. A Comisión presentaralle o seu informe ao Consello Europeo sobre os resultados destas actividades nun Informe de situación anual, como dispón a estrutura de gobernanza de Europa 2020.

## OBXECTIVOS CLAVE EN MATERIA DE RENDEMENTO

1. Obxectivos en materia de banda larga:
  - Banda larga básica para todos en 2013: cobertura de banda larga básica para o 100 % dos cidadáns europeos (base de referencia: en decembro de 2008 a cobertura DSL total era dun 93 % da poboación da UE).
  - Banda larga rápida para 2020: cobertura de banda larga de 30 Mbps ou superior para o 100 % dos cidadáns europeos (base de referencia: en xaneiro de 2010 un 23 % dos abonos á banda larga alcanzaban polo menos os 10 Mbps).
  - Banda larga ultrarrápida para 2020: un 50 % dos fogares europeos deberán contar con abonos por encima dos 100 Mbps (non hai base de referencia).
2. Mercado único dixital:
  - Promoción do comercio electrónico: un 50 % da poboación deberá efectuar compras en liña para 2015. (base de referencia: en 2009, un 37 % de usuarios con idades comprendidas entre os 16 e os 74 anos efectuaron pedidos de bens ou servizos con carácter privado nos 12 meses anteriores).
  - Comercio electrónico transfronteirizo: un 20% da poboación deberá efectuar compras transfronteirizas en liña para 2015 (base de referencia: en 2009, un



8% de usuarios entre os 16 e os 74 anos efectuaran pedidos de bens ou servizos a provedores doutros países da UE nos 12 meses anteriores).

- Comercio electrónico para as empresas: un 33 % das PEME deberán efectuar compras ou vendas en liña para 2015 (base de referencia: en 2008, un 24 % e un 12 % das empresas comprou ou vendeu, respectivamente, de forma electrónica, por un valor igual ou superior ao 1 % do seu volume total de compras ou a súa facturación).
- Mercado único dos servizos de telecomunicacións: para 2015 a diferenza entre as tarifas de itinerancia e as nacionais deberá aproximarse a cero (base de referencia: en 2009, o prezo medio dun minuto en itinerancia ascendía a 0,38 céntimos (por chamada efectuada), e o prezo medio por minuto de todas as chamadas na UE era de 0,13 céntimos (incluída a itinerancia)).

### 3. Inclusión dixital:

- Aumentar a utilización regular da internet dun 60 % a un 75 % en 2015 e, entre os colectivos desfavorecidos, dun 41 % a un 60 % (a base de referencia son as cifras de 2009).
- Diminuír á metade a parte de poboación que nunca usou a internet para 2015 (ata un 15 %) (base de referencia: en 2009, un 30 % de persoas con idades comprendidas entre os 16 e os 74 anos non usara nunca a internet).

### 4. Servizos públicos:

- Administración electrónica para 2015: Un 50 % dos cidadáns utilizan a administración electrónica, e máis da metade desa cifra cobren formularios en liña (base de referencia: en 2009, un 38 % de persoas con idades comprendidas entre os 16 e os 74 anos usaran a administración electrónica nos 12 meses anteriores, e un 47 % delas cubrira formularios en liña).
- Servizos públicos transfronteirizos: En 2015 deberán estar dispoñibles en liña todos os servizos públicos transfronteirizos clave contidos nunha lista que acordarán os Estados membros en 2011 (non hai base de referencia).

5. Investigación e innovación:

- Fomento da I+D nas TIC: Duplicación do investimento público a 11 000 millóns de euros (base de referencia: a cifra nominal de créditos orzamentarios públicos de I+D dedicados ás TIC (CPPID-TIC) ascendía en 2007 a 5 700 millóns).

6. Economía con baixa emisión de carbono:

- Promoción do alumeado con baixo consumo de enerxía: Redución de polo menos un 20 % do consumo de enerxía en alumeado para 2020 (non hai base de referencia).

### **16.1.3. PLAN AVANZA 2.**

Avanza é o primeiro Plan que supuxo unha verdadeira aposta real do Goberno e do conxunto da sociedade española polo desenvolvemento da sociedade da información (SI) e do coñecemento.

Avanza logrou que o sector das telecomunicacións e da sociedade da información se convertera, como sector estratéxico, en motor e impulso do desenvolvemento doutros sectores. A SI, como elemento necesario en calquera actividade económica ou industrial, ten un efecto xeral e horizontal no conxunto da economía e constitúe un elemento esencial para vertebrar a recuperación económica.

O sector TIC está adquirindo en España un volume de negocio e unha presenza de uso e desenvolvemento de produtos e servizos tan importante que permiten situalo xa como un dos nosos grandes sectores produtivos.

Un dos principais obxectivos do Plan Avanza2 é contribuír á recuperación económica do noso país grazas ao uso intensivo e xeneralizado das TIC, cunha especial atención aos proxectos que compaxinen, ademais, a sustentabilidade e o aforro enerxético.

Neste contexto, Avanza2 ten como reto non xa tanto a dinamización da oferta como o fomento da demanda, así como no aproveitamento do impulso do desenvolvemento do sector para a consolidación dunha industria TIC propia especializada en sectores estratéxicos e sempre envorcado na PEME, na que se centra a maior parte dos esforzos.

As iniciativas de Avanza2 agrúpanse en cinco eixes de actuación:

1. Eixe Capacitación: Desde o Plan Avanza 2 abóndase esta capacitación desde dous puntos de vista, a persoa como cidadán que forma parte da sociedade e a persoa como traballador que se integra nunha empresa. Na vertente da persoa como cidadán, préstase especial atención ao uso e á aceptación das TIC e á utilización dos servizos dixitais por parte dos cidadáns en risco de exclusión dixital e foméntase a igualdade de xénero na rede. Doutra banda, na vertente da persoa como traballador, obsérvase que o uso xeral das TIC nas pequenas empresas e as microempresas. Dada a importancia que representa este segmento de empresas no tecido produtivo e na creación de emprego, resulta fundamental impulsar a penetración das TIC nelas mediante accións específicas de capacitación e promoción.

Dentro deste eixe, establécense os seguintes programas:

- a) Na liña de Capacitación Cidadanía: Capacitación Tecnolóxica, Xénero, Maiores, Persoas con Discapacidade, Infancia, Outros Colectivos, Equipamento e conectividade, Inmigrantes.
  - b) Na liña de Capacitación PEME: Dinamización PEME, Solucións sectoriais, Formación e Equipamento e conectividade.
2. Eixe Contidos e Servizos Dixitais: Preténdese impulsar a industria española relacionada coa produción, xestión e distribución de contidos dixitais,



destacando que este tipo de industria que non deixou de crecer nos últimos anos no noso país, despertando cada día maior interese entre creadores, produtores, editores, distribuidores, agregadores de contidos e operadores. Doutra banda débese ter en conta o desenvolvemento dos servizos que presta a administración. As vantaxes que nos ofrece a administración electrónica son un feito constatado, e por iso, o próximo reto consiste en fomentar o uso de servizos avanzados por parte da cidadanía e as empresas.

Dentro deste eixe, establécense os seguintes programas:

- a) Na liña de Contidos: Contidos Dixitais e Centros do Coñecemento.
- b) Na liña de Servizos Dixitais: Solucións EELL, Concello Dixital, Cidades Dixitais, Administración electrónica da Administración Xeral do Estado, Educación, Sanidade e Xustiza.

- 3. Eixe Desenvolvo do Sector TIC: Neste eixe do Plan Avanza 2 búscase apoiar a empresas que desenvolvan novos produtos, procesos, aplicacións, contidos e servizos TIC, promovendo, como prioridades temáticas básicas, a participación industrial española na construción da internet do Futuro. Xa que logo, fomentar a innovación e a investigación industrial é apostar pola mellora da competitividade do sector TIC.

Dentro deste eixe, establécense os seguintes programas:

- a) Fomento de Competitividade e Innovación.
- b) Propiedade Intelectual.
- c) Software Libre.
- d) Promoción Tecnolóxica.

- 4. Eixe Infraestruturas: O obxectivo que se pretende alcanzar a través das medidas contempladas neste apartado é a de dispoñer dunhas infraestruturas de telecomunicacións adecuadas ás cambiantes necesidades sendo

fundamentais para o desenvolvemento da sociedade da información. A súa extensión a toda a cidadanía permite loitar contra a fenda dixital e de xénero, ofrecer servizos electrónicos avanzados á cidadanía e ás empresas, aumentar a produtividade do tecido industrial e xerar crecemento económico.

Dentro deste eixe, establécense os seguintes programas:

- a) Banda larga.
- b) Telecentros.
- c) Televisión Dixital Terrestre.

5. Eixe Confianza e Seguridade: Este eixe do Plan Avanza 2 centrará os seus obxectivos e áreas de actuación exclusivamente no desenvolvemento das políticas públicas para a seguridade da información orientadas a particulares e empresas, contribuíndo ao resto de políticas nacionais para a construción da confianza desde a cooperación e a coordinación. A misión será a de impulsar a construción da confianza a través de políticas públicas proactivas e de carácter preventivo en relación coa seguridade da información centradas nos particulares e nas empresas, especialmente as PEME, promovendo a participación de todos os axentes implicados.

Dentro deste eixe, establécense os seguintes programas:

- a) Seguridade da Información.
- b) DNI electrónico.

## ESTRATEGIA 2011-2015

O Consello de Ministros aprobou o 16 de xullo de 2010 o acordo polo que se aproba a Estrategia 2011-2015 do Plan Avanza 2. Esta segunda fase dá continuidade ao Plan Avanza, incorporando as actuacións en execución e actualizando os seus obxectivos iniciais para adecualos aos novos retos da sociedade en rede.



No ano 2004, o Goberno era consciente da importancia de xeneralizar o uso e o impacto das novas tecnoloxías na economía e a sociedade. Por iso xurdiu da necesidade de establecer “un plan de converxencia con Europa e entre Comunidades Autónomas e Cidades Autónomas” neste ámbito, denominado Plan Avanza.

O Plan Avanza, que foi aprobado polo Consello de Ministros o 4 de novembro de 2005, permitiu alcanzar unha masa crítica no noso país, tanto en termos de mercado como de usuarios, na aceptación xeneralizada das TIC e na cobertura global de servizos TIC, o que facilitará enormemente o progreso nos próximos anos.

Unha vez alcanzados unha boa parte dos obxectivos formulados e sendo conscientes da necesidade de seguir avanzando cara a unha sociedade do coñecemento, comeza unha nova etapa integrada por cinco eixes estratéxicos de actuación: Infraestruturas, Confianza e Seguridade, Capacitación Tecnolóxica, Contidos e Servizos Dixitais e Desenvolvemento do Sector TIC.

Unha das principais contribucións do Plan Avanza 2 é coadxuvar ao cambio de modelo económico do noso país a través das TIC, xa que a xeneralización do seu uso permite e permitirá un incremento da competitividade e a produtividade, ademais de favorecer a igualdade de oportunidades, dinamizando a economía e consolidando un modelo de crecemento económico sustentable.

A primeira fase do Plan Avanza perseguía recuperar o atraso de España respecto da Unión Europea, especialmente en cobertura e conectividade. A Estratexia 2011-2015 do Plan Avanza 2 pretende situar a España nunha posición de liderado no desenvolvemento e uso de produtos e servizos TIC avanzados.

Trala presentación do Plan Avanza 2 e unha vez determinada a súa estrutura, o Consello de Ministros procedeu a aprobar a estratexia dese plan para o período 2011-

2015. Esa estratexia non está vinculada a uns orzamentos concretos senón que marca unhas prioridades que se adoptarán e desenvolverán dentro dos escenarios de consolidación orzamentaria aprobados polo Goberno.

No proceso de elaboración da Estratexia cómpre destacar o consenso que suscitou entre as forzas políticas. En concreto, o 21 de decembro de 2009, o Senado aprobou por unanimidade un documento de propostas que foron incorporadas integramente na Estratexia 2011-2015 do Plan Avanza 2.

Así mesmo, na elaboración da Estratexia colaboraron tamén o sector privado e o conxunto de axentes sociais, políticos e institucionais co fin de lograr a máxima eficacia e eficiencia das iniciativas identificadas. Para o Goberno a elaboración e o desenvolvemento dun Plan con estas características é unha tarefa común que require da participación e o esforzo de toda a sociedade española.

Así mesmo, a Estratexia enmárcase dentro das iniciativas que se están elaborando no ámbito europeo. A Comisión Europea aprobou o 19 de maio de 2010 unha Comunicación sobre a “Axenda Dixital Europea”, que ten por obxectivo promover o desenvolvemento da sociedade da información e as TIC para a reactivación económica e a creación de emprego na UE e un horizonte temporal o ano 2015, tomando así a substitución do i2010.

Tomando como punto de partida o Plan Avanza aprobado no ano 2005, así como o marco europeo no que se encadran este tipo de iniciativas, identificáronse 34 retos concretos que debe abordar España no ámbito das TIC. Neste contexto, a Estratexia 2011-2015 do Plan Avanza 2 consiste en centrar os seus esforzos na consecución dos seguintes 10 obxectivos que facilitarán a superación dos retos definidos:

1. Promover procesos innovadores TIC nas AAPP
2. Estender as TIC na sanidade e o benestar social

3. Potenciar a aplicación das TIC ao sistema educativo e formativo
4. Mellorar a capacidade e a extensión das redes de telecomunicacións
5. Estender a cultura da seguridade entre a cidadanía e as empresas
6. Incrementar o uso avanzado de servizos dixitais pola cidadanía
7. Estender o uso de solucións TIC de negocio na empresa
8. Desenvolver as capacidades tecnolóxicas do sector TIC
9. Fortalecer o sector de contidos dixitais garantindo a mellor protección da propiedade intelectual no actual contexto tecnolóxico e dentro do marco xurídico español e europeo.
10. Desenvolver as TIC verdes.

Para a consecución dos 10 obxectivos definidos, identificáronse máis de 100 medidas concretas que se deben articular, así como os indicadores de seguimento que medirán o seu grao de consecución.

Adicionalmente, identificáronse un conxunto de reformas normativas, necesarias tanto para eliminar barreiras existentes á expansión e uso das TIC, como para garantir os dereitos dos cidadáns na sociedade da información. Neste apartado destacan a Lei de medidas de impulso da sociedade da información, e a Lei de acceso electrónico dos cidadáns aos servizos públicos.

Doutra banda, en canto ao modelo de execución para a posta en marcha destas medidas, mantense o modelo de colaboración con todos os niveis da Administración pública, en especial coas comunidades autónomas e as entidades locais, así como das entidades sen fins de lucro e as empresas privadas, iniciado polo Plan Avanza.

A Estratexia 2011-2015 do Plan Avanza 2 consta dun texto base, no que se destaca o papel das TIC na economía e o crecemento, os logros do Plan Avanza na súa primeira fase, o marco europeo concretado na Axenda Dixital Europea 2010-2015 aprobada durante a presidencia española, os principais retos de futuro no ámbito da sociedade

da información e os 10 obxectivos que servirán para conseguir eses retos, e dun anexo no que se recompilan as máis de 100 medidas concretas que se deben poñer en marcha.

## AVALIACIÓN E SEGUIMIENTO

Para garantir o éxito do Plan Avanza é fundamental asegurar a avaliación e seguimento permanente das actuacións que se realicen, valorando así a consecución de obxectivos suscitados en cada unha das áreas de actuación, á vez que serven para orientar a adaptación do plan aos cambios.

A documentación de avaliación e seguimento dispoñible no sitio web do Plan Avanza é a seguinte:

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 Converxencia Plan Avanza.
  - Indicadores de evolución da sociedade da información.
  - Balance actuacións SETSI.
4. Información internacional
  - Estudo do Plan Avanza pola OCDE.

Pódese atopar toda a información necesaria sobre este tema na dirección <http://www.planavanza.es/>.

## **16.2. REFERENCIAS**

- Comunicación da Comisión ao Parlamento Europeo, ao Consello, ao Comité Económico e Social europeo e ao Comité das Rexións – Unha Axenda Dixital para Europa, con data 28 de agosto de 2010.
- Sitio web Eur-Lex no enderezo <http://eur-lex.europa.eu/>, integrado no sitio web oficial da Unión Europea.
- Sitio web da Comisión Europea dedicado á Estratexia Europa 2020 no enderezo [http://ec.europa.eu/europe2020/index\\_es.htm](http://ec.europa.eu/europe2020/index_es.htm)
- Sitio web do Ministerio de Industria, Turismo e Comercio dedicado ao Plan Avanza2 na dirección <http://www.planavanza.es/>.

Autor: Jesús Rodríguez Castro

Xefe do Servizo de Informática do Concello de Santiago de Compostela

Colexiado do CPEIG

# **17. INICIATIVAS DO GOBERNO GALEGO: OSIMGA, REDE CEMIT, PLAN DE BANDA LARGA 2013, AXENDA DIXITAL 2014.GAL, ESTRATEXIA DE IMPULSO AO SECTOR TIC. SISTEMAS DE INFORMACIÓN.**

## **TEMA 17. INICIATIVAS DO GOBERNO GALEGO. OSIMGA. REDE CeMIT, PLAN DE BANDA LARGA 2013. AXENDA DIXITAL 2014.gal. ESTRATEXIA DE IMPULSO DO SECTOR TIC.**

### **17.1. OSIMGA**

### **17.2. REDE CeMIT**

### **17.3. PLAN DE BANDA LARGA 2013.**

### **17.4. AXENDA DIXITAL 2014.gal**

### **17.5. ESTRATEXIA DE IMPULSO DO SECTOR TIC**

### **17.6. REFERENCIAS**

### **17.1. OSIMGA**

O Observatorio da Sociedade da Información e a Modernización de Galicia (OSIMGA) é un órgano asesor para a valoración da evolución da sociedade da información, a modernización administrativa e a Administración electrónica nas administracións públicas de Galicia, e para a participación e colaboración coas distintas administracións públicas nestas materias

Creado e regulado polo Decreto 21/2010, do 4 de febreiro (DOG, 26/02/2010), o OSIMGA está adscrito á Secretaría Xeral de Modernización e Innovación Tecnolóxica da Xunta de Galicia.

Este decreto atribúelle ao observatorio entre as súas funcións as de desenvolver ou promover estudos e análises de datos que permitan coñecer o nivel de desenvolvemento, a tendencia e posibles problemáticas que poden afectar á extensión da sociedade da información en Galicia e a aplicación do modelo de e-Goberno nas administracións públicas galegas. O OSIMGA elabora informes de situación e de



evolución e facilita datos a outros organismos competentes na materia, contribuíndo á definición estratéxica de políticas públicas.

Así mesmo, o observatorio analiza o estado de desenvolvemento da sociedade da información para toda a cidadanía e, en especial, no que respecta aos colectivos en risco de exclusión, promovendo liñas de actuación que potencien a súa incorporación e permanencia en condicións de igualdade efectiva. Entre as observacións de carácter xeral cómpre salientar que o OSIMGA porá en marcha enquisas sobre a sociedade da información en Galicia e sobre a e-Administración na Xunta e nas entidades locais.

A web do OSIMGA (<http://www.osimga.org/>) é unha canle aberta de comunicación e difusión dos datos, informacións, estudos e outros materiais elaborados polo observatorio. Ademais subministra unha selección de novas relacionadas coa modernización da Administración autonómica galega e a sociedade da información en Galicia.

Os principais obxectivos do observatorio son:

1. Desenvolver ou promover compilacións, estudos e análises de datos que permitan coñecer cunha visión global o nivel de desenvolvemento, a tendencia e os posibles problemas que afecten á extensión da sociedade da información en Galicia e á aplicación do modelo de e-Goberno nas administracións públicas galegas.
2. Facilitar análises comparativas e aliñacións de datos con outros marcos xeográficos.
3. Promover o intercambio de experiencias e información entre administracións, con outros observatorios, organismos ou entidades.
4. Impulsar a organización de eventos formativos, reunións de expertos ou grupos de traballo.
5. Promover e xestionar a elaboración e difusión de publicacións técnicas, impresas ou electrónicas, específicas e monográficas ou de publicación periódica.

6. Xestionar e ofrecer periodicamente e, como mínimo, a través dunha web específica, información sobre o nivel de desenvolvemento da sociedade da información en Galicia, eventos formativos, noticias de actualidade, ou ligazóns con outras fontes de información, observatorios ou entidades.
7. Elaborar e presentar publicamente informes que reflectan o estado de situación ou a evolución prevista.
8. Facilitar datos a outros organismos e entidades con competencias específicas na materia.
9. Analizar o estado de desenvolvemento da sociedade da información para toda a cidadanía e, en especial, no que respecta ás mulleres, ás persoas con discapacidade, ás persoas maiores e aos colectivos con risco de exclusión, promovendo liñas de actuación que potencien a súa incorporación e permanencia activa en condicións de igualdade efectiva.
10. Avaliar e servir de elemento para a definición de políticas públicas en materia de sociedade da información e modernización da Administración.

## DOCUMENTOS E MEMORIAS

O Sistema de indicadores da sociedade da información de Galicia é un conxunto de indicadores estatísticos que permite monitorizar, dun xeito sintético, rigoroso e transparente, a evolución da sociedade da información en Galicia, ofrecendo unha visión de conxunto da situación e do seu grao de avance.

Este modelo de indicadores foi elaborado tomando como referencia as recomendacións establecidas no código de boas prácticas das estatísticas europeas.

O Sistema de indicadores ofrece información referente ao nivel de equipamento e utilización de produtos e servizos TIC por parte da poboación e as empresas galegas, realizando ademais un tratamento específico do sector galego das tecnoloxías da

información e das comunicacións (sector TIC), así como un seguimento da Administración electrónica en Galicia.

## **17.2. REDE CeMIT**

A Rede de Centros para a Modernización e a Inclusión Tecnolóxica (CeMIT) é unha iniciativa posta en marcha pola Xunta da Galicia que busca impulsar as TIC e a sociedade da información na comunidade galega. Esta rede forma parte da Axenda Dixital 2014.gal, enmarcada no Plan Estratéxico Galicia 2010-2014 que ten como fin acadar a converxencia tecnolóxica con Europa no horizonte do ano 2020.

A Rede CeMIT nace cos obxectivos estratéxicos de vertebrar territorial e socialmente Galicia, en especial onde a fenda dixital se fai máis evidente, e impulsar, potenciar e difundir os coñecementos nas tecnoloxías da información e a comunicación en tres colectivos principalmente: cidadanía, profesionais TIC e empregados públicos

Así pois, a nova Rede CeMIT configúrase como un importante vehículo para a posta en práctica de iniciativas orientadas a impulsar o emprego das TIC de cara a fomentar a empregabilidade, a competitividade empresarial, a e-Inclusión, o e-Benestar e o pulo da e-Administración.

A nova Rede de Centros para a Modernización e a Inclusión Tecnolóxica de Galicia (Rede CeMIT) é unha iniciativa impulsada dende a Xunta de Galicia en colaboración cós concellos galegos, para potenciar o uso das TIC e a sociedade da información en Galicia.

A Rede convértese deste xeito nun instrumento esencial de soporte á nova estratexia en materia de sociedade de información, definida a través da Axenda Dixital 2014.gal, contribuíndo a vertebrar territorial e socialmente Galicia, impulsar o crecemento do sector empresarial tradicional, especializar os profesionais do sector TIC, e potenciar os coñecementos tecnolóxicos do empregado público.

A Rede CeMIT ofrece un amplo abano de servizos que se divide nos seguintes tres grandes bloques:

#### a) FORMACIÓN

A Formación é un dos servizos principais que ofrecerá a nova rede a cidadáns, profesionais TIC, empresas, empregados públicos e axentes territoriais a través de dúas modalidades:

- Formación presencial: Impartirase directamente dende os centros da rede a través de métodos que combinan a exposición de conceptos coa demostración de procesos e coa execución guiada por parte do grupo, para o que se definirán as accións de formación que se detallan a continuación: Formación en alfabetización dixital, formación avanzada de profesionais TIC, formación multimedia e audiovisual, e formación de empregados públicos
- Formación en liña: Permitiralles aos cidadáns realizar actividades formativas a través dun centro virtual de formación con dúas funcións complementarias: titorización e interacción.

Tamén se contempla a formación mixta baseada no concepto de *blended learning*, é dicir, que combina actividades presenciais, síncronas e en liña.

#### b) ACTIVIDADES DE DIFUSIÓN

A organización de charlas e xornadas de sensibilización e divulgación das actividades da rede, a captación de usuarios e introdución a temas relacionados coas novas tecnoloxías serán actividades que forman parte da carta de servizos da nova rede e que serán planificadas en función das necesidades e demandas detectadas.

### c) AULA ABERTA

Os centros da rede tamén se converterán en “aulas abertas”, auténticos espazos nos que os seus usuarios/as, dentro dun horario establecido, poderán acceder libre e gratuitamente á utilización das aulas, para o que contarán co apoio e asesoramento dos axentes TIC.

Deste xeito, as aulas convértense en verdadeiros espazos abertos nos que calquera cidadán pode, sen custo ningún, achegarse ás novas tecnoloxías e facer uso delas de modo persoal e independente.

A estratéxica localización das súas instalacións, ao longo de máis de 50 comarcas e 89 concellos, favorece que calquera dos seus usuarios non deba percorrer grandes distancias para atopar unha Aula CeMIT na que se impartan algunha das máis de 1.000 actividades formativas previstas. Esta dispersión xeográfica permite garantir a correcta vertebración territorial e social de Galicia, especialmente onde a fenda dixital se fai máis evidente.

**CENTROS DE ALTA ESPECIALIZACIÓN: A ESCOLA GALEGA DE ADMINISTRACIÓN PÚBLICA E O CENTRO DE NOVAS TECNOLOXÍAS DE GALICIA.**

A Escola Galega de Administración Pública (EGAP) é un organismo público pertencente á Xunta de Galicia, e a súa finalidade é deseñar e impartir o programa de formación destinado aos empregados públicos de Galicia. Dado que é un instrumento de primeira orde para a profesionalización da Función Pública e ten o obxectivo final de lle proporcionar á sociedade galega os mellores servizos, constitúe unha compoñente indispensable para acadar os obxectivos estratéxicos da Rede CeMIT

O Centro de Novas Tecnoloxías de Galicia (CNTG) contribúe activamente na formación e capacitación dos profesionais TIC galegos a través de cursos especializados e

certificacións tecnolóxicas de primeiro nivel. Deste xeito, o CNTG orienta a súa actividade cara aos profesionais dos sectores privado e público, ocupados ou en busca de emprego, que demanden formación técnica de alto nivel relacionada co mundo das novas tecnoloxías. Deste xeito, constitúen un dos alicerces sobre o que se sustenta a Rede CeMIT no que respecta á formación especializada.

### **17.3. PLAN DE BANDA LARGA 2013.**

O Plan director de telecomunicación de banda larga busca garantir que as infraestruturas de telecomunicacións contén coa capacidade necesaria para facer posible o acceso de todos os galegos á sociedade da información. De feito, pretende dotar de estratexia, actuacións e un modelo de xestión en materia de despregamento de infraestruturas de telecomunicacións á Comunidade galega.

A Xunta de Galicia asume a coordinación dos axentes implicados na elaboración do plan, asegurando orde, eficiencia e un uso óptimo dos recursos. As autoridades rexionais e locais serán as mellor situadas para planificar os proxectos de banda larga.

A Xunta de Galicia aprobou o 18 de febreiro de 2010 o Plan Banda Larga de Galicia 2010-2013, que define a estratexia a seguir para alcanzar as seguintes metas:

- Reducir o desequilibrio territorial proporcionando acceso á banda larga de calidade a toda a poboación galega.
- Impulsar a competitividade e innovación nas empresas proporcionando acceso á banda larga aos sectores produtivos para extraer o máximo aproveitamento das novas tecnoloxías.
- Modernizar os servizos públicos proporcionando acceso á banda larga a todos os núcleos con puntos de demanda pertencentes á Administración.
- Maximizar a cooperación asegurando un despregamento baseado na eficiencia e na cooperación de todos os axentes implicados.

Por tanto, o Plan Director de Banda Larga de Galicia é un instrumento esencial e necesario para a definición das políticas de infraestruturas de Galicia que permitiría, entre outros:

- Impulsar unha estratexia global, encamiñada a situar a Galicia no núcleo avanzado da sociedade da información.
- Garantir a capacidade de acceso dos galegos á sociedade da información baixo condicións de homoxeneización de calidade de servizo e custo.
- Asegurar a vertebración dixital do noso territorio, como elemento de compensación de desequilibrios culturais, tecnolóxicos e socioeconómico, de inclusión social e de eliminación da fenda dixital.
- Extraer o máximo aproveitamento das posibilidades das novas tecnoloxías como dinamizadoras económicas e xeradoras de competitividade e innovación nos diferentes sectores produtivos e como medio para promover a equidade, a sustentabilidade e a calidade dos servizos públicos.
- Impulsar a modernización da Administración Pública autonómica e local, empregando toda a potencialidade que ofrece hoxe a tecnoloxía.

## ReDe – REXISTRO DE DEMANDANTES

ReDe é unha ferramenta de consulta que proporciona información sobre a cobertura de banda larga alcanzada coas actuacións do Plan Banda Larga 2010-2013 (PDBL). Grazas a ReDe calquera cidadán pode facer uso do seu navegador web habitual para obter información sobre a cobertura de banda larga ou rexistrar demandas.

## OFICINA TÉCNICA DO PLAN DE BANDA LARGA

A Oficina Técnica é un recurso da Xunta de Galicia que, dentro do marco do Plan Banda Larga, pon en marcha distintos servizos para apoiar o desenvolvemento das distintas actuacións do plan:

Os principais obxectivos da Oficina Técnica son coordinar e tutelar a execución do plan e velar pola consecución con éxito de proxectos específicos liderados e executados por un grupo/área e por aqueles proxectos de alcance máis amplo, que sexan tractores e involucren a máis dunha área/grupo ou a outro tipo de axentes. Deste xeito, a Oficina Técnica constitúe un punto único de referencia para todos os axentes involucrados no Plan de Banda Larga fomentando o avance homoxéneo das distintas actuacións do plan e incentivando a eficiencia e efectividade das mesmas.

A Oficina Técnica pon en marcha distintos servizos para apoiar o desenvolvemento das distintas actuacións do Plan de Banda Larga, axilizando así a consecución dos seus obxectivos. Ditos servizos agrúpanse segundo a súa índole en servizos de Xestión, Control e Seguimento das actuacións do plan, así como, en servizos orientados á atención do cidadán en todo o referente aos proxectos de despregamento de rede de banda larga derivados do Plan de Banda Larga.

#### **17.4. AXENDA DIXITAL 2014.gal**

Galicia marcouse como obxectivo, dentro do actual marco establecido polo Plan Estratéxico Galicia 2010-2014, o reto de converxer co horizonte europeo para 2020.

Deste Plan xorde a Axenda Dixital de Galicia, como aposta pola definición dunha estratexia clara en materia de sociedade da información, que nos permita competir como rexión no novo mercado único dixital europeo definido pola Axenda Dixital para Europa e na nova economía do coñecemento, como camiño para unha recuperación económica sustentable.



Dentro do contexto da Axenda Dixital de Galicia, o último ano supuxo o arranque para iniciativas básicas na creación de infraestruturas, como o Plan de Banda Larga ou o Centro de Proceso de Datos Integral, e a aposta decidida pola Administración electrónica, impulsando o Decreto 198/2010, de 2 de decembro, polo que se regula o Desenvolvemento da Administración Electrónica na Xunta de Galicia y nas entidades dela dependentes, desenvolvendo proxectos para a mellora de servizos públicos dixitais e fomentando e divulgando o uso do TIC, como a rede CeMIT ou o proxecto Abalar.

A Axenda Dixital de Galicia enfróntase a un importante cambio de enfoque estratéxico: o seu obxectivo é pasar dunha sociedade que utiliza o TIC, a unha sociedade galega que se serve das novas tecnoloxías para xerar un crecemento sustentable, para mellorar as súas cotas de participación na toma de decisións e para contribuír á súa calidade de vida sobre a base do coñecemento. Para logralo, contará co impulso e a participación activa de todos os axentes implicados na sociedade da información.

Este enfoque marcouno a Comisión Europea, que deseñou unha estratexia para axudarnos a saír fortalecidos da crise e a converter a UE nunha economía que goce de altos niveis de emprego, de produtividade e de cohesión social. Este é o labor de "Europa 2020: Unha estratexia para un crecemento intelixente, sustentable e integrador" (Bruxelas, 3.3.2010 - COM(2010) 2020), que constitúe unha nova visión da economía social de mercado de Europa para o século XXI, propondo tres prioridades que se reforzan mutuamente:

- Crecemento intelixente: desenvolvemento dunha economía baseada no coñecemento e a innovación.
- Crecemento sustentable: promoción dunha economía que faga un uso máis eficaz dos recursos, que sexa máis verde e competitiva.

- Crecemento integrador: fomento dunha economía con alto nivel de emprego que teña cohesión social e territorial.

Neste contorno, Europa 2020 establece sete iniciativas para catalizar os avances en cada un dos temas fixados como prioritarios. Unha delas, consiste na definición da Axenda Dixital para Europa (Bruxelas, 19.05.2010 COM (2010) 245) que fai das tecnoloxías da información e da comunicación (TIC) a peza crave para que Europa consiga as súas ambicións para 2020.

Algúns dos eixos de actuación nos que se estrutura a Axenda Dixital para Europa co obxectivo de contribuír ao crecemento económico de Europa son os seguintes:

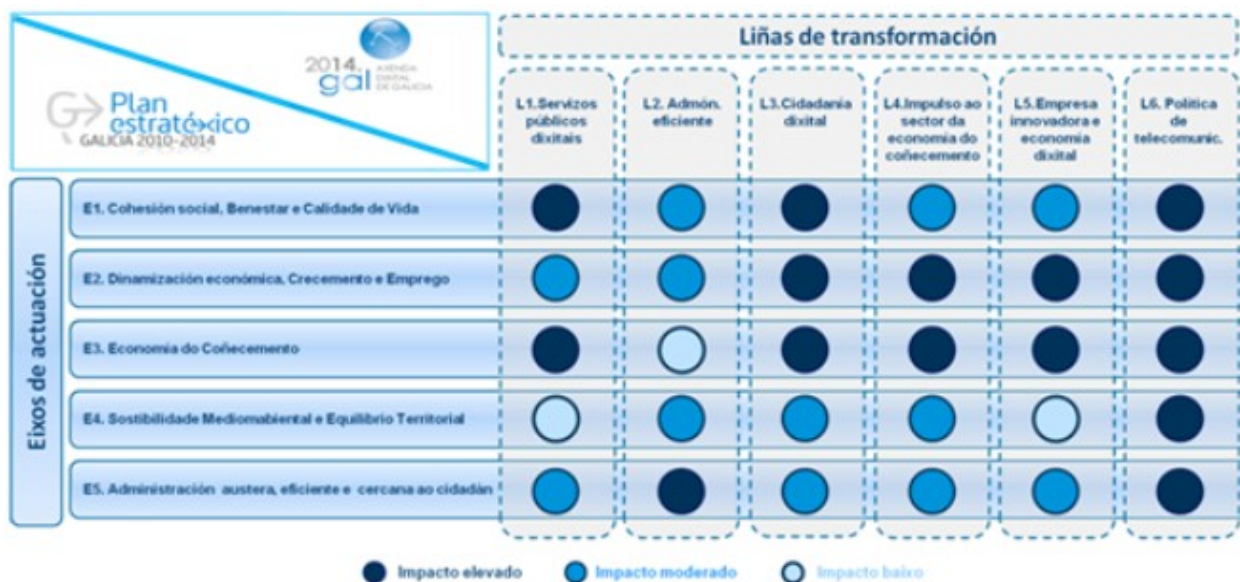
- Servizos Públicos Dixitais: é necesario o desenvolvemento de novos e mellores servizos públicos dixitais, que reactiven a demanda e fagan explícitas as vantaxes da economía dixital e o goberno aberto.
- Uso de internet, seguridade e confianza: Europa necesita unha Internet máis segura, na que os cidadáns sexan capaces de aproveitar todas as potencialidades a través dunha adecuada alfabetización dixital, especialmente dos colectivos máis desfavorecidos ou reticentes ao seu uso.
- Fortalecer a competitividade do sector TIC europeo: hai que reforzar a competitividade do sector TIC apostando pola investigación, o desenvolvemento e a innovación mediante programas mellor adaptados ás especiais características das empresas do sector, especialmente as PEME.
- Mercado Único Dixital: a UE debe crear un verdadeiro Mercado Único Dixital, soporte fundamental da economía do coñecemento en Europa, e promover de maneira activa os mercados europeos existentes de contidos dixitais, mediante solucións prácticas que impulsen novos modelos de negocio.
- Infraestruturas: a UE debe contar con infraestruturas sólidas, máis rápidas e eficientes, especialmente respecto da banda larga e as redes de futuro. É necesario adoptar medidas concretas para superar a fenda dixital alcanzando o

obxectivo do 100% de cobertura de banda larga básica para todos os cidadáns en 2013 e promover unha ampla penetración da banda larga de velocidade ultrarrápida en 2020.

As políticas deben estar plenamente aliñadas coa Axenda Dixital Europea para chegar en condicións excelentes ao novo período de financiamento a partir de 2014. A Axenda Dixital impulsará a inclusión de Galicia no novo contexto dixital europeo de forma definitiva no horizonte 2014. Galicia ten que ser un país que compita no novo mercado único dixital europeo: Galicia ten que pensar de forma global.

O Plan Estratéxico Galicia 2010-2014 define un novo modelo socioeconómico que pretende unha modernización para toda Galicia, que nos implique e inclúanos a todos. As novas tecnoloxías deben servir como catalizadoras dos eixos marcados no Plan Estratéxico, como mecanismo facilitador da cohesión social, da calidade de vida dos galegos, da xeración de emprego de calidade e como impulsor dunha Administración austera, eficiente e próxima ao cidadán. Este reto ten como resultado a Axenda Dixital de Galicia, que dá resposta á estratexia da Xunta de Galicia no emprego das novas tecnoloxías.

A continuación pode verse como se aliña a Axenda Dixital de Galicia co Plan Estratéxico Galicia 2010 -2014



Ademais do **Plan Estratéxico Galicia 2010-2014**, a nova Axenda tamén estará integrada con outros plans estratéxicos, como o Plan Galego de I+D+i, co Plan de Banda Larga de Galicia, con Plans de competitividade de diferentes sectores estratéxicos para Galicia (automoción, madeira, téxtil, construción naval, enerxía, pedra e turismo) e coas Axendas Dixitais Locais que promoven o desenvolvemento da sociedade da información nunha contorna máis próxima á cidadanía.



## ESTRATEGIA

Para alcanzar o salto cualitativo implícito no reto que se formula Galicia establécense sete liñas estratéxicas dentro da Axenda Dixital de Galicia:

### L1. SERVIZOS PÚBLICOS DIXITAIS.

Está a realizarse un gran esforzo para sentar as bases para un desenvolvemento xeneralizado da Administración dixital, que en boa lóxica, deberá traducirse nunha explosión de servizos dixitais durante estes próximos anos.

A innovación que impulsa esta axenda dixital debe proxectarse sobre o noso sistema de gobernanza. Está demostrado que un uso axeitado das TIC por parte das

Administracións ten a capacidade de transformar as relacións que se establecen entre os gobernos e a cidadanía contribuíndo esa transformación ao desenvolvemento da sociedade e a unha mellora da calidade de vida.

A inclusión das TIC, para que se realice de forma axeitada, leva consigo aparelado un cambio no modelo de Administración e na forma en que se prestan os servizos públicos.

Por todo iso dende a Xunta se puxo en marcha o plan e-Goberno 2013, iniciativa baixo a que se desenvolven todos os plans de modernización e mellora dos servizos públicos a través das TIC.

#### Obxectivos:

- Incluir as TIC en todos os ámbitos dos servizos públicos. Pasar do concepto de “Administración electrónica” ao concepto de “e-Goberno”.
- Adaptar o modelo de Administración para as novas posibilidades de xestión a través das TIC.
- Prestar os servizos públicos transmitindo seguridade e confianza, asumindo o reto da interoperabilidade.
- Facilitar a vida á cidadanía mediante a mellora dos servizos prestados en ámbitos como: sanidade, educación, xustiza, benestar, etc.
- Mellorar a competitividade do tecido produtivo galego.
- Garantir uns servizos públicos homoxéneos en todo o territorio mediante a colaboración entre as administracións públicas.

#### Enfoque e aspectos clave:

- Desenvolvemento completo da Administración electrónica, que implica cambios organizativos, normativos e tecnolóxicos.
- Colaboración entre todas as AAPP de Galicia. Afrontar o reto da interoperabilidade e garantir a homoxeneidade na prestación pública.

- Fomento da participación cidadá. Informar das políticas e colaborar coa cidadanía na súa execución, avaliación e deseño de futuras.
- Posta en marcha de servizos públicos dixitais.
- Desenvolvemento de plans de modernización sectorial.

## L2. ADMINISTRACIÓN EFICIENTE.

A Administración pública xoga un papel moi importante no desenvolvemento da sociedade da información en dúas áreas fundamentais:

- Como usuaria das TIC, co fin de mellorar a calidade dos servizos públicos, modernizar a Administración, profundar na transparencia da súa actuación, promover a participación cidadá e garantir os principios de eficiencia, eficacia, calidade e sustentabilidade.
- Como dinamizador da sociedade da información, por medio da formulación e execución de políticas que promovan a penetración do TIC na sociedade e o seu acceso a todos os axentes sociais.

Neste sentido, é obxectivo desta liña transformar a Administración pública autonómica desde dentro, como usuaria do TIC, realizando accións de homoxeneización en canto á estratexia tecnolóxica se refire e adoptando criterios de economía de escala que permitan a redución de custos e mellora dos servizos prestados.

Existen modelos para manter e mellorar o papel do TIC dentro da organización e, en xeral, a incorporación do TIC na actividade da Administración melloran a calidade de vida do cidadán, proporcionando ferramentas eficaces para a redución de tempos e custos.

Obxectivos:

- Proporcionar servizos de calidade e eficaces aos usuarios aliñados coas necesidades e directrices estratéxicas.
- Xestión eficiente do gasto: Facer máis e mellor con menos.
- Homoxeneizar e consolidar sistemas de xestión TIC, baixo unhas directrices operativas e estratéxicas unificadas de interoperabilidade.
- Transferencia e compartición do coñecemento TIC en Galicia.

#### Enfoque e aspectos clave:

- A xestión dos recursos TIC da Xunta (aplicacións, datos, tecnoloxía e infraestrutura) considérase ámbito de xestión interno e será transparente para os usuarios que consuman estes servizos.
- Política global de aforro de consumo de enerxía e residuos derivados dos servizos TIC, denominada sustentabilidade a través de políticas de Green IT.
- Xestión unificada dos activos TIC co obxectivo principal da consolidación dos servizos mediante a súa centralización nun único CPD e a estandarización da plataforma tecnolóxica.
- Racionalización dos sistemas de información.
- Actividades destinadas ao aseguramento e ao control da calidade dos sistemas.
- Estratexia TIC de consolidación de servizos; evolución de servizos cara a *Cloud Computing*. A Xunta actuará como provedor de servizos de *cloud computing* para o resto das unidades da Administración.

Débense tomar medidas de austeridade e racionalidade do gasto TIC a través de dúas grandes accións: a centralización da función de compras de activos e servizos TIC e a consolidación contratos en servizos agregados de maior volume.

A Xunta de Galicia lanzou unha iniciativa para a promoción, difusión e fomento da utilización de tecnoloxías baseadas en software libre e fontes abertas.

#### L3. CIDADANÍA DIXITAL.



Galicia quere ser un país cohesionado cuns cidadáns e cidadás que sexan competentes tanto para utilizar contidos e servizos dixitais avanzados como, especialmente, para colaborar activamente na súa creación e desenvolvemento e poñelos ao servizo do benestar individual e colectivo. Para iso é imprescindible que a súa cidadanía teña as competencias dixitais e a motivación necesarias para participar activamente no seu desenvolvemento.

As persoas necesitan aprender continuamente novas ideas e capacidades ou participar en actividades de formación permanente. Desta forma, esta capacidade de aprendizaxe poderá aplicarse a novas tarefas o que se traducirá en beneficios económicos e sociais.

Nesa tarefa o TIC abordan un papel dobre: por unha banda, ser un medio valioso para a aprendizaxe permanente ao longo da vida e, por outro, ser unha área en avance que esixe e facilita a mellora constante das competencias individuais.

### Obxectivos

- Cohesionar territorial e socialmente Galicia mediante a eliminación da fenda dixital e o impulso dos nativos dixitais.
- Incrementar a empregabilidade grazas ao desenvolvemento das capacidades tecnolóxicas que derivan do uso das TIC.
- Mellorar a calidade de vida dos cidadáns e garantir a súa autonomía persoal universalizando a cultura dixital na nosa comunidade.

### Enfoque e aspectos clave:

- No ámbito da cidadanía dixital é preciso evolucionar dende un enfoque tradicional “as TIC polas TIC: o obxectivo é introducir as TIC”, ao enfoque centrado no cidadán: “Quero estar máis capacitado para afrontar todos os retos da vida, e as TIC axúdanme a estalo”; e dun enfoque local: “illas de



alfabetización dixital” a un enfoque global e integrado: “a alfabetización dixital é cousa de todos”.

- Aposta por definir estratexias dixitais no sistema educativo orientadas a crear “nativos dixitais”

#### L4. IMPULSO AO SECTOR DA ECONOMÍA DO COÑECEMENTO

O Plan Estratéxico 2010-2014 e a nova Axenda Dixital de Galicia fan un recoñecemento da importancia do sector TIC para contribuír á dinamización e a aumentar a competitividade da economía rexional, calidades que o converten non só nun sector estratéxico, senón nun sector tractor do resto de sectores estratéxicos de Galicia.

##### Obxectivos:

- Consolidar un sector TIC competitivo, innovador e xerador de emprego cualificado, capaz de facer fronte aos retos da nova economía do coñecemento.
- Construír un sector TIC cohesionado e integrador, que actúe como motor do resto de sectores estratéxicos de Galicia.
- Converter o sector TIC nun sector forte en busca da excelencia tecnolóxica, que estimule a creación dunha clase emprendedora e creativa.

##### Enfoque e aspectos clave:

- Posicionamento do sector da economía do coñecemento existente en Galicia.
- Capacitación e especialización do capital humano, xunto con políticas de persoal capaces de atraer persoal cualificado ao sector e fomentar a retención de coñecemento nas empresas.
- Creación e consolidación de empresas de base tecnolóxica.
- Facer de Galicia unha fonte de coñecemento tecnolóxico “dende as universidades e para os sectores estratéxicos da rexión”.

- Especialización das empresas en segmentos altamente innovadores e co desenvolvemento dos mercados nos que actúan.
- Consolidar estruturas eficientes de apoio á innovación e refinar os servizos de financiamento existentes, orientando os sistema de axudas a mellorar a competitividade das empresas do sector da economía do coñecemento.
- Aliñamento da oferta do sector TIC coa demanda do tecido empresarial galego.

Deste xeito o sector TIC non só se converterá nun sector estratéxico en si mesmo, senón que tamén actuará como motor dos sectores estratéxicos de Galicia impulsando un novo modelo produtivo baseado na economía do coñecemento.

## L5. EMPRESA INNOVADORA E ECONOMÍA DIXITAL

As empresas galegas, independentemente do seu tamaño e sector, utilizarán intensiva e extensivamente as TIC para innovar tanto no desenvolvemento de produtos e servizos que satisfagan plenamente aos seus clientes, como na súa propia operativa e modelo de negocio, de maneira que poidan transformarse optimizando en cada momento as súas capacidades competitivas.

É preciso que as empresas galegas, especialmente PEME e microempresas, sexan capaces de utilizar as TIC para ser máis eficientes, aumentar a súa produtividade e innovar. Ademais, as TIC ofrecen unha gran oportunidade para que pequenas e medianas empresas poidan competir en mercados até agora inaccesibles.

Impulso do sector TIC: O sector TIC de Galicia debe ser un dos sectores estratéxicos da economía do futuro, e debe converterse en catalizador da competitividade do resto de sectores e da modernización da Administración. Este impulso pasa polo aliñamento dos esforzos de todos os axentes deste sector —universidades, centros tecnolóxicos, empresas, etc.— para crear un círculo virtuoso entre oferta e demanda TIC,

convertendo a este sector en tractor do resto de sectores estratéxicos grazas ao uso das TIC e tamén en beneficio da demanda tecnolóxica.

As TIC preséntanse como a grande oportunidade das empresas galegas, sen exclusión por tamaño ou sector, de optimizar a súa competitividade no mercado e de innovar tanto no desenvolvemento de novos produtos e servizos, como na súa propia operativa, acadando maiores competencias e contribuíndo ao crecemento económico sostible da sociedade galega.

#### Obxectivos:

- Contribuír á creación de emprego e ao crecemento económico sostible de Galicia creando un novo modelo produtivo.
- Facer máis competitivos os sectores estratéxicos de Galicia mediante a incorporación das TIC aos seus modelos de negocio (automoción, construción naval, enerxía, pedra e rocas ornamentais, téxtil, madeira, turismo).
- Facilitar a incorporación de microempresas e autónomos á sociedade do coñecemento, reducindo a fenda dixital para converxer con España e Europa.

#### Enfoque e aspectos clave:

Dende hai uns anos as empresas galegas están a facer fronte a unha importante transformación tanto interna como na súa contorna social e económica. Neste contexto tan cambiante o seu éxito depende da súa capacidade para ser competitivas nos mercados globais, e a incorporación das novas tecnoloxías ten moito que dicir neste sentido. Necesítase impulsar:

- A incorporación das TIC como unha vantaxe competitiva: “as TIC como investimento e non como gasto”.
- Enfoque centrado nas empresas, nos seus obxectivos e nas súas necesidades concretas.

- Enfoque global e coordinado, capaz de integrar a oferta en TIC coas necesidades das empresas dos diferentes sectores estratéxicos de Galicia.
- Ademais débese apostar por un enfoque segmentado das necesidades TIC das empresas galegas.
- O novo modelo de incorporación das TIC ás empresas dos sectores estratéxicos de Galicia debe entenderse coma un proceso constante

## L6. POLÍTICAS DE TELECOMUNICACIÓNS

As infraestruturas de telecomunicacións constitúen a canle de acceso de cidadáns e empresas aos servizos avanzados da sociedade da información, e é por iso que resulta necesario dispor dunha rede destas infraestruturas moderna e sustentable que garanta o acceso a novos servizos e que contribúa así ao desenvolvemento económico e ao progreso do noso país.

### Obxectivos:

- Garantir o acceso á sociedade da información a toda a sociedade galega.
- Mellorar os servizos ofrecidos á cidadanía a través da modernización dos servizos e infraestruturas de telecomunicacións corporativas soporte dos sistemas e procesos da Xunta.

### Enfoque e aspectos clave:

O primeiro obxectivo acádase a través de tres liñas de actuación:

- Execución das accións definidas no Plan Director de Banda Larga.
- Transformar o modelo de negocio de Retegal como operador de telecomunicacións neutro.
- Promover a localización en Galicia da Axencia Estatal de Radiocomunicacións e impulsar medidas que faciliten a implantación de operadoras con interese en investir no despregamento de infraestruturas en Galicia.

O segundo obxectivo desta liña, a mellora de servizos ofrecidos á cidadanía, instrumentábase fundamentalmente a través das seguintes liñas de actuación:

- Mellorar as infraestruturas das redes corporativas soporte dos sistemas e procesos da Xunta de Galicia.
- Evolucionar a Rede de Investigación de Galicia (RECETGA) dende un modelo de rede baseado en aluguer de circuítos a un novo modelo baseado na adquisición de fibra.
- Crear un Servizo de Comunicación de Emerxencias de Galicia.
- Impulsar o fogar dixital.

#### L7. MEDIDAS INSTRUMENTAIS DE SEGUIMIENTO E COOPERACIÓN.

Por ultimo, unha sétima liña, que lle dá soporte ao desenvolvemento das anteriores. Nesta liña, a Xunta de Galicia como elemento dinamizador do sector TIC rexional pretende establecer unha política de austeridade e simplificación de estruturas organizativas, de tal forma que se transforme nunha Administración áxil, de confianza e segura.

Neste sentido, tamén dentro desta liña, e para buscar o máximo aliñamento e coordinación, e polo tanto sinerxías e aforro de custes, adquire unha clara relevancia a necesidade do desenvolvemento das necesarias actuacións de coordinación e liderado integrador no marco das actuais vías de cooperación no eido tecnolóxico con concellos e deputacións, traballando así por consolidar unha Axenda Dixital Única para Galicia.

O modelo actual de prestación de servizos informáticos e de comunicacións na Xunta de Galicia signifícase por representar un estrito seguimento de mecanismos, procedementos e prazos moi dilatados, tanto para a adquisición de bens e servizos (Lei de contratos do sector público) como para a contratación de persoal (Convocatoria pública de emprego, procesos de consolidación de postos, etc.),

mecanismos que veñen establecidos pola necesaria aplicación en todos os seus termos e requisitos da normativa que afecta aos organismos públicos, sexa cal sexa a súa actividade.

Na presente lexislatura, a aparición da Secretaría Xeral de Modernización e Innovación Tecnolóxica (SXMIT) constituíu un punto de inflexión na orientación das políticas TIC da Xunta, no sentido de que supoñía a constatación de que estas determinan un instrumento de alto nivel estratéxico polo seu potencial para impulsar a modernización da Administración pública, así como a súa capacidade para impulsar e sustentar o desenvolvemento social e económico de Galicia

#### Obxectivos:

A SXMIT integrou unha grande cantidade de competencias co obxecto de que se facilite o desenvolvemento dunha estratexia tecnolóxica eficaz da Xunta e postúlase como o embrión dun novo modelo de xestión das políticas tecnolóxicas para a administración autonómica de tal maneira que se garanta:

- O aliñamento no desenvolvemento das TIC coas directrices políticas da Xunta;
- A racionalización de custos;
- A mellora da eficiencia e a eficacia da Administración territorial e das actuacións que se establezan;
- Que as TIC consigan transformar os servizos públicos de maneira que se convertan en elemento de dinamización económica e permitan aumentar a competitividade e a innovación en todos os sectores produtivos.

#### Enfoque e aspectos clave:

Nesta liña, tal e como se comentou, establécese a necesidade de constituír unha nova entidade de xestión das TIC de carácter público e adscrita a todos os niveis á Xunta de Galicia que aglutine as competencias que son responsabilidade da SXMIT e que

concentre os recursos humanos, materiais e orzamentarios asociados aos actuais departamentos TIC dispersos nas consellerías da Xunta de Galicia.

O Consello da Xunta de Galicia que tivo lugar o 21 de xullo de 2011 aprobou o plan de posta en marcha da Axencia de Modernización Tecnolóxica de Galicia (AMTEGA) co obxectivo de consolidar un modelo de xestión integrado das TIC na Administración autonómica.

A creación da Axencia permitirá unha maior eficiencia e unha redución de gasto ao integrar os servizos tecnolóxicos dos distintos departamentos da Xunta baixo unha mesma dirección. Un total de 558 profesionais da escala de tecnoloxías da información que desempeñan as súas funcións nos distintos departamentos da Xunta.

Este modelo permitirá xestionar as iniciativas e actuacións que sobre tecnoloxías da información se desenvolvan na Xunta de Galicia, así como proporcionar un novo modelo de xestión das TIC para a Administración Autonómica co obxecto de xestionar de xeito máis eficaz e eficiente os recursos globais, e orientarse cara a políticas de optimización e redución do gasto.

### **17.5. ESTRATEXIA DE IMPULSO DO SECTOR TIC**

O sector das tecnoloxías da información e da comunicación está a converterse nunha das áreas produtivas claves no desenvolvemento económico e social de Galicia, pola súa condición de acelerador do cambio tecnolóxico e polo seu carácter transversal ao resto de sectores. O número de empresas galegas do sector TIC no ano 2009 situábase en 1.542 empresas, o que supón un 9,8 % máis que en 2006.

O sector empresarial das TIC ocupa unha posición estratéxica pola súa capacidade de xeración de emprego. O nivel de emprego no sector TIC situouse no ano 2009 nos 16.327 traballadores/as, o que representa o 1,59% da poboación ocupada galega. A

evolución da ocupación neste sector mostra un continuo crecemento nos últimos anos.

O peso deste segmento empresarial tamén se reflicte claramente na súa contribución ao impulso e desenvolvemento da I+D. No ano 2008, o 45,6% das empresas galegas do sector dispoñían de persoal con dedicación relacionada coa I+D e un 37,1% realizou proxectos de I+D+i no último ano.

## LIÑA TRANSFORMA TIC

Neste contorno, 2014.gal Axenda Dixital de Galicia definiu unha liña de impulso ao sector da economía do coñecemento co obxectivo de convertelo nun sector que sexa capaz de dar soporte á competitividade de Galicia e que se consolide coma un sector de peso na economía galega.

2014.gal persegue a consecución duns obxectivos, a través desta liña:

- Consolidar un hipersector TIC competitivo, innovador e xerador de emprego cualificado, que se converta en sector estratéxico para a economía galega.
- Que ese sector sexa cohesionado e integrador. Que actúe tamén como motor do resto de sectores estratéxicos de Galicia.
- A creación dunha clase emprendedora e creativa estimulada por ese hipersector TIC.
- Busca da excelencia tecnolóxica.

As liñas da Axenda Dixital de Galicia, e principalmente as L4 e L5, explican máis en detalle os obxectivos, enfoque e aspectos clave deste plan de impulso do sector TIC.

## MAPA DE CAPACIDADES TECNOLÓXICAS DE GALICIA.



A Xunta de Galicia está a poñer en marcha, como unha das actuacións dentro da estratexia de impulso do sector TIC, un programa de demanda temperá de tecnoloxía innovadora.

Este programa promoverá a identificación de solucións tecnolóxicas innovadoras que acheguen vantaxes competitivas ás administracións públicas e, por tanto, permitan contar con cada vez mellores servizos públicos que dean soporte ás necesidades dos cidadáns e empresas de Galicia.

Ademais, a través deste sistema incentivaranse os procesos de innovación no sector TIC para o desenvolvemento de solucións diferenciais e con vantaxes competitivas que contribúan ao pulo do sector en Galicia e á exportación de novos servizos TIC a novos mercados fóra da mesma.

Como primeira actividade dentro deste programa, e dentro do ámbito sociosanitario, elaborouse o mapa de capacidades tecnolóxicas de Galicia.

Trátase dun documento vivo, que ten a intención de recoller o conxunto das capacidades e coñecementos tecnolóxicos dos diferentes axentes que desenvolven a súa actividade no ámbito sanitario e social de Galicia. Isto inclúe tanto entidades galegas que desenvolven proxectos neste ámbito en Galicia, no resto do territorio nacional e proxectos internacionais, como empresas de ámbito nacional e/ou internacional que desenvolven proxectos de temática sociosanitaria no ámbito xeográfico concreto de Galicia.

O mapa inclúe a experiencia e coñecementos tecnolóxicos, ademais de información detallada de numerosos proxectos, de todos os grupos de investigación TIC de Galicia que desenvolven o seu traballo no ámbito mencionado e de diferentes centros tecnolóxicos galegos ademais do sector empresarial.

Este instrumento serve como punto de partida para coñecer as capacidades tecnolóxicas galegas neste ámbito e para orientar mellor as actuacións que a partir de agora leven a cabo dentro deste programa para o impulso do sector tecnolóxico.

## LIÑA EconomiC-IT

Neste mundo globalizado, Galicia debe construír unha economía intelixente, sustentable e integradora, impulsando a competitividade e mellorando a produtividade do tecido empresarial, eliminando as debilidades estruturais existentes, incentivando a innovación e a calidade, apoiando a creación de novas empresas e xerando un alto nivel de emprego.

As TIC son a grande oportunidade das empresas galegas para facer fronte a eses retos, pois melloran a eficiencia das empresas e facilitan a innovación. Con todo, en Galicia o nivel de dotación e uso das TIC nas microempresas, que conforman a maior parte do tecido empresarial en Galicia, esta lonxe de converxer coa media europea. Existe una profunda fenda entre as PEME e as microempresas. Estas ultimas presentan un preocupante desinterese pola oferta tecnolóxica, seguramente producido polo descoñecemento.

Neste contorno, 2014.gal Axenda Dixital de Galicia definiu unha liña estratéxica “Empresa innovadora e Economía Dixital” co obxectivo de promover a sociedade da información no tecido empresarial galego.

Coa posta en marcha desta liña promoverase a utilización intensiva e extensiva das TIC para crear redes de colaboración que lles permitan competir con éxito en calquera sector ou mercado e para innovar tanto no desenvolvemento de produtos como na súa propia operativa e modelo de negocio.

Máis concretamente, os obxectivos estratéxicos que persegue a Axenda Dixital a través da definición desta liña son os seguintes:

- Contribuír a creación de emprego e ao crecemento económico sostible de Galicia creando un novo modelo produtivo.
- Facer máis competitivos os sectores estratéxicos de Galicia mediante as incorporacións das TIC aos seus modelos de negocio (automoción, construción naval, enerxía, téxtil)
- Facilitar a incorporación das microempresas e autónomos á sociedade da información, reducindo a fenda dixital para converxer con España e Europa.

O proceso de introdución das TIC nos sectores produtivos debe pasar primeiramente polo denominador Plan de demanda anticipada tecnolóxico-industrial. Este plan permite garantir a perfecta incorporación das novas tecnoloxías, xa que esta aliñada coas necesidades específicas de cada sector.

Ademais é necesario deseñar actuacións mais e mellor focalizadas apostando por unha segmentación das necesidades TIC nas empresas galegas.

A figura do titor tecnolóxico asociado á rede CeMIT xogará un papel moi importante, axudando a coñecer a situación das empresas identificando cales son as súas necesidades concretas.

## CENTRO DEMOSTRADOR TIC DE GALICIA

O Centro Demostrador TIC de Galicia é o instrumento operativo enmarcado no eixo de actuación economIC-T: “Empresas DIXITAL E INNOVADORA” da Axenda Dixital 2014.gal, e ponse en marcha en Galicia a través dun convenio entre a Secretaría Xeral de Modernización e Innovación Tecnolóxica, a Consellería de Traballo e Benestar e a entidade pública empresarial Red.es.

A misión do Centro é facilitarlles ás empresas TIC os medios para acercar a súa oferta de produtos ás empresas doutros sectores produtivos, de forma que poidan desenvolver produtos adaptados ás necesidades de mercado, con dous obxectivos: incrementar a demanda de produtos TIC e adaptar esta demanda ás necesidades de innovación dos sectores estratéxicos.

Pódese atopar abundante información sobre os contidos deste tema no enderezo <http://imit.xunta.es/>.

## **17.6. REFERENCIAS**

- Lei 11/2007, do 22 de xuño, de acceso electrónico dos cidadáns aos servizos públicos.
- Decreto 198/2010, do 2 de decembro, polo que se regula o desenvolvemento da Administración electrónica na Xunta de Galicia e nas entidades dela dependentes.
- iMIT – Iniciativas de Modernización e Innovación Tecnolóxica, da Xunta de Galicia (<http://www.imit.xunta.es/>).
- Área sobre a Axenda Dixital para Europa no sitio web da Comisión Europea ([http://ec.europa.eu/information\\_society/digital-agenda/index\\_en.htm](http://ec.europa.eu/information_society/digital-agenda/index_en.htm)).
- “Anotacións e comentarios ao decreto de Administración electrónica da Xunta de Galicia”, editado polo Colexio Profesional de Enxeñaría en Informática 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.

Autor: Jesús Rodríguez Castro

Xefe do Servizo de Informática do Concello de Santiago de Compostela

Colexiado do CPEIG



# **18. MODELO ENTIDADE- RELACIÓN. MODELO RELACIONAL. NORMALIZACIÓN.**

## **TEMA 18. MODELO ENTIDADE-RELACIÓN. MODELO RELACIONAL. NORMALIZACIÓN**

---

### **ÍNDICE**

#### **18.1.- Modelo de Datos**

#### **18.2.- Modelo Entidade - Relación (E-R)**

##### *18.2.1 Parte estática do modelo E/R*

###### 18.2.1.1 Entidade

###### 18.2.1.2 Relación ou interrelación

###### 18.2.1.3. Dominio

###### 18.2.1.4 Atributos

##### *18.2.2 Parte dinámica do modelo E/R*

###### 18.2.2.1 Tipo de correspondencia

###### 18.2.2.2 Entidades débiles

###### 18.2.2.3. Papel ou rol

###### 18.2.2.4 Atributos multivaluados e compostos

###### 18.2.2.5 Atributos derivados

#### **18.3.- Modelo Entidade Relación Estendido**

##### *18.3.1 Cardinalidade*

##### *18.3.2 Xerarquía subconxunto*

##### *18.3.3 Xeneralización*

##### *18.3.4 Tipos de relacións*

##### *18.3.5 Control de redundancias*

##### *18.3.6 Dimensión temporal*

#### **18.4.- Modelo Relacional**

##### *18.4.1 Elementos*

##### *18.4.2 Restricións*

#### **18.5.- Normalización de Relacións.**

#### **18.6.- Tradución de Esquemas E/R a Esquemas Relacionais.**

#### **18.7.- Bibliografía**



### **18.1.- MODELO DE DATOS**

Chámase datos o conxunto de propiedades que caracterizan un fenómeno, e información o conxunto de valores que poden tomar estas propiedades xunto coas relacións ou dependencias entre estas.

Os modelos de datos son ferramentas de abstracción que permiten representar a realidade captando as restricións semánticas que nela se poidan dar.

Cando no mundo real se dá información de calquera suceso ou obxecto sempre os datos subministrados van acompañados dunha semántica ou dun significado. Do mesmo xeito estes datos están suxeitos a unhas restricións e nós entendemos os datos subministrados só se entendemos o dominio e as restricións de significados que acompañan a información. Non obstante, cando aparecen os ordenadores e as bases de datos se empezan a informatizar, ocorre que se tende a almacenar datos separando a estes da súa interpretación, isto é, da súa semántica. Como consecuencia foi necesaria a aparición dos modelos de datos como unha ferramenta que axudase a incorporar significado aos datos almacenados.

Deste xeito, os modelos de datos proporcionan mecanismos de abstracción que permiten a representación da parte do mundo real que nos interesa rexistrar. Esta representación concíbese en dous niveis: o das estruturas que fan posible a representación da información, e o da información en si mesma.

Isto lévanos a diferenciar entre o que se denomina o esquema da base de datos (descrición específica en termos dun modelo de datos) e a colección de datos en si mesma que é o que denominamos base de datos.

O primeiro paso na representación dun problema do mundo real é a caracterización deste, ou o que é o mesmo, a determinación mediante un proceso de simplificación dos datos de interese (de entre todos os que interveñen no problema) e os seus límites (universo do discurso).

Os modelos de datos ofrecen distintos niveis de abstracción que facilitan a representación dos datos:

**Clasificación.** É a acción de crear unha categoría a partir das características comúns a un conxunto de exemplares. Por exemplo, a partir dos elementos Pedro, Xoán e Cristina podemos crear a categoría profesor de instituto.

O seu proceso inverso é a particularización.

**Agregación.** É a capacidade de considerar un obxecto sobre a base dos elementos que o constitúen. Por exemplo, podemos crear a clase coche a partir das clases volante, rodas, motor e carrozaría.

O seu proceso inverso é a desagregación.

**Xeneralización.** É similar á clasificación, pero creando unha categoría a partir das características comúns a un conxunto doutras categorías. Por exemplo, a partir das categorías profesor de matemáticas, profesor de física e profesor de informática, podemos crear a categoría profesor de instituto.

O seu proceso inverso é a especialización.

Segundo o nivel de abstracción que apliquemos, podemos falar de tres tipos de modelos de datos:

**Modelo conceptual.** Describe os tipos ou clases de obxectos dende un punto de vista estrutural. Para cada un destes tipos de obxectos describe as súas propiedades e o dominio e restricións de cada unha, así como as relacións entre eles. (Modelo entidade/relación).

**Modelo lóxico.** Representa o problema baixo as restricións específicas do tipo de Sistema Xestor de Base de Datos (SXBD) que se aplique en cada caso específico. (Modelo relacional para o caso dos SXBD relacionais).

**Modelo físico.** Representa o problema dende o punto de vista da súa implantación no sistema de tratamento utilizado e os métodos e mecanismos que se van usar no seu almacenamento.

Un modelo de datos define as regras mediante as cales se deben estruturar os datos do mundo real.

A representación dun mundo real mediante un determinado modelo dá lugar a un esquema, o cal describe as categorías existentes. Non obstante, a realidade contempla ademais dos aspectos estáticos, os aspectos dinámicos. Polo tanto as propiedades do mundo real son de dous tipos:

**Estáticas** relativamente invariantes no tempo, que é o que se adoita coñecer como estruturas. Este tipo de propiedades está compostas por:

Elementos permitidos como: os obxectos (entidades, relacións, rexistros...), asociacións entre obxectos, propiedades dos obxectos e asociacións (atributos, elementos de datos...), dominios (conxuntos de valores que poden tomar as propiedades).

Elementos non permitidos ou restricións, posto que non todos os valores, cambios de valor ou estruturas están permitidos no mundo real. Cada modelo ten por si mesmo limitacións en canto ás estruturas que permite:

As restricións impostas polo modelo coñécense como restricións inherentes

As restricións que permiten capturar a semántica do universo de discurso que se quere modelar e verificar a corrección dos datos almacenados na base de datos. Estas últimas restricións coñécense como restricións de integridade ou semánticas.

As restricións de integridade son impostas polo usuario, mentres que as restricións inherentes ao modelo son impostas directamente polo modelo.

**Dinámicas** Son as operacións que se aplican aos datos ou valores almacenados nas estruturas, os cales varían ao longo do tempo ao lles aplicar esas operacións. A aplicación de calquera operación sobre os valores dos elementos debe deixar estes cun estado válido, é dicir os valores dos elementos deben pertencer a algunha das categorías definidas no esquema e deben cumprir as restricións de integridade.

A compoñente estática dun modelo de datos defínese a través da linguaxe de definición de datos (DDL) e a compoñente dinámica defínese a través da linguaxe de

manipulación de datos (DML), constituíndo ambas as dúas compoñentes a linguaxe de datos. Tamén se pode mencionar a linguaxe de control de datos (DCL) que engade unha capa de seguridade.

### ***18.2.- MODELO ENTIDADE - RELACIÓN (E-R)***

Proposto por Peter Chen en dous artigos (1976 e 1977). É un modelo moi estendido que experimentou unha serie de ampliacións ao longo dos anos.

O modelo apóiase en dous conceptos, o concepto de entidade e o concepto de relación. Este modelo de datos permite representar case calquera restrición do deseño de datos.

O modelo E/R percibe o mundo real como unha serie de obxectos relacionados entre si e pretende representalos graficamente mediante un mecanismo de abstracción. Este mecanismo de abstracción está baseado nunha serie de símbolos, regras e métodos que permitirán representar os datos de interese do mundo real, ofrecendo ao deseñador unha ferramenta para illar o modelo de consideracións relativas á máquina e aos usuarios.

Tal e como vimos nos apartados anteriores distinguiremos entre a estática do modelo e a dinámica deste

#### ***18.2.1 Parte estática do modelo E/R***

Chen distingue no modelo E/R os seguintes elementos: entidade, relación, atributo e dominio

##### ***18.2.1.1 Entidade***

Unha entidade é un obxecto real ou abstracto de interese nunha organización e acerca do cal se pode e quere obter unha determinada información; persoas, cousas, lugares, etc., son exemplos de entidades

A estrutura xenérica que describe un conxunto de entidades aplicando a abstracción denomínase tipo de entidade, mentres que entidade se refire a cada unha das ocorrencias ou exemplares dese tipo de entidade. Así pois, asociado ao concepto de entidade xorde o concepto de ocorrencia de entidade. Unha ocorrencia de entidade é unha realización concreta dunha entidade. Deste xeito, "Hospital" é un tipo de entidade mentres que "CHOU" é unha ocorrencia ou exemplar.

Unha entidade debe cumprir as seguintes regras:

Debe ter existencia propia (veremos que hai un tipo de entidades que en puro rigor non cumpre esta restrición como son as entidades débiles)

Cada ocorrencia dun tipo de entidade ten que poder distinguirse dos demais

Todas as ocorrencias dun mesmo tipo de entidade deben ter as mesmas propiedades ou atributos

Unha entidade represéntase graficamente no modelo E/R mediante un rectángulo e no interior deste escríbese en maiúsculas o nome do tipo de entidade.

ENTIDADE

Existen dous tipos de entidades:

**Regulares:** os seus exemplares teñen existencia por si mesmos, p. ex. LIBRO.

**Débiles** nas que a existencia dun exemplar depende de que exista certo exemplar doutro tipo de entidade. Veranse no apartado 2.2.2

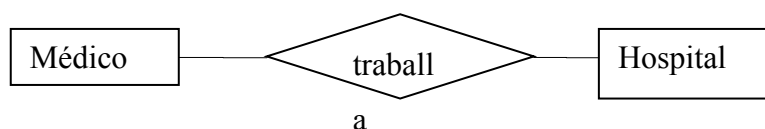
#### 18.2.1.2 Relación ou interrelación

Unha interrelación é unha asociación entre entidades e caracterízase por unhas determinadas restricións que determinarán as entidades que poden ou non participar desa relación.

A interrelación represéntase graficamente por un rombo etiquetado co nome da interrelación en maiúsculas unido mediante arcos ás relacións que vincula.

Asociado ao concepto de interrelación xorde o concepto de ocorrencia de interrelación.

Unha ocorrencia de interrelación é a asociación concreta de ocorrencias de entidade de diferentes entidades. Por exemplo, se temos as entidades MEDICO e HOSPITAL, e a interrelación "traballa en", unha ocorrencia de interrelación será: MARTA GARCÍA traballa no CHOU.



Unha interrelación queda caracterizada por tres propiedades:

Nome: as interrelacións deben ter un nome que as identifique univocamente.

Grao: número de tipos de entidade sobre as que se realiza a asociación. A interrelación do exemplo anterior será binaria, é dicir, o seu grao sería dous.

Tipo de correspondencia: Número máximo de ocorrencias de cada tipo de entidade que poden intervir nunha ocorrencia do tipo de interrelación.

As relacións poden ter atributos propios.

#### 18.2.1.3. Dominio

Representa o conxunto de valores posibles dunha determinada propiedade ou atributo dun tipo de entidade ou dun tipo de interrelación. En termos de abstracción, é unha especialización dun conxunto. Co que se pode dicir que o dominio é un conxunto de valores homoxéneos cun nome.

Represéntase por un círculo pequeno acompañado do seu nome en minúsculas.

É importante resaltar neste punto que os dominios teñen existencia propia e é o que realmente captura unha semántica do mundo real. O que aconteceu moi a miúdo é que se tende a confundir dominio con atributo.

#### 18.2.1.4 Atributos

É cada unha das posibles propiedades ou características dun tipo de entidade ou tipo de interrelación. Os atributos toman valor nun dominio polo que un atributo é unha determinada interpretación dun dominio e varios atributos poden tomar valores no mesmo dominio. Por exemplo, se temos o atributo COR o dominio sobre o que se define podería ser: (LARANXA, BRANCO, AZUL e NEGRO).

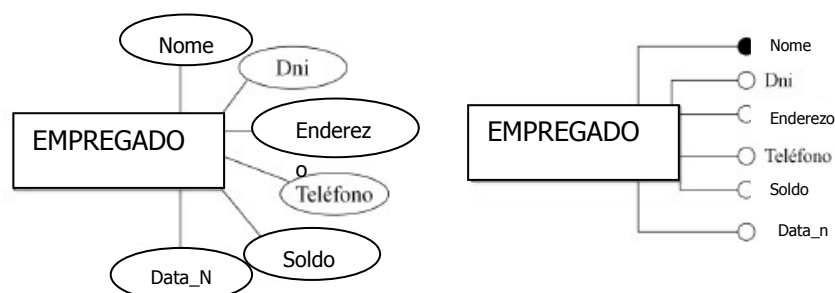
Pódese representar graficamente de 2 formas:

Por un círculo pequeno unido por un arco ao tipo de entidade e acompañado do nome do atributo.

Encerrando nun ovalo o nome do atributo unido por un arco ao tipo de entidade.

En función das características do atributo respecto da entidade distínguense dous tipos de atributos:

**Atributo identificador clave:** distingue de xeito único unha ocorrencia de entidade do resto de ocorrencias de entidade. Normalmente, o atributo identificador é único, pero pode haber casos nos que haxa varios atributos identificadores, polo que denominaremos a cada un deles **atributo identificador candidato**. Elixiremos un como identificador clave e o resto serán atributos identificadores. Representase graficamente:



**Atributo descriptor:** caracteriza unha ocorrencia de entidade pero non a distingue do resto de ocorrencias de entidade.

Unha relación pode ter atributos ao igual que as entidades.

### ***18.2.2 Parte dinámica do modelo E/R***

Diciamos que o interese dos modelos de datos é captar tanta semántica como sexa posible do mundo real. Co que vimos ata o momento comprobamos que se permite establecer calquera número de relacións diferentes entre tipos de entidade pero non podemos establecer restricións do tipo:

Un médico só traballa nun hospital

Nun hospital traballan n médicos

Todos os socios do videoclub alugaron polo menos unha película

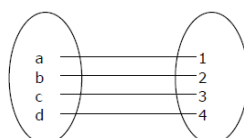
A continuación analízanse polo miúdo todos os aspectos das relacións que nos permitirán captar toda a semántica desexada.

#### **18.2.2.1 Tipo de correspondencia**

Denomínase tipo de correspondencia ao tipo de asociación que se establece entre as entidades relacionadas. Concretamente, pódese definir o tipo de correspondencia como o número máximo de ocorrencias dunha entidade asociada a unha ocorrencia doutra ou da mesma entidade a través dunha relación.

Para unha relación binaria, é dicir, de grao dous, entre as entidades A e B, existen tres tipos posibles de correspondencias:

**Correspondencia 1:1** Unha ocorrencia da entidade A asóciase como máximo cunha ocorrencia da entidade B e viceversa, como se pode observar na figura

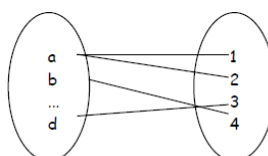




Entidad	Entidad
e A	e B

Un exemplo deste tipo de correspondencia pode ser que un cliente ten unha única conta bancaria nunha sucursal determinada e unha conta determinada dunha sucursal pertence a un único cliente.

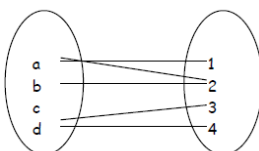
**Correspondencia 1:N** Unha ocorrencia da entidade A asóciase cun número indeterminado de ocorrencias da entidade B, pero unha ocorrencia da entidade B asóciase como máximo cunha ocorrencia da entidade A. Se fose ao revés a correspondencia sería N:1.



Entidad	Entidad
e A	e B

Un exemplo deste tipo de correspondencia pode ser que unha persoa vive nunha cidade e nunha cidade viven moitas persoas.

**Correspondencia N:M** Unha ocorrencia da entidade A asóciase cun número indeterminado de ocorrencias da entidade B e viceversa.



Entidad	Entidad
e A	e B

Un exemplo deste tipo de cardinalidade pode ser que un proveedor subministra varios produtos e cada produto pode ser subministrado por varios provedores.

#### 18.2.2.2 Entidades débiles

O concepto de entidade débil está directamente relacionado coas restricións de tipo semántico do modelo E/R e, máis concretamente, coa denominada restrición de existencia.

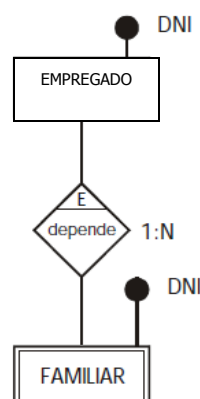
Esta restrición establece o feito de que a existencia dunha entidade non ten sentido sen a existencia doutra, é dicir, unha entidade ten dependencia de existencia doutra cando sen a primeira a segunda carecería de sentido.

Isto leva consigo que a desaparición das ocorrencias da entidade da cal depende a súa existencia leve á desaparición das ocorrencias da entidade débil que dependan delas. Por exemplo, un exemplar da entidade EDICIÓN non existiría se non houbo un exemplar correspondente na entidade LIBRO. As entidades débiles represéntanse graficamente por dous rectángulos concéntricos e no interior o nome da entidade.

ENTIDADE DÉBIL

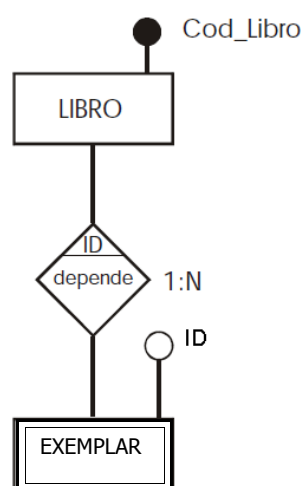
Hai dous tipos de dependencias das entidades débiles respecto ás entidades regulares:

*Dependencia en existencia* os exemplares da entidade débil non poden existir se desaparece o exemplar da entidade regular co que están relacionados, pero a entidade débil pode ser identificada sen necesidade de identificar a entidade forte relacionada, é dicir, a entidade débil ten un atributo identificador clave.



No exemplo é evidente que se desaparece un empregado da base de datos a existencia dos seus familiares carece de sentido, é dicir, a entidade FAMILIAR ten dependencia de existencia respecto da entidade EMPREGADO. Non obstante, cada unha das ocorrencias da entidade familiar pode identificarse por si mesma.

*Por identificación* a entidade débil non ten sentido en si mesma e non pode ser identificada sen a entidade forte relacionada, é dicir non ten un atributo identificador clave senón tan só un descritor discriminador e necesita o atributo clave da entidade forte para poder identificar de xeito único as súas ocorrencias de entidade.



No exemplo, o atributo identificador crave será Cod\_Libro (como clave da entidade forte LIBRO) máis ID como discriminador da entidade EXEMPLAR.

Como conclusión ao concepto de entidade débil convén resaltar as circunstancias seguintes:

A dependencia en existencia non implica unha dependencia en identificación, feito que se sucede no caso inverso pois unha entidade que depende doutra polo seu atributo clave non terá sentido sen a existencia desta última.

Nunha interrelación con cardinalidade N:M nunca haberá entidades débiles. A razón é que a suposta ocorrencia da entidade débil que se tivese que borrar podería estar

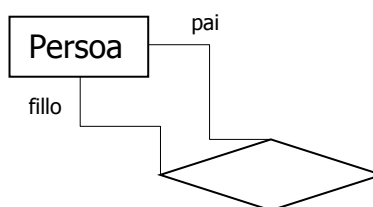
asociada a máis dunha ocorrencia da suposta entidade forte, o que implicaría a imposibilidade do seu borrado, feito este en clara contraposición coa definición de entidade débil.

### 18.2.2.3. Papel ou rol

É a función que cada unha das entidades realiza nunha interrelación concreta. Graficamente represéntase indicando o nome do rol na liña que une as entidades coas relacións.

Os roles xogan un papel especialmente importante en relacións reflexivas onde é necesario coñecer os dous roles que o mesmo tipo de entidade xoga nunha determinada relación.

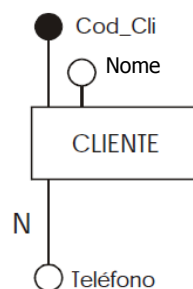
A razón está en que estamos a asociar entre si ocorrencias dunha mesma entidade de forma que cada unha delas ten un significado diferente. No exemplo, unha ocorrencia de PERSOAS fará papel de 'pai' e a outra papel de 'fillo'.



### 18.2.2.4 Atributos multivaluados e compostos

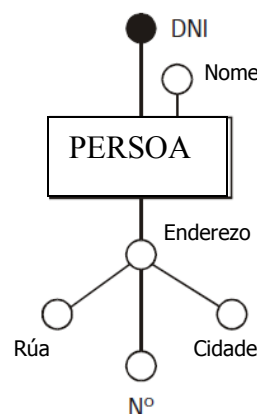
Un último tipo de restricións que se deben ter en conta á hora de realizar o deseño conceptual dunha base de datos co modelo E/R son as que afectan á tipoloxía dos diferentes atributos. Dende este punto de vista podemos definir dous tipos diferentes de atributos respecto aos manexados ata o momento, que son os seguintes:

**Atributos multivaluados.** Son aqueles atributos que para unha mesma ocorrencia da entidade toman máis dun valor. Por exemplo se cada cliente pode ter máis dun teléfono e é de interese gardar todos os seus posibles valores, o atributo teléfono sería multivaluado. Representátese etiquetando o seu arco cun valor de cardinalidade N.



**Atributos Compostos.** Son aqueles que agrupan en si mesmos, por afinidade ou por forma de uso, máis dun atributo. Por exemplo o atributo "endereço" engloba os atributos rúa, número, cidade, provincia e código postal.

Representátese especificando os seus atributos compoñentes rodeando a este e enlazándoos ao símbolo do atributo composto mediante arcos.



#### 18.2.2.5 Atributos derivados

Son aqueles que se poden calcular a partir doutros. Por exemplo, se temos a entidade PERSOA cos atributos DNI, nome, data\_nacemento e idade, o último atributo (idade) pode obterse a partir doutro atributo (a data de nacemento) e é, polo tanto, redundante. Este tipo de atributos deben eliminarse do esquema.

### **18.3.- MODELO ENTIDADE RELACIÓN ESTENDIDO**

O modelo E/R co paso do tempo sufriu unha serie de modificacións tanto no seu simbolismo gráfico, coma na ampliación dos seus elementos.

#### **18.3.1 Cardinalidade**

Este primeiro concepto en certo modo estaba tratado de forma implícita no modelo E/R orixinal. Non obstante, foi posteriormente cando se lle deu certa relevancia e mesmo unha forma de representación.

O concepto cardinalidade, tamén denominado "clase de pertenza", permite especificar se todas as ocorrencias dunha entidade participan ou non na interrelación establecida con outra(s) entidade(s):

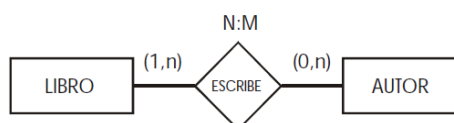
Se toda ocorrencia da entidade A debe estar asociada con polo menos unha ocorrencia da entidade B á que está asociada por unha determinada interrelación, dise que a clase de pertenza é obrigatoria, é dicir, a cardinalidade mínima é 1.

Pola contra, se non toda ocorrencia da entidade A necesita estar asociada con algunha ocorrencia da entidade B asociada, dise que a clase de pertenza é opcional, é dicir, a cardinalidade mínima é 0.

Podemos definir a **cardinalidade dun tipo de entidade** como o número mínimo e máximo de ocorrencias dun tipo de entidade que poden estar relacionadas cunha ocorrencia do outro tipo de entidade que participan no tipo de interrelación.

A súa representación gráfica é unha etiqueta do tipo (0,1), (1,1), (0,n) ou (1,n) segundo corresponda, ao lado das entidades asociadas pola relación tal como se pode observar no seguinte exemplo, onde o primeiro elemento da tupla é a cardinalidade mínima, e o segundo elemento da tupla é a cardinalidade máxima, que coincide co tipo de correspondencia

Exemplo: 'Un libro pode estar escrito por ningún, un ou varios autores. Un autor escribe polo menos un libro e pode escribir varios. '



### **18.3.2 Xerarquía subconxunto**

A descomposición de tipos de entidade en varios subtipos é unha necesidade moi habitual no modelado conceptual. No mundo real pódense identificar varias xerarquías de entidades. A interrelación que se establece entre un supertipo e os seus subtipos corresponde á noción de "É-UN" (IS-A) ou máis exactamente "é un tipo de".

Para a súa representación utilízase un triángulo invertido, coa base paralela ao rectángulo que representa o supertipo.

O concepto xerarquía subconxunto establece que unha entidade A é un subconxunto doutra entidade B cando toda ocorrencia da primeira tamén é unha ocorrencia da segunda, e o contrario non ten por que ser certo.

Polo tanto, teremos unha xerarquía subconxunto cando cada ocorrencia dunha entidade xenérica poida ser tamén unha ocorrencia doutras entidades que, potencialmente, son subconxuntos non disxuntos (solapados). É dicir, nas entidades subconxunto poden aparecer ocorrencias repetidas.

#### Características:

Toda ocorrencia dun subtipo é unha ocorrencia do supertipo, as cardinalidades serán sempre (1,1) no supertipo e (0,1) ou (1,1) nos subtipos.

Todo atributo do supertipo pasa a ser un atributo dos subtipos.

A entidade subconxunto pode ter atributos, ademais de ter os atributos da entidade xenérica, pero sempre as entidades subconxunto se encontran identificadas pola clave da entidade xenérica. Ademais todos os atributos comúns das entidades subconxunto deberían aparecer na entidade xenérica para evitar repetir os atributos en cada unha das entidades subconxunto.

### **18.3.3 Xeneralización**

O concepto de xerarquía de xeneralización ou xeneralización establece que unha entidade xenérica X é unha xeneralización doutras entidades especializadas se cada

ocorrência da primeira é unha ocorrência e soamente unha das outras entidades. Ás veces este concepto coñécese tamén como xerarquía de especialización.

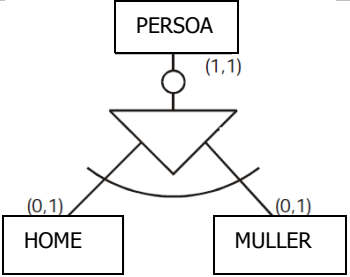
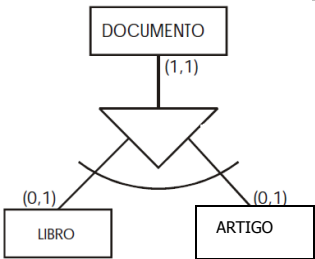
Terase unha xerarquía de xeneralización cando a entidade xenérica se divida nunha serie de entidades en función do valor que tome un determinado atributo da entidade xenérica.

A xeneralización ten dúas restricións semánticas asociadas:

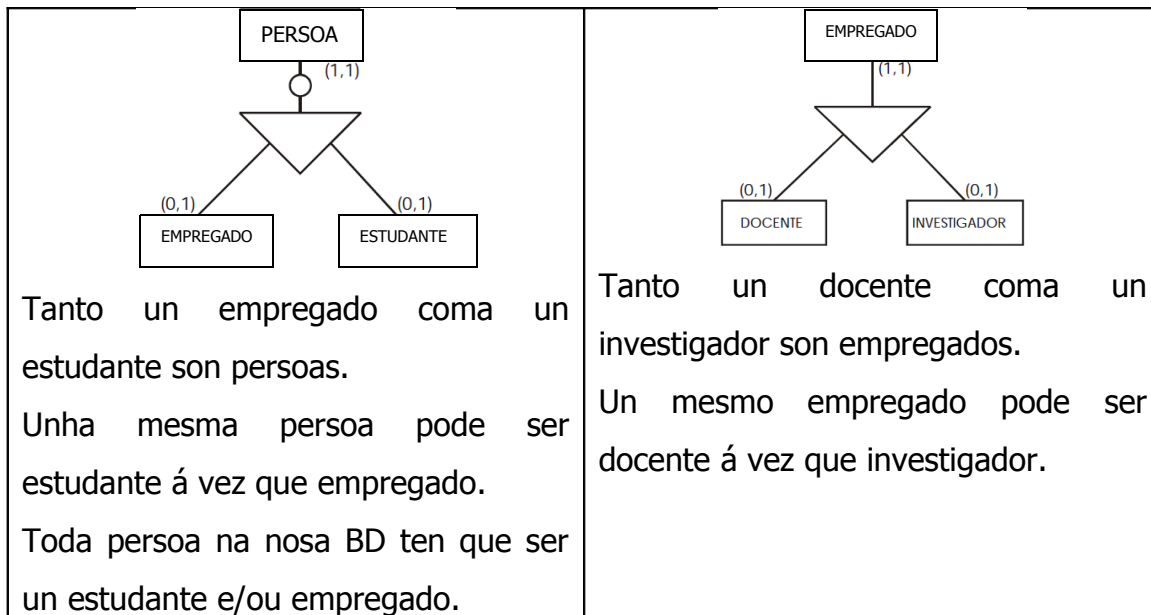
**Totalidade** se todo exemplar do supertipo ten que pertencer a algún subtipo. O caso contrario chámase **Parcialidade**.

**Solapamento** se un mesmo exemplar do supertipo pode pertencer a máis dun subtipo. O caso contrario chámase **Exclusividade**.

Poden existir interrelacións de cada unha das catro combinacións posibles, e representaríanse da seguinte forma:

TOTAL SEN SOLAPAMENTO	PARCIAL SEN SOLAPAMENTO
 <p>Tanto un home coma unha muller son persoa.</p> <p>Unha persoa non pode ser á vez home e muller.</p> <p>Toda persoa ten que ser un home ou unha muller.</p>	 <p>Tanto un artigo coma un libro son documentos.</p> <p>Un mesmo documento non pode ser á vez un artigo e un libro.</p> <p>Pode haber documentos que non sexan nin artigos nin libros.</p>
TOTAL CON SOLAPAMENTO	PARCIAL CON SOLAPAMENTO

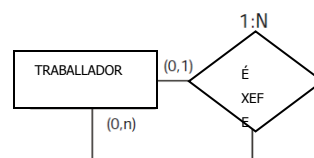




#### **18.3.4 Tipos de relacións**

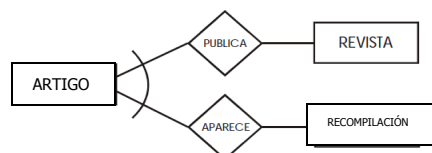
A. RELACIÓNS REFLEXIVAS Son interrelacións nas que intervén un único tipo de entidade (unarias).

Exemplo: Un traballador pode ser xefe de ningún traballador ou pode selo de varios traballadores, mentres que un traballador só é dirixido por ningún ou un traballador



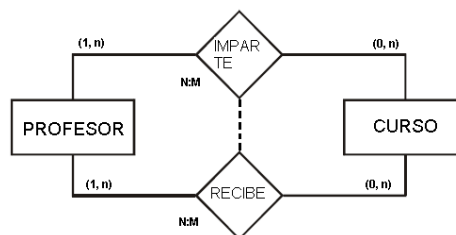
**B. INTERRELACIÓNS CON RESTRICIÓNS DE EXCLUSIVIDADE.** Dúas interrelacións que implican un mesmo tipo de entidade participan dunha restrición de exclusividade se os exemplares desa entidade poden participar dunha ou outra interrelación, pero non de ambas as dúas.

Recolleuse no esquema que nunha determinada biblioteca os artigos están publicados en revistas ou aparecen en recompilacións, pero non en ambos as dúas



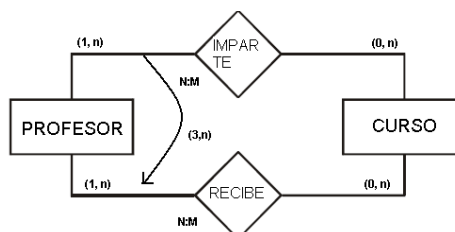
**C. INTERRELACIÓNS CON RESTRICIÓNS DE EXCLUSIÓN.** Dúas interrelacións entre os mesmos dous tipos de entidade son exclusivas se un exemplar do primeiro tipo de entidade e outro exemplar do segundo tipo de entidade só poden estar relacionados por unha das dúas interrelacións, nunca por ambas as dúas simultaneamente.

Un profesor non pode recibir e impartir o mesmo curso, aínda que ao contrario que na restrición anterior pode impartilo ou recibilo.



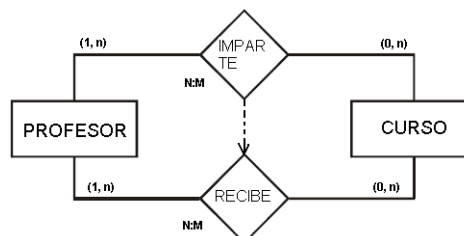
**D. INTERRELACIÓNS CON RESTRICIÓNS DE INCLUSIVIDADE.** Son dúas interrelacións que implican un mesmo tipo de entidade, nas que os exemplares da entidade tiveron que participar dunha interrelación cunha cardinalidade determinada para poder participar da outra.

Para que un profesor poida impartir un curso, tivo que recibir o curso un mínimo de 3 veces.



**E. INTERRELACIÓNS CON RESTRICIÓNS DE INCLUSIÓN.** Son aquelas que se establecen entre os mesmos dous tipos de entidade e que restrinxen unha interrelación entre dous exemplares de cada unha das entidades á vinculación deses dous mesmos exemplares a través da outra interrelación.

Todo exemplar de profesor que estea unido a un exemplar de curso mediante a interrelación imparte ten necesariamente que estar unido ao mesmo exemplar de curso mediante a interrelación recibe.



**F. AGREGACIÓN.** É un tipo especial de interrelación que permite representar tipos de entidade compostos que se forman a partir doutros máis simples. Existen dúas clases de agregacións

Composto/Compoñente O supertipo de entidade obtense pola unión dos subtipos. Representase da seguinte forma	
Membro/Colección: O supertipo de entidade é unha colección de elementos dun mesmo subtipo. Representase como:	

### 18.3.5 Control de redundancias

No modelo E/R é necesario evitar as redundancias para non ter problemas de inconsistencias da representación. Un elemento dun esquema é redundante se pode ser eliminado sen perda de semántica.

Existen dúas formas principais de redundancia:

- Nos atributos (atributos derivados ou calculados): Aínda que son redundantes, non dan lugar a inconsistencias sempre que no esquema se indique a súa condición de derivados e a fórmula mediante a que se deben calcular.
- Nas interrelacións (tamén chamadas interrelacións derivadas): Unha interrelación é redundante se a súa eliminación non implica perda de semántica porque existe a posibilidade de realizar a mesma asociación de exemplares por medio doutras interrelacións. Para iso é condición necesaria pero non suficiente que forme parte dun ciclo.

A existencia dun ciclo non implica a existencia de interrelacións redundantes.

Para que unha interrelación poida ser eliminada por redundante tense que cumprir:

- Que exista un ciclo.
- Que as interrelacións que compoñen o ciclo sexan equivalentes semanticamente,
- Que despois de eliminar a interrelación se poidan seguir asociando os exemplares das dúas entidades que estaban interrelacionadas
- Que a interrelación non teña atributos ou que estes poidan ser transferidos a outro elemento do esquema co fin de non perder a súa semántica.

#### ***18.3.6 Dimensión temporal***

É necesario establecer un método semántico e gráfico que recolla dalgún modo, no esquema conceptual, o transcurso do tempo e a súa influencia na forma en que cambian os datos. Existen varias aproximacións:

- A máis simple constitúena os atributos de tipo data asociados a algunhas entidades ou interrelacións:
  - Para sucesos instantáneos, é dicir, sen duración, abondará cun só atributo deste tipo.

- Para poder almacenar feitos que transcorren nun intervalo de tempo determinado necesitaremos unha data\_inicio e unha data\_fin.
- Nas bases de datos históricas, nas que unha interrelación entre dous exemplares concretos se poida repetir no tempo, o atributo data será multivaluado.
- Cando é necesario representar a evolución dun tipo de entidade ao longo do tempo utilízase un atributo de estado, que indicará en que estado concreto se encontra a entidade.

En moitos casos leva asociado outro atributo, que é a data na que se produciu o cambio de estado ou o intervalo de tempo en que permaneceu no devandito estado.

#### **18.4.- MODELO RELACIONAL**

É un modelo lóxico de datos, desenvolvido por Codd, que introduciu a teoría matemática das relacións no campo das BD e supuxo un importante paso na investigación dos SXBD. O documento de Codd propón un modelo de datos baseado na "Teoría das relacións", onde os datos se estruturan lóxicamente en forma de relacións —táboas—, sendo un obxectivo fundamental do modelo manter a independencia desta estrutura lóxica respecto ao modo de almacenamento e a outras características de tipo físico (independencia de ordenación, indexación e dos camiños de acceso).

Este novo modelo de datos perseguía os seguintes obxectivos:

- Independencia lóxica: engadir, eliminar ou modificar calquera elemento da BD non debe repercutir nos programas e/ou usuarios que accedan a vistas destes.
- Independencia física: o modo no que se almacenan os datos non debe influír na súa manipulación lóxica e, polo tanto, os usuarios que acceden a eses datos non deben modificar os seus programas por cambios no almacenamento físico.

- **Flexibilidade:** poder ofrecer a cada usuario os datos da forma máis axeitada á súa aplicación.
- **Uniformidade:** As estruturas lóxicas dos datos presentan un aspecto uniforme (táboas), o que facilita a concepción e manipulación da BD por parte dos usuarios.
- **Sinxeleza:** As características anteriores, así como unhas linguaxes de usuario moi sinxelas, producen como resultado que o modelo de datos relacional sexa doado de comprender e utilizar por parte do usuario final.

### **18.4.1 Elementos**

O modelo relacional introduce a súa propia terminoloxía para denominar os obxectos e elementos utilizados:

- 1. Relación.** É o elemento central do modelo relacional. Son matrices bidimensionais (táboas) caracterizadas por un nome, un conxunto de atributos (dimensión vertical da táboa = columnas) e un conxunto de tuplas (dimensión horizontal = filas).

Cada tupla está formada polo conxunto de valores que toma cada un dos atributos para un elemento da relación.

Nas relacións podemos falar de dous compoñentes:

- **Intensión** é a parte definitoria e estática da relación. Define a estrutura abstracta de datos e as restricións de integridade desta. É o que chamaremos *esquema de relación*.
- **Extensión** é o conxunto de tuplas que satisfai o esquema de relación nun instante dado e está almacenado na base de datos. Varía co transcurso do tempo.

O número de tuplas dunha relación nun instante dado denomínase **cardinalidade** da relación, e normalmente varía co transcurso do tempo. O número de columnas ou atributos denomínase **grao** da relación.

- 2. Dominio.** É o conxunto definido, finito e homoxéneo dos valores atómicos posibles dun determinado atributo.

Cada atributo está ligado a un determinado dominio e representa o uso dun dominio para unha determinada relación.

Os dominios poden estar definidos por intensión (conxunto definido mediante unha serie de regras abstractas) ou por extensión (conxunto finito de valores posibles).

**3. Claves dunha relación.** Unha clave é unha(s) columna(s) na que os valores identifican unha única fila dunha táboa. Hai varias clases de claves

- *Clave candidata.* Cada un dos conxuntos mínimos de atributos que identifiquen sen ambigüidade e de forma única cada unha das tuplas dunha relación.
- *Clave primaria ou principal.* De entre todas as claves candidatas dunha relación, na definición do esquema deberase especificar cal delas se considera como identificador primario. O resto das claves candidatas denominaranse *claves alternativas*.
- *Claves foráneas* ou *claves alleas* son o conxunto de atributos dunha relación que se corresponden coa clave primaria doutra relación do modelo. Proporcionanlle ao modelo relacional os mecanismos axeitados para representar as (inter)relacións existentes entre os obxectos do problema.
  - Pode referenciar a clave primaria da mesma táboa (relacións reflexivas)
  - Debe ter sempre un valor correspondente na táboa onde é clave primaria
  - Debe estar formada por toda a clave primaria e non só unha parte dela
  - Pode ter nulos
  - Pode ter valores duplicados
  - Unha táboa pode conter múltiples claves foráneas, onde cada unha representa a relación con outra táboa

### **18.4.2 Restricións**

No modelo relacional existen restricións, é dicir, estruturas ou ocorrencias non permitidas, sendo preciso distinguir entre restricións inherentes (propias do modelo) e restricións semánticas (de usuario).

#### Restricións inherentes

1. Non se define ningunha orde nos elementos que forman unha relación, nin no sentido horizontal (tuplas) nin no vertical (atributos). A orde é sempre irrelevante.
2. En toda relación é obrigatoria a existencia da clave primaria, e polo tanto non pode haber dúas tuplas iguais.
3. Cada atributo dunha tupla só pode tomar un único valor do dominio sobre o cal está definido.
4. Regra de integridade de clave ou entidade: ningún dos atributos que forman parte dunha clave primaria dunha relación pode tomar un valor nulo para ningunha tupla desa relación.

#### Restricións semánticas

1. Declaración de clave primaria (PRIMARY KEY): Permite declarar un atributo ou un conxunto de atributos como clave primaria dunha relación, polo que os seus valores non se poderán repetir nin admitirán nulos.
2. Unicidade (UNIQUE): indica que os valores dun atributo (ou conxunto) non poden repetirse nunha relación. Esta restrición permite definir claves candidatas.
3. Obrigatoriedade (NOT NULL), indica que un atributo (ou conxunto) non admite nulos
4. Integridade referencial (restrición de clave allea): permiten que as claves foráneas dunha relación referencien unha tupla válida da relación pai. O usuario pode especificar, na definición do esquema relacional, as operacións que deben levarse a cabo cando se produce o borrado ou modificación dunha tupla na relación pai. As posibilidades son:



- Borrado/modificación en ferverza (CASCADE). O borrado ou modificación dunha tupla na relación pai provoca o borrado ou modificación de todas as tuplas relacionadas na relación filla.
  - Borrado / modificación restrinxido (NON ACTION). Se existen tuplas relacionadas na relación filla, non se permite o borrado ou modificación das tuplas da relación pai.
  - Borrado / modificación con posta a nulos (SET NULL). Pon a nulo os valores de todos os atributos que conforman a clave allea na relación filla. Só está permitido cando eses valores se poidan poñer a nulo.
  - Borrado / modificación con posta a un valor por defecto (SET DEFAULT). Similar ao anterior, pero os atributos que conforman a clave allea na relación filla póñense a un valor especificado previamente na definición do esquema.
5. Restricións de rexeitamento. Na definición do esquema relacional poden impoñerse outra serie de restricións que garantan a integridade do modelo, e polo tanto, da información almacenada na base de datos. Estas restricións deben ser verificadas en toda operación de actualización para que o novo estado constitúa unha ocorrencia válida do esquema; en caso de que a operación intente violar a condición impídese que a operación se leve a cabo, como son:
- Restricións de verificación (CHECK). Especifican condicións que deben cumprir os valores de determinados atributos dunha relación, como poden ser os atributos de existencia obrigatoria (NOT NULL).
  - Asercións (ASSERTION). Permiten especificar condicións entre os elementos de distintas relacións do esquema.
  - Disparadores (TRIGGER). Permiten especificar condicións e accións que se leven a cabo cando se efectúe unha acción determinada sobre algunha relación do esquema

### **18.5.- NORMALIZACIÓN DE RELACIONES.**

Ao estudar a estrutura do modelo relacional, dedúcese que a información da nosa base de datos pode representarse por medio dun conxunto de obxectos (relacións e dominios) e dun conxunto de regras de integridade.

No modelo relacional, como nos demais modelos de datos, o deseño dunha base de datos pódese abordar de dúas formas distintas:

- Obtendo o esquema relacional directamente a partir da observación do noso universo do discurso, de forma que plasmemos a nosa percepción deste nun conxunto de esquemas de relación, os cales conterán os atributos e as restricións de integridade que representan os obxectos e regras que puidemos captar na nosa análise do mundo real.
- Realizando o proceso de deseño en dúas fases, na primeira lévase a cabo o deseño conceptual, por exemplo no modelo E/R, obténdose o correspondente esquema conceptual; na segunda, este transfórmase nun esquema relacional seguindo unhas determinadas regras de transformación.

Estas relacións que resultan da observación do mundo real ou da transformación ao modelo relacional do esquema E/R elaborado na etapa de modelado conceptual, poden presentar algúns problemas, derivados de fallos na percepción do universo do discurso, no deseño do esquema E/R, ou no paso ao modelo relacional;

Entre estes problemas cabe destacar os seguintes:

- Incapacidade para almacenar certos feitos.
- Redundancias e, polo tanto, posibilidade de inconsistencias,
- Ambigüidades.
- Perda de información (aparición de tuplas repetidas).
- Perda de dependencias funcionais, é dicir, de certas restricións de integridade que dan lugar a interdependencias entre os datos.
- Existencia de valores nulos.

- Aparición, na base de datos, de estados que non son válidos no mundo real (anomalías de inserción, borrado e modificación).

En definitiva, o esquema relacional debe ser sempre analizado para comprobar que non presenta os problemas anteriormente citados, evitando a perda de información e a aparición de estados que non son válidos no mundo real.

Para evitar que se poidan dar estes problemas, existen unha serie de regras ou formas normais. Estas formas normais serán aplicadas normalmente a bases de datos xa implantadas en forma de relacións (táboas), o que nos permitirá pasar a outras relacións (táboas) que non dean os problemas anteriormente descritos.

Existen seis formas normais. As tres primeiras na maior parte dos casos son suficientes para normalizar os esquemas de relación.

### **1. Primeira Forma Normal (1FN).**

Dise que unha relación está en 1FN cando cada atributo só toma un valor do dominio simple subxacente. É dicir, cada atributo ten asociado un dominio do cal só toma un valor en cada tupla.

É unha restrición inherente ao modelo relacional, polo que o seu cumprimento é obrigatorio e afecta ao número de valores que poden tomar os atributos dunha relación.

### **2. Segunda Forma Normal (2FN).**

Dise que unha relación está en 2FN se:

- Está en 1FN.
- Cada atributo non principal da relación ten dependencia funcional completa respecto da clave primaria desa relación, isto é, o valor dos atributos non principais da relación vén determinado polo valor de todos os atributos da clave.

Por exemplo, a relación:

<b>Matrícula (DNI, materia, nome, apelidos, curso, nota, aula, lugar)</b>
---

Non está en 2FN, posto que nome e apelidos dependen unicamente de DNI e non do valor de materia. Igualmente, curso depende unicamente de materia, e non do valor de DNI.

Para pasar a 2FN, descomponse a relación noutras tres, da forma:

<b>Matrícula2 (DNI, materia, nota, aula, lugar)</b>
---

<b>Alumno (DNI, nome, apelidos)</b>
-------------------------------------

<b>Materia (materia, curso)</b>
---------------------------------

### 3. Terceira Forma Normal (3FN).

Unha relación R satisfai a terceira forma normal (3FN), se e soamente se está en 2FN, e cada atributo non principal (atributo que non forma parte da clave) da relación non depende funcionalmente doutros atributos non principais desa relación. É dicir, non poden existir dependencias entre os atributos que non forman parte da clave primaria da relación R.

De se considerar, como é lóxico, que cada aula está situada fisicamente nun único lugar, pódese observar que a relación Matricula2, a cal está en 2FN, segue presentando problemas debidos a que existe unha dependencia entre os atributos aula e lugar (non se encontra, polo tanto, en 3FN),

Para eliminar os problemas que ocasiona na relación Matricula2 a existencia desta dependencia funcional, esta relación debe descompoñerse en dúas relacións, quedando o esquema da forma:

<b>Matrícula3 (DNI, materia, nota, aula)</b>
--

<b>Situación (aula, lugar)</b>
--------------------------------

<b>Alumno (DNI, nome, apelidos)</b>
-------------------------------------

<b>Materia (materia, curso)</b>
---------------------------------

#### 4. Forma Normal de Boyce-Codd (FNBC).

É unha redefinición máis estrita da 3FN, xa que esta presentaba certos problemas en relacións con varias claves candidatas compostas que se solapaban. Por iso en 1974, Boyce e Codd definiron a chamada forma normal que leva o seu nome (FNBC). Baséase no concepto de determinante funcional.

Chámase determinante funcional a un atributo ou a un conxunto de atributos dunha relación R do cal depende funcionalmente de forma completa algún outro atributo da mesma relación.

Unha relación R satisfai a forma normal de Boyce-Codd (FNBC) se e soamente se está en 1FN, e cada determinante funcional é unha clave candidata da relación R, isto é, ningún atributo facilita información doutro atributo que non é clave candidata.

Por exemplo, no esquema:

**Matrícula4** (DNI, materia, apelidos, nomee, nota, aula)

**Situación** (aula, lugar)

**Materia** (materia, curso)

(onde *materia*, *apelidos*, *nome* é unha clave candidata e *DNI*, *materia* é outra clave candidata da relación Matrícula4).

Neste caso, o esquema está en 3FN pero non está en FNBC, posto que DNI é un determinante funcional (apelidos e nome dependen de DNI) e non é clave candidata da relación. Para poñer o esquema en FNBC hai que descompoñer Matrícula4 en 2 relacións, de tal forma que queda un esquema similar ao obtido no apartado anterior:

**Matrícula3** (DNI, materia, nota, aula)

**Alumno** (DNI, nome, apelidos)

**Situación** (aula, lugar)

**Materia** (materia, curso)

## 5. Cuarta Forma Normal (4FN)

Está baseada na eliminación das dependencias multivaluadas. Dise que nunha relación existe unha dependencia multivaluada ( $\alpha \twoheadrightarrow \beta$ ), se os valores dun conxunto de atributos  $\beta$  depende unicamente do valor que tome outro conxunto de atributos  $\alpha$ , de forma independente ao resto de atributos da relación.

Por exemplo, se temos unha relación para un concesionario con todos os modelos de coches que se vende, coa súa cor e equipamento respectivo:

<b>Concesionario (<u>modelo</u>, <u>cor</u>, <u>equipamento</u>)</b>
--

e sabemos que pode vender dous modelos, *utilitario* e *berlina*. Se o modelo utilitario se pode vender en cor azul ou verde con dous tipos de equipamento (base ou normal) e se o modelo berlina se pode vender en cor prata ou azul con equipamentos normal ou luxo.

Neste caso, se sabemos que o modelo é utilitario, sabemos os posibles valores para a cor e o equipamento, e polo tanto existen dúas dependencias multivaluadas:  $\text{modelo} \twoheadrightarrow \text{cor}$  e  $\text{modelo} \twoheadrightarrow \text{equipamento}$ , e a relación encóntrase en 4FN pero non en FNBC

Para poñer o esquema en 4FN débese descompoñer a relación noutras dúas da forma:

<b>Concesionario1 (<u>modelo</u>, <u>cor</u>)</b>
---

<b>Concesionario 2 (<u>modelo</u>, <u>equipamento</u>)</b>
--

## 6. Quinta Forma Normal (5FN).

Está baseada na eliminación das dependencias de reunión. Dise que existe unha dependencia de reunión se a relación se pode construír sobre a base da reunión natural das proxeccións desa relación sobre os atributos que a forman.

Unha relación está en 5FN se e soamente se toda dependencia de reunión nesa relación está implicada polas claves candidatas entre si, e non por calquera outro atributo desa relación.

Por exemplo, na relación: **Docencia (DNI, materia, aula)**

que define as aulas que se asignan a cada materia e os alumnos matriculados nela (cada alumno matriculado nunha materia recibe clase en todas as aulas asignadas a esta), existe dependencia de reunión entre os atributos DNI, materia e aula.

Para eliminar as dependencias de reunión e poñelo en 5FN, descomponse a relación noutras tres:

**Docencia1 (DNI, materia)**

**Docencia2 (materia, aula)**

**Docencia3 (DNI, aula)**

### **18.6.- TRADUCCIÓN DE ESQUEMAS E/R A ESQUEMAS RELACIONAIS.**

1. Aplicar a 1FN aos obxectos que forman parte do esquema, isto é:
  - Eliminar os atributos multivaluados. Transfórmanse en entidades débiles dependentes en existencia da entidade da cal formaban parte, con relación un a moitos se o atributo é un identificador alternativo ou moitos a moitos no caso contrario.
2. Os tipos de entidade transfórmanse a relacións no esquema relacional.
3. Os tipos de interrelación binarias un a un transfórmanse en xeral en dúas táboas mediante propagación da clave, isto é, engádese a unha das táboas como clave foránea o identificador principal da outra táboa coa que está relacionado.

Dependendo das cardinalidades mínimas de cada tipo de entidade, temos:

- *Cardinalidade mínima un en ambos os dous casos:* propagación da clave cara a calquera dos dous lados.

- *Cardinalidade mínima un en ambos os dous casos e dependencia en identificación, co mesmo identificador principal en ambos os dous tipos de relacións:* transfórmanse ambos os dous tipos de entidade nunha única táboa.
  - *Só unha dos dous tipos de entidades ten cardinalidade mínima cero:* convértese cada tipo de entidade nunha táboa e propágase a clave cara ao lado de cardinalidade mínima cero.
  - *Cardinalidade mínima cero en ambos os dous casos:* pódese facer unha táboa nova (tres táboas), para evitar a existencia de demasiados valores nulos nas táboas.
4. Os tipos de interrelación binarias un a moitos transfórmanse en xeral en dúas táboas mediante propagación da clave cara ao lado moitos. Existe un caso especial:
    - *Cardinalidade mínima cero na entidade do lado un (0,1):* para evitar a presenza de demasiados valores nulos, xéranse tres táboas, unha por cada tipo de entidade e outra cos identificadores de ambas as dúas entidades e os atributos (se os hai) da interrelación. A clave principal será o identificador principal do tipo de entidade con cardinalidade máxima n. O identificador principal do outro tipo de entidade será clave foránea nesta táboa.
  5. Os tipos de interrelación binarias moitos a moitos transfórmanse sempre en tres táboas mediante propagación da clave cara ao lado moitos; unha por cada tipo de entidade e outra cos identificadores de ambas as dúas entidades e os atributos (se os hai) da interrelación. A clave principal desta táboa estará composta polos identificadores principais de ambos os dous tipos de entidades.
  6. Os tipos de interrelación nos que interveñen máis de dous tipos de entidade, transfórmanse da mesma forma que os tipos de interrelación binarias moitos a moitos.
  7. Os tipos de interrelación reflexivas transfórmanse:



- En interrelacións reflexivas do tipo N:M, transfórmanse da mesma forma que os tipos de interrelación binarias moitos a moitos, é dicir, xérase unha táboa para o tipo de entidade e outra para o tipo de interrelación.
  - En interrelacións reflexivas do tipo 1 :N, pódese proceder de dúas formas: xérase unha única táboa para o tipo de entidade engadindo como clave foránea o identificador principal desta; ou créanse dúas táboas, unha para o tipo de entidade e outra para o tipo de interrelación co identificador principal da entidade duplicado (nun caso é a clave principal e noutro a clave foránea da outra táboa).
8. Os atributos das interrelacións, cando hai propagación da clave, tamén se propagan.
9. As relacións xerárquicas de xeneralización - especialización pódense transformar de tres formas:
- Transformando o tipo de entidade pai nunha relación e colgando dela os atributos comúns e non comúns de todos os tipos de entidade fillo.
  - Crear unha relación para o tipo de entidade pai, cos atributos comúns, e outra relación para cada unha dos tipos de entidade fillo.
  - Crear unha relación para cada unha dos tipos de entidade fillo e poñendo en cada unha delas todos os atributos comúns do tipo de entidade pai. Só serve en caso de xerarquía total.
10. As dependencias en identificación e en existencia, para evitar a existencia de valores nulos na clave foránea da relación proveniente do tipo de entidade débil, ao transformarse deben obrigir o borrado e actualización en fervenza (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

Colexiado do CPEIG

# **19. SISTEMAS DE XESTIÓN DE BASES DE DATOS. BASES DE DATOS XML NATIVAS. MONITORES TRANSACCIONAIS.**

## TEMA 19: SISTEMAS DE XESTIÓN DE BASES DE DATOS. BASES DE DATOS XML NATIVAS. MONITORES TRANSACCIONAIS.

---

### ÍNDICE

<b>19.1 Sistemas de Xestión de Bases de Datos (SXBD).....</b>	<b>3</b>
19.1.1 <i>Introdución.....</i>	3
19.1.2 <i>SXBD obxectivo e 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>Obxectivos e beneficio.....</i>	10
19.1.4.2 <i>Niveis de descrición de datos.....</i>	10
19.1.4.3 <i>Contorno.....</i>	13
19.1.4.4 <i>Compoñentes dun SXBD.....</i>	13
19.1.4.5 <i>Modelos de datos.....</i>	14
19.1.5 <i>Estrutura xeral dun SXBD.....</i>	16
19.1.6 <i>SXBD relacionais (SXBD-R).....</i>	18
19.1.6.1 <i>Características dos SXBD-R.....</i>	18
19.1.6.1.1 <i>Estruturas de datos: relacións e claves.....</i>	18
19.1.6.1.2 <i>Operadores asociados.....</i>	20
19.1.6.1.3 <i>Aspectos Semánticos.....</i>	21
<b>19.2 Bases de Datos XML Nativas.....</b>	<b>22</b>
19.2.1 <i>Bases de datos XML.....</i>	22
19.2.1.1 <i>Bases de datos habilitadas para XML.....</i>	23
19.2.2 <i>Bases de datos XML nativas.....</i>	23
<b>19.3 Monitores transaccionais.....</b>	<b>24</b>
19.3.1 <i>Vantaxes dos monitores transaccionais.....</i>	24
19.3.2 <i>Arquitecturas.....</i>	25
19.3.2.1 <i>Modelo dun proceso por cliente.....</i>	25
19.3.2.2 <i>Modelo de proceso único.....</i>	25



19.3.2.3 Modelo de moitos servidores, un router.....	25
19.3.2.4 Modelo de moitos servidores, moitos routers.....	26
<b>19.4 Bibliografía.....</b>	<b>26</b>

## **19.1 SISTEMAS DE XESTIÓN DE BASES DE DATOS (SXBD)**

### **19.1.1 Introducción**

Para que unha base de datos funcione correctamente precisa dun *software* que xestione todas as súas operacións e que ademais proporcione unha interface de comunicación para os usuarios facilitando o acceso aos datos contidos nela. Este tipo de software son os denominados *Sistemas de xestión de bases de datos* ou *SXBD*.

Segundo unha definición formal, un Sistema de xestión de bases de datos, "*é un conxunto coordinado de programas, procedementos, linguaxes, etc., que lles subministra tanto aos usuarios non informáticos, como aos analistas programadores, ou ao administrador, os medios necesarios para describir e manipular os datos integrados na base, mantendo a súa integridade, confidencialidade e seguridade*".

Este grupo definido de software encargado de ofrecer soporte ás bases de datos aporta unha serie de facilidades para o manexo das bases de datos. Estas facilidades tradúcense nunha serie de linguaxes que permiten operar contra as distintas bases de datos que soporta o SXBD, sendo os principais:

- **Linguaxe de definición de datos ou DDL** (Data Definition Language): permite definir os esquemas conceptuais dunha base de datos.
- **Linguaxe de manipulación de datos ou DML** (Data Manipulation Language): subministra operacións para a realización de consultas e actualizacións da información contida nas bases de datos.
- **Linguaxe de control de datos ou DCL** (Data Control Language): permite administrar e controlar o acceso aos datos existentes nunha base de datos.

Desde os anos 70, o grupo ANSI/X3/SPARC é o encargado de ocuparse da normalización dos SXBD, publicando en 1975 un informe provisional onde propón unha arquitectura de 3 capas para os SXBD que posteriormente se revisaría e

detallaría en 1977. Con todo, ata 1985 non se presentou o *Modelo de referencia* para a estandarización dos SXBD (Modelo ANSI).

### **19.1.2 SXBD obxectivo e características**

Para un sistema xestor de bases de datos o seu obxectivo principal é o de ofrecer un contorno idóneo para a extracción, manipulación almacenamento da información das bases de datos. Os SXBD realizan unha xestión centralizada de todas as peticións de acceso funcionando de interface entre os usuarios e a base de datos. Tamén é o xestor da estrutura física dos datos e do seu almacenamento, polo que en definitiva, libera os usuarios de coñecer a organización física exacta dos datos, así como de crear os algoritmos de almacenamento, actualización ou consulta da información contida na base de datos.

Non todos os SXBD son iguais nin teñen as mesmas funcionalidades, posto que dependen de cada produto e do modelo de base de datos que xestionen. Independentemente disto, existen unha serie de características que se poderían identificar como comúns a todos eles e que foron definidas por Codd e revisadas con posterioridade, a medida que as novas necesidades se foron integrando. As características necesarias para que un SXBD poida cubrir as necesidades dun usuario son:

- Co fin de simplificar o mantemento das aplicacións que fan uso das bases de datos, un SXBD debe manter a independencia entre as solucións software e a estrutura da base de datos. Esta independencia non é completa pero cada vez aproxímanse máis a esta esixencia.
- Na medida do posible, non debe existir redundancia de datos, é dicir, estes non deben de estar almacenados varias veces. Con isto conséguese asegurar a coherencia dos datos.
- Un SXBD ofrece as ferramentas necesarias a un usuario para:
  - Almacenar datos.

- Acceder á información.
- Actualizar os datos.

Estas ferramentas han de proporcionar estes servizos de tal xeito que resulte transparente ao usuario.

- Permite o acceso de múltiples usuarios á mesma base de datos e no mesmo momento. Cando isto se produce, se algún dos usuarios está realizando operacións de actualización dos datos, o SXBD ha de asegurarse de realizar unha correcta xestión da concorrencia evitando a corrupción dos datos ou que estes se volvan inconsistentes. Para realizar esta xestión o SXBD fai un correcto uso dos bloqueos das bases de datos.
- Ofrécelles aos usuarios un catálogo ao cal poden acceder onde se almacenan, dun xeito centralizado, as descrições dos datos. Este servizo é o que permite a eliminación e detección das redundancias de datos e denomínase *dicionario de datos*.
- Realiza as transaccións garantindo que as actualizacións correspondentes a unha transacción se van realizar, ou no caso de que non sexa posible realizar algunha, ningunha terá efecto. Isto débese a que durante unha transacción se producen accións que cambian o contido da base de datos. Se por algún motivo a transacción falla, daquela a base de datos pasa a un estado de inconsistencia, posto que non todos os cambios da transacción se produciron, obrigando ao SXBD a desfacer os cambios para que a base de datos volva a un estado consistente.
- Garante a recuperación das bases de datos. Se ocorre algún problema que provoque que a información se vexa afectada, un fallo de *hardware* ou software que fagan abortar o SXBD, ou que un usuario interrompa unha operación antes de que se finalice a transacción, o SXBD debe proporcionar os mecanismos necesarios para liquidar este tipo de situacións e recuperar a base de datos a un estado consistente.



- Proporciona seguridade ás bases de datos, é dicir, restrinxe mediante diferentes niveis, que o acceso ás bases de datos só o realizarán usuarios autorizados, protexendo as bases de accesos non autorizados, xa sexan accidentais ou non.
- Un SXBD garante a integridade das bases de datos. Achega un conxunto de regras que a base de datos non pode violar conseguindo así a validez e consistencia dos datos.
- Proporciona ferramentas para a administración das bases de datos. Este conxunto de ferramentas permiten unha serie de funcionalidades:
  - Importación e extracción de datos
  - Monitorización do funcionamento e obtención de datos estatísticos sobre o uso das bases de datos.
  - Reorganización de índices
  - Optimización do espazo liberado para a súa reutilización.
- Mantén unha dispoñibilidade continua, garantindo que en todo momento as bases de datos están accesibles. Proporciona que as tarefas de administración, xestión e mantemento se poidan levar a cabo sen interromper o correcto funcionamento das bases de datos.
- Todo SXBD intégrase cun xestor de comunicacións, software encargado de xestionar o acceso dos usuarios que realicen a conexión coa máquina que serve de soporte ao SXBD dun xeito remoto a través dunha rede de datos. O xestor de comunicacións non forma parte dun SXBD pero si é preciso que o SXBD se integre con el.
- Posúe unha DDL, linguaxe de definición de datos, para a creación e modificación das bases de datos.



- Posúe unha DML, linguaxe de manipulación de datos, para a inserción, manipulación e consulta da información contida nas bases de datos.
- Posúe unha DCL, linguaxe de control de datos, para controlar o acceso á información das bases de datos.
- Garante a escalabilidade e elevada capacidade de proceso, é dicir, é capaz de aproveitar os recursos da máquina dispoñibles, aumentando a súa capacidade de procesado a medida que dispoña de recurso.
- É capaz de almacenar enormes cantidades de datos sen que o usuario perciba unha degradación no rendemento do sistema.

### **19.1.3 Evolución**

Nos primeiros inicios da informática os datos formaban parte dos programas, integrados como constantes. Posteriormente, coa aparición dos ficheiros como colección de datos homoxénea, empézase a diferenciar a estrutura lóxica que representa o punto de vista do usuario e a estrutura física dos datos.

Esta diferenciación faise máis evidente coa aparición nos sistemas operativos de subsistemas de xestión de datos, pero non resulta suficiente para romper a dependencia entre os datos e os programas e viceversa, e de ambos con respecto á máquina.

Para limar estas dependencias existentes entre os datos e as aplicacións, comézanse a utilizar arquitecturas que diferencian a estrutura lóxica dos datos, representación dos datos orientados cara ao problema, da estrutura física, representación orientada cara á máquina. Esta diferenciación funciona a través dunha transformación ou *mapping* que fai as tarefas de conversión entre unha estrutura e outra.

#### **19.1.3.1 Arquitectura en 2 capas**

Coa aparición dos primeiros SXBD nos anos 60, os sistemas pasan dunha orientación centrada no proceso a unha orientación enfocada cara ás bases de datos.

Isto produce que os datos e as relacións entre os mesmos se sitúen na bases de datos, conseguindo illalos das aplicacións. Esta evolución provoca un cambio nas tendencias das estruturas de datos facendo que a estrutura lóxica sexa máis flexible e sinxela, mentres que a estrutura física se volva máis complexa co fin de mellorar o rendemento.

Os primeiros SXBD facilitan en gran medida a descrición e o almacenamento das relacións permitidas caracterizando ao mesmo tempo os distintos modelos de datos: xerárquico, rede, relacional.

A arquitectura seguida por estes SXBD estaba definida en dous niveis:

- *Estrutura global*, coa características lóxicas e físicas: Esquema
- *Vistas lóxicas externas* dos usuarios: Subesquemas

#### 19.1.3.2      *Arquitectura en 3 capas*

A organización ANSI (American National Standards Institute) publica no ano 1975 un informe que resultaría clave para o desenvolvemento dos SXBD. Neste informe indícase a necesidade de evolucionar os SXBD co fin de conseguir unha total independencia entre os datos e as aplicacións. Para tal propósito propón un modelo arquitectónico en 3 capas e define á súa vez o modelo conceptual para conseguilo.

Neste informe a estrutura global do modelo de 2 niveis divídese dando lugar a dúas estruturas, nunha quédanse os aspectos lóxicos e o esquema conceptual, mentres que na outra se queda cos aspectos físico ou esquema interno.

Mediante esta definición, os SXBD que seguen esta normativa mostran internamente os tres niveis perfectamente diferenciados:

- **Nivel interno ou físico:** representa o nivel máis baixo de abstracción e neste nivel é onde se describe en detalle a estrutura física da base de datos, dispositivos de almacenamento físico, estratexias de acceso, índices, etc. Para iso interactúa co sistema operativo e co xestor de ficheiros. En definitiva o esquema interno especifica qué datos son almacenados e cómo,

además de describir a estrutura da base de datos en forma de modelo conceptual de almacenamento.

- **Nivel conceptual:** correspóndese co nivel intermedio de abstracción e describe os datos que son almacenados na base de datos e as relacións existentes entre eles. Tamén describe a base de datos segundo a súa estrutura de deseño. Neste nivel a base de datos resulta unha colección de rexistros lóxicos sen descritores de almacenamento. Mediante este nivel conséguese o illamento da representación da información dos requirimentos da máquina e das esixencias dos usuarios.
- **Nivel externo ou lóxico:** supón o de maior grao de abstracción e contén as vistas externas da base de datos asociadas a un esquema externo. Proporciona a cada tipo de usuario unicamente a parte do esquema que resulta relevante para el e para a cal ten acceso. Cada base de datos pode ter tantas vistas como necesite.

Con esta arquitectura preténdese conseguir que o esquema conceptual sexa unha descrición estable e independente do nivel superior e do inferior, é dicir, independente tanto das vistas como do almacenamento dos datos. Coa consecución desta independencia as bases de datos convértense en sistema máis flexibles e adaptables.

#### **19.1.4      *Modelo de referencia ANSI***

No ano 1985 publícase un estudo no cal se presenta un modelo para a estandarización dos SXBD. Este estudo, "*Modelo de referencia para a estandarización dos sistemas xestores de bases de datos*", foi presentado polo Database Architecture Framework Task Group, membro do ANSI/X3/SPARC Database System Study Group.

Este modelo de referencia non supón un estándar senón que supón simplemente un marco conceptual para a simplificación do traballo de estandarización dos distintos elementos e as súas relacións dentro dun SXBD.

Parte da arquitectura de tres niveis proposta por ANSI sobre a cal se realiza unha serie de revisións e simplificacións, ademais de describir as interaccións dun SXBD.

Os datos dentro do modelo de referencia pasan polos tres niveis descritos pola arquitectura, pero estes niveis agora están separados e illados por un conxunto de interfaces que lles proporciona completa independencia entre si.

#### *19.1.4.1 Obxectivos e beneficio*

O modelo de referencia desenvólvese cos seguintes propósitos:

- Crear unha ferramenta que guíe o desenvolvemento e coordinación para o proceso de estandarización no ámbito dos SXBD.
- Aportar as descrições das distintas interaccións dun SXBD co resto de compoñentes dos sistemas de información.
- Proporcionar un marco común de descrición dos SXBD co fin de facilitar os procesos de formación.
- Clasificar os distintos produtos segundo as súas características e funcionalidades.
- Ofrecer un punto de axuda aos usuarios nos procesos de análises, cambio e implantación de SXBD.

Seguindo estes propósitos xerais, o modelo de referencia pretende garantir ou presentar os seguintes beneficios, despois de estandarizados os SXBD:

- A portabilidade das aplicacións
- Melloras na produtividade e procesos de aprendizaxe.
- Simplificación dos procesos de avaliación e selección dos SXBD.
- Ofrecer a posibilidade de intercambiar datos entre distintos SXBD.

#### *19.1.4.2 Niveis de descrición de datos*

Os datos dentro do modelo de referencia pasan polos tres niveis descritos pola arquitectura, pero estes niveis agora están separados e illados por un conxunto de interfaces que lles proporciona completa independencia entre si.

Debido á existencia dos tres niveis independentes, esquema conceptual, externo e interno, xéranse dentro do modelo de referencia 3 tipos de funcións de administración:

1. *Administración de empresa:* encargado do deseño do esquema conceptual.
2. *Administración da base de datos:* especifica o esquema interno de tal xeito que se adapta o mellor posible ao esquema conceptual xa almacenado en forma de metadatos.
3. *Administración de aplicacións:* constrúe os esquemas externos partindo do esquema conceptual e xestiona os distintos programas de aplicación que utilizan as bases de datos.

Dentro desta estrutura lóxica de tres tipos de esquemas diferéncianse dúas fases ou seccións:

- **Definición:** é realizada por funcións de programa e os seus correspondentes interfaces, os cales producen os metadatos que se almacenan no dicionario de datos que é o núcleo da arquitectura.

A base de datos comeza coa creación do esquema conceptual por parte do administrador da empresa. Este rol foi chamado así por ANSI e reflicte o que hoxe se coñece como deseñador da base de datos. Ese esquema é procesado mediante o procesador do esquema conceptual, converténdoo en metadatos.

A través da interface posibilitase aos outros dous administradores, administrador da base de datos e o de aplicacións, o acceso ao esquema conceptual co cal constrúen os seus respectivos esquemas, internos e externos mediante os seus interfaces e os seus procesadores que almacenan a información correspondente a estes esquemas nos metadatos.

As etapas máis significativas da fase de definición son:



- Especificación do esquema conceptual mediante a linguaxe de definición.
  - Compilación do esquema conceptual por parte do procesador do esquema conceptual.
  - Almacenamento do esquema conceptual no dicionario de datos.
  - Procesado do esquema conceptual para a creación dos esquemas internos e externos por parte dos seus respectivos procesadores.
  - Control e almacenaxe dos esquemas internos e externos na base de datos por parte dos seus procesadores.
- **Manipulación:** é realizada por accións do usuario. Unha vez definida a base de datos o usuario pode realizar funcións de manipulación dos datos (inserción, borrado, modificación) mediante a linguaxe de manipulación de datos.

O proceso de manipulación por parte dun usuario consta dos seguintes puntos ou pasos dentro dun SXBD.

- Para a realización de operacións sobre a base de datos un usuario fai uso da súa interface, polo xeral unha aplicación, para enviar unha petición.
- Esta petición é transformada polo transformador externo/conceptual o cal fai uso dos metadatos para obter o esquema correspondente.
- O resultado envíase ao transformador interno que xera o esquema interno facendo uso tamén dos metadatos.
- Dese esquema interno trasládase ao transformador interno de almacenamento mediante o cal se accede aos datos utilizando para iso os metadatos.

- Unha vez obtidos os datos, estes sofren o proceso inverso para presentalos ao usuario nun formato adecuado.

#### *19.1.4.3 Contorno*

Un SXBD non resulta un sistema illado, é dicir, está situado dentro dun contorno. Por iso na descrición dun SXBD requírese da especificación das súas interfaces e dos compoñentes ou subsistemas que interaccionan con el. Nun contorno dun SXBD pódense atopar os seguintes elementos:

- Programas de aplicación e procesadores de linguaxe de aplicación.
- Sistemas de dicionario de datos.
- Sistemas operativos.
- Sistemas de xestión de ficheiros.
- Sistemas distribuídos e protocolos.
- Ferramentas de xestión.

#### *19.1.4.4 Compoñentes dun SXBD*

No modelo de referencia de ANSI un dos enfoques para estudar os sistemas xestores de base de datos é o dos compoñentes. Este enfoque consiste en separar o SXBD en distintas partes e, ao posuír diversas interfaces de comunicación, posibilitar o ensamblado dun SXBD con partes procedentes de distintos subministradores, co fin de conseguir a compatibilidade entre os módulos e unha compatibilidade no mercado. Neste punto o modelo de referencia revisa a complexa arquitectura ANSI/SPARC, que posúe un elevado número de interfaces, simplificándoa e realizando o proceso de análise para a recollida dos requisitos sen chegar nunca á implantación.

O obxectivo do modelo de referencia ANSI/X3 é describir interrelacións do SXBD, pero non indicar nada sobre a súa instrumentación.

O modelo de referencia define os compoñentes que debe ter todo SXBD. Os compoñentes propostos son:





- **Sistema de control de transformación de datos (SCTD).** É o núcleo do SXBD e proporciona unha serie de operadores para a descrición e manipulación dos datos. Está baseado nun modelo de datos coa capacidade de soportar á súa vez a descrición e manipulación doutros modelos de datos.
- **Interface de linguaxe de datos (LD)** que posibilita aos usuarios e aos procesadores especificar as súas peticións para a recuperación dos datos.
- **Interface de linguaxe de datos interno (LD-i)** que permite o uso dos servizos dos procesadores que soportan o funcionamento dos SXBD, en especial os do SO.

Adicionalmente, no contorno do SXBD destacan as ferramentas de xestión de datos (FXD), que son compoñentes de soporte lóxico, como as linguaxes de cuarta xeración (L4X), soporte para axuda á decisión, facilidades para realizar o axuste (*tuning*), utilidades para o envorcado de ficheiros, sistemas de dicionario de datos, etc.

#### *19.1.4.5 Modelos de datos*

Un modelo de datos resulta unha abstracción do universo do discurso, é dicir un "*Conxunto de conceptos, regras e convencións que permiten describir os datos dunha parcela do mundo real (universo do discurso)*".

O modelo de datos considérase tamén unha ferramenta intelectual que serve de apoio á hora de deseñar unha base de datos, xa que nun proceso de deseño dunha base de datos o que se pretende é crear unha modelización dun problema presente no mundo real.

O modelo de datos debe recoller as propiedades existentes dentro do universo do discurso e pódense dividir en dous tipos:

- *Estáticas:* Invariantes no tempo e conforman a compoñente estática do modelo de datos que é o conxunto de regras que permiten a xeración da estrutura e que se definen mediante a linguaxe de definición de datos.
  - Conxunto de obxectos, entidades e os seus atributos.
  - Conxunto de asociacións entre obxectos, interrelacións.
  - Conxunto de restricións, inherentes ou opcionais.
- *Dinámicas:* Varían co tempo e correspóndense coa compoñente dinámica do modelo de datos. Supón o conxunto de operadores aplicables sobre a estrutura e defínense mediante a linguaxe de manipulación de datos.

Entre os modelos de datos convencionais instrumentados nos SXBD establécense tres grupos ordenados cronoloxicamente:

- **Modelo xerárquico.** Responde a unha estrutura arborescente a varios niveis. Cada nivel da xerarquía está composto dun ou varios grupos de datos (nodos), de cada un dos cales poden depender outros nodos quedando unidos por ramas. Os nodos e as ramas determinan unha relación do tipo 1:n. A forma de recuperar os datos é percorrendo os distintos niveis segundo o camiño definido pola sucesión de nodos na árbore. Este modelo asume que certos datos son máis importantes que outros.
- **Modelo en rede.** É bastante máis flexible ca o xerárquico, pois permite establecer múltiples conexións, combinando varias xerarquías arborescentes. Obtéñense relacións n:m. Estas relacións permítenlle ao usuario acceder a un dato sen ter que percorrer todas as xerarquías.
- **Modelo relacional.** Proposto teoricamente por Codd en 1970. É recoñecida a súa superioridade fronte aos anteriores. Baseado na álgebra e cálculo relacional, fai posible o proceso de conxuntos de datos e non simples rexistros como no caso dos seus antecesores. Basicamente caracterízase, en canto á súa estrutura, por dispoñer dos datos organizados



en táboas (relacións) de filas similares (tuplas) cada unha cun conxunto de campos (atributos) en columnas. Non existen vinculacións entre táboas visibles para o usuario, e ademais cúmprense certas restricións.

En todos eles os obxectos que permiten son:

- Entidades
- Atributos
- Dominios
- Interrelacións

Con todo os tres tipos de modelos diferéncianse basicamente no modo de representación das relacións entre entidades e no xeito de acceder á base de datos.

#### **19.1.5 Estrutura xeral dun SXBD**

Os principais módulos do SXBD son:

- **O compilador da DDL.** Comproba a sintaxe das sentenzas da DDL e actualiza as táboas do dicionario de datos ou catálogo que conteñen os metadatos.
- **O precompilador da DML.** Converte as sentenzas da DML embebidas na linguaxe anfitrión, en sentenzas listas para o seu procesamento por parte do compilador de linguaxe anfitrión e ademais extrae esas sentenzas DML para que poidan ser procesadas de forma independente polo compilador da DML.
- **O compilador da DML.** Comproba a sintaxe das sentenzas da DML e pásallas ao procesador de consultas.
- **O procesador de consultas.** Realiza a transformación das consultas nun conxunto de instrucións de baixo nivel que se dirixen ao xestor da base de datos.



- **O xestor da base de datos.** Serve de interface para os programas de aplicación e as consultas dos usuarios. O xestor da base de datos acepta consultas e examina os esquemas externo e conceptual para determinar que rexistros se requiren para satisfacer a petición. Daquela o xestor da base de datos realiza unha chamada ao xestor de ficheiros para executar a petición.

Os principais compoñentes do xestor da base de datos son os seguintes:

- *O xestor de transaccións.* Realiza o procesamento das transaccións.
- *O xestor de buffers.* Transfire os datos entre memoria principal e os dispositivos de almacenamento secundario.
- *O xestor de ficheiros.* Xestiona os ficheiros en disco onde se almacena a base de datos. Este xestor establece e mantén a lista de estruturas e índices definidos no esquema interno. Para acceder aos datos pasa a petición aos métodos de acceso do sistema operativo que se encargan de ler ou escribir nos ficheiros físicos que almacenan a información da base de datos.

No esquema proposto reflíctense distintos bloques nos que se indican:

- Tipos de usuarios que poden acceder ao SXBD
- Métodos utilizados polos usuarios para acceder á información.
- SXBD que se divide en:
  - O primeiro subsistema é o encargado de recibir as peticións e dirixilas ao xestor da base de datos ou ao dicionario de datos.
  - O segundo é o xestor da base de datos, que posúe un xestor de transaccións, un xestor de *buffer* e o xestor de ficheiros.
  - A base de datos cos seus índices e o dicionario de datos.

### **19.1.6 SXBD relacionais (SXBD-R)**

Os sistemas xestores de base de datos relacionais están baseados no **modelo relacional** o cal intenta representar o universo do discurso mediante a álgebra relacional e as súas principais características son:

Baseado nun modelo matemático cun conxunto de regras e algoritmos establecidos, permitindo que se desenvolvan linguaxes de acceso e manipulación moi potentes e fiables.

A estruturación dos datos realízase mediante relacións que son modeladas utilizando táboas bidimensionais que representan as entidades como as súas relacións.

Establece regras de integridade que posibilitan a incorporación de aspectos semánticos e o traslado de restricións ou comportamentos dos datos ao esquema conceptual, que doutra forma, non se poderían modelar só coas táboas.

#### **19.1.6.1 Características dos SXBD-R**

As súas tres principais características son as estruturas de datos, os operadores asociados e os aspectos semánticos.

##### **19.1.6.1.1 Estruturas de datos: relacións e claves**

Elementos:

- **Relación:** subconxunto dun produto cartesiano entre conxuntos de atributos que no modelo relacional se mostra como unha táboa con  $m$  filas e  $n$  columnas.
- **Atributo:** representan as columnas dunha táboa e correspóndense coas propiedades das entidades. Estes atributos están limitados por un dominio que especifica o rango de valores que poden tomar podendo ser compartido por varios atributos.



- *Dominio*: rango de valores que un atributo pode adoptar. Este rango é dependente do tipo de atributo e os valores do dominio deben ser homoxéneos.
- *Tuplas*: nome que se lle asocia a cada unha das filas dunha táboa que se corresponden con cada unha das ocorrencias da relación que se representa na táboa. A súa orde non é relevante.
- *Cardinalidade da relación*: número de tuplas dunha relación.
- *Grao da relación*: número de atributos dunha relación.

Dentro dos elementos que conforman a estrutura de datos os máis importantes son as relacións, cuxas características máis importantes son:

- Todas as tuplas dunha relación están formadas polo mesmo número, tipo de atributos e na mesma orde.
- A orde das tuplas carece de relevancia.
- En cada atributo dunha tupla só pode aparecer un valor que ademais debe pertencer ao dominio correspondente.
- Non poden existir dúas tuplas iguais na mesma relación. Isto provoca que exista un ou varios atributos que sirvan para distinguir unhas tuplas doutras denominados *claves candidatas*.

Algunha destas claves candidatas son seleccionadas polo administrador ou deseñador da base de datos para a identificación de tuplas; nese caso, a clave denomínase *clave primaria* e non pode adoptar nunca o valor nulo. O resto de claves candidatas que non son seleccionadas como primarias denomínanse *claves alternativas ou secundarias*.

Ademais unha relación pode incluír dentro dos seus atributos a clave primaria doutra relación, pasando esta a ser *clave foránea* da primeira relación.

#### **19.1.6.1.2 Operadores asociados**

A álgebra coa que se move o modelo relacional está formada por un conxunto de operadores asociados e é completa, é dicir, garante matematicamente que con ela se pode realizar calquera acceso á base de datos.

Os operadores utilizan as relacións do modelo como operandos. Os operadores máis importantes móstranse a continuación:

- **Unión.** A unión de dúas relacións "A" e "B" produce o conxunto de tuplas formado polas tuplas de "A" e as tuplas de "B". Só é aplicable a relacións co mesmo grao e cos mesmos atributos.
- **Diferenza.** A diferenza entre dúas relacións "A" e "B" é o conxunto de tuplas da relación A que non están en "B". Só é aplicable a relacións co mesmo grao e cos mesmos atributos.
- **Produto cartesiano.** O produto cartesiano de dúas relacións "A" de grao m e "B" de grao n, está formado polo conxunto de todas as posibles tuplas de m+n atributos cos m primeiros valores de "A" e os n restantes de "B".
- **Proxección.** Considerando "x" un subconxunto de atributos da relación "A", a *proxección* do atributo "x" sobre a relación "A" é a relación formada polos atributos de "A" correspondentes cos do subconxunto "x".
- **Selección.** Se "F" resulta unha fórmula que está composta por operadores lóxicos, aritméticos e de comparación e os operandos correspóndense con valores dos atributos dunha relación "A", daquela a selección de "F" sobre "A" é o conxunto resultante formado polas tuplas de "A" que cumpren a condición establecida por "F".

Partindo deste conxunto de operadores pódense xerar outros derivados como a intersección, o cociente ou a unión natural.

### **19.1.6.1.3 Aspectos Semánticos**

Cando unha característica do contorno ou do universo do discurso non se pode modelar mediante a definición dunha relación, esta debe definirse mediante un nivel de descrición superior pasando a formar parte dos aspectos semánticos. Estes aspectos, desde un punto de vista práctico, son restricións que se engaden ás propias do modelo relacional e que o seu propósito é o de garantir a integridade e validez dos datos. Á súa vez tamén aportan un maior grao de información ao esquema lóxico de datos.

Dentro deste conxunto de restricións pódense identificar dous grupos:

- *Restricións de usuario.* Son restricións que se aplican aos valores pertencentes ao dominio dos atributos, por exemplo nun atributo data, limitar os meses a 12 e os días a 31.
- *Integridade referencial.* As restricións pertencentes á integridade referencial ocúpense do mantemento das referencias existentes entre as propias relacións.

Para manter a integridade referencial, cando se realiza algunha tarefa de borrado ou modificación das tuplas cómpre realizar algunha das seguintes accións.

- Impedir a operación, para asegurarse de que unha vez establecida a relación entre dúas tuplas de distintas táboas non se pode desfacer.
- Transmitir en fervenza, é dicir se se borra ou modifica unha tupla, todas aquelas que fan referencia a ela tamén se deben borrar ou modificar.
- Poñer a nulo, manter a integridade asignando o valor nulo ao atributo que realiza as tarefas de clave foránea.
- Establecer valor por omisión ou lanzar un procedemento de usuario que o estableza.



## **19.2 BASES DE DATOS XML NATIVAS**

A maioría das aplicacións tradicionais de negocio e das aplicacións baseadas na internet dependen de bases de datos, xa que nelas se almacena información crucial para o seu bo funcionamento. Tamén se sabe que XML é o presente e futuro da administración de datos, pois esta linguaxe permitiu romper barreiras e crear un xeito estándar de procesar a información.

Pois ben, a aplicación de XML tamén afectou ao mundo das bases de datos, dando lugar a un novo enfoque e creando unha nova xeración de bases de datos denominadas bases de datos XML e bases de datos XML nativas.

As bases de datos nativas son totalmente distintas ás bases de datos tradicionais posto que malia que poden soportar XML ségueno realizando dun xeito relacional.

Pola contra, as bases de datos XML brindan unha nova capacidade sobre as relacionais, e é o feito de que permiten obter os resultados das consultas directamente en XML.

### **19.2.1 Bases de datos XML**

No conxunto de bases de datos que fan uso do XML é posible caracterizar tres tipos de arquivos XML:

- **Centrados en datos:** constan de moitos elementos de datos de pequeno tamaño e teñen unha estrutura regular e ben definida. Úsase como mecanismo de intercambio ou para mostrar datos.
- **Centrados en documentos:** están formados por poucos elementos e con estrutura impredecible en tamaño e contido. Enfócanse a sistemas documentais e de xestión de contidos.
- **Híbridos:** mestura partes dos dous tipos anteriores.

#### *19.2.1.1 Bases de datos habilitadas para XML*

Analizan un documento XML no seu correspondente modelo relacional ou de obxectos. A principal característica é ter un mapeo obxecto-relacional entre o contido XML e as táboas no SXBD-R. As bases de datos relacionais habilitadas para XML son boas para certo tipo de contido de documentos XML centrado nos datos, o cal ten unha estrutura fixa e se axusta ben a táboas relacionais e non ten información xerárquica.

#### **19.2.2 Bases de datos XML nativas**

Segundo o DBXml Group, *"as bases de datos XML nativas son BD que almacenan XML usando un formato que permite un procesamento máis rápido"*.

Son bases de datos especialmente deseñadas para almacenar documentos XML e xa que logo son bases de datos centradas en documentos que definen un modelo lóxico para o documento XML. Respectan a estrutura do documento, permiten facer consultas sobre esa estrutura e recuperan o documento tal e como foi inserido orixinalmente.

As súas características principais son as seguintes:

- Non teñen ningún modelo de almacenamento físico subxacente concreto
- Almacenamento de documentos en coleccións.
- Validación de documentos.
- Soportan unha ou máis linguaxes de consulta entre eles XML.
- Permiten a creación de índices para acelerar consultas realizadas frecuentemente.
- Crean un identificador único para cada documento XML.
- Teñen unha gran variedade de estratexias para actualizar e borrar documentos.

### **19.3 MONITORES TRANSACCIONAIS**

Os monitores transaccionais son aplicacións de control que realizan tarefas de monitorización das transferencias de datos que se producen dentro dunha organización. A súa intención é a de controlar as transaccións que se producen nos terminais, xa sexan locais ou remotos. O seu obxectivo é garantir que un proceso de transacción se produce de xeito correcto e no caso de non ser así, lanzar os procedementos necesarios para liquidar o problema e manter a integridade do sistema.

Un monitor transaccional en certo modo rompe a execución das aplicacións en transaccións para asegurarse que todas as bases de datos se actualizan mediante unha única transacción.

Esta capacidade que garante a unicidade dunha transacción resulta moi útil en sistemas de xestión de reservas e en calquera tipo de sistema no que ocorra un elevado número de transaccións.

Recibe peticións de consulta ou de procesado procedentes dos clientes para executalas nun ou varios servidores de bases de datos. O monitor transaccional encola estas peticións e priorízalas para posteriormente envorcalas sobre os sistemas de xestión de datos.

Unha das vantaxes que presentan os monitores transaccionais é que unha vez que unha transacción é aceptada polo monitor, este asume a responsabilidade de levala a cabo, liberando á súa vez ao cliente e posibilitando que este continúe co seu procesamento.

#### **19.3.1 Vantaxes dos monitores transaccionais**

- Ofrecen a capacidade de actualización de múltiples bases de datos nunha única conexión, establecendo un pool de conexións.

- Permiten que sexa posible manter estable un sistema con conectividade a múltiples fontes de datos e de distintos tipos arquivos planos, XML, datos non relacionais, *mainframes*, etc.
- Proporcionan mecanismos para priorizar as transaccións.
- Supoñen un aumento na seguridade e robustez dun sistema

### **19.3.2      *Arquitecturas***

#### *19.3.2.1      Modelo dun proceso por cliente*

Non se utiliza unha sesión por cliente ou terminal, son os procesos servidores os encargados de comunicarse cos terminais, manexar a autenticación e executar as accións.

- Supón un elevado consumo de memoria.

#### *19.3.2.2      Modelo de proceso único*

Todos os clientes e terminais remotos conéctanse a través dun único proceso servidor.

- Utilízase en contornos cliente-servidor
- O proceso servidor é un proceso multifío, o que ofrece baixo custo no intercambio de fíos.
- Non ofrece protección entre aplicacións
- Non recomendable para bases de datos distribuídas ou paralelas.

#### *19.3.2.3      Modelo de moitos servidores, un router*

Múltiples aplicacións con procesos servidores que acceden a bases de datos comúns. Os clientes comunícanse coas aplicacións servidoras mediante un único proceso de xestión das conexións que redirecciona as solicitudes.

- Procesos servidores independientes para cada aplicación
- Os procesos servidores son multifío
- Válido para bases de datos paralelas e distribuídas.

#### *19.3.2.4      Modelo de moitos servidores, moitos routers*

Utiliza múltiples procesos de comunicación cos clientes.

- Os clientes comunícanse cos *routers* que redireccionan as peticións cara aos servidores apropiados.
- Utilízase un control e 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, marzo 1986)
- de Miguel e 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 e 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

Colexiado do CPEIG



## **20. SQL. LINGUAXE DE DEFINICIÓN DE DATOS (DDL). LINGUAXE DE MANIPULACIÓN DE DATOS (DML) E DCL.**

## **Tema 20 SQL. Linguaxes de definición de datos (DDL). Linguaxes de manipulación de datos (DML) e DCL.**

---

### **ÍNDICE**

#### **20.1.- SQL**

*20.1.1 Partes da linguaxe SQL*

*20.1.2 Modos de traballo con SQL*

#### **20.2.- Linguaxe de Definición de Datos (DDL)**

*20.2.1 Obxectos da base de datos*

*20.2.2 Xestión de táboas*

*20.2.3 Xestión de vistas*

*20.2.4 Xestión de índices*

#### **20.3.- Linguaxe de Manipulación de Datos (DML)**

*20.3.1 Inserción de valores nunha táboa*

*20.3.2 Borrado de valores dunha táboa*

*20.3.3 Modificación de valores dunha táboa*

*20.3.4 Consulta de datos*

*20.3.5 Consultas sobre múltiples táboas.*

*20.3.6 Subconsultas*

*20.3.7 Operacións con consultas*

#### **20.4.- DCL. Linguaxe de control de datos**

*20.4.1 Seguridade*

*20.4.2 Transaccións*

#### **20.5.- Bibliografía**

### **20.1.- SQL**

A SQL (Structured Query Language) é unha linguaxe estandarizada de peticións (query) a bases de datos relacionais. É a linguaxe de manipulación de bases de datos relacionais máis estendida, despois de converterse nun estándar de feito.



Permite realizar consultas utilizando os recursos da álgebra relacional combinados co cálculo relacional de tuplas.

**SQL é unha linguaxe declarativa** na que o importante é definir qué se desexa facer, por riba de como facelo. Con esta linguaxe pretendíase que as instrucións se puidesen escribir coma se fosen ordes humanas; é dicir, utilizar unha linguaxe o máis natural posible. De aí que se considere unha linguaxe de cuarta xeración.

A base teórica de SQL é bastante forte. As operacións funcionan en termos de conxuntos e non de rexistros individuais. Ademais non inclúe ningunha especificación de localización dos datos ou ruta de acceso deixando esta tarefa ao intérprete da linguaxe.

A primeira definición do modelo relacional de bases de datos foi publicada por Codd en 1970. O traballo de Codd foi desenvolvido inmediatamente por empresas e universidades. A SQL foi desenvolvida no centro de investigación de IBM baixo o nome SEQUEL (Structured English Query Language) en 1974 e 1975. A versión SEQUEL/2 cambiou de nome a SQL por motivos legais. IBM comezou a traballar nunha versión de SEQLTL/2 (SQL) chamada System R que estivo operativa en 1977.

En 1986 publicouse o estándar ANSI da linguaxe que, posteriormente foi adoptada por ISO en 1987, o que converte SQL en estándar mundial como linguaxe de bases de datos relacionais.

En 1989 aparece o estándar ISO (e ANSI) chamado SQL89 ou SQL1. En 1992 aparece a nova versión estándar de SQL (a día de hoxe segue sendo a máis coñecida) chamada SQL92. En 1999 apróbase unha nova SQL estándar que incorpora melloras que inclúen triggers, procedementos, funcións... e outras características das bases de datos obxecto-relacionais; ese estándar coñécese como SQL99.

O último estándar é o do ano 2008 (SQL2008). ISO/IEC 9075-1:2008

### **20.1.1 Partes da linguaxe SQL**

Podemos considerar dúas fases na vida da base de datos: a etapa de preparación e posta en marcha e a etapa de explotación. Esta última é o obxectivo final de todo o sistema e as tarefas de preparación realizaranse antes de entrar nesa fase de utilidade para a organización.

A linguaxe SQL componse dun conxunto de instrucións ao igual que calquera linguaxe tradicional. Debido á existencia das dúas fases antes descritas adóitanse agrupar estas instrucións en tres "sublinguaxes" que en particular en bases de datos relacionais son as seguintes:

- **Linguaxe de definición de datos, DDL** (Data Description Language): É a linguaxe utilizada para a creación e mantemento da estrutura da base de datos. Utilízase para definir e modificar os esquemas das relacións, crear ou destruír índices e eliminar relacións. Permite tamén a definición de vistas e permisos de acceso para os usuarios. É a linguaxe que utiliza o administrador das bases de datos para realizar as súas tarefas.
- **Linguaxe de manipulación de datos, DML** (Data Manipulation Language). Inclúe todas as instrucións para realizar consultas ás bases de datos, inserir, modificar ou eliminar datos. Esta é a que utilizan os usuarios finais na fase de explotación da base de datos. A parte da DML que permite realizar consultas sobre os datos da BD chámase DQL (Data Query Language), pero é unha parte da DML.
- **Linguaxe de control de datos, DCL** (Data Control Language). Existen unha serie de tarefas relacionadas coas bases de datos que non están incluídas en ningún dos dous grupos antes descritos xa que non son propiamente de descrición nin de manipulación de datos. Mediante esta linguaxe establécense as restricións adicionais necesarias para controlar a privacidade e a integridade da información almacenada na base de datos.

Ademais, as linguaxes comerciais, e a SQL en particular, inclúen outras facilidades como son control de principio e final das operacións ou o bloqueo de datos mentres dura unha consulta.

### ***20.1.2 Modos de traballo con SQL***

Os modos en que a linguaxe SQL actúa sobre unha base de datos son os seguintes.

- Modo interactivo: O usuario da base de datos establece un diálogo co sistema xestor de base de datos (SXBD) a través do intérprete de SQL. Desta forma pode realizar operacións interactivamente sobre a base de datos introducindo calquera sentenza SQL e sen restrición na orde destas.

As sentenzas SQL así introducidas son traducidas polo intérprete de SQL que producirá a solicitude correspondente para o xestor da base de datos que a xestionará e xerará unha resposta para o usuario.

- Dende un programa: O usuario executa unha aplicación sobre o sistema operativo. A aplicación pode ser de dous tipos:
  - Programa escrito integramente en SQL ou mellor en extensións desta que inclúen as estruturas de programación habituais (bucles e selección). Un exemplo disto é PL/SQL de Oracle que é unha linguaxe procesual que permite desenvolver programas que acceden á base de datos vía SQL. Estes programas ou módulos de sentenzas SQL son en realidade guións que o intérprete SQL vai seguindo.
  - Programa escrito nunha linguaxe convencional de programación con partes escritas en SQL. Isto é o que se chama SQL embebida e a linguaxe que contén o texto SQL chámase linguaxe anfitrión (host). Neste caso as instrucións da linguaxe de programación execútanse polo procedemento habitual mentres que as sentenzas SQL se pasan a un módulo especial de execución do SXBD. Unha implantación da SQL embebida establece as relacións que deben manter os obxectos da base

de datos cos obxectos do programa anfitrión e restricións de funcionamento. Este modo de traballo admite dúas variantes:

- SQL estática: o programa non admite cambios durante a execución. Este é o método utilizado na maioría das aplicacións.
- SQL dinámica: se durante a execución se debe modificar algún parámetro tense que utilizar SQL dinámica. Isto resulta menos eficiente que un programa SQL estático e utiliza técnicas dinámicas de manexo de variables, o que dificulta a tarefa de programación.

## **20.2.- LINGUAXE DE DEFINICIÓN DE DATOS (DDL)**

Os datos en bases de datos relacionais almacénanse en táboas. Unha táboa componse de filas e columnas ou rexistros e campos correspondentes a entidades e atributos dunha relación. A todas as estruturas lóxicas de datos chámaseselles dunha forma xenérica obxectos das bases de datos.

Normalmente nun SXBD existen varios usuarios que deberán dispoñer en primeiro lugar de acceso ao sistema operativo da máquina. Cada usuario para o SXBD estará identificado por un nome, unha palabra clave e unhas propiedades. Todo iso é fixado e administrado polo administrador da base de datos (ABD) que é un usuario especial con dereitos sobre todos os obxectos.

O normal é que as estruturas de datos que van ser compartidas sexan creadas polo administrador pero isto non é un requisito imprescindible dado que pode haber usuarios para os que sexa de interese manter as súas propias bases de datos que compartirán con parte ou toda a organización.

O creador ou propietario dunha táboa pode permitir o acceso á súa táboa a outros usuarios do sistema pero pode que lle interese tamén permitir o acceso a unha parte da táboa. Para estes casos creárase unha vista (view). Nunha vista selecciónanse

algúns atributos ou algunhas tuplas da táboa e permítese que usuarios seleccionados as poidan manexar.

A busca dun rexistro nunha táboa é unha busca secuencial. Unha forma de axilizar a busca consiste en ordenar os rexistros segundo algún criterio e preguntar polos rexistros segundo esa orde. Se existe unha táboa na que se anota o valor característico de cada rexistro e a súa dirección, a busca chámase indexada e esta táboa auxiliar chámase índice.

Nun sistema multiusuario cada usuario ten un conxunto de obxectos que lle pertencen de diferentes tipos como táboas, índices ou vistas. A este conxunto adóitaselle chamar esquema.

Todos os obxectos citados ata agora deben crearse e configurarse antes de pasar ao uso da base de datos. Estas tarefas realízanse con DDL.

Cada obxecto dunha base de datos ten un nome que serve para localizalo ao longo da súa vida. Estes nomes teñen un ámbito onde son recoñecidos. Cada nome debe ser único no seu ámbito. Os obxectos que pertencen a un esquema (táboas, índices, etc.) teñen ese esquema como ámbito máximo. Por iso un nome de táboa, por exemplo, pode repetirse en distintos esquemas de usuarios diferentes pero non dentro do mesmo esquema.

Ademais destas normas básicas as diferentes aplicacións teñen as súas propias regras sobre ámbitos.

Resumindo, cunha DDL pódese facer:

- Xestión de táboas
- Xestión de vistas
- Xestión de índices

### **20.2.1 Obxectos da base de datos**

Segundo os estándares, unha base de datos é un conxunto de obxectos pensados para xestionar datos. Estes obxectos están contidos en esquemas. Un **esquema** representa a estrutura da base de datos. Os elementos que inclúe un esquema son táboas, dominios, vistas, restricións, disparadores e outros construtores.

No estándar SQL existe o concepto de **catálogo** que serve para almacenar esquemas. Así o nome completo dun obxecto viría dado por:

catálogo.esquema.obxecto
--------------------------

Se non se indica o catálogo toma o catálogo por defecto. Se non se indica o esquema enténdese que o obxecto está no esquema actual.

### **Tipos de datos e dominios**

Un dominio é un conxunto do cal toma os seus valores unha columna ou atributo dunha relación. Segundo este concepto os tipos de datos predefinidos son dominios.

Algúns dos tipos de datos predefinidos no estándar son:

- Integer (4 Bytes) e SmallInt (2 Bytes)
- Decimal (precisión, (escala)). Representa un decimal de coma fixa. Se se omite a escala suponse 0.
- Float. Representa un decimal de coma variable.
- Char (n) Cadea de caracteres de lonxitude fixa (de n caracteres).
- Varchar (n) Cadea de caracteres de lonxitude variable (de máximo n caracteres).
- Date (data), Time (hora), TimeStamp (data e hora).
- Boolean, bit
- CLOB. Representa textos de gran lonxitude.

- BLOB. Representa binarios de gran lonxitude.

### Definición de dominios

Unha definición de dominios é un tipo de datos especializado que se pode utilizar na definición de columnas. A súa sintaxe é a seguinte.

```
CREATE DOMAIN nome dominio tipo de datos  
    [ DEFAULT valor defecto ]  
    [ definición de restricións de dominio ];
```

Onde:

- tipo de datos: un dos proporcionados por SQL
- valor defecto: Especifica o valor por omisión para columnas definidas deste dominio. Será asignado a cada columna con ese dominio, se non ten xa a súa propia cláusula DEFAULT
- definición de restricións de dominio: implica unha restrición que se aplica a toda columna definida sobre o dominio. Defínese coa cláusula

```
[CONSTRAINT nome_restrición] CHECK (expresión condicional)
```

Exemplo: Enumeración de posibles valores das cores para un dominio particular

```
CREATE DOMAIN Cor VARCHAR(8) DEFAULT 'senCor'  
    CONSTRAINT cor_valida  
    CHECK (VALUE IN ( 'vermello', 'amarelo', 'azul', 'verde', 'senCor' ) );
```

### **20.2.2 Xestión de táboas**

Unha táboa é un obxecto da base de datos que almacena datos.

Para describir unha táboa utilízase a sentenza CREATE, especificando o nome e as características da táboa.

As características básicas que debe de ter unha táboa son:

- Definición dos atributos ou columnas
- Restricións de integridade

Para definir unha columna haberá que dicir o nome e tipo de datos que se van almacenar nese campo da táboa

### **Restricións de integridade**

Denomínase restrición de integridade a unha propiedade que debe cumprirse para manter nas táboas os criterios de deseño.

As restricións teñen un nome para poder ser manipuladas posteriormente e poden afectar a unha táboa enteira ou a unha columna ou atributo (restricións de táboa ou restricións de columna).

A restrición de táboa é algunha característica de mantemento da integridade que se asocia á táboa ao creala. Esta restrición aplicarase aos valores que conteña a táboa, logo supoñerá unha validación dos datos ao introducilos ou modificalos.

As restricións de columnas indican certas características que deben asociarse á columna que se está a describir.

En SQL as restricións de integridade fíxanse mediante unha sentenza CONSTRAINT.

A sintaxe de restricións para táboas é a seguinte:

```
[CONSTRAINT nome_restrición] (  
    [UNIQUE | PRIMARY KEY (atrib1[,atrib2]...)]  
    [FOREIGN KEY (atrib1 [,atrib2]...)  
        REFERENCES táboa(atrib1[,atrib2]...)  
    [ON UPDATE [CASCADE | NON ACTION | RESTRICT | SET  
        NULL | SET DEFAULT]  
    [ON DELETE [CASCADE | NON ACTION | RESTRICT | SET  
        NULL | SET DEFAULT] ]  
    [CHECK condición]
```



)

A sintaxe de restricións para atributos é a seguinte:

```
[CONSTRAINT nome_restrición] (  
    [NOT NULL]  
    [UNIQUE | PRIMARY KEY]  
    REFERENCES táboa(atrib1[,atrib2]...)  
        [ON UPDATE [CASCADE | NON ACTION | RESTRICT | SET  
            NULL | SET DEFAULT]  
        [ON DELETE [CASCADE | NON ACTION | RESTRICT | SET  
            NULL | SET DEFAULT] ]  
    [CHECK condición]  
)
```

As restricións que se poden establecer son:

- NOT NULL: aplícase a un campo e indica que non pode conter valores nulos.
- UNIQUE: a(s) columna(s) non pode conter valores duplicados. Debe declararse como NOT NULL e non poden formar parte da clave primaria.
- PRIMARY KEY: denota a(s) columna(s) que son clave principal da táboa. Teñen valor único e non nulo.
- CHECK: pódese aplicar a un atributo ou a toda a táboa. Indica unha condición que debe satisfacer cada atributo ou cada fila da táboa antes de ser inserida borrada ou actualizada.
- FOREIGN KEY / REFERENCES: cando entre dúas táboas se establece unha relación as tuplas dunha relaciónanse coas da outra mediante certos campos clave en cada táboa. A táboa da que parte a relación chámase táboa primaria e a outra chámase táboa secundaria.

Chámase **clave allea** (foreign key) o conxunto de atributos da táboa secundaria que é clave principal na táboa primaria. Esta última debe ser clave principal ou única.

Unha relación mantén a integridade referencial se cumpre as seguintes dúas condicións:

- Toda tupla da táboa filla está asociada cunha tupla da táboa pai.
- Se unha tupla da táboa filla non cumpre o anterior, o valor que ten a columna da clave allea é nulo.

A restrición de integridade referencial debe establecerse na táboa filla. Úsanse certos parámetros para fixala

- FOREIGN KEY: indica que columna ou columnas constitúen a clave allea nunha restrición de integridade referencial. Aplícase na restrición de táboa.
- REFERENCES: especifica a táboa pai. Se non indica a que clave primaria ou única se refire a clave allea enténdese que a clave referenciada é a clave primaria da táboa indicada.

As seguintes opcións fan que o xestor manteña a integridade referencial

- a) ON [DELETE | UPDATE] CASCADE: Borra ou actualiza o rexistro na táboa pai e automaticamente borra ou actualiza os rexistros coincidentes na táboa filla. Sen esta cláusula non se permite borrar ou actualizar un rexistro principal que teña rexistros secundarios asociados.
- b) ON [DELETE | UPDATE] RESTRICT: Non se pode borrar ou actualizar un rexistro na táboa pai mentres non se borre ou actualice o rexistro secundario asociado na táboa filla.



- c) ON [DELETE | UPDATE] SET NULL: Borra ou actualiza o rexistro na táboa pai e establece en NULL a ou as columnas de clave foránea na táboa filla.
- d) ON [DELETE | UPDATE] NON ACTION: Significa ningunha acción no sentido de que un intento de borrar ou actualizar un valor de clave primaria non será permitido se na táboa referenciada hai unha valor de clave foránea relacionado.
- e) ON [DELETE | UPDATE] SET DEFAULT: Borra ou actualiza o rexistro na táboa pai e establece o valor por defecto da ou as columnas de clave foránea na táboa filla.

## 1) Creación dunha táboa

A sintaxe básica da instrución é a seguinte.

```
CREATE TABLE nometáboa (  
    atributo1 tipo1 [restricións de atributo]  
    [,atributo2 tipo2 [NOT NULL] [UNIQUE] [DEFAULT valor]  
    [Restricións da táboa])
```

A creación dunha táboa engloba as definicións de atributos e/ou restricións:

- a) **A DEFINICIÓN DE ATRIBUTOS** realízase dando o nome do atributo (axústase ás mesmas regras que os nomes de táboas) e o seu tipo. Opcionalmente pódese indicar unhas restricións de atributos:
  - a. Not null: restrición de valor non nulo.
  - b. Definicións de restricións de clave primaria, valor UNIQUE, clave allea.
  - c. Definición de restricións xerais coa cláusula check.
- b) **A DEFINICIÓN DE RESTRICIÓNS DE INTEGRIDADE / SEMÁNTICAS:**  
Permiten ao deseñador restrinxir o rango de valores dunha táboa. As



restricións poden ser de columna se afectan a unha soa columna, ou de táboa se afectan a unha ou máis columnas, tal como se viu no apartado anterior.

Exemplo:

```
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 dunha táboa

Para modificar unha táboa xa creada utilízase o comando ALTER TABLE co que poden especificarse novas columnas, novas restricións (ADD) ou ben modificarse unha columna (MODIFY). A sintaxe é:

```
ALTER TABLE table (  
    [ADD (col1|restric1) (,col2|restric2)...]  
    [ALTER (col1 tipo1(,col2 tipo2)...)]  
    [DROP CONSTRAINT restrición]  
    [DROP COLUMN columna [CASCADE | RESTRICT] ]  
)
```

- A engadir unha columna a unha táboa xa existente hai que ter en conta que **non** está permitido NOT NULL na definición dunha nova columna, e se se desexa introducir un valor para a columna, en cada fila existente, hai que especificalo coa cláusula DEFAULT ao engadir a columna.
- Só se pode cambiar o tipo ou diminuír o tamaño dunha columna se ten valores nulos en todas as columnas.
- Só se poden borrar restricións que teñan nome.
- Ao eliminar unha columna dunha táboa podemos indicar a opción:
  - CASCADE: elimina a columna e toda restrición ou vista que lle fai referencia.
  - RESTRICT: só elimina a columna se ningunha vista nin restrición lle referencia.

Por exemplo, a sentenza:

```
ALTER TABLE EMP (  
    ADD ADDRESS VARCHAR(12) DEFAULT "Unknow";  
    ALTER ENAME VARCHAR(30)
```

)

Modifica a lonxitude do atributo ENAME e engádelle o campo ADDRESS.

### 3) Destrución dunha táboa

A sintaxe para eliminar unha táboa é:

```
DROP TABLE nome_da_táboa [CASCADE | RESTRICT]
```

Para executar esta instrución débense ter suficientes privilexios no sistema ou ser o propietario da táboa.

O parámetro opcional:

- **RESTRICT:** Destrúe a táboa só se non se lle fai referencia dende ningunha outra táboa (clave allea), nin é táboa base dunha vista.
- **CASCADE:** Elimina a táboa xunto coas restricións e vistas que a referencian.

Despois da execución da sentenza DROP calquera referencia á táboa dará un erro. A táboa borrarase independentemente de que conteña datos ou non.

#### **20.2.3 Xestión de vistas**

Unha vista é unha táboa virtual, é dicir, unha táboa que non existe fisicamente na base de datos pero que lle aparece ao usuario coma se existise. As vistas non teñen datos almacenados propios, distinguibles e fisicamente almacenados. No seu lugar, o sistema almacena a definición da vista (é dicir, as regras para acceder ás táboas base fisicamente almacenadas para materializar a vista).

As vistas teñen varias utilidades:

- Mostrar aos usuarios os datos que lles interesan.
- Protexer os datos.
- Reestruturar datos que poden estar distribuídos en diferentes soportes de maneira que aparezan como unha táboa.

- Crear interfaces para aplicacións que esperan unha estrutura de táboas distinta á de creación. Mediante as vistas as aplicacións independízanse da estruturación real dos datos.

## Creación dunha vista

Úsase a sentenza CREATE VIEW cuxa sintaxe é:

```
CREATE [OR REPRACE] VIEW nome_da_vista [lista_de_campos]
AS consulta
```

Cando se executa unha sentenza de creación de vista realízase unha consulta que selecciona tuplas e atributos dunha ou varias táboas. Exemplo: se se lle quere dar unha lista de empregados á empresa de seguridade que controla o acceso ao edificio, utilizarase unha vista sobre a táboa orixinal:

```
CREATE VIEW EMP_SECURITY
AS  SELECT EMPNO, ENAME
    FROM EMP
```

Por defecto, a vista toma os nomes dos atributos seleccionados dende as táboas base, sempre que ningún atributo sexa o resultado dunha operación aritmética ou función de agregado. Se se desexa cambiar os nomes dos atributos utilízase a lista\_de\_campos.

## Modificación da estrutura dunha vista

A estrutura dunha vista non pode ser modificada como tal. O que se pode facer é utilizar unha sentenza de creación coa cláusula OR REPLACE que substituirá unha vista por outras.

O comando de SQL ALTER VIEW utilízase para recompilar unha vista. Isto débese facer cando se modificaron as táboas bases da vista para actualizar a vista sobre as novas estruturas. A súa sintaxe é:

```
ALTER VIEW vista COMPILE
```

Despois desta instrución toda referencia á vista dende outro obxecto destrúese.

### **Destrucción dunha vista**

A instrución DROP VIEW permite eliminar unha vista que fose creada anteriormente

```
DROP VIEW view
```

#### ***20.2.4 Xestión de índices***

Nunha base de datos un índice é un medio de acceder aos rexistros dunha forma máis rápida que co simple percorrido secuencial dunha táboa. O índice é un obxecto da base de datos que conterá unha entrada para cada valor das columnas indexadas, coa dirección do rexistro onde debe buscarse ese valor.

Un dos usos máis comúns dos índices é o mantemento dunha táboa ordenada por distintos criterios.

Só é recomendable crear índices para aqueles campos que teñan moitas buscas pois o índice ocupa espazo e ten que actualizarse cada vez que se borra, actualiza ou insire un elemento nunha táboa.

### **Creación dun índice**

A instrución para crear un índice é CREATE INDEX

```
CREATE INDEX nome índice  
ON nome_táboa (campo{, campo})  
[NOSORT]
```

Especifícase o nome da táboa sobre a que crea o índice, así como o campo ou campos sobre os que se indexa. É posible crear índices concatenados, que se forman con máis dunha columna. Emprégase en caso de columnas que sempre se consultan xuntas.

A opción NOSORT que aparece nalgúns sistemas SQL fai que aforre tempo e espazo na creación dun índice facendo que se a táboa se encheu con rexistros que están



fisicamente ordenados co mesmo criterio que o índice se poida evitar a ordenación que se produce ao crear o índice.

```
CREATE INDEX IND_EMPRE ON EMPRESA (Abre_emp)
```

### **Eliminar un índice**

Para destruír un índice utilízase a cláusula DROP INDEX

```
DROP INDEX índice
```

## **20.3.- LINGUAXE DE MANIPULACIÓN DE DATOS (DML)**

Chámanse manipulacións aquelas operacións sobre unha base de datos que non afectan á estrutura desta senón ao seu contido. Estas operacións realízanse con DML (Data Manipulation Language). As manipulacións posibles sobre unha base de datos son as seguintes:

- Inserir valores en tuplas (INSERT)
- Eliminar unha tupla (DELETE)
- Actualizar o valor dun campo nunha ou varias tuplas (UPDATE)
- Consultar ou listar todos ou algúns campos dun grupo de tuplas (SELECT)

As operacións de manipulación pódense facer tanto en táboas coma en vistas xa que estas non son máis que táboas lóxicas.

### **20.3.1 Inserción de valores nunha táboa**

Para inserir unha fila ou tupla nunha táboa xa creada utilízase o comando INSERT cuxa sintaxe é:

```
INSERT INTO nome_táboa [columna (,columna)*]  
VALUES (valor (,valor)*)}
```

Se non se especifican nomes de columnas, os valores inseridos deben corresponder en cantidade e tipo de datos cos atributos da táboa e teñen que estar na mesma orde coa que se creou a táboa.

Pódense especificar unhas columnas e outras, non tendo en conta que as columnas non especificadas tomarán o valor por defecto, se se definiu, ou NULL.

```
INSERT INTO DEPT (DEPTNO, DNAME, LOC)
                VALUES (90, 'CONTABILIDADE', 'OURENSE')
```

Para inserir varias tuplas cunha soa instrución pódese utilizar unha subconsulta que devolva tuplas de estrutura compatible coa da táboa:

```
INSERT INTO nome_táboa [columna (,columna)*]
consulta
```

### **20.3.2 Borrado de valores dunha táboa**

Para borrar unha fila utilízase o comando DELETE cuxa sintaxe é a seguinte:

```
DELETE FROM nome_táboa
        [WHERE condición]
```

Con esta instrución bórranse todas as tuplas que cumpran a condición WHERE. Se non se inclúe esta, bórranse todos os elementos da táboa. Por exemplo, para borrar o departamento "CONTABILIDADE":

```
DELETE FROM DEPT WHERE DNAME = "CONTABILIDADE"
```

### **20.3.3 Modificación de valores dunha táboa**

Para modificar os valores de determinadas tuplas dunha táboa utilízase a sentenza UPDATE coa seguinte sintaxe:

```
UPDATE nome_táboa
```

```
SET columna1=valor1{,columna2=valor2)*}  
[WHERE condición]
```

Coa cláusula SET especificase as columnas que se deben modificar cos seus novos valores e coa cláusula WHERE selecciónanse as filas que se deben actualizar. Se non hai WHERE, aplícase a modificación a todas as filas. Por exemplo, se se quere conceder a todo empregado do departamento de Informática un aumento salarial do 18%.

```
UPDATE EMP  
    SET SAL = SAL*1.18  
    WHERE DEPTNO IN (SELECT DEPTNO  
                     FROM DEPT  
                     WHERE DNAME='INFORMÁTICA')
```

#### **20.3.4 Consulta de datos**

Unha consulta serve para extraer os datos almacenados nunha base de datos. A consulta en SQL consta de tres partes:

- Cláusula SELECT: para indicar que atributos se desexan consultar
- Cláusula FROM: indica sobre que relación ou relacións se quere facer a consulta
- Cláusula WHERE: indica as condicións que deben cumprir as tuplas para ser seleccionadas

A súa sintaxe abreviada é a seguinte:

```
SELECT * | {[DISTINCT] columna | expresión [[AS] alcume],...}  
    FROM táboas  
    [WHERE condicións_where]  
    [GROUP BY columnas_group]  
    [HAVING condicións_having]  
    [ORDER BY columnas_orde]
```

O efecto dunha consulta como esta é o seguinte:

- Realízase o produto cartesiano das relacións citadas na cláusula FROM
- Aplícase o operador selección da álgebra relacional para seleccionar aquelas tuplas do produto cartesiano que fagan verdadeiro o predicado WHERE
- Proxéctase o resultado obtido sobre os atributos especificados en SELECT

### **Selección de atributos**

A consulta máis sinxela é seleccionar todas as tuplas dunha táboa. Por exemplo, seleccionar todos os datos de todos os empregados.

```
SELECT EMPNO, ENAME, JOB, MGR, HIREDATE, SAL, COMM, DEPTNO  
FROM EMP
```

Utilízase o asterisco (\*) como comodín para seleccionar todos os campos. A sentenza anterior é equivalente a:

```
SELECT * FROM EMP;
```

Pódense seleccionar columnas individuais: "Lista todos os salarios"

```
SELECT SAL FROM EMP
```

Nunha táboa, algunhas columnas terán valores repetidos. Se só se queren mostrar os valores diferentes dunha columna nunha táboa hai que usar a palabra clave **DISTINCT** anteposta ao nome da columna

```
SELECT DISTINCT SAL FROM EMP
```

Pódese cambiar o nome que se lle dá á cabeceira da columna no resultado da instrución SELECT. Para iso utilízase un alcume co comando AS despois do nome da columna.

```
SELECT SAL AS Salario FROM EMP
```

## Orde

Por defecto SQL non ordena os resultados, para ordenalos, utilízase a cláusula ORDER BY:

```
ORDER BY campo1 [ASC|DESC], campo2 [ASC|DESC],...
```

O modo de ordenación indícase para cada campo:

- ASC ordena ascendente
- DESC ordena descendente

## Consulta con expresións

Tamén se poden realizar consultas nas que se avalíe unha expresión.

Por exemplo, se se dispón dunha táboa co salario bruto anual dos empregados dunha empresa, é posible consultar o seu soldo neto mensual. Supoñendo que se paguen 14 pagas anuais e que se coñeza o tipo de IRPF a instrución para realizar esta consulta sería:

```
SELECT ENAME, (SAL/14)(1-IRPF/100) FROM EMP
```

## Condições para restrinxir a consulta

Para restrinxir as tuplas que se obteñen, pódense impoñer condicións. Para iso úsase a cláusula WHERE que admite os seguintes operadores

Operadores Relacionais (comparación): >, >=, <, <=, =, <>: Estes operadores utilízanse para comparar datos.

Operadores lóxicos: AND, OR, NOT: Utilízanse para unir condicións.

```
SELECT * FROM EMP
      WHERE DEPTNO =99
            AND SAL >1250;
```

Ademais, as condicións unidas por AND, OR e NOT admiten paréntese. Se non se poñen parénteses a prioridade, de maior a menor, é NOT, AND e OR.

### Consulta de pertenza a un rango

Pódese comprobar se unha expresión entra ou non dentro dun rango marcado. Utilízase o operador BETWEEN. A sintaxe é:

```
expresión [NOT] BETWEEN expresión [AND expresión]
```

```
SELECT * FROM EMP
      WHERE EMPNO BETWEEN 9 AND 54
```

### Consultas de pertenzas a unha lista

Co operador IN compróbase se un elemento pertence a unha lista de valores. A sintaxe da condición é:

```
elemento[NOT] IN lista_expresións | subconsulta
```

Exemplo:

```
SELECT * FROM EMP
      WHERE ENAME IN('Pepe Martínez' e 'Xosefa Martín')
```

Selecciona da táboa de empregados os datos de 'Pepe Martínez' e 'Xosefa Martín'.

### Consulta con patróns

Coa utilización do operador LIKE pódese buscar unha cadea de caracteres dentro doutra. A sintaxe é a seguinte:

```
<cadea>[NOT] LIKE <cadea>
```

É unha comparación de igualdade pero admite comodíns:

- %: pódese substituír por calquera número de caracteres (0 ou máis).
- Os SXBDR tamén admiten substituír un único carácter.

Exemplo: Para seleccionar aqueles elementos da táboa ALUMNO na que o campo Nome empece pola cadea "Martes"

```
SELECT * FROM EMP WHERE ENAME LIKE 'Ma%'
```

## **Funcións de agregación**

Existen funcións que permiten calcular, dende unha sentenza SQL, sumas, medias aritméticas, etc. de datos. Moitas destas funcións aceptan o parámetro DISTINCT|ALL. Se toma o valor ALL (valor por defecto) indica que deben considerarse todas as aparicións aínda que sexan repetidas e se é DISTINCT deben ignorarse as repeticións. Algunhas das máis importantes funcións son:

- AVG (atributo): media aritmética dos valores de atributo.
- MIN (atributo): valor mínimo dos valores de atributo.
- MAX (atributo): valor máximo dos valores de atributo.
- SUM (atributo): suma os valores de atributo.
- COUNT (atributo): conta o número de filas onde atributo non é nulo.
- COUNT (\*): conta o número de filas incluíndo aquelas con nulos.
- LCASE (atributo): transforma atributo a maiúsculas.
- UCASE (atributo): transforma atributo a minúsculas.
- MID (atributo, m [n]): devolve unha porción de atributo comezando no carácter m e con n caracteres de lonxitude.
- LEN (atributo): devolve a lonxitude de atributo.

```
SELECT AVG (SAL) FROM EMP  
SELECT COUNT (*) FROM EMP
```

## Consulta con agrupamento de filas

As funcións de agregación adóitanse utilizar combinadas coa cláusula de agrupamento GROUP BY, que agrupa o resultado por unha serie de atributos.

Unha instrución SELECT con este parámetro devolve grupos de tuplas en lugar de tuplas individuais. Como resultado da consulta aparecerá un resumo da información por cada grupo en lugar de todas as filas.

Por exemplo para listar os números de departamento e a suma dos salarios de cada un deles utilizaríase:

```
SELECT DEPTNO, SUM(SAL)  
FROM EMP  
GROUP BY DEPTNO
```

A expresión dun GROUP BY pode conter referencias a calquera campo das táboas nomeadas en FROM. Non obstante a lista de expresións que seguen ao SELECT non pode conter máis que:

- Constantes
- Funcións de grupo (AVG, MAX, MIN, COUNT, SUM)
- Expresións idénticas ás da cláusula GROUP BY
- Expresións que devolvan o mesmo valor para todas as tuplas que formen parte dun grupo.

Non se poden seleccionar atributos que non se poidan agrupar polos atributos indicados no GROUP BY.



Se nunha consulta aparece unha cláusula WHERE e unha GROUP BY primeiro seleccionaranse as tuplas que cumpran a condición do WHERE e despois aplícase o agrupamento.

### Restricións nos agrupamentos

Cando se selecciona un conxunto de atributos agrupados por un ou máis atributos, pódense impoñer condicións aos grupos (é dicir, condicións aos atributos que se están a seleccionar). É a cláusula HAVING, que sería o equivalente á cláusula WHERE pero aplicada aos grupos. Por exemplo,

"Lista a suma dos soldos agrupada por departamentos, pero só aqueles nos que a suma sexa maior que 7.000"

```
SELECT SUM(SAL), DEPTNO
      FROM EMP
      GROUP BY DEPTNO
      HAVING SUM(SAL)>7.000
```

### ***20.3.5 Consultas sobre múltiples táboas.***

É máis que habitual necesitar nunha consulta datos que se encontran distribuídos en varias táboas. As bases de datos relacionais baséanse en que os datos se distribúen en táboas que se poden relacionar mediante un campo.

Para realizar consultas a máis dunha táboa, abonda con indicar na cláusula FROM as táboas separadas por comas e engadir as condicións necesarias na cláusula WHERE.

```
SELECT ENAME, DNAME
      FROM EMP, DEPT
```

Este exemplo realiza o produto cartesiano da táboa EMP e DEPT e devolvería para cada rexistro da táboa EMP, todos os rexistros da táboa DEPT.

Se se quere facer correctamente, asociando nome de traballador co departamento no que traballa, utilízase un criterio de comparación pola clave allea, por exemplo:

```
SELECT ENAME, DNAME
      FROM EMP, DEPT
     WHERE EMP.DEPTNO = DEPT.DEPTNO
```

Os nomes dos atributos, en caso de que as táboas teñan atributos co mesmo nome, irán precedidos polo nome da táboa e un punto, como en EMP.DEPTNO. Se non existe confusión posible poden indicarse sen o nome da táboa, como por exemplo DNAME, que só existe na táboa DEPT.

Para evitar repetir continuamente o nome das táboas, pódese especificar un alcume, engadíndolle ao nome da táboa na cláusula from o alcume.

A partir da versión SQL 1999 ideouse unha nova sintaxe para consultar varias táboas. A razón foi separar as condicións de asociación respecto das condicións de selección de rexistros. A sintaxe completa é:

```
SELECT táboa1.column1, táboa1.column2... táboa2.column1, táboa2.column2...
FROM táboa1
    [CROSS JOIN táboa2] |
    [NATURAL JOIN táboa2] |
    [JOIN táboa2 USING (columna)] |
    [JOIN táboa2 ON (táboa1.columna=táboa2.columna)] |
    [LEFT|RIGHT|FULL OUTER JOIN táboa2 ON (tbl1.column=tbl2.column)]
```

- **CROSS JOIN.** Realiza un produto cruzado entre as táboas indicadas. Iso significa que cada tupla da primeira táboa se combina con cada tupla da segunda táboa. É dicir se a primeira táboa ten 10 filas e a segunda outras 10, como resultado obtéñense 100 filas, resultado de combinar todas entre si.

```
SELECT ENAME, DNAME
      FROM EMP CROSS JOIN DEPT
```



- **NATURAL JOIN.** Establece unha relación de igualdade entre as táboas a través dos campos que teñan o mesmo nome en ambas as dúas táboas:

```
SELECT ENAME, DNAME  
FROM EMP NATURAL JOIN DEPT
```

Nese exemplo obtéñense a lista dos empregados e os nomes dos departamentos aos que pertencen a través dos campos que teñan o mesmo nome en ambas as dúas táboas. Hai que asegurarse de que só son as claves principais e secundarias das táboas relacionadas as columnas nas que o nome coincide, doutro modo fallaría a asociación e a consulta non funcionaría.

- **JOIN USING.** Permite establecer relacións indicando que columna (ou columnas) común ás dúas táboas hai que utilizar. As columnas deben de ter exactamente o mesmo nome en ambas as dúas táboas:

```
SELECT ENAME, DNAME  
FROM EMP JOIN DEPT USING (DEPTNO)
```

- **JOIN ON** Permite establecer relacións cunha condición que se establece manualmente, o cal é útil para asociacións cuxos campos nas táboas non teñen o mesmo nome:

```
SELECT ENAME, DNAME  
FROM EMP e JOIN DEPT d ON (e.DEPTNO=d.DEPTNO)
```

- **OUTER JOIN** Utilizando as formas vistas ata agora de relacionar táboas só aparecen no resultado da consulta filas presentes nas táboas relacionadas. É dicir na consulta anterior só aparecen empregados relacionados coa táboa de departamentos. Se hai empregados que non están en departamentos, estes non aparecen (e se hai departamentos que non están na táboa de empregados, tampouco saen).
- Para solucionar isto, utilízanse relacións laterais ou externas (outer join):

- táboa1 LEFT OUTER JOIN táboa2 ON. Obtén os datos da táboa 1 estean ou non relacionados con datos da táboa 2.
- táboa1 RIGHT OUTER JOIN táboa2 ON. Obtén os datos da táboa 2 estean ou non relacionados con datos da táboa 1.
- táboa1 FULL OUTER JOIN táboa2 ON. Obtén os rexistros non relacionados de ambas as dúas táboas.

### **20.3.6 Subconsultas**

Son sentenzas SELECT que se encontra aniñadas dentro doutras SELECT. Estas sentenzas escríbense entre paréntese para advertir o xestor que se debe de executar primeiro. Permite solucionar consultas que requiren para funcionar o resultado previo doutra consulta.

```
SELECT ENAME
      FROM EMP
     WHERE SAL >= (SELECT AVG(SAL) FROM EMP)
```

Dá como resultado a listaxe dos empregados que superan a media de soldo. Primeiro realízase a operación do SELECT da cláusula Where e seguidamente execútase o SELECT do principio.

Unha subconsulta que utilice os valores >, <, >=... *ten que devolver un único valor*, doutro modo acontece un erro. Ademais teñen que ter o mesmo tipo de columna para relacionar a subconsulta coa consulta que a utiliza (non pode acontecer que a subconsulta teña dúas columnas e ese resultado se compare usando unha soa columna na consulta xeral).

### **A cláusula (NOT) EXISTS**

A cláusula EXISTS (ou NOT EXISTS) comproba se unha subconsulta devolve algún valor (EXISTS) ou non devolve ningún (NOT EXISTS). Por exemplo:

"Lista os departamentos que non contratasen a ningún o 28 de decembro 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")
```

A consulta de primeiro nivel busca na táboa de departamentos os nomes e, para cada fila, comproba —mediante a subconsulta— que para ese número de departamento non existan empregados que fosen contratados o 28 de decembro de 2010.

### Consulta con cuantificadores

Denomínanse cualificadores a certos predicados que permiten utilizar subconsultas que devolven varias filas na columna correspondente a un atributo.

Por exemplo se se quere mostrar o soldo e nome dos empregados cun soldo que supera o de calquera empregado do departamento de vendas. A subconsulta necesaria para ese resultado mostraría todos os soldos do departamento de vendas. Pero non poderemos utilizar un operador de comparación directamente xa que esa subconsulta devolve máis dunha fila. A solución a isto é utilizar os cuantificadores entre o operador e a consulta, que permiten o uso de subconsultas de varias filas.

A sintaxe de uso dentro de condicións é a seguinte:

expresión operador\_relacional cuantificador {lista\_exps | subconsulta}

Os cuantificadores son:

- **ANY ou SOME:** A comparación cun ANY (ou SOME, equivalente) é verdadeira se o é para algún valor dos obtidos cunha subconsulta.

- **ALL.** Neste caso a comparación é verdadeira se o é con todos os valores devoltos pola consulta subordinada e falsa no caso contrario. Por exemplo: para saber o empregado co soldo máis alto de toda a empresa.

```
SELECT ENAME
FROM EMP
WHERE SAL > = ALL(SELECT SAL FROM EMP)
```

### **20.3.7 Operacións con consultas**

Existen certos operadores que permiten combinar os conxuntos de tuplas que se obteñen de dúas consultas SELECT e obter un novo conxunto de tuplas. Estas operacións corresponden con operadores da álgebra relacional e son os seguintes:

- UNION e UNION ALL realizan a unión das tuplas obtidas por dúas consultas que se especifican como operandos. UNION non inclúe as tuplas repetidas mentres que UNION ALL si as inclúe. UNION corresponde á unión de relacións da álgebra relacional.

Para iso ambas as dúas instrucións teñen que utilizar o mesmo número e tipo de columnas

```
SELECT nome FROM empregados
UNION
SELECT nome FROM visitantes
```

Isto crea unha táboa que inclúe os nomes dos empregados e visitantes

- INTERSECT permite unir dúas consultas SELECT de modo que o resultado serán as filas que estean presentes en ambas as dúas consultas. Equivale ao operador intersección da álgebra relacional.

```
SELECT tipo,modelo FROM produtos
WHERE chip="QWER-21"
INTERSECT
SELECT tipo,modelo FROM produtos
```

```
WHERE chip="WDFV-23"
```

- MINUS combina dúas consultas SELECT de forma que aparecerán os rexistros do primeiro SELECT que non estean presentes no segundo. Corresponde á diferenza da álgebra relacional.

```
SELECT tipo,modelo FROM produtos
```

```
WHERE chip="QWER-21"
```

**MINUS**

```
SELECT tipo,modelo FROM produtos
```

```
WHERE chip="WDFV-23"
```

As dúas consultas sobre as que se aplique calquera destes operadores deben devolver tuplas coa mesma estrutura.

## **20.4.- DCL. LINGUAXE DE CONTROL DE DATOS**

Co nome de linguaxe de control de datos (DCL Data Control Language) faise referencia á parte da linguaxe SQL que se ocupa dos apartados de seguridade e da integridade no procesamento concorrente.

### **20.4.1 Seguridade**

A linguaxe SQL supón un nivel xeral de seguridade do software xestor da base de datos e as súas sentenzas utilízanse para especificar restricións de seguridade. O esquema de seguridade SQL baséase en tres conceptos:

- Os usuarios son os actores da base de datos. Cada vez que o xestor da base de datos recupera, insire, suprime ou actualiza datos, faino a conta dalgún usuario.
- Os obxectos da base de datos son os elementos aos cales se pode aplicar a protección de seguridade SQL. A seguridade aplícase xeralmente a táboas, vistas e columnas

- Os privilexios son as accións que un usuario ten permitido efectuar para un determinado obxecto da base de datos.

A creación e eliminación de usuarios en SQL non é estándar, dependendo de cada produto comercial. Non obstante, a concesión e revogación de privilexios se é estándar e está recollida nas sentenzas GRANT e REVOKE.

### **Concesión de privilexios: GRANT**

A sentenza GRANT utilízase para conceder privilexios de seguridade sobre obxectos da base de datos a usuarios específicos. Normalmente a sentenza GRANT é utilizada polo propietario da táboa ou vista para proporcionar a outros usuarios acceso aos datos. A sentenza GRANT inclúe unha lista específica dos privilexios a conceder, o nome do obxecto ao cal se aplican os privilexios e a lista de usuarios aos cales se conceden os privilexios. A sintaxe é a seguinte:

```
GRANT listaPrivilexios  
ON listaObxectos  
TO listaUsuarios  
[WITH GRANT OPTION]
```

- ListaPrivilexios: Concédense todos (ALL) ou un subconxunto de privilexios (separados por comas) que permiten borrar, inserir, consultar, actualizar ou modificar (DELETE, INSERT, SELECT, UPDATE, ALTER) unha táboa, vista ou un conxunto delas.
- ListaObxectos: Obxectos aos que se lle aplican os privilexios.
- ListaUsuarios: Concédense a todos os usuarios (PUBLIC) ou a unha lista de usuarios.
- WITH GRANT OPTION: Indica que aqueles usuarios aos que se concedeu estes privilexios poden á súa vez concedelos (nunca máis dos que se teñen actualmente) a outros usuarios por medio de sentenzas GRANT.



Por norma xeral os privilexios de acceso aplícanse sobre todas as columnas na táboa ou vista, pero tamén se pode especificar unha lista de columnas co privilexio UPDATE.

```
GRANT UPDATE (SAL) ON EMP TO grupoNóminas
```

Só o propietario dun obxecto pode conceder os privilexios deste. O propietario é sempre o creador deste.

As operacións co esquema da base de datos (CREATE, DROP, etc.) só poden ser realizadas polo propietario do esquema.

### **Revogación de privilexios: REVOKE**

Os privilexios que se concederon coa sentenza GRANT poden ser retirados coa sentenza REVOKE. A sentenza REVOKE ten unha estrutura que se asemella estreitamente á sentenza GRANT, especificando un conxunto específico de privilexios que deben ser revogados, para un obxecto da base de datos específico, para un ou máis usuarios. Unha sentenza REVOKE pode retirar todos ou parte dos privilexios que previamente se concederon a un usuario. É necesario especificar que un usuario só pode retirar os privilexios que el mesmo lle concedeu a outro usuario.

```
REVOKE ListaPrivilexios  
ON ListaObxectos  
FROM ListaUsuarios
```

A utilización de vistas combinada cunha definición de usuarios e unha concesión xuízosa de privilexios constitúe o mecanismo de seguridade que o administrador da base de datos SQL utiliza para levar a cabo as políticas de seguridade do sistema.

### **20.4.2 Transaccións**

Enténdese por transacción o efecto producido por un grupo de instrucións DML executadas unha tras outra, é dicir, unha transacción é un conxunto de accións que ou ben se realizan todas, ou ben non se realiza ningunha.

En SQL unha transacción comeza implicitamente na primeira instrución que altera o estado da información almacenada na base de datos. Para preservar as propiedades ACID (Atomic, Consistent, Isolate, Durable) dunha transacción, SQL dispón de dúas sentenzas que permiten que os cambios realizados por unha transacción queden reflectidos permanentemente na base de datos (comprometer)

- COMMIT [WORK]. Remata a transacción actual gravando permanentemente as modificacións.
- ROLLBACK [WORK]. Obriga o sistema a volver ao estado anterior ao inicio da transacción.

Tamén é posible que cada ámbito de programación e/ou SXBD dispoña de elementos adicionais para o control de concorrencia que poidan ser utilizados polo usuario, como por exemplo bloqueos.

Dende o momento en que a unha base de datos poden acceder diferentes usuarios ao mesmo tempo, en cada instante poderemos ter distintas transaccións que manipulen a base de datos á vez.

As transaccións especifican un nivel de illamento que define o grao en que se debe illar unha transacción das modificacións de recursos ou datos realizadas por outras transaccións. En teoría, toda transacción debe estar completamente illada doutras transaccións, pero na realidade, por razóns prácticas, isto pode non ser certo sempre. Os niveis de illamento descríbense en canto aos efectos secundarios da simultaneidade que se permiten, como as lecturas desfasadas ou ficticias.

O estándar SQL define catro niveis de illamento transaccional en función de tres eventos que son permitidos ou non dependendo do nivel de illamento. Estes eventos son:

- *Lectura sucia.* As sentenzas SELECT son executadas sen realizar bloqueos, pero podería usarse unha versión anterior dun rexistro. Polo tanto, as lecturas non son consistentes ao usar este nivel de illamento.
- *Lectura non repetible.* Unha transacción volve ler datos que previamente lera e encontra que foron modificados ou eliminados por unha transacción cursada.
- *Lectura fantasma.* Unha transacción volve executar unha consulta, devolvendo un conxunto de rexistros que satisfán unha condición de busca e encontra que outros rexistros que satisfán a condición foron inseridos por outra transacción cursada.

Os niveis de illamento SQL defínense sobre a base de se permiten cada un dos eventos definidos anteriormente.

Niveis de illamento:

<b>Nivel de illamento</b>	<b>Comportamento Permitido</b>		
	Lect. Sucia	Lect. Non Repetible	Lect. Fantasma
Lectura non confirmada	SI	SI	SI
Lectura confirmada	NON	SI	SI
Lectura repetible	NON	NON	SI
Serializable	NON	NON	NON

A sentenza para controlar o nivel de illamento en SQL é:

```
SET TRANSACTION ISOLATION LEVEL {READ UNCOMMITTED | READ COMMITTED | REPEATABLE READ | SERIALIZABLE }
```

- **READ UNCOMMITTED.** Especifica que as instrucións poden ler filas que foron modificadas por outras transaccións pero aínda non se confirmaron.
- **READ COMMITTED.** Especifica que as instrucións non poden ler datos que fosen modificados.
- **REPEATABLE READ.** Especifica que as instrucións non poden ler datos que foron modificados pero aínda non confirmados por outras transaccións e que ningunha outra transacción pode modificar os datos lidos pola transacción actual ata que esta finalice.
- **SERIALIZABLE.** Especifica que as instrucións non poden ler datos que fosen modificados, pero aínda non confirmados, por outras transaccións. Ningunha outra transacción pode modificar os datos lidos pola transacción actual ata que a 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. Oitava Edición. Pearson. Prentice Hall.
- Piattiani, Esparza Marcos, Caleiro 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 Rodríguez Martínez

Subdirector de Sistemas Escola Superior Enxeñaría Informática Ourense

Colexiado do CPEIG

# **21. SISTEMAS CRM (CUSTOMER RELATIONSHIP MANAGEMENT) E ERP (ENTERPRISE RESOURCE PLANNING). A INFORMATIZACIÓN DOS PROCEDEMENTOS. BPM (BUSINESS PROCESS MANAGEMENT). SISTEMAS DE XESTIÓN DOCUMENTAL. XESTIÓN DO COÑECEMENTO.**



## Tema 21: CRM. ERP. BPM. Sistemas de Xestión Documental. Xestión do Coñecemento.

### ÍNDICE

<b>21.1. CRM.....</b>	<b>1</b>
21.1.1. Definición de CRM (Customer Relationship Management).....	1
21.1.2. Principios de CRM.....	4
21.1.3. Historia de CRM.....	5
21.1.4. Proceso de Formación CRM.....	7
21.1.5. Avaliación do CRM .....	9
21.1.6. Consideracións sobre a implantación dun CRM.....	10
<b>21.2. ERP.....</b>	<b>11</b>
21.2.1. Definición de ERP (Enterprise Resource Planning).....	11
21.2.2. Obxectivos da implantación dun ERP.....	12
21.2.3. Arquitectura dun ERP.....	13
21.2.4. Principais Módulos dun ERP.....	17
21.2.5. Implantación.....	20
<b>21.3. BPM.....</b>	<b>23</b>
21.3.1. Definición de BPM.....	23
21.3.2. Estrutura do BPM.....	23
21.3.3. Obxectivos da aplicación.....	24
21.3.4. BPM e Workflow.....	24
21.3.5. BI x BPM.....	25
<b>21.4. Sistemas de Xestión Documental.....</b>	<b>27</b>
21.4.1. Definición de Sistemas de Xestión Documental.....	27
21.4.2. Funcións da Xestión documental.....	28
21.4.3. Ciclo de Vida dos Documentos.....	29
21.4.4. Beneficios da Xestión Documental.....	30
<b>21.5. Xestión do Coñecemento.....</b>	<b>31</b>
21.5.1. Definición de Xestión do Coñecemento.....	31
21.5.2. Cuestións sobre xestión do coñecemento.....	32
<b>21.6. Bibliografía.....</b>	<b>34</b>

### **21.1. CRM**

#### **21.1.1. Definición de CRM (Customer Relationship Management)**

Antes de comezar a examinar os fundamentos conceptuais de CRM, cómpre definir que é CRM. Unha estreita perspectiva da xestión de relacións cos clientes é o marketing de bases de datos, facendo fincapé nos aspectos promocionais do

marketing vinculados aos esforzos de base de datos.

Outro estreito e relevante punto de vista é considerar CRM só como a retención de clientes no que se utiliza unha variedade de tácticas de marketing para conseguir os clientes ou manterse en contacto con eles despois de que a venda se realice.

Pódese definir o marketing relacional como *"un esforzo integrado para identificar, manter e construír unha rede entre os consumidores particulares e fortalecer continuamente a rede para o beneficio mutuo de ambas partes, a través de contactos interactivos, individualizados e de valor engadido nun período de tempo"*.

O tema central de todos os CRM e as perspectivas de marketing de relacións é que se centra nas relacións de cooperación e de colaboración entre a empresa e os seus clientes, e mesmo con outros posibles actores de marketing.

CRM baséase na premisa de que, ao ter unha mellor comprensión das necesidades dos clientes e dos seus desexos, poderemos mantelos por máis tempo e venderlles máis.

Realizáronse unha serie de análises estatísticas dos datos de satisfacción de clientes que abarcan os resultados de máis de 20.000 enquisas a clientes realizadas en 40 países.

As conclusións deste estudo foron:

- i. Un cliente totalmente satisfeito contribúe 2,6 veces máis aos ingresos da empresa ca un cliente pouco satisfeito.
- ii. Un cliente totalmente satisfeito contribúe con 17 veces máis ingresos ca un cliente algo insatisfeito.
- iii. Un cliente totalmente insatisfeito reduce os ingresos nunha taxa igual a 1,8 veces o que un cliente totalmente satisfeito contribúe a unha empresa.





- iv. Reducir a deserción de clientes (polo menos nun 5%) traducirase en aumento dos beneficios entre un 25% a 85%, dependendo do tipo de industria de que se trate.

Un aspecto importante do CRM é a selección dos clientes. Como varios estudos demostraron, non todos os clientes son igual de rendibles (de feito, nalgúns casos o 80% das vendas veñen a través dun 20% dos clientes). A empresa polo tanto, debe ser selectiva e adaptar os seus programas e esforzos de marketing á segmentación e selección dos clientes apropiados.

Nalgúns casos, podería mesmo levarse a cabo a "*subcontratación dalgúns clientes*" para que a empresa empregue mellor os seus recursos naqueles clientes que poden servir mellor e crear valor mutuo. Con todo, o obxectivo dunha empresa non é minguar a súa base de clientes, senón identificar os programas apropiados para os clientes, os métodos que sexan rendibles e crear valor para a empresa e o cliente. Polo tanto, o CRM defínese como:

*"Unha estratexia integral e un proceso de adquisición, retención e asociación cos clientes selectivos para crear un valor superior tanto para a empresa como para o cliente."*

Como está implícito na definición anterior, o propósito de CRM é mellorar a produtividade do marketing. A produtividade do marketing lógrase mediante unha eficiencia cada vez maior na comercialización e pola mellora da eficacia do marketing. En CRM, a eficiencia do marketing lógrase grazas aos procesos de cooperación e colaboración o que permitirá reducir os custos de transacción e os custos xerais de desenvolvemento para a empresa. Dous importantes procesos de CRM son o desenvolvemento proactivo do negocio do cliente e a construción de relacións coa maioría dos clientes importantes. Estas situacións conducen á creación dun valor superior.

O concepto básico é que o cliente non é alguén fóra da organización senón que é unha parte da organización.

### **21.1.2. Principios de CRM**

#### Diferenciar os clientes:

- Non todos os clientes son iguais.
- É importante recoñecer e premiar a os mellores clientes.
- Cada cliente vólvese particularmente importante.
- Para o mesmo produto ou servizo non todos os clientes poden ser tratados por igual e o CRM debe saber distinguir entre un cliente de alto valor e un cliente de baixo valor.

Para diferenciar aos clientes é necesario que o CRM os entenda nos seguintes aspectos:

- Sensibilidade, gustos, preferencias e personalidades.
- Estilo de vida e idade.
- Nivel de cultura e educación.
- Características físicas e psicolóxicas.

Hai que diferenciar os distintos tipos de situacións:

- i. Clientes de baixo valor que requiren un gran investimento.
- ii. Clientes de baixo valor con potencial de converterse en clientes con alto valor nun futuro próximo.
- iii. Clientes de alto valor que requiren de servizos de alto valor.
- iv. Clientes de alto valor que requiren de servizos de baixo valor.

*Manter os clientes existentes:*

Establecer unha clasificación dos clientes entre, *moi satisfeitos* e *moi decepcionados* axuda á organización a mellorar os niveis de satisfacción dos clientes e os resultados que se ofrecen. A medida que o nivel de satisfacción de cada cliente mellora, tamén mellorará a permanencia dos clientes coa empresa.

- *Maximizar o valor de tempo:* Se se conseguen identificar circunstancias como a etapa da vida ou o evento que desencadeou a necesidade no cliente, os vendedores poden maximizar a probabilidade de realizar unha venda.
- *Aumentar a lealdade:* Os clientes leais son máis rendibles. Hai que innovar e satisfacer as necesidades dos clientes para que permanezan vinculados á empresa.

### **21.1.3. Historia de CRM**

Mirando cara atrás na historia dunha instantánea de marketing, podemos ver a seguinte evolución e clara progresión:

- 1960: a era do marketing masivo.
- 1970: comezo da segmentación, campañas de correo directo e telemarketing.
- 1980: expansión do marketing Niche (localizar un pequeno segmento do mercado e crear un produto ou servizo para ese segmento).
- 1990: marketing Relacional. O “boom” dos centros de telemarketing. Desenvolvemento das relacións cos clientes. Recoñecemento do verdadeiro valor da lealdade.

O desenvolvemento da relación co cliente ten antecedentes históricos que se remontan á era industrial: do mesmo xeito que os artesáns adoitaban desenvolver produtos á medida para cada cliente, esta interacción directa conduciu á vinculación relacional entre o produtor e o consumidor.

Na era industrial, coa produción masiva e a chegada dos intermediarios non había interaccións frecuentes entre os produtores e os consumidores. Nos últimos anos con todo, varios factores contribuíron ao rápido desenvolvemento e evolución de CRM. Estes inclúen:

- O crecente proceso de des-intermediación en moitas industrias debido á aparición de novidosas tecnoloxías informáticas que permiten aos produtores interactuar directamente cos clientes finais. Por exemplo, en moitas industrias, tales como aeroliñas, software do fogar e mesmo de consumo, o proceso de intermediación está cambiando rapidamente a natureza do marketing e volvendo o marketing relacional moito máis popular.
- Os avances na tecnoloxía da información, redes e tecnoloxías de fabricación axudaron ás empresas a poñerse ao nivel da competencia. Como resultado a calidade do produto e o custo xa non son importantes vantaxes competitivas.
- O crecemento da economía de servizos. Dado que os servizos adoitan ser producidos e entregados na mesma institución, minimízase o papel dos intermediarios.
- Outra forza impulsora da adopción de CRM foi o movemento de calidade total. Cando as empresas adoptaron o TQM fíxose necesaria a participación de clientes e provedores na execución do programa a todos os niveis da cadea de valor. Isto necesita unha estreita relación de traballo cos clientes.



- As expectativas dos clientes están cambiando case a diario. Os clientes agora elixen a forma de comunicarse coas empresas a través de diversas canles dispoñibles. Tamén hoxe en día os consumidores esperan un alto grao de personalización.
- Importancia do tempo real. As canles interactivas como o correo electrónico, caixeiros automáticos e centros de chamadas débense sincronizar coas actividades do cliente. A velocidade do cambio dos negocios require flexibilidade e unha rápida adopción das tecnoloxías.
- Na actual era da competencia, os comerciantes vense obrigados a estar máis preocupados pola retención de clientes e fidelización de clientes.
- Como varias investigacións descubriron, reter aos clientes é menos custoso e é, de feito, unha vantaxe competitiva sostible maior que a adquisición doutros novos.
- É máis vantaxoso desenvolver relacións máis estreitas cuns poucos provedores que desenvolver máis provedores con relacións máis impersonais.
- Ademais os vendedores preocúpanse de manter ao cliente durante un longo período en lugar de por unha venda esporádica.
- A globalización dos mercados mundiais fai que sexa necesaria a xestión de contas globais para os clientes.

#### **21.1.4.      *Proceso de Formación CRM***

No proceso de formación, as tres áreas de decisión máis importantes son:

- A definición do propósito que se ten para (ou obxectivos) usar un CRM.
- A elección das partes (ou parellas dos clientes) para os programas de CRM apropiados.
- O desenvolvemento de programas (ou esquemas relacionais de actividade) para a participación de relación co cliente.

### Propósito de CRM

O obxectivo xeral de CRM é mellorar a produtividade do marketing e mellorar o valor para as partes que participan na relación. Ao perseguir e conseguir os obxectivos operacionais, tales como a redución dos custos de distribución, a racionalización do procesamento de pedidos, a xestión de inventario, a redución do custo de adquisición de clientes e a retención de clientes, as empresas poderían lograr unha maior eficiencia de marketing.

Pódese mellorar a efectividade do marketing con:

- Unha coidadosa selección dos clientes para os seus distintos programas.
- A individualización e a personalización da oferta de mercado para anticipar e satisfacer as necesidades emerxentes dos clientes.
- A construción da lealdade e o compromiso do cliente.
- A asociación para entrar en novos mercados e desenvolver novos produtos.
- A redefinición do campo de xogo competitivo para a empresa.

Deste xeito, indicando os obxectivos e definindo o propósito do CRM nunha empresa, axuda a clarificar a natureza dos programas de CRM e as actividades que deben levar a cabo os socios.

A definición do propósito tamén axudará na identificación dos socios adecuados, relacionando as expectativas e capacidades necesarias para cumprir coas metas comúns. Ademais, a definición do propósito axudará a avaliar o desempeño do CRM mediante a comparación dos resultados obtidos cos obxectivos. Estes obxectivos poden ser especificados como obxectivos financeiros, obxectivos de marketing, obxectivos estratéxicos, obxectivos operativos e os obxectivos xerais.

### Partes da relación

Na fase inicial, unha empresa ten que decidir que tipo de clientes, de clientes específicos ou de grupos de clientes serán o foco das súas actividades de CRM.

### Programas CRM

Unha revisión coidadosa da literatura e a observación das prácticas empresariais suxiren que hai tres tipos de programas de CRM:

- Marketing continuo
- Marketing un a un
- Programas de asociación.

Estes adoptan diferentes formas dependendo de se están destinados aos consumidores finais, a consumidores-distribuidores ou clientes empresa-a-empresa.

#### **21.1.5. Avaliación do CRM**

Sen as medidas de rendemento adecuadas para avaliar os esforzos de CRM é difícil tomar decisións obxectivas respecto da continuación, modificación, mellora ou finalización dos programas de CRM.

Se a relación cos clientes é tratada como un activo intanxible da empresa, a súa valoración económica pode ser avaliada utilizando os fluxos de efectivo futuros.

Outra das medidas globais que utilizan as empresas para supervisar o rendemento de CRM é a medición da satisfacción da relación co cliente.

Mediante a medición de satisfacción da relación, poderíase estimar a tendencia de inclinación de calquera das partes de continuar ou terminar a relación. Esta tendencia

tamén podería ser estimada indirectamente mediante a medición da lealdade do cliente.

#### **21.1.6. Consideracións sobre a implantación dun CRM**

Un dos aspectos máis interesantes do desenvolvemento de CRM é a multitude de interfaces de cliente que na actualidade ten unha empresa para xestionar. Ata hai pouco, a interface directa das empresa cos clientes era principalmente a través do persoal de vendas ou axentes de servizo.

Na contorna actual a maioría das empresas interactúan cos seus clientes a través dunha gran variedade de canles, incluíndo persoal de vendas, persoal de servizo, centros de atención telefónica, páxinas de Internet, contas en redes sociais, departamentos de marketing, etc. Para grandes clientes tamén se inclúen funcións cruzadas, isto é, equipos que poden incluír ao persoal de varios departamentos funcionais. Aínda que cada unha destas unidades pode funcionar de xeito independente, comparten información sobre clientes individuais e as súas interaccións coa empresa en tempo real. Por exemplo, un cliente que acaba de realizar un pedido a través Internet e, posteriormente, chama ao centro de chamadas para a verificación de pedidos, espera que o persoal do centro de chamadas coñeza os detalles da historia da súa orde.

Polo tanto, CRM eficaz require dun sistema de información de primeira liña que comparta información relevante dos clientes entre todos os departamentos funcionais. As bases de datos e as ferramentas de minería de datos son moi valiosas tanto para os sistemas de CRM.

Con todo, o desafío consiste en desenvolver unha plataforma CRM integrada que recolla os datos de entrada correspondentes a cada interface de cliente e, ao mesmo tempo, ofrezca a información adecuada sobre a estratexia precisa para gañar





a lealdade do devandito cliente. Por exemplo, se o persoal do centro de chamadas non pode identificar ou diferenciar un cliente de alto valor, entón sería unha tremenda perda de oportunidade para a compañía.

## **21.2. ERP**

### **21.2.1. Definición de ERP (Enterprise Resource Planning)**

Actualmente, na sociedade da información, o activo máis importante para unha empresa é a información. Os procesos ou sistemas que se empregue en cada empresa e como se traballe con esa información é o que distinguirá a unhas empresas doutras, e fará que as empresas consigan ou non beneficios. Polo tanto, é obvio, que resulta fundamental para unha empresa ter uns sistemas de tratamento de información actualizados e modernos que axuden nos procesos de negocio a reducir tempos, a diminuír custos, etc.

Nas PEME adóitanse usar distintos sistemas software para automatizar distintas tarefas e funcións por separado, aínda que isto non se considera realmente eficiente. Para resolver os problemas que poden existir pola mala comunicación dos distintos sistemas, xorden os Sistemas de Xestión Empresarial ou ERP (Enterprise Resource Planning), que se poden definir como *un paquete de software que integra toda a xestión da empresa* (financeira, de produción, loxística, comercial e de recursos humanos). Os ERP están deseñados para modelar e automatizar a maioría dos procesos básicos da empresa, desde a xestión financeira ata a produción nun único sistema de información.

Os ERP son **sistemas transaccionais**, é dicir, están deseñados para traballar con procesos da empresa, soportalos, procesar os datos e obter deles información específica.

Un ERP permite xestionar de xeito eficiente e integrado a información da empresa,

permitindo a comunicación das diferentes áreas do negocio mediante procesos electrónicos. A función principal dun ERP é estandarizar e organizar os datos internos e procesos da empresa, converténdoo en información útil para o proceso de toma de decisións. Con todo, é necesario ter en conta que aínda que estes sistemas apoian o proceso de toma de decisións, a decisión final é dos administradores que son os que teñen a responsabilidade de facer o máis adecuado para a empresa en cada momento.

Algunhas das principais características dun ERP son:

- Integrables
- Interfaces con outras aplicacións
- Modulares
- Multiplataforma
- Optimizan as operacións das empresas, permitíndolles avaliar, implantar e xestionar máis facilmente o seu negocio
- Sistemas abertos
- Universais

Os sistemas ERP actualmente xa se usan en todo tipo de empresas, xa sexan grandes ou de pequeno tamaño. Con todo, ao principio os sistemas ERP só se usaban en grandes empresas con múltiples fábricas e socios ao redor do mundo. Nestas grandes empresas os sistemas ERP empregaban diferentes linguaxes, tipos de moeda e soportaban operacións tanto centralizadas, como descentralizadas ou multi-sitio.

*Un sistema ERP é un tipo de software que permite á compañía integrar os procesos de negocio dunha empresa, acceder á información en tempo real e producir e compartir datos.*

### **21.2.2. Obxectivos da implantación dun ERP**

Ao decidir implantar un ERP, adóitase facer con algún ou varios dos seguintes obxectivos:

- Consegir un alto grao de integración de datos.
- Consegir acceso a información precisa e fiable. Ter toda a información centralizada baixo un mesmo sistema garante que os datos serán correctos.
- Optimización dos procesos empresariais. Un proceso empresarial é unha actividade que ofrece unha serie de saídas con certo valor engadido a partir dunhas entradas. A implantación dun ERP pretende mellorar estes procesos diminuindo os custos dos mesmos e aumentando a produtividade.
- Posibilidade de compartir información entre todos os compoñentes da organización. Cun ERP a información está dispoñible para todos e elimínase a redundancia dos datos.
- Supresión de datos e operacións innecesarias. Tendo información compartida, as operacións como a procura de datos a través dos diferentes sistemas deixan de ser necesarias.
- Redución de tempos e custos dos procesos.

### **21.2.3.      *Arquitectura dun ERP***

Xeralmente a arquitectura dos ERP adoitan coincidir nos seguintes aspectos:

- Base de datos común que favorece a coherencia de datos e a integración dos datos xerados.
- Arquitectura modular. Cada módulo céntrase nun proceso diferente da empresa como recursos humanos, vendas, produción, etc.
- Interconexión de módulos.

Os ERP ao ser modulares permiten que a implantación do sistema se realice por etapas, de tal xeito que o impacto na organización é menor, de cada transacción con respecto ao sistema anterior. Xeralmente ao implantar un ERP empézase polo

departamento financeiro e aos poucos vanse integrando os outros departamentos.

A arquitectura básica dun ERP componse de:

- Aplicacións técnicas.
- Arquitectura para dar soporte ao resto de módulos.
- Ferramentas de administración para todo o sistema.

Cada provedor dun sistema ERP define o nivel de modularidade do seu produto, non existindo un estándar global. De feito cada provedor en función da súa política comercial ou técnica decide que módulos desenvolve e como os vai a integrar.

### *1. Características da arquitectura dun ERP*

#### **Modelo Cliente-Servidor**

Os ERP seguen un modelo cliente-servidor, onde o devandito servidor almacena os datos dos que fan uso os distintos programas.

O servidor debe permitir:

- Autorización de privilexios de cada cliente.
- Autenticación da identidade do cliente.
- Privacidade e seguridade dos datos.
- Protección dos recursos de rede.

#### **Flexibilidade**

O software do ERP debe ser flexible e:

- Incorporar un sistema de configuración.
- Permitir adaptarse ás necesidades da empresa.

### **Modularidade**

Un ERP divídese nunha serie de módulos que se caracterizan por:

- Presentan unha interface común.
- Cada módulo implanta a funcionalidade dunha área en concreto.
- Os módulos deben ser facilmente integrables entre si.
- Facilitade na aprendizaxe e redución do custo. Ao tratarse de sistemas modulares e manexarse estes de forma similar, a formación do persoal é máis rápida.

### **Integración**

Nun ERP tense unha base de datos común que garante a integridade dos datos e elimina a redundancia. Desta forma a empresa vese como un único sistema onde a información que se actualice nun punto, quedará actualizada para o resto de devandito sistema.

### **Seguridade**

De cara a un sistema ERP podemos considerar dous tipos de seguridade:

- 1.Privilexios de acceso á aplicación: os usuario executarán unicamente aquelas aplicacións que sexan imprescindibles para o seu traballo e ningunha máis.
- 2.Privilexios de acceso a datos: estarán xestionados polos SGBD ou directamente pola aplicación. Un SGBD ten como obxectivo garantir que os datos que contén só estean dispoñibles para as persoas autorizadas.

Para garantir a seguridade utilízanse algunhas ou varias destas técnicas:

- Identificación de usuario. Ao identificar ao usuario obtense a lista de recursos do sistema aos que o devandito usuario ten acceso ademais de que operacións pode realizar sobre os devanditos recursos.
- Determinación de accesos permitidos.



- Lista de autorizacións que identifican os datos accesibles e as operacións posibles sobre os mesmos.
- Establecemento de distintos niveis de autorización, de tal forma que todos os usuarios dun grupo ou nivel poderán realizar as mesmas operacións.

### **Interface de Usuario**

A interface permite a comunicación entre o usuario e o sistema. Existen dous tipos de interfaces de usuario.

- Interface gráfica. A interface gráfica ofrece un acceso homoxéneo a todos os módulos do sistema.
- Interface por consola (baseada en comandos). A interacción baséase nunha serie de ordes que se transmiten entre o usuario e o sistema mediante un teclado.

### **Simulación**

Mediante a simulación pódese saber cales serán as consecuencias dunha decisión, o que resulta de gran valor para saber se se debe ou non adoptar esa decisión.

A simulación adóitase empregar en:

- *Planificación financeira:* pódense obter os gráficos dos efectos dos plans de produción. Pódense realizar informes sobre a previsión de stock ou ata qué punto se cobren custos.
- *Custos de actividade:* pódense calcular as consecuencias dun posible cambio no sistema.
- *Planificación das necesidades materiais:* pódense simular fluxos de bens para decidir que artigos se deben fabricar, cales adquirir, etc.



- *Plan de producción:* pódense obter distintos plans de produción de distintos produtos para avaliar a viabilidade dos mesmos.
- *Planificación das necesidades de capacidades:* pódense simular as consecuencias de atrasos, traballar con prioridades, inclusión de traballo atrasado nun momento puntual, etc.

### **Trazabilidade**

Nun sistema, trátase de poder determinar que compoñentes participan na elaboración dos produtos finais e seguir os procesos de forma recursiva, determinando a orixe das materias primas, centros de traballo e operarios que participaron no proceso.

En caso dun produto defectuoso, a trazabilidade permite detectar o punto onde se produciu o erro e depurar responsabilidades.

### **Intercambio electrónico de datos**

O EDI permite establecer comunicación entre os socios de forma electrónica, enviándose pedidos, facturas, etc. Deste xeito se simplifica enormemente o feito de xestionar múltiples instalacións dunha mesma empresa.

#### **21.2.4. Principais Módulos dun ERP**

Os ERP compóñense dunha serie de módulos que se corresponden coas distintas áreas funcionais da empresa. O tipo, funcionalidade e extensión dos módulos dos distintos ERP son distintos, aínda que xeralmente todos os ERP conteñen os módulos básicos para o funcionamento e xestión da empresa.

De forma xeral os módulos cumpren coas seguintes características:

- Integración co resto dos módulos.



- Implantación no departamento onde se necesite.
- Autonomía propia.

Aínda que a implantación dun ERP pode realizarse de forma modular, a implantación dun conxunto de módulos incrementa de forma notable o éxito dun ERP empresarial.

A seguir comentaranse as características dos principais módulos presentes nun ERP.

- Vendas e Distribución (Loxística)

Este módulo permite levar a cabo as actividades de venda e distribución dos produtos.

Mediante as funcións dese módulo pódese:

- Información sobre as contas dos clientes
- Información sobre os pedidos e o seu estado
- Información sobre as facturas pendentes
- Control de calidade
- Administración de vendas
- Xestión de sistemas de transporte
- Control de calidade
- Xestión de compras
- ...

## 2. Producción e Fabricación

Os ERP implantan módulos de produción e fabricación que permiten empregar distintos métodos ou estratexias de produción en diferentes ambientes, como son:

- *Just In Time*
- Baixo stock
- Contra pedido
- Proxectados
- Procesos

Dentro do módulo de produción, permítense as seguintes funcionalidades:





- Planificar a produción
- Xestión das ordes de produción
- Xestión de custos
- Análises da produción
- Control da produción

### 3. Contabilidade e Finanzas

Trátase dun módulo moi importante que ofrece gran cantidade de informes sobre a situación económica da empresa.

Este módulo encárgase, entre outras, de operacións relacionadas con:

- *Xestión de Contas*: pódese realizar un control completo tanto dos pagos como dos cobros pendentes, a xestión de caixa e aboamentos.
- *Custos de actividade*: pódese realizar un control de gastos de cada actividade.
- *Contabilidade xeral*: pódense realizar todas as operacións que doutra forma deberían realizarse manualmente, así como os peches de fin de mes e anual.
- *Custos de recursos*: pódense tratar os gastos xerais directos mellorando estimación dos custos.
- *Tesourería*: pódense realizar todas operacións básicas de pagos e cobros.
- *Xestión de Nóminas*: pódense automatizar todas as tarefas relacionadas coas nóminas. Cálculo de impostos, pagos á Seguridade Social, horas extra, etc.
- *Xestión de contratos*: inclúen todas as actividades relacionadas con:
  - Auditoría de contratos.
  - Definición de contratos.
  - Confección de informes.
  - Cálculo de custos actuais e proxectados
  - Progreso da facturación.

### 4. Mantemento e Xestión de Proxectos

Este módulo axuda a optimizar a produción e na maioría dos casos inclúese no

módulo de loxística. Neste módulo inclúense:

- Xestión do mantemento e servizos
- Seguimento e control de proxectos.

### **5. Recursos Humanos**

Neste módulo intégranse as ferramentas para obter un coñecemento da contorna económica e administrativa do persoal. As accións que se realizan habitualmente con este módulo son as relacionadas con:

- Estatísticas de persoal
- Xeración de Nóminas
- Planificación de quendas e xestión de tempos
- Perfís profesionais dos traballadores
- Formación e desenvolvemento

### **21.2.5. *Implantación***

A implantación dun sistema ERP adoita ser complexa e custosa pola cantidade de recursos que engloba e os seus requisitos a nivel técnico e organizativo.

A implantación dun sistema ERP pode significar importantes cambios nos procesos internos, que poden ter repercusión tanto na estrutura organizativa como nas actividades e os postos de traballo da empresa. Por isto, para reducir os problemas derivados da implantación é fundamental que a formación dos empregados da organización sexa moi boa xa que se van converter nos usuarios do sistema, ademais estes deben participar activamente en todo o proceso de implantación e adaptación da ferramenta.

A implantación dun ERP iníciase cunha análise técnica e funcional, e cunha avaliación

das restricións económicas e temporais que poden influír na execución do proxecto. Nun primeiro momento débense analizar os distintos ERP dispoñibles no mercado e identificar cal se axusta máis ás necesidades da empresa.

Xa que logo, nesta primeira etapa da implantación hai que definir:

- Qué módulos se van implantar (Alcance funcional)
- Qué departamentos e procesos se verán afectados (Alcance organizativo)
- Viabilidade do proxecto considerando:
  - Orzamento dispoñible
  - Integración con outras plataformas e sistemas
  - Calendario de implantación

### *Factores de éxito*

Para ter éxito na implantación do ERP é necesario considerar unha serie de factores determinantes, como son:

- Ter unha clara definición dos obxectivos
- A empresa debe estar comprometida e informada do cambio en todos os departamentos e xerarquía da empresa
- Realizar unha planificación realista da implantación a todos os niveis
- Formación e soporte aos usuarios
- Boa documentación do sistema
  - Técnica
  - Procedementos
  - Usuario

Unha vez implantado o ERP o traballo non finaliza, senón que debe considerarse tamén o mantemento, actualización, cambios na situación legal, aparición de novos estándares, incorporación de novos módulos, etc.



## 6. Problemas na Implantación

Un sistema ERP ofrece moitas vantaxes a unha empresa, pero sempre tendo en conta o esforzo necesario e os requisitos para a súa implantación, non só a nivel económico senón técnico e de persoal.

Unha implantación de ERP pode fallar, os principais motivos polos que isto sucede adoitan ser algúns dos seguintes:

- Insuficiente formación dos usuarios
- Pouca vinculación de todas as áreas da empresa co proxecto
- A información é inexacta ou incompleta ao iniciar a implantación do novo sistema
- Cambio na administración da empresa mentres se está a producir a implantación
- Mala escolla dunha ferramenta ERP

## 7. Análise Económica

Un dos aspectos de maior influencia á hora de implantar un ERP é o económico. Dentro da análise económica é necesario ter en conta:

- Equipamento hardware e software necesario: identificar o hardware e software mínimo para a implantación do sistema, tanto no ámbito do cliente como do servidor.
- Licenzas do ERP: algúns sistemas de ERP son software libre e outras solucións son propietarias, é necesario considerar o custo destas licenzas e o tipo de tarifa que se vaia aplicar, por número de usuarios, intervalo temporal, etc.
- Formación do persoal e consultoría externa para a implantación.
- Gastos de mantemento do sistema ERP.
- Custos dos servizos de telecomunicacións.

### **21.3. BPM**

#### **21.3.1. Definición de BPM**

O *Business Process Management* ou BPM xurdiu nos Estados Unidos e empezou sendo usado principalmente por empresas interesadas en novas ferramentas para a implantación e o control de estratexias. BPM apareceu a partir do auxo que tivo a integración dos ERP nas grandes empresas privadas.

O propósito de BPM é controlar como todos os recursos da empresa, físicos, humanos, financeiros e tecnolóxicos, participan e se integran nas accións operacionais que levan cara ás metas organizacionais a partir da definición de prioridades.

BPM permite realizar unha xestión global dos procesos incluíndo a súa definición, análise, execución, seguimento e administración; ademais proporciona soporte para a interacción entre persoas e distintas ferramentas informáticas.

A meta dun sistema BPM é ter un rexistro dos procesos corporativos e mellorar tanto a produtividade como a eficiencia. As ferramentas BPM polo tanto, son aplicacións que avalían, analizan e optimizan a xestión dos procesos e, xa que logo, a xestión global do negocio.

#### **21.3.2. Estrutura do BPM**

Un sistema BPM debe dar soporte ás actividades básicas da xestión dunha empresa, como son:

- Definir unha estratexia para guiar o rendemento.
- Traducir esta estratexia en indicadores, obxectivos e metas.
- Guiar o progreso en relación coas metas.
- Avaliar as causas, no caso de que haxa metas non alcanzadas.
- Seleccionar e implantar accións correctivas.

Os sistemas BPM axudan á empresa a realizar un mellor control dos seus propios procesos, a modificalos cando é necesario e a realizar as tarefas importantes con maior eficiencia. Este tipo de sistemas permite ao usuario ter un maior control sobre a automatización de procesos.

### **21.3.3.      *Obxectivos da aplicación***

O obxectivo dun sistema BPM non é refacer sistemas herdados, senón automatizar fluxos de traballo para que se realicen de forma máis rápida e simple.

Outro aspecto relacionado directamente co BPM é a necesidade de reducir o ciclo de integración. A maioría das empresas xa teñen os seus sistemas montados, con maior ou menor nivel de complexidade. As ferramentas BPM extraen dos sistemas existentes as actividades que forman parte dos procesos, ademais de complementar e supervisar as aplicacións instaladas.

Logo de ser identificadas, estas actividades son almacenadas nun repositorio de procesos, así, cando a empresa decide cambiar ou elaborar un novo proceso, o BPM analiza o seu repositorio e emprega un modelo existente, o cal elimina a necesidade dunha personalización extremada das aplicacións, o que repercute no tempo de traballo e custos.

### **21.3.4.      *BPM e Workflow***

O BPM xorde a partir dos sistemas de *Workflow*, que apareceron a finais da década dos 80. Este tipo de ferramenta consiste nun conxunto de solucións software onde se inclúen todos os procesos que se necesitan para administrar o rendemento da empresa, as metodoloxías que guían a algúns procesos e os indicadores empregados

para avaliar o rendemento, tendo en conta os obxectivos operacionais e estratéxicos. A pesar do feito de que a orixe de BPM podémola atopar en *workflow*, a súa intención non é a de substituír a outros programas software.

Os sistemas de *workflow* tiñan a súa base na automatización do fluxo de traballo, pola súa banda o BPM permite que os usuarios reciban as tarefas que teñen que realizar xunto coas súas instrucións nos seus sistemas persoais.

Ademais, BPM permite realizar representacións gráficas de todos os tipos de trámites, fluxos e posibles desvíos, incluíndo separación de documentos, fluxos alternativos, etc.

As ferramentas de *Workflow* tendían a usar cada unha a súa propia notación gráfica, con todo, as ferramentas BPM, grazas á notación definida pola *Business Process Management Initiative*, adoitan empregar unha notación común, o que simplifica moito os procesos de formación dos usuarios.

Os sistemas de *Workflow* non incorporaban as operacións que se realizaban en sistemas externos a eles, con todo, grazas á evolución nas tecnoloxías de integración de sistemas, o BPM permite realizar, ademais do que facían os sistemas *Workflow*, unha transferencia de datos entre sistemas para que se poidan desempeñar tarefas automaticamente en sistemas externos e obter os resultados das devanditas accións.

#### **21.3.5. BI x BPM**

Aínda que BPM non é unha ferramenta estritamente estratéxica, como as solucións de *Business Intelligence* (BI), cuxo propósito é a axuda na toma de decisións, BPM pode coordinarse perfectamente con este tipo de ferramentas e mesmo suplir algunhas das súas carencias. Malia todo é importante ter en conta que son dous tipos de ferramentas distintas con propósitos diferentes.

BPM oríentase ao axuste da operación e das decisións estratéxicas dunha empresa. As

ferramentas de BI pola súa banda, polo menos as tradicionais, oriéntanse máis a realizar un seguimento do que xa sucedeu na empresa. Estas solucións de BPM traballan cunha visión máis ampla da empresa que o BI, que se orienta a un ámbito departamental.

BPM ten un enfoque cara á oportunidade e é proactivo, ademais de incorporar e analizar información e alertas en tempo real; pola súa banda BI é reactivo e opera con informacións históricas da empresa.

BPM céntrase no control das actividades que foron identificadas para un proceso, as cales xerarán datos e informacións que deben ser estudados e consolidados como indicadores, que é o que empregan as ferramentas de BI, xunto con outros datos, para producir informes de apoio á toma de decisións.

As solucións BI oriéntanse a analizar o rendemento e actuación actual e pasada da empresa, mentres que o BPM oriéntase cara á avaliación da situación actual e futuro, sendo polo tanto ferramentas complementarias .

Así, queda claro que BI e BPM son conceptos distintos e complementarios.



## **21.4. SISTEMAS DE XESTIÓN DOCUMENTAL**

### **21.4.1. Definición de Sistemas de Xestión Documental**

Un sistema de xestión documental defínese como un conxunto de elementos e relacións entre eles que ten o propósito de normalizar, controlar e coordinar todas as actividades e procesos que afectan en calquera medida aos documentos xerados no transcurso da actividade dunha organización. As operacións máis habituais que se realizan sobre estes documentos abarcan todo o seu ciclo de vida, desde a súa creación ata o seu almacenamento e posta a disposición dos usuarios.

Ademais, un sistema de xestión documental ten que satisfacer o seguinte:

- Conservar os atributos básicos dos documentos, que lles confiren o seu valor informativo, legal e probatorio.
  - Orixinalidade
  - Autenticidade
  - Integridade
  - Veracidade
- Manter a organización dos documentos integrados nun contexto. Isto implica conservar unha interrelación cos outros documentos que xorden da mesma función, actividade, que son producidos polo mesmo departamento ou organismo, que forman parte da mesma serie, etc.

#### *Software de xestión documental*

O software de xestión documental abrangue todos aqueles programas software deseñados para xestionar grandes cantidades de documentos. Nestes documentos

non necesariamente debe existir organización dentro dos seus contidos, de feito, o máis común é que o contido destes documentos non garde unha organización clara.

Existen diversos métodos que utilizados en combinación coas bibliotecas de documentos e unha serie de índices, permiten un acceso rápido á información almacenada nos devanditos documentos, os cales, habitualmente están comprimidos e adoitan almacenar, ademais do texto plano, outros contidos multimedia como imaxes, vídeos, etc.

Entre os obxectivos que se perseguen á hora de implantar uns sistemas de xestión documental cómpre mencionar:

- Salientar a importancia que teñen os documentos dentro de calquera tipo de organización, pública ou privada.
- Facilitar a recuperación de información de forma rápida, exacta e efectiva.
- Analizar a produción documental, para evitar documentos innecesarios ou que non paga a pena almacenar pasado certo tempo.
- Conseguir que os arquivos sexan útiles e significativos como unidades de información non só dentro da empresa senón tamén externamente.

Antes de montar un sistema de xestión documental é necesario realizar unha serie de consideracións previas que podemos agrupar nas seguintes categorías:

- Administrativas: céntrase todo o que pode influír na administración da empresa.
- Económicas: refírese á avaliación do aforro que xera a xestión de documentos.

Para a implantación deste tipo de sistema, é necesario tamén realizar un diagnóstico e unha avaliación dos requisitos tanto técnicos como administrativos.

#### **21.4.2. Funcións da Xestión documental**

As principais funcións da xestión documental son:

- Almacenamento
- Captura
- Conservación
- Consulta
- Creación
- Difusión
- Eliminación
- Ingreso
- Uso

#### ***21.4.3. Ciclo de Vida dos Documentos***

O ciclo de vida dun documento abarca todas as fases polas que un documento pasa, desde que se crea ata que se arquiva ou elimina.

Os documentos poden ter distintos valores que son:

- *Valor Primario (Administrativo)*: o seu propósito é deixar constancia dunha actividade.
  - Valor fiscal ou contable: acreditar o cumprimento das obrigas contables ou tributarias.
  - Valor legal ou xurídico: a súa finalidade é, entre outras, servir de proba ante a lei.
- *Valor Secundario*:
  - Valor Informativo: o seu propósito é servir de base para a reconstrución de calquera actividade realizada.
  - Valor Histórico: serve de fonte para a investigación histórica.

As distintas fases que atravesará un documento son:



- Arquivo de Oficina (Documentación Activa): fase na cal os documentos son creados ou recibidos por algún departamento, sobre os cales se pode realizar unha serie de operacións de edición.
- Arquivo Xeral (Documentación semiactiva): nesta etapa a principal función é a consulta da documentación e a actividade que recibe este tipo de documentación é menor que no Arquivo de Oficina.
- Arquivo Histórico (Documentación Inactiva): nesta etapa a documentación só ten utilidade como fonte de información histórica. As consultas que recibe son menores.

#### **21.4.4. Beneficios da Xestión Documental**

Realizar unha boa xestión dos documentos repercute na empresa cunha serie de beneficios, como son:

- Obter información precisa das actividades da empresa que sirva de apoio para actividades futuras, toma de decisións, etc.
- Facilitar a realización das actividades da empresa.
- Documental as políticas e o proceso de toma de decisións.
- Garantir a continuidade da empresa en caso de fallo masivo nos sistemas, catástrofe, etc.
- Cumprir cos requisitos legais que existen con algún tipo de ficheiro de datos.
- Almacenamento de evidencias das actividades relacionadas coa empresa e entidades externas.
- Manter un histórico da evolución da entidade.
- Centralizar o almacenamento de documentos.
- Facilitar a prestación de servizos aos usuarios da empresa.

## **21.5. XESTIÓN DO COÑECEMENTO**

### **21.5.1. Definición de Xestión do Coñecemento**

Non existe unha definición universalmente aceptada da xestión do coñecemento. Con todo, existen numerosas definicións de diversos expertos.

En xeral, a xestión do coñecemento é a conversión do coñecemento tácito en coñecemento explícito e o seu intercambio dentro da organización. A xestión do coñecemento é o proceso mediante o cal as organizacións xeran valor dos seus activos intelectuais. Definidos deste xeito, faise evidente que a xestión do coñecemento ten que ver co proceso de identificación, adquisición, distribución e mantemento dos coñecementos que son esenciais para a organización.

Se considera a xestión do coñecemento nun contexto máis amplo, entón existen múltiples definicións, con todo, todas elas apuntan á mesma idea, aínda que cada unha se centre nun aspecto particular da xestión do coñecemento.

- Unha definición orientada aos resultados pode afirmar que a xestión do coñecemento é “ter o coñecemento adecuado no lugar correcto, no momento adecuado e no formato correcto”.
- Unha definición orientada ao proceso pode afirmar que a xestión do coñecemento consiste “na xestión sistemática dos procesos polos cales o coñecemento se identifica, crea, une, comparte e aplica”.
- Unha definición orientada á tecnoloxía pode presentar unha fórmula de xestión do coñecemento como “*Business Intelligence* + motores de busca + axentes intelixentes”.

### **21.5.2. Cuestións sobre xestión do coñecemento**

Existen dous aspectos principais na xestión do coñecemento, que son a *xestión da información* e a *xestión das persoas*. Visto desde esta perspectiva, a xestión do coñecemento é, por unha banda, a información e, pola outra, a xente.

A maioría de empresarios e directivos están familiarizados co manexo de información a longo prazo. Este termo asóciase coa xestión do coñecemento en relación cos obxectos, que son identificados e controlados polos sistemas de información.

A práctica da xestión da información foi amplamente aceptada cando os executivos se decataron de que a información era un recurso importante, que debía ser manexado correctamente, para que as empresas poidan mellorar a súa competitividade.

Como consecuencia do crecemento da práctica da xestión da información, os conceptos de análises "*da información*" e "*planificación da información*", desenvolvéronse, proporcionando ferramentas adicionais para os profesionais.

Na vertente teórica a xestión da información evolucionou converténdose en xestión do coñecemento.

Na práctica, a xestión do coñecemento implica, entre outros, a identificación e mapeo dos activos intelectuais dunha organización. Isto significa, basicamente, a identificación de quen sabe que dentro da empresa.

Cando se mira desde esta perspectiva, a xestión do coñecemento pode ser considerado como un proceso de realización dunha auditoría dos activos intelectuais. Mais, a xestión do coñecemento vai máis aló deste nivel da cartografía e tamén implica a creación de coñecemento para obter vantaxes competitivas e a

conversión de grandes cantidades de datos da organización en información de fácil acceso.

Demostrouse unha e outra vez que cando o coñecemento se xestiona ben, hai unha redución significativa no tempo necesario para completar as tarefas e a duplicación innecesaria evítase.

Como xa comentamos, un aspecto da xestión do coñecemento é a xestión de persoas. Basicamente, trátase da xestión do coñecemento tácito que reside dentro das cabezas das persoas. Na práctica implica a xestión do coñecemento que existe xunto aos procesos organizativos que implica unha serie complexa de capacidades dinámicas, *know-how* e outras capacidades relacionadas co coñecemento.

Co fin de xestionar de forma eficaz ás persoas que posúen o coñecemento tácito que se desexa, é esencial ter en conta a súa diversidade cultural e os valores sociais, actitudes, aspiracións e gustos. Se isto se fai con éxito, pode conducir á creación de novos coñecementos que doutro xeito non se consegue mediante a xestión de información por si soa.

Malia a importancia dos dous aspectos da xestión do coñecemento, a cal está ben recoñecida por moitas organizacións, o verdadeiro potencial da xestión do coñecemento aínda queda por alcanzarse. De feito, non todas as organizacións con algún sistema de xestión do coñecemento son conscientes de que teñen estes sistemas.

A maioría das organizacións teñen algún tipo de sistema para a xestión do coñecemento explícito, xa sexa simple ou complexa, aínda que, non necesariamente se refiran a el como un sistema de xestión do coñecemento. Doutra banda, a xestión do coñecemento tácito non é común e a tecnoloxía actual baseada na xestión do coñecemento non se desenvolveu de forma plenamente eficaz para a extracción de

coñecemento tácito. Aínda que o coñecemento tácito é a base do coñecemento organizacional, é algo tan persoal que é difícil de formalizar e comunicar.

Ambos aspectos da xestión do coñecemento presentan dúas cuestións inmediatas:

- Facer que o coñecemento da organización sexa máis produtivo.
- Producir beneficios significativamente maiores que os previstos.

A xestión do coñecemento ofrece unha excelente oportunidade para adoptar estratexias de negocio que antes eran imposibles. Por exemplo, pódese abrir a porta á creación dunha rede case ilimitada que mellore as relacións con clientes e provedores. Na mellora de relacións cos clientes, a xestión do coñecemento fai posible o descubrimento de novos problemas e oportunidades a través do uso óptimo dos activos de coñecemento, tales como o contrato de venda, os rexistros, os datos demográficos dos clientes, etc. É precisamente deste xeito como a xestión do coñecemento pode complementar e mellorar o impacto doutras iniciativas da organización como a xestión da calidade total, o proceso de reenxeñería de negocios, e a aprendizaxe organizacional.

É evidente a partir desta discusión que as iniciativas de xestión do coñecemento se poden aplicar nunha variedade de ámbitos para lograr resultados superiores en case calquera tipo de organización. E é posible alcanzar estes resultados, independentemente do nivel de dispoñibilidade tecnolóxica ou o sector do 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 e Michael Zerres.
4. *ERP: Making It Happen*. Thomas F. Wallace e Michael H. Kremzar.
5. *Introduction to Knowledge Management*. Filemon A. Uriarte Jr.

**Autor:** Francisco Javier Rodríguez Martínez

Subdirector de Sistemas, Escola Superior Enxeñería Informática Ourense

Colexiado do CPEIG

# **22. DATAWAREHOUSE. DATA MARTS. ARQUITECTURA. ANÁLISE MULTIDIMENSIONAL E ARQUITECTURAS OLAP. ROLAP/MOLAP/HOLAP. MINARÍA DE DATOS. XERACIÓN DE INFORMES Á DIRECCIÓN.**



## **Tema 22: Datawarehouse. Data Marts. Arquitectura. Análise multidimensional e arquitecturas OLAP. ROLAP/MOLAP/HOLAP. Minería de datos. Xeración de informes para a dirección.**

---

### **ÍNDICE**

<b>22.1 Datawarehouse.....</b>	<b>3</b>
22.1.1 <i>Estrutura Multidimensional.....</i>	3
22.1.2 <i>Características dun Datawarehouse.....</i>	4
22.1.3 <i>Os Metadatos.....</i>	6
22.1.4 <i>Elementos que compoñen un Datawarehouse.....</i>	6
22.1.5 <i>Vantaxes principais dun Datawarehouse.....</i>	9
<b>22.2 Data Marts.....</b>	<b>10</b>
<b>22.3 Análise multidimensional e arquitecturas OLAP.....</b>	<b>13</b>
22.3.1 <i>Análise Multidimensional e OLAP.....</i>	13
22.3.2 <i>Sistemas OLAP.....</i>	16
22.3.3 <i>OLAP como sistema de información executiva.....</i>	16
22.3.4 <i>Operadores OLAP.....</i>	17
<b>22.4 ROLAP, MOLAP E HOLAP.....</b>	<b>19</b>
22.4.1 <i>ROLAP.....</i>	19
22.4.1.1 <i>Vantaxes dos sistemas ROLAP.....</i>	19
22.4.1.2 <i>Desvantaxes dos sistema ROLAP.....</i>	20
22.4.2 <i>MOLAP.....</i>	20
22.4.2.1 <i>Vantaxes dos sistemas ROLAP.....</i>	20
22.4.2.2 <i>Desvantaxes dos sistema ROLAP.....</i>	21
22.4.3 <i>HOLAP.....</i>	21
22.4.3.1 <i>Particionamento vertical.....</i>	21
22.4.3.2 <i>Particionamento horizontal.....</i>	21
<b>22.5 Minería de Datos.....</b>	<b>22</b>
22.5.1 <i>Características principais.....</i>	22
22.5.2 <i>Técnicas principais.....</i>	23
22.5.3 <i>Algoritmos empregados.....</i>	24
<b>22.6 Xeración de informes á dirección.....</b>	<b>26</b>

<b>22.7 Bibliografía.....</b>	<b>29</b>
-------------------------------	-----------

## **22.1 DATAWAREHOUSE**

### **22.1.1 Estrutura Multidimensional**

A estrutura multidimensional de bases de datos é unha variante do modelo relacional, a cal fai uso de estruturas multidimensionais, nas cales mantén a información organizada e nas que é capaz de expresar, á súa vez, as relacións entre os datos contidos nelas. Estas estruturas multidimensionais son visualizadas como cubos datos que á súa vez poden conter outros cubos datos, considerando cada unha das caras dos cubos como unha dimensión dos datos.

As celas que conforman a estrutura multidimensional conteñen información agregada que se relaciona cos elementos ao longo de cada unha das súas dimensións. É dicir, unha única cela pode chegar a conter as vendas totais dun determinado artigo nunha zona xeográfica específica para un tipo de venda concreto nun período determinado (vendas do procesador XMX-01, en Galicia, a través do portal web, no mes de abril).

A principal achega que ofrece esta estruturación multidimensional é que supón un modelo compacto e facilmente comprensible, e isto permite a manipulación e visualización de elementos de datos que posúen un elevado número de interrelacións.

Debido a todo isto as estruturas multidimensionais pasaron a formar parte das estruturas de bases de datos máis utilizadas, chegando a converterse nas estruturas máis importantes para as bases de datos analíticas que soportan as aplicacións que levan a cabo *procesamento analítico en liña, OLAP*, onde é vital obter unha resposta rápida ao realizarse unha serie de consultas de elevada complexidade.

Xeralmente unha organización ou entidade almacena os seus datos en bases de datos deseñadas para introducir e almacenar os mesmos mediante o proceso OLTP (On-Line Transaction Process, Proceso de Transaccións On-Line). Este proceso realiza dun xeito idóneo as tarefas de inserción, modificación ou borrado de rexistros, pero

resulta ineficiente á hora de realizar consultas complexas. Os Datawarehouse xorden como solución aos problemas que suscita o realizar análise de datos sobre unha base de datos OLTP.

O termo *Datawarehouse* ou almacén de datos representa un conxunto ou compendio de datos atendendo a unha temática, non volátil, integrado, de tempo variable, que é utilizado para achegar maior información e en menor tempo ao proceso de toma de decisións no ámbito da xerencia empresarial.

Desde un punto de vista máis concreto, un *Datawarehouse* é unha base de datos de carácter corporativo. Esta base de datos caracterízase pola integración e depuración de información procedente dunha ou múltiples fontes de datos, co fin de procesala e así ofrecer a posibilidade de analizala desde un maior número de perspectivas e a unha maior velocidade de resposta sobre as posibles consultas que sobre ela se realicen.

A vantaxe principal que achega un Datawarehouse ten a súa orixe nas estruturas ou modelos nos que organiza e almacena a información, os principais son:

- Modelo de táboas en estrela.
- Modelo de táboas en copo de neve.
- Cubos relacionais.

Debido a isto, a persistencia da información dun Datawarehouse é homoxénea e fiable, e proporciona, á súa vez, a posibilidade de realizar consultas e de tratar a información dun xeito xerárquico.

### **22.1.2      *Características dun Datawarehouse***

Os aspectos polos cales se caracteriza un Datawarehouse son os seguintes:

- **Temático:** orientado sobre a información que resulta relevante para a organización. O proceso de desenvolvemento do Datawarehouse, lévase a cabo co fin de realizar dun xeito eficiente as consultas sobre a información



que ofrece maior interese ás actividades esenciais da entidade, compras, vendas, produción, etc. En ningún momento se teñen en conta outro tipo de procesos como xestión ou facturación.

Os datos son organizados en temas, facilitando así o seu acceso e entendemento por parte dos usuarios. Desta forma tamén se ven beneficiadas as consultas, posto que toda a información referente a unha temática se atopará agrupada.

- **Integrado:** é capaz de incorporar nunha soa solución integral datos recompilados de diversos sistemas operacionais e fontes de información, as cales poden ser tanto de carácter interno na organización coma externo. Ademais permite que esas fontes de información externa conteñan os datos en distintos formatos. A estrutura na cal se realiza a integración dos datos debe ser consistente, para o que se deben eliminar as inconsistencias que existan entre os distintos sistemas operacionais.
- **Histórico:** a variable temporal forma parte da información implícita contida nun Datawarehouse. En contraposición cos sistemas operacionais, os cales sempre son reflexo do estado da actividade no momento presente, é dicir non reflicten a temporalidade da información, un Datawarehouse proporciona a capacidade de analizar tendencias que se produzan ao longo dunha etapa e comparalas con outras anteriores. En definitiva, almacena os datos coma se realizase fotos que se corresponden cos distintos momentos ou períodos de tempo.
- **Non volátil:** o repositorio de información contida dentro dun Datawarehouse só existe para ser consultada, non para modificar o seu contido, o cal proporciona a esta información carácter permanente. Isto significa que cando se realiza unha actualización do Datawarehouse,

unicamente se incorporan os últimos valores que tomaron as variables contidas nel, pero non se realiza ningún tipo de acción que altere os valores xa existentes.

### **22.1.3 Os Metadatos**

Outro valor engadido que proporciona un Datawarehouse son os metadatos, ou datos que describen outros datos. Estes metadatos achegan nova información sobre os valores existentes no Datawarehouse, mellorando a descrición dos datos e proporcionando novo coñecemento, o que permite, por exemplo, coñecer a procedencia da información, o seu grao de fiabilidade, a súa periodicidade de refresco ou mesmo o algoritmo utilizado para calculala.

Os metadatos, ademais de ampliar información permítenlle ao Datawarehouse realizar unha serie de procesos que simplifican e posibilitan obter a información dun xeito automático desde os sistemas operacionais aos sistemas informacionais.

Os obxectivos principais que seguen os metadatos son:

- **Ofrecerlle soporte ao usuario final:** grazas á súa propia linguaxe de negocio, facilitan o acceso ao Datawarehouse indicando qué información está contida e o significado que esta proporciona. Tamén poden ser utilizados por outras ferramentas para construír informes, consultas, etc.
- **Ofrecer soporte técnico:** supoñen un gran punto de apoio para os técnicos que xestionan o Datawarehouse, xa que son de grande axuda en aspectos de auditoría, na xestión da información histórica, na propia administración do Datawarehouse, etc.

### **22.1.4 Elementos que compoñen un Datawarehouse**

Os elementos máis importantes que conforman un Datawarehouse son:

1. **Fontes de datos:** as fontes de datos forman parte do Datawarehouse desde o principio, posto que son a orixe dos datos que este ha conter. As





fontes de datos poden pertencer a diversos ámbitos, tanto dentro como fóra da organización, desde sistemas operacionais propios a fontes externas.

2. **ETL (Extracción, transformación e carga):** representa a parte do sistema que realiza o proceso de construción do Datawarehouse. Para iso fai uso das fontes de datos desde as cales extrae a información para logo procesalas e almacénalas.

- *Extracción:* recuperación da información procedente das distintas fontes de datos.
- *Transformación:* proceso mediante o cal se realizan tarefas de filtrado, limpeza, depuración, homoxeneización e agrupación da información.
- *Carga:* este proceso encárgase da organización e a actualización dos datos e dos metadatos do Datawarehouse.

3. **Servidor de datos:** compoñente que realiza os labores de xestión do Datawarehouse. Para levar a cabo estas tarefas adoita facer uso dos recursos ofrecidos polo sistema operativo e polo xestor de base de datos.

Para o almacenamento dos datos pódense diferenciar dúas posibilidades en función do tipo de bases de datos e xestor da mesma empregados:

- Bases de datos relacionais e un sistema xestor de base de datos relacional ou SGBDR.
- Bases de datos multidimensionais, cun xestor de base de datos multidimensional ou SGBDM.

Debe ofrecer:

- Servizo de mantemento.

- Servizo de distribución para poder exportar os datos cara a outros servidores de bases de datos descentralizadas e a outros sistemas de soporte de decisións.
  - Servizo de seguridade, arquivo, backup, recuperación, etc.
4. **Ferramentas de acceso:** estas ferramentas achegan técnicas para a captura de datos dun xeito rápido, co fin de que poidan ser analizados desde distintos puntos de vista. Tamén realizan tarefas de transformación dos datos en información útil para o usuario. Este tipo de ferramentas denomínanse *business intelligence tools* e sitúanse a nivel conceptual sobre o Datawarehouse. Algunha destas ferramentas son:
- Consultas SQL.
  - Ferramentas MDA, Multidimensional Analysis.
  - Ferramentas OLAP, On-Line Analytical Processing.
  - Ferramentas ROLAP, Relational On-Line Analytical Processing.
  - Ferramentas MOLAP, Multidimensional On-Line Analytical Processing.
  - Ferramentas HOLAP, Hybrid On-Line Analytical Processing.
  - Ferramentas de Minería de Datos.
5. **Repositorio/Metadatos:** o repositorio axuda aos usuarios a saber qué é o que hai almacenado no Datawarehouse e cómo poden acceder ao que queren. Ademais realiza diversas funcionalidades como:
- Catalogar e describir a información dispoñible.
  - Especificar o propósito da información.
  - Reflectir as relacións dos datos.



- Indicar o propietario da información.
- Relacionar as estruturas técnicas de datos coa información de negocio
- Especificar as relacións entre os datos operacionais e as regras de transformación.
- Limitar a validez da información.

### **22.1.5      *Vantaxes principais dun Datawarehouse***

As achegas máis importantes que ofrece un Datawarehouse son as seguintes:

- Facilita a implantación de sistemas de xestión integral da relación co cliente desde o núcleo dunha organización.
- Posibilita a utilización de técnicas de modelización e análise estatística para a procura de relacións ocultas entre os datos almacenados, o cal ofrece un valor engadido ao sistema de xestión da información.
- Ofrece unha ferramenta de apoio á toma de decisións en calquera área funcional, grazas á información integrada e global que proporciona.
- Proporciona a capacidade de aprendizaxe sobre os datos pasados para a predicción de posibles situacións futuras.

## 22.2 DATA MARTS

A solución aos problemas relacionados coa análise de datos sobre unha base de datos OLTP son solucionados coa creación dos datawarehouse (base de datos independente orientada a consultas). Con todo, cando os datawarehouse aumentan o seu tamaño vólvense cada vez máis complexos, o que provoca un decrecemento no rendemento das consultas, deixando de ser útil o modelo centralizado. Como resposta a esta baixada de rendemento xorden os Data Marts, que son almacéns de datos que se especializan por áreas ou temáticas, como poden ser vendas ou compras.

Os Data Marts adoitan recibir a información desde o datawarehouse, ou almacén de datos centralizado, e poden estar situados en máquinas distintas, noutras BBDD, redes, etc. Tamén poden integrar a información desde distintas fontes. Segundo estes dous modelos de extracción da información, existen dous tipos de Data Mart:

- *Data Mart dependente*, cuxos datos veñen proporcionados desde un datawarehouse. Na ilustración 9 pódese observar o funcionamento dun Data Mart cun datawarehouse.
- *Data Mart independente*, onde os datos son extraídos de diversas fontes de información dos sistemas operacionais.

Un Data Mart representa unha pequena porción dun datawarehouse, o que significa que soporta un número de usuarios máis reducido, e, xa que logo, pódense optimizar para realizar o proceso de recuperación da información dun xeito máis rápido.

Un Data Mart é, en realidade, unha base de datos específica dun departamento ou sección, dedicada unicamente aos datos relevantes que se producen nese ámbito. Debido a esta especialización dispoñen dunha estrutura óptima de datos adaptada á

análise da información desde todas as perspectivas que afecten aos procesos dese ámbito.

Para a creación dun Data Mart é necesario atopar a estrutura idónea para a análise da información. Esta estrutura pode estar montada tanto sobre un sistema OLTP como sobre un datawarehouse, ou pola contra, pode sosterse sobre un sistema OLAP. Por iso pódense establecer dous tipos de Data Marts:

- **Data Mart OLTP:** son Data Marts baseados nun datawarehouse, pero é habitual que incorporen melloras para ofrecer un maior rendemento adaptando as necesidades de cada área ao Data Mart.

Neste tipo de Data Marts as estruturas máis comúns son:

- *Táboas report*, que son táboas de feitos reducidas que agregan as dimensións oportunas.
  - *Vistas materializadas*, que se constrúen coa mesma estrutura que as táboas report para explotar a reescritura das consultas. Este tipo de estrutura é dependente do SGBD.
- **Data Mart OLAP:** baséanse en cubos OLAP que se xeran en función dos requisitos de cada área, agregando as dimensións e os indicadores necesarios de cada cubo relacional. Os modos de creación, explotación e mantemento deste tipo de estrutura é moi dependente da ferramenta que se utilice para a súa manexo.

Os Data Marts grazas a este tipo de estruturas óptimas para a análise ofrecen unha serie de vantaxes como:

- Elevada rapidez de consulta da información.
- Reducido conxunto de datos.
- A información válidase directamente.



- Realizar facilmente históricos dos datos.
- Posibilidade de Consultas SQL e MDX sinxelas.

## **22.3 ANÁLISE MULTIDIMENSIONAL E ARQUITECTURAS OLAP.**

A primeira aparición do termo OLAP (On-Line Analytical Processing) foi publicada en 1993 por Edgar F. Codd. Malia todo, en 1970 xa existían produtos que realizaban consultas OLAP. Codd definiu OLAP como un tipo de procesamento de datos caracterizado por permitir a análise multidimensional.

### **22.3.1 *Análise Multidimensional e OLAP***

A multidimensionalidade desde o punto de vista dun proceso analítico en liña consiste en transformar os datos procedentes desde varias fontes, táboas dunha base de datos, arquivos,... e convertelos nunha estrutura onde estes estean agrupados en dimensións separadas e heteroxéneas. Estas estruturas denomínanse *cubos*.

As dimensións constitúen as perspectivas de alto nivel dos datos que representan a información máis importante dun negocio. Estas dimensións nunha solución OLAP tenden a ser invariables.

A análise multidimensional fundaméntase en modelar a información en dimensións, feitos e medidas.

- **Medidas:** é un tipo de dato que contén información que utilizan os usuarios nas súas consultas coas que son capaces de medir o grao de rendemento dun proceso.
- **Dimensións:** entidades ou colección de entidades que se atopan relacionadas e que son usadas para determinar ou identificar o contexto das medidas.

O tipo e o número de dimensións para cada unha das medidas do modelo é un proceso que debe realizarse coidadosamente, posto que ao definir as dimensións, engadir, eliminar ou cambiar propiedades particulares das



dimensións candidatas varía o contexto e tamén o significado da medida candidata.

Unha dimensión ten compoñentes denominados *membros* (dimensión tempo, membro trimestre) e entre os membros poden existir xerarquías (un mes pode considerarse dentro dun trimestre).

As dimensións conteñen:

- Entidades de dimensión.
- Atributos de dimensión.
- Xerarquías de dimensión.
- Niveis de agregación.

Para referenciar as dimensións utilízanse as *chaves de dimensión*.

- **Feitos:** identifican a existencia de valores específicos dunha ou máis medidas para unha combinación concreta de dimensións. Mediante un feito pódese representar desde un obxecto de negocio ata unha transacción e ata un evento utilizado polos usuarios.

Os feitos conteñen:

- Un identificador para cada feito.
- Chaves de dimensión, que o enlazan coas dimensións.
- Medidas.
- Tipos de atributos normalmente derivados doutros datos do modelo.



Unha característica fundamental e moi importante deste modelo é que ten a capacidade de representarse de xeito vectorial. Os feitos sitúanse de xeito lóxico nunha cela, a cal se atopa na intersección de certas coordenadas segundo o modelo  $(x, e, z, \dots)$ , onde, ademais, cada unha das coordenadas que se atopan nas celas representan unha dimensión.

A utilización da correspondencia entre os elementos do modelo, é dicir, os feitos e as coordenadas, e os da base de datos, a táboa de feitos e dimensións, é fundamental para poder levar a cabo a análise multidimensional nunha base de datos. Nunha base de datos pódense reflectir os feitos e as dimensións nunha táboa, e debido a isto é posible utilizar a linguaxe SQL para a definición dun modelo multidimensional nunha base de datos relacional. Malia isto, foi necesario realizar unha serie de extensións do modelo relacional para poder dar soporte ás funcionalidades e necesidades propias da análise multidimensional. Estas funcionalidades son:

1. Declaración de Dimensións e Xerarquías. O modelo relacional non incorporaba nin trataba con anterioridade estes conceptos.
2. Acceso máis rápido aos datos. Para engadir esta mellora utilizáronse métodos de xeración de índices para datos espaciais desde o punto de vista multidimensional.
3. Cálculo de valores previamente agrupados para a optimización de consultas.
4. Definición de operacións de navegación nas dimensións e de agrupación de medidas como:
  - *Slice-and-dice:*
  - *Drill-down*
  - *Roll-up*
  - *Pivot*

- *Drill-across*
- *Drill-through*

Partindo das primeiras propostas, o modelo multidimensional non precisa dunha almacenaxe previa nunha base de datos multidimensional, senón que propón que o acceso á información pode facerse directamente a múltiples fontes, bases de datos (xa sexan relacionais ou multidimensionais), follas de cálculo, arquivos e mesmo permite que os datos poidan proceder directamente dos usuarios finais.

Malia estas primeiras ideas, determinouse a través da experiencia de que a análise OLAP ten un mellor desempeño se a fonte de datos é única, e aínda mellor se esa fonte de información é á súa vez unha base de datos multidimensional, por exemplo un Datawarehouse.

### **22.3.2      *Sistemas OLAP***

Os sistemas OLAP son un conxunto de métodos que permiten consultar a información contida nos datos de diversos xeitos. Esta versatilidade e multiplicidade de opcións de visualización vén producida pola clasificación dos datos en diferentes dimensións que poden ser visualizadas unhas con outras combinándoas para obter diferentes análises da información.

A información dun modelo OLAP é vista como un cubo, os cales son determinados polas categorías descritivas ou dimensións e valores cuantitativos, as medidas. Este modelo de datos multidimensional simplifica moito as tarefas que o usuario pode realizar sobre os datos, consultas complexas, filtrar en subconxuntos,...

### **22.3.3      *OLAP como sistema de información executiva***

Como clasificación dos sistemas OLAP pódense considerar dentro do grupo de aplicacións ou sistemas de información para executivos (EIS), que se empregan para proporcionar ao nivel estratéxico información que resulte relevante á hora de tomar decisións.

Se comparamos os sistemas OLAP co resto de EIS podemos afirmar que as ferramentas OLAP ofrecen unha opción moito máis xeral, é dicir son máis xenéricas:

- Funcionan sobre un sistema de información como os datawarehouse.
- Permiten a creación de agregacións e combinacións dos datos de moitos xeitos, posibilitando a realización de análises máis estratéxicas de datos.
- Posúe operadores para realizar tarefas específicas (Drill, Roll, Slice-and-Dice, ...).
- O resultado pode ser expresado de xeito matricial ou híbrido.

#### **22.3.4 Operadores OLAP**

Estas ferramentas das solucións OLAP permítenlle ao usuario ter unha visión multidimensional da información para cada unha das actividades de análises. Cos operadores realízanse consultas simplemente seleccionando atributos do esquema multidimensional sen ter que ter coñecemento da estrutura interna na que se almacenan os datos, posto que a propia ferramenta OLAP se encarga de xerar a consulta e de enviala ao sistema de xestión de consultas.

Unha consulta consiste na obtención de medidas sobre os feitos parametrizadas polos atributos das dimensións e limitadas polas condicións impostas sobre as dimensións. As ferramentas OLAP ofrecen unha serie de novos operadores que refinan esas consultas. Os operadores son os xa mencionados anteriormente no punto “Análise multidimensional e OLAP”.

- **Drill ou disgregación:** posibilita a introdución dun novo criterio de agrupación na análise, disgregando os grupos actuais. Actúa sobre o operador orixinal *informa* co cal non é necesario crear ou realizar un novo informe. Existen varias variantes:
  - *Drill-down*, permite visualizar os datos do nivel inferior da dimensión actual dentro dunha xerarquía definida. Mostra os datos detallados que en conxunto determinan o valor.



- *Drill-across*, visualiza a información contida noutro modelo multidimensional; sen detallar nin consolidar a información cambia o modelo multidimensional que se está consultando. Para realizar esta operación ambos modelos han de ter unha dimensión común.
  - *Drill-through*, similar a drill-down, consulta a información do nivel inferior á dimensión actual. Con todo, drill-through navega por fóra do modelo multidimensional establecendo un enlace entre este e o sistema fonte, sobre o cal consulta os datos do nivel detallado directamente. Para poder utilizar este operador débese establecer acceso ao sistema fonte desde o sistema OLAP.
- **Roll ou agregación:** permite que se elimine un criterio de agrupación na análise, agregando os grupos actuais. Actúa sobre o informe xa creado e non é preciso realizar un novo. Variantes:
  - *Roll-up*, tamén coñecido como drill-up, encárgase de pasar ao nivel superior da xerarquía da dimensión actual. Para iso consolida os datos do nivel actual e mostra o valor consolidado que corresponde co nivel superior da dimensión.
  - *Roll-across*, funciona dun xeito parecido ao *Roll-up*, salvo que non se realiza sobre xerarquías dunha dimensión, senón que elimina un criterio de análise eliminando da consulta unha dimensión.
- **Slice-and-Dice:** permite seleccionar e proxectar datos no informe. Selecciona a información dun membro dunha dimensión; trabállase cun subconxunto dos datos para un valor determinado dun nivel nunha

dimensión. Con frecuencia este operador é empregado sobre un eixe temporal para poder analizar tendencias e atopar patróns.

- **Pivot:** con este operador permítese cambiar a orientación das dimensións nun informe. Selecciona a orde de visualización das dimensións co fin de analizar os datos desde distintas perspectivas.

## **22.4 ROLAP, MOLAP E HOLAP**

### **22.4.1 ROLAP**

É un tipo de organización da información a nivel físico que se implanta sobre tecnoloxía relacional, pero incorpora algunhas facilidades que incrementan o seu rendemento.

ROLAP (Relational On-Line Analytic Processing) posúe as virtudes dun sistema xestor de bases de datos relacional sobre o cal se incorporan unha serie de ferramentas e extensións para poder ser utilizado como un datawarehouse ou almacén de datos. As principais características dos sistemas ROLAP son:

- Almacena os datos nunha base de datos relacional.
- Utilización de índices de mapas de bits.
- Utilización de índices de *join*.
- Técnicas de particionamento de datos.
- Optimizadores de consultas.
- Extensións de SQL (drill, roll, etc).

#### **22.4.1.1 Vantaxes dos sistemas ROLAP**

- Utilización completa da integridade e seguridade que ofrecen as bases de datos relacionais.

- É escalable para volumes grandes.
- Os datos poden ser compartidos con outras aplicacións que utilicen a linguaxe SQL.
- Datos e estruturas máis dinámicas.

#### 22.4.1.2      *Desvantaxes dos sistema ROLAP*

- As consultas resultan máis lentas.
- A súa construción adoita resultar custosa.
- Os índices non se manteñen de xeito automático.
- Os cálculos atópanse limitados polas funcións da base de datos.

### **22.4.2      *MOLAP***

A función principal dos sistemas MOLAP (Multidimensional On-Line Analytic Processing) é a de almacenar fisicamente os datos nestas estruturas específicas de tipo multidimensional facendo coincidir a representación interna dos datos coa representación que as capas superiores dan á información.

Posúen estruturas específicas para o almacenamento da información, achegando tamén técnicas para a compactación dos datos, o cal mellora o rendemento do almacén de datos.

As características máis importantes dos sistemas MOLAP son:

- Incorporan tecnoloxía optimizada para a realización das consultas e da análise, a cal está fundamentada no modelo multidimensional.
- Ten un motor especializado.
- Constrúe os datos e almacénaos en estruturas multidimensionais.

#### 22.4.2.1      *Vantaxes dos sistemas ROLAP*

- Maior rendemento á hora de executar as consultas.

- Pouco tempo de cálculos realizados no momento.
- Pode realizar a escritura de xeito directo na base de datos.
- Ofrece a posibilidade de formular cálculos máis sofisticados.

#### 22.4.2.2      *Desvantaxes dos sistema ROLAP*

- O tamaño vén limitado pola arquitectura do cubo.
- Só é capaz de xestionar os datos se estes se atopan almacenados nun cubo.
- Procesos de mantemento e de copias de seguridade limitados.
- Non explota a capacidade de paralelismo que ofrecen as bases de datos.
- Introduce redundancia de datos.

### **22.4.3      *HOLAP***

Este tipo de sistemas HOLAP (Hybrid On-Line Analytic Processing) están considerados como sistemas híbridos entre os ROLAP e os MOLAP, posto que incorpora características de ambos. Para iso utiliza un motor relacional para almacenar parte dos datos nunha base de datos de tipo relacional e utiliza unha base de datos multidimensional para outra parte da información.

#### 22.4.3.1      *Particionamento vertical*

Neste modo, HOLAP mellora a velocidade das consultas almacenando as agregacións nun sistema MOLAP, mentres que para optimizar o tempo, os datos son detallados nun sistema ROLAP.

#### 22.4.3.2      *Particionamento horizontal*

Un sistema HOLAP en modo de particionamento horizontal almacena parte dos datos, normalmente os máis recentes particionados por unha das dimensións (dimensión tempo por exemplo) en modo MOLAP, co que consegue un aumento na velocidade de resposta das consultas. Por outra banda mantén nun sistema ROLAP os datos máis antigos. Tamén este modo permite que os cubos se almacenen uns en sistemas MOLAP e outros en sistemas ROLAP.

## **22.5 MINERÍA DE DATOS**

O concepto de *Data Mining* ou Minería de datos vén determinado polo método de extracción da información contida nos datos. A minería de datos obtén información contida nos datos, pero dunha forma indirecta, posto que esta se atopa implícita nos datos e non se pode acceder a ela directamente.

A minería de datos *prepara, sonda e explora* o conxunto de datos co fin de conseguir información que dalgún modo se atopa oculta. Esta ocultación da información débese a que normalmente para un experto o que resulta relevante é a información contida nas relacións, fluctuacións e dependencias dos datos, non os datos en si. Esta información é polo xeral descoñecida, o cal ofrece un valor moi importante, posto que pode resultar de grande utilidade aos procesos dunha organización.

Está formada por un conxunto de técnicas dirixidas á obtención do coñecemento procesable oculto nas bases de datos. Estas técnicas fundamentan a súa base na intelixencia artificial e na análise estatística para xerar modelos co fin de poder abordar a solución a problemas de predicción, clasificación e segmentación.

A minería de datos é un proceso que inverte a dinámica do método científico posto que neste primeiro se formulan as hipóteses e logo desenvólvese un experimento para a obtención dos datos que as confirmen ou refuten, obtendo así novo coñecemento. Na minería de datos solicítase unha colección de datos coa intención de que destes xurdan hipótese. Espérase que dos propios datos describan ou indiquen como son para poder validar as hipóteses aparecidas cos datos mesmos. É por este motivo que a minería de datos debe realizarse cun enfoque exploratorio e non confirmador.

### **22.5.1 Características principais**

As principais características que determinan un sistema de minería de datos son:





- Traballa coa información contida no máis oculto das bases de datos ou almacéns de datos analizando información almacenada durante anos.
- Adoitan ser solucións cunha arquitectura cliente-servidor.
- Posúen gran variedade de ferramentas para a extracción da información.
- As ferramentas son facilmente combinables entre si.
- Son os usuarios finais os que fan uso das ferramentas para indagar no conxunto de datos e obter respostas rápidas.
- É habitual facer uso dun procesamento paralelo que acelere o proceso debido á existencia dunha gran cantidade de datos.
- Produce cinco tipos de información:
  - Asociacións
  - Secuencias
  - Clasificacións
  - Agrupamentos
  - Prognósticos.

### **22.5.2      *Técnicas principais***

As técnicas máis importantes que se utilizan para levar a cabo este proceso son:

- *Redes Neurais*: é unha técnica que provén da intelixencia artificial para a detección de categorías comúns nos datos, xa que é capaz de detectar e aprender complexos patróns e características dos datos.

Un punto forte das redes neuronais é que son capaces de traballar con conxuntos incompletos de datos e mesmo con algúns paradoxais que en función do problema poden ser vantaxosos ou resultar un inconveniente.

- *Árbores de Decisión:* esta técnica represéntase en forma de árbore, sendo cada nodo unha decisión, os cales xeran unha serie de regras mediante as cales clasifican os datos.

Son sinxelos de utilizar, admiten tanto atributos discretos como continuos e tratan ben tanto os atributos non significativos coma os valores faltantes. Ademais son facilmente interpretables.

- *Algoritmos Xenéticos:* son técnicas que imitan a evolución das especies mediante a xeración de mutacións, a reprodución e selección. Proporcionan ferramentas para integrar na construción e adestramento doutras estruturas, por exemplo as redes neuronais. Están baseados no principio de supervivencia dos máis aptos.
- *Clustering (Agrupamento):* técnica que agrupa datos dentro dunha serie de clases, que poden ser predefinidas ou non, seguindo os criterios de distancia ou similitude, de modo que os datos contidos dentro dunha clase son similares entre si e distintos cos contidos nas outras clases. É un método moi flexible e facilmente combinable con outras técnicas de minería de datos.
- *Aprendizaxe Automática:* técnica procedente da intelixencia artificial na que se trata de inferir coñecemento partindo do resultado obtido mediante algunha das outras técnicas anteriormente mencionadas.

### **22.5.3 Algoritmos empregados**

Os algoritmos utilizados na minería de datos pódense clasificar en:

- **Supervisados**
  - Predín o valor dun atributo dun conxunto de datos unha vez coñecidos outros atributos.
  - Partindo dos datos cuxos atributos son coñecidos, indúcense novas relacións entre atributos.



- Constan de dúas fases:
  - *Adestramento*: nesta fase constrúese un modelo usando un subconxunto de datos coñecidos.
  - *Proba*: próbase o modelo co resto dos datos.
- **Non Supervisados**
  - Utilízanse cando unha aplicación non se atopa o suficientemente madura ou non ten as capacidades necesarias para realizar unha solución predictiva.
  - Descubren patróns e tendencias nos datos.
  - Co descubrimento da información pódense levar a cabo accións que reporten nun beneficio.

## **22.6 XERACIÓN DE INFORMES Á DIRECCIÓN**

Os aplicacións para a xeración de informes á dirección ou *Sistemas de Información para Executivos (EIS)*, son ferramentas software que se basean en sistemas de apoio ás decisións (DSS Decision Support System) proporcionándolle á xerencia dunha organización acceso fácil e sinxelo á información que resulta clave para o éxito da súa compañía, xa sexa interna ou externa.

O obxectivo principal deste tipo de aplicacións é poñer a disposición dos executivos unha serie de ferramentas que mostren o abano completo do estado dos indicadores de negocio que lle interesan en tempo real, ofrecendo á súa vez a capacidade dunha análise detallada daqueles que non estean conseguindo as expectativas ou as planificacións establecidas a priori.

Este tipo de sistemas pódense definir como solucións para mostrar informes e listaxes (query & reporting) das distintas áreas de negocio dunha forma consolidada, facilitando unha monitorización completa e real dunha organización.

Ofrecen, ademais, un acceso rápido e efectivo á información compartida, para o que fan uso de interfaces gráficas moi visuais e intuitivas. Incorporan tamén alertas e informes baseados en excepción, así como históricos e análises de tendencias.

Mediante estes sistemas, o seguimento do comportamento dunha organización ou dun área de negocio faise dun xeito fácil e comparable a través do tempo.

Dentro destes sistemas, o máis común é atopar os termos de Informes (Reports), Cadro de Mando (Dashboard) e Cadro de Mando Integral (Balanced ScoreCard).

### **Informes**

Os informes son a ferramenta máis común de transmitir toda a información obtida dun sistema de *business intelligence*. Un informe pódese describir como un documento, ou conxunto de documentos, que contén datos utilizados para o seu

estudo e análise por parte da dirección. Poden estar compostos por unha simple táboa de datos ou por unha vista máis complexa con datos agregados, con datos transformados mediante a aplicación de fórmulas ou con sistemas de navegación interactiva a través dos datos (habitualmente ampliando a vista de cada fila na táboa).

A característica principal dun informe é que non lle ofrece ao lector do mesmo ningún tipo de conclusión ou visión predefinida dos datos. Aínda que un informe inclúa datos analíticos, datos agregados, datos calculados ou algún gráfico é o propio lector o que debe extraer conclusións ou determinar as próximas accións tomando como base os datos presentados no informe.

## Dashboard

Un cadro de mando é unha interface de carácter visual que ofrece en cada momento diferentes vistas ou perspectivas das diferentes métricas ou indicadores (tamén denominados KPI Key Performance Indicators) que se consideraron como relevantes para un proceso de negocio ou os obxectivos dunha empresa. Un KPI é un indicador da execución e o rendemento dunha tarefa ou actividade diaria que se considera fundamental desde o punto de vista da dirección para o seu seguimento. A idea que subxace a un KPI é que non é unha métrica simple do negocio, senón que está deseñado de forma que describe e alerta sobre distintas circunstancias, permitindo detectar e intervir naquelas situacións que así o requiran.

Un dashboard presenta tres características diferenciadoras:

Mostra os datos de forma gráfica. Isto proporciona unha visión moita máis centrada nos indicadores de rendemento, nas posibles comparacións entre datos e aqueles datos que sexan unha excepción ou que identifiquen unha anomalía.

Só mostran aqueles datos que son necesarios para un determinado obxectivo empresarial.

Ademais, inclúe conclusións predefinidas que son relevantes para os obxectivos do cadro de mando e que axudan ao lector a realizar a súa propia análise.

### Cadro de Mando Integral

Un cadro de mando integral (Balanced Scorecard) é unha representación visual da estratexia da empresa. O cadro de mando integral permite dunha forma sinxela presentar os indicadores ou métricas críticas para o negocio e contrastalas coa estratexia de negocio que se pretende para a organización.

O cadro de mando integral debe mostrarse dunha forma visual e ser a referencia a calquera persoa da organización para ver:

O rendemento das iniciativas específicas a distintas unidades de negocio ou desde un punto de vista global a toda a compañía.

Os obxectivos individuais referenciados ao contexto global da compañía mediante unha representación visual.

Os cadros de mando integral deséñanse sempre co fin de aumentar a produtividade de toda a organización, porque indica en tempo real como se está comportando un empregado, un equipo, un departamento ou toda a empresa, de acordo aos obxectivos definidos no plan estratéxico. Isto convérteo nun sistema de xestión estratéxica da empresa, que permite:

Formular estratexias consistentes e que estas sexan transparentes a toda a organización.

Comunicar as estratexias definidas pola dirección a través de toda a organización.

Coordinar os obxectivos das diversas unidades organizacionais (equipos, departamentos, seccións, etc.) de acordo ao mesmo plan estratéxico.

Conectar os obxectivos de cada unidade organizacional coa planificación financeira e orzamentaria da organización.

Medir dun modo sistemático a realización, propoñendo accións correctivas oportunas por parte da dirección ou por cada un das unidades organizacionais implicadas.

## **22.7 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 e 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 e 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

Colexiado do CPEIG



## **23. SISTEMAS DE XESTIÓN DE CONTIDOS. E-LEARNING. ACCESIBILIDADE E USABILIDADE. W3C.**

## **Tema 23.- Sistemas de Xestión de Contidos. E-learning. Accesibilidade e Usabilidade. W3C**

---

### **ÍNDICE**

#### **23.1 Sistemas de Xestión de Contidos**

- 23.1.1 Introducción aos sistemas de xestión de contidos.*
- 23.1.2 Funcionalidade dos SXC*
- 23.1.3 Arquitectura xeral dos sistemas de xestión de contidos.*
- 23.1.4 Categorias*
- 23.1.5 Criterios de valoración*
- 23.1.6 JOOMLA!*
- 23.1.7 WORDPRESS*
- 23.1.8 DRUPAL*

#### **23.2 E-LEARNING**

- 23.2.1 Introducción*
- 23.2.2 Concepto*
- 23.2.3 Plataformas de e-Learning*
- 23.2.4 Vantaxes*
- 23.2.5 Inconvenientes*
- 23.2.6 Estandarización*
- 23.2.7 Plataforma Moodle*

#### **23.3 Accesibilidade e Usabilidade**

- 23.3.1 Accesibilidade como calidade dos sistemas*
- 23.3.2 Limitacións na accesibilidade*
- 23.3.3 Promovendo a accesibilidade*
- 23.3.4 Usabilidade*

#### **23.4 W3C**

#### **23.5 Bibliografía**

### **23.1 SISTEMAS DE XESTIÓN DE CONTIDOS**

#### **23.1.1 Introducción aos sistemas de xestión de contidos.**

Os sistemas de xestión de contidos, en diante SXC (CMS en inglés), son un tipo

especial de software orientado á creación, administración e distribución de contidos dixitais. Os SXC proporcionan unha estrutura ou *framework* para dar soporte a tarefas básicas e complexas de xestión de contido. Están principalmente orientados para servir como marco de publicación de contidos na rede a través da web. O éxito deste tipo de sistemas radica fundamentalmente na facilidade de uso, establecendo mecanismos sinxelos para a creación de contidos, a súa actualización, a súa administración e categorización, e a súa publicación. Proporcionar facilidade no manexo de contidos implica outorgar un maior dinamismo no fluxo da información.

Unha das súas principais características é que permiten separar o contido da presentación, cuestión que proporciona versatilidade á hora de realizar cambios no deseño. Ademais, proporcionan ferramentas que permiten descentralizar a publicación de contidos na web.

Un aspecto clave na xestión de contidos é a categorización da información. A capacidade de establecer mecanismos que permitan localizar a información útil é outra das características propias dos sistemas de xestión de contidos. Esta capacidade baséase no uso de metadatos que serven para lles proporcionar información engadida aos contidos publicados, e que son utilizados polos buscadores e clasificadores de información.

### **23.1.2 Funcionalidade dos SXC**

A funcionalidade xeral ofrecida polos SXC pode agruparse en cinco bloques, fundamentalmente:

- Creación de contido : Realízase de forma sinxela. Os CMS aportan ferramentas para que os creadores sen coñecementos técnicos en páxinas web poidan concentrarse no contido. A forma habitual consiste en proporcionar un editor de texto WYSIWYG, no que o usuario ve o resultado final mentres escribe. O uso deste tipo de editores é moi sinxelo. O acceso aos mesmos é moi cómodo, xa

que só se require para iso un equipo con acceso á internet e un navegador web.

- Xestión de contido : Todo o contido creado almacénase na base de datos que utiliza o sistema. Na propia base de datos é onde tamén se gardan datos relacionados coa estrutura da web ou os usuarios autorizados.
- Xestión de usuarios: A maioría dos SXC presentan unha xestión de usuarios na que cada un conta con diferentes permisos para xestionar o contido. Dependendo dos permisos dos usuarios, pódense atopar distintos roles que van desde o administrador xeral da plataforma, ata o usuario final que consulta a información.
- Publicación de contido : Unha vez creado o contido, os SXC proporcionan diferentes mecanismos para proceder á súa publicación. Pódese asignar unha data de publicación ou ben pódese publicar directamente. Na publicación do contido, o aspecto que terá vén marcado polo modelo marcado para a sección onde se atope a información, que habitualmente se corresponde cun conxunto de estilos predefinidos. Esta separación entre contido e forma representa unha característica moi importante dos SXC dado que permite que se poida modificar o estilo dun portal web sen necesidade de modificar o contido.
- Presentación de contido: Os SXC xestionan automaticamente a accesibilidade do sitio web, proporcionando mecanismos de adaptación ás necesidades de cada usuario e ademais son perfectamente compatibles coa maioría dos navegadores web existentes. O sistema encárgase de xestionar outros aspectos como os menús de navegación, engadindo ligazóns de forma automática. Tamén xestionan todos os módulos, internos ou externos, que sexan incorporados ao sistema.

Dentro do ciclo de actividades que se corresponde coa funcionalidade dos CMS, é necesario definir un conxunto de roles ou usuarios aos que se asocian unha serie de tarefas:

1. Autor: Que pode ser calquera membro usuario do sistema que desexe publicar contido.
2. Publicador: que revisa esa información e autoriza a súa publicación en tempo e forma adecuadas.
3. Administrador do sistema: desempeña funcións técnicas que consisten en optimizar o rendemento e arquitectura do sistema. Poden ademais propoñer os modelos de deseño e os sistemas de categorización máis adecuados, de acordo cos provedores de información e encárganse de manter o sistema en constante mellora e actualización.

A definición de roles ou usuarios é dependente da plataforma final que se pode escoller como SXC, e van desde os presentados anteriormente ata unha definición de gran fin, onde se especifican roles intermedios e se diversifican máis as tarefas. O sistema de xestión de contidos controla e axuda a manexar cada paso deste proceso, incluíndo os labores técnicos de publicar os documentos a un ou máis sitios.

### ***23.1.3 Arquitectura xeral dos sistemas de xestión de contidos.***

A arquitectura destes sistemas é modular, proporcionando un marco de desenvolvemento que facilita a implantación de novas funcionalidades. Neste sentido, os SXC incorporan unha gran variedade de módulos que permiten estender o funcionamento do sistema. Existen módulos para a xestión integral dun sitio web, para a xestión de páxinas xeradas dinamicamente, e outros módulos que posibilitan a personalización do sistema por parte do usuario.

Os SXC, como software, poden definirse como un *framework* que habitualmente consta de dúas partes diferenciadas:

- *Backend* ou parte administrativa: A través do *backend* poden controlarse todos os aspectos relativos á configuración do *framework*, a administración do

contido (creación, categorización, edición, publicación, eliminación), a personalización do contorno de consulta (*frontend*), actualización e configuración de novas funcionalidades.

- *Frontend* ou parte pública: A través do *frontend* pódense consultar os contidos publicados, acceder ás funcionalidades proporcionadas para os usuarios configuradas desde o *backend*, e tamén serve para recoller certos datos de entrada.

A separación do sistema en *frontends* e *backends* é un tipo de abstracción que axuda a manter as dúas principais partes do SXC separadas. Dentro da arquitectura de SXC contéplase a existencia dunha ou varias bases de datos, responsables fundamentalmente da persistencia do contido publicado a través do SXC e de todos os datos relativos á configuración do sistema.

O fluxo básico é que xestor responde ás solicitudes de páxinas que se formulan desde os lectores, recuperándoas na base de datos, compoñendo os modelos definidos e devolvendo ao servidor web o contido final que este lle ofrece ao lector.

Os SXC, ao seren aplicacións web, execútanse no servidor web onde estean aloxados. Dependendo das tecnoloxías utilizadas para o desenvolvemento do SXC, a complexidade do servizo web que soporta a plataforma será maior. O acceso aos SXC realízase a través dos navegadores web. Cando un usuario realiza unha petición dunha páxina, o xestor de contidos é o encargado de interactuar co servidor para xerar unha páxina dinámica, cun formato definido, e cun contido que se extrae da base de datos.

### **23..4 Categorías**

En canto á categorización dos SXC, non existe unha clasificación estrita, senón máis ben, categorizacións en función de determinadas características propias dos

sistemas. Así pois, podemos clasificalos en función da linguaxe de programación no que se desenvolvan, segundo a súa licenza (código aberto ou software privativo), e mesmo pola súa funcionalidade (Blogs, Wikis, Foros, ...)

### ***23.1.5 Criterios de valoración***

Á hora de proceder á implantación dun SXC, é necesario ter en conta unha serie de criterios que nos servirán para establecer, en función da situación, cal é o SXC máis adecuado. Estes criterios son os seguintes:

- **Código aberto ou código propietario:** No caso dos SXC de tipo privativo, é dicir, os comercializados por empresas baixo licenzas restritivas, non se permite o acceso ao código fonte por parte de terceiros. Con todo, cos SXC de código fonte aberto, esta limitación non existe, dado que os desenvolvedores si que permiten o acceso libre e a modificación do código. Esta característica é moi importante posto que o poder dispoñer do código fonte proporciona o poder modificar o produto, aportándolle novas funcionalidades ou mesmo corrixindo posibles erros. Esta é unha faceta moi importante relacionada coa evolución do produto. Outra vantaxe dos SXC de código libre é o custo, posto que este tipo de xestores de contido son gratuítos, sen ningún custo de licenzas. No caso dos SXC comerciais, o custo pode chegar a ser moi elevado, sobre todo para un particular. Ademais de todo isto, ao redor dos xestores de contido de código libre adoitan existir comunidades de usuarios que comentan as súas experiencias co uso destes sistemas, aportan novidades e desenvolven novas funcionalidades.
- **Arquitectura técnica:** O SXC ten que ser fiable, robusto e adaptable a futuras necesidades. Para iso, é preciso ter en conta cal é a arquitectura do sistema, que tecnoloxías se utilizaron, e analizar o deseño da plataforma, co obxectivo de poder emprender ampliacións nas funcionalidades ofrecidas en



caso de ser necesario. Tamén é conveniente que permita separar contido, presentación e estrutura, de acordo cos estándares establecidos para o sitio web. Para iso, é altamente recomendable decantarse polo uso de sistemas que fagan uso de motores de modelos, así como uso de definicións de estilos baseadas en follas de estilo (CSS).

- **Grao de desenvolvemento:** É moi importante que a ferramenta seleccionada teña un grao de madurez adecuado para poder desenvolver a funcionalidade requirida, e que se dispoña de módulos ou compoñentes para lle poder engadir funcionalidade.
- **Soporte, posición no mercado e opinións:** A ferramenta ten que ter soporte tanto polos creadores como polos desenvolvedores. É fundamental que unha ferramenta sexa coñecida por moitos usuarios e expertos, pois este feito pode axudar a posibles usuarios a se decidir polo SXC en cuestión. Habitualmente as grandes comunidades de usuarios e desenvolvedores atópanse ao redor dos SXC libres, proporcionando un marco ideal para o rápido desenvolvemento destes sistemas así como do seu mantemento.
- **Usabilidade:** Partindo da premisa de que existen diferentes roles con diferenciación clara de tarefas, debemos de ter en conta que determinados perfís de usuarios non teñen por que ter coñecementos técnicos. Iso implica que o SXC ten que ser fácil de aprender e utilizar.
- **Accesibilidade:** Temos que ter en conta que no momento en que traballamos con SXC, o sistema debe estar preparado para o uso por parte da maior cantidade de usuarios posible. Xa que logo, é sempre recomendable que o portal web cumpra un estándar de accesibilidade.
- **Velocidade de descarga:** É importante que as páxinas solicitadas polos usuarios se carguen rápido. A natureza das páxinas dinámicas e a separación de estrutura, presentación e contido contribúen a que as páxinas sexan máis lixeiras.



### **23.1.6 JOOMLA!**

#### **23.1.6.1 Introducción**

Joomla! é un dos SXC con maior impacto e distribución. Isto foi proporcionado polo feito de ser un sistema de código aberto, desenvolvido nunha das linguaxes maioritarias para a internet como é PHP. Está recollido baixo licenza GPL e actualmente conta cunha das maiores comunidades de usuarios e desenvolvedores. Este administrador de contidos pode traballar na internet ou nas intranets e require dunha base de datos MySQL, así como dun servidor web, preferiblemente HTTP Apache.

#### **23.1.6.2 Arquitectura**

En canto ao seu deseño, desde o punto de vista de desenvolvemento, Joomla! está programado en PHP baixo un patrón Modelo-Vista-Controlador, integrando un motor de modelos, e permitindo separar totalmente a capa de presentación da lóxica dos datos. Esta posibilidade modular proporciona unha gran facilidade para estender o sistema. As funcionalidades en Joomla! engádense nos módulos ou compoñentes. Estes módulos ou compoñentes son partes do sistema que se executan de forma independente, baixo o patrón MVC, e intégranse perfectamente dentro do SXC principal. Existen repositorios libre da comunidade de usuarios e desenvolvedores onde se poden atopar centos de módulos gratuítos para estender as funcionalidades de Joomla!. Con todo, esta cota tamén representa un modelo de negocio para moitas empresas que proporcionan os seus produtos en forma de módulos para Joomla!. Así pois, o deseño patronizado mediante MVC e o uso de tecnoloxías maduras como PHP e MySQL fai que resulte relativamente sinxelo ampliar as funcionalidades deste SXC a partir da execución propia de módulos que satisfagan algunha funcionalidade concreta.

O SXC Joomla presenta unha arquitectura en tres niveles: nivel de extensións, nivel de aplicación e de desenvolvemento.

O nivel superior, de extensións, componse de extensións do marco de desenvolvemento de Joomla e das súas aplicacións. Nesta capa sitúanse os módulos, compoñentes e modelos (*templates*). O nivel do medio, de aplicación, consiste nunha serie de aplicacións que estenden do "core" para lles dar soporte aos módulos e compoñentes. Implanta tamén as aplicacións necesarias para a administración (*backend*) así como a arquitectura principal do *frontend*. O nivel inferior, correspondente ao de desenvolvemento, consta do conxunto de clases PHP que o forman, as bibliotecas que son utilizadas polo marco de desenvolvemento ou se instalan para uso polos desenvolvedores e finalmente os *plug-ins*, que estenden a funcionalidade.

Algunhas características básicas que se inclúen en Joomla! son: sistema adaptado para mellorar o rendemento web, versións imprimibles de páxinas e xeración directa en pdf, módulos de flash con noticias, integración con blogs e foros, módulos nativos para a xestión de enquisas, calendarios, procura no sitio web e internacionalización da linguaxe. O nome de Joomla! provén dunha pronunciación fonética para anglófonos da palabra suahili *jumla*, que significa "todos xuntos" ou "como un todo". Foi escollido como unha reflexión do compromiso do grupo de desenvolvedores e a comunidade do proxecto.

### **23.1.6.3 Comunidade de desenvolvemento**

A comunidade de Joomla, para o desenvolvemento das súas múltiples fronteiras, usa diferentes formas de comunicación como son o uso de salas de chat a través de IRC, participación en foros especializados, listas de correo, "wikis" e blogs. A xestión de administración principal do proxecto está delegada ao grupo principal, coñecido como "Core Team". Este grupo de desenvolvedores representa a columna vertebral do proxecto, xa que son os encargados de guiar a Joomla! dentro do movemento de código aberto. Este grupo esta composto por diferentes perfís, con variadas experiencias e totalmente multidisciplinar. Leva activo desde o ano 2005,

aproximadamente co nacemento oficial de Joomla!. A súa responsabilidade principal radica na organización con respecto Joomla na súa estrutura funcional como organización e non unicamente na programación do sistema de xestión de contidos.

Ademais do grupo principal ou *Core Team*, existen tamén outros grupos que se crearon para enriquecer o coñecemento que a comunidade Joomla proporciona. Cada un dos grupos especialízase nun aspecto específico de Joomla! que é importante para a expansión e desenvolvemento. O grupo principal non pode estar en cada discusión destes temas, por iso existe unha estrutura xerarquizada onde un responsable de cada grupo de desenvolvemento se encarga de comunicarse de forma directa co grupo principal.

Ademais do traballo da comunidade de usuarios e desenvolvedores, existe unha organización que proporciona soporte para moitos aspectos do proxecto. Trátase da Open Source Matters Inc (OSM), que é unha organización sen ánimo de lucro de orixe estadounidense. O obxectivo fundamental desta organización é dar soporte á parte legal e financeira do proxecto de código aberto Joomla. Recentemente a OSM incorporouse como unha organización sen ánimo de lucro de Nova York, proporcionando unha garantía de continuidade para o proxecto e actividades futuras, proporcionando o soporte necesario para que as comunidades de usuarios e desenvolvedores poidan seguir participando.

#### **23.1.6.4 Principais características**

As principais características que fixeron de Joomla un dos mellores SXC do momento son as seguintes:

- **Usabilidade da súa interface:** Esta característica faise principalmente notoria na interface de administración. O obxectivo fundamental é que calquera persoa sen coñecementos técnicos poida ter control do sistema, para acurtar a curva de aprendizaxe das tarefas administrativas.

- **Xestión de contido:** O sistema presenta unha estrutura xerárquica para xestionar o contido baseada en agrupacións de artigos (a unidade fundamental de contido) que se organizan en seccións e categorías. Permite crear menús e submenús, subir imaxes e ficheiros, así como syndicar de forma nativa noticias mediante RSS.
- **Xestión de usuarios:** Existen dous tipos de usuarios básicos: os usuarios invitados, que son aqueles que acceden ao portal navegando, que non posúen ningunha conta no sistema e que habitualmente están capacitados para consultar os artigos, e os usuarios rexistrados que son aqueles que dispoñen dunha conta (nome de usuario/contrasinal) para autenticarse no sitio e acceder a funcionalidades específicas. Dentro dos usuarios rexistrados existen distintos roles cada un cunha serie de privilexios. A xestión das contas e permisos dos usuarios en Joomla! pode facerse de forma nativa, ou ben facendo uso dun sistema externo como LDAP.
- **Personalizable:** Grazas á combinación do uso de estándares, e ao deseño desencaixado proporcionado polo patrón MVC, a presentación do contido pódese personalizar de forma moi sinxela. A aparencia do *frontend* é perfectamente modificable grazas ao uso de modelos. Estes modelos poden modificarse de xeito sinxelo permitindo que se adapten ás necesidades do sistema.
- **Extensibilidade:** Como xa se comentou con anterioridade, unha das principais características que definen este software é a capacidade modular da plataforma, que permite o desenvolvemento e integración dunha gran cantidade de módulos e compoñentes que permiten estender as funcionalidades do sistema. A facilidade no desenvolvemento destas pezas software proporcionou que actualmente exista un gran número de extensións e módulos existentes, programados pola comunidade de usuarios, que aumentan as posibilidades da aplicación con novas características e que se integran facilmente no sistema. Como exemplo de extensións dispoñibles, cítanse

xestores de documentos, galerías de imaxes multimedia, motores de comercio e venda electrónica, calendarios, etc.

- **Multiplataforma:** Debido á utilización de tecnoloxías libres estandarizadas, este SXC pode correr sobre calquera sistema operativo, xa sexa GNU/Linux, en Windows ou en Mac OSX. Os únicos requisitos son dispoñer na máquina dun servidor web, e dunha base de datos MySQL.

### **23.1.7 WORDPRESS**

#### **23.1.7.1 Introducción**

A popularidade crecente dos blogs ou bitácoras como medio popular para difundir contido tivo tamén cabida dentro do desenvolvemento dos sistemas de xestión de contidos. WordPress é un SXC enfocado precisamente á creación de blogs, especialmente orientado a ofrecer comodidade para a ardua tarefa de manter os sitios web periodicamente actualizados.

WordPress está desenvolvido en PHP e MySQL, baixo licenza GPL, o que tamén implica que é software libre e xa que logo o seu código é modificable e adaptable. Neste sentido, comparte moitas das vantaxes que esta filosofía lles outorga a outros SXC como Joomla!.

O fundador do proxecto de WordPress é Matt Mullenweg. WordPress foi creado a partir do desaparecido b2/cafelog e actualmente é o SXC máis popular orientado á creación de blogs. As causas do seu enorme crecemento están relacionadas coa súa licenza libre, a facilidade de uso e as características que proporcionan en xeral os sistemas de xestión de contido.

Do mesmo xeito que a maioría dos SXC máis populares, WordPress está implantado baixo un patrón MVC. Sumado a isto, ao proporcionarse como produto libre, posibilitase o labor da enorme comunidade de desenvolvedores para revisións e execución de módulos que engadan novas funcionalidades. Este é outro dos factores

que proporcionou a súa crecente expansión.

Como ocorre con Joomla!, sumado ao traballo da comunidade libre de desenvolvedores, o liderado do proxecto recae sobre unha entidade chamada Automattic.

### **23.1.7.2 Características**

Algunhas características básicas que definen WordPress son as seguintes:

- Proporciona un sistema de publicación web baseado en entradas ordenadas por data.
- A estrutura e deseño visual do sitio depende dun sistema de modelos, que é independente do contido en si. Separación da capa de presentación.
- Apóstase decididamente polas recomendacións do W3C, pero é dependente sempre do modelo que se vai usar.
- A xestión e execución corre a cargo do sistema de administración cos *plugins* e os *widgets* que usan os modelos.
- Como noutros SXC, existe unha xerarquía de usuarios/roles, e WordPress permite múltiples autores ou usuarios.
- Aínda que o sistema está orientado a configurar un único blog ou bitácora por sistema instalado, permite múltiples blogs ou bitácoras.
- Dispón de múltiples ferramentas para organizar o contido (artigos) en categorías.
- Dispón de compoñentes visuais para a edición dos artigos (compoñentes WYSIWYG "What You See Is What You Get")
- Permite comentarios e ferramentas de comunicación entre blogs.

- Dispón de funcionalidades necesarias para a sindicación de contidos nos principais formatos estándar (RSS 2.0 e ATOM 1.0).
- Subida e xestión de adxuntos e arquivos multimedia.
- Sistema de busca integrada dentro da plataforma.

### **23.1.8 DRUPAL**

#### **23.1.8.1 Introducción**

Outro dos máis coñecidos no mundo dos SXC é Drupal. Drupal é un sistema de xestión de contido, similar en canto á súa arquitectura e orientación a Joomla!. É un sistema modular multipropósito e moi configurable. Permite xestionar e publicar artigos, imaxes, ou outros arquivos. O seu deseño modular permite integrar unha gran cantidade de servizos diferentes como foros, enquisas, votacións, blogs e administración de usuarios e permisos.

Drupal é un sistema dinámico. Isto implica que, como en todos os anteriores, o contido se almacena de forma persistente nunha base de datos, e as páxinas que se demandan desde o *frontend* de consulta son xeradas dinamicamente. O sistema encárgase de acceder ao contido da base de datos e montar a páxina que subministrará o servidor web.

É un programa libre, con licenza GNU/GPL, escrito en PHP baixo un patrón de deseño MVC, o que de novo facilita a súa modificación e adaptabilidade, potenciando o traballo da extensa comunidade de usuarios.

Algunhas características propias de Drupal no que atinxe ao seu desenvolvemento son a calidade do seu código e das páxinas xeradas. Fai especial fincapé no respecto dos estándares da web, e unha énfase particular na usabilidade e consistencia de todo o sistema.

O deseño de Drupal faino especialmente idóneo para construír e xestionar comunidades na internet. Con todo, grazas ás súas características de flexibilidade e adaptabilidade, así como a gran cantidade de módulos adicionais dispoñibles, converte a Drupal nun SXC de propósito xeral, capaz de adecuarse a moitos tipos diferentes de sitio web.

### **23.1.8.2 Características**

As súas características principais son as seguintes:

- **Extensibilidade:** Grazas á extensa comunidade de usuarios e desenvolvedores, dispón dunha gran cantidade de módulos con distintas funcionalidades: foro, galería, enquisas, boletín de noticias, correo electrónico, chat, etc.
- **Código aberto:** Ao estar dispoñible o código fonte baixo os termos da licenza GNU/GPL, é posible estender ou adaptar Drupal segundo as necesidades.
- **Personalización:** A capa de presentación está perfectamente illada do resto do sistema, facendo a aparencia totalmente configurable en función das preferencias dos usuarios.
- **Xestión de usuarios:** Como todo SXC, dispón dunha xerarquía de usuarios/roles e dun sistema interno para xestionalos e permitir a autenticación. Esta última pode facerse ben de forma local ou utilizando un sistema de autenticación externo.
- **Xestión de contidos:** Proporciona un sistema de control de versións, que permite seguir e revisar todas as actualizacións do contido. Dispón dun sistema de temas ou modelos que permite separar o contido do sitio da presentación. Tamén conta coa posibilidade de exportar o contido en formato RDF/RSS para ser utilizado por outros sitios web.
- **Multiplataforma:** Pode funcionar con calquera servidor web (Apache, Microsoft IIS) e en sistemas como Linux, Windows, Solaris, BSD e Mac OS X.



Ao estar executado en PHP é portable.

## **23.2 E-LEARNING**

### **23.2.1 Introducción**

Nos últimos anos apareceron sistemas informáticos orientados ao ensino e aínda que o obxectivo de todos eles é moi similar, os medios mediante os cales chegan a ese obxectivo varían en gran medida. Involucrar as novas tecnoloxías no ámbito do ensino, introducindo as mesmas como ferramenta fundamental do proceso de aprendizaxe, desembocou na aparición dun novo termo coñecido como e-Learning. As tecnoloxías asociadas englóbanse nun conxunto de sistemas que tratan de proporcionar os medios e mecanismos adecuados para facilitar os procesos de aprendizaxe en practicamente todas as áreas de coñecemento. Con todo, moitos destes sistemas, mal identificados como “sistemas de e-Learning”, céntranse unicamente na xestión e clasificación de documentos para poñelos a disposición de alumnos e docentes, como é o caso dos sistemas de xestión de contidos, ou dos sistemas de xestión documental. Aínda que certamente facilitan a tarefa de busca e organización de información, este tipo de sistemas non realizan ningún tipo de seguimento do proceso de aprendizaxe dos alumnos.

A idea de e-Learning, e en consecuencia, dos sistemas de e-Learning, pretende precisamente abarcar esa fase do proceso de aprendizaxe, proporcionando os mecanismos necesarios para realizar o seguimento do proceso de forma íntegra.

### **23.2.2 Concepto**

O concepto de e-Learning defínese de moitas formas diferentes,

fundamentalmente debido a que os actores que del fan uso son moi diversos, cada cal coa súa idiosincrasia e co seu ámbito de aplicación.

A nivel xeral, pódese definir o e-Learning como a educación a distancia completamente virtualizada a través das novas posibilidades tecnolóxicas que hai dispoñibles, como as novas redes de comunicación, e fundamentalmente a rede de redes, a internet. Fundamentalmente utilízanse para iso ferramentas ou aplicacións de hipertexto, que proporcionan a vantaxe de ser totalmente portables e accesibles desde calquera plataforma. A idea é que este tipo de sistemas dean soporte aos procesos de ensino-aprendizaxe. Este tipo de sistemas poden englobarse como un subgrupo dos sistemas de xestión de contidos, entendendo estes últimos como unha xeneralización, e asumindo os sistemas de e-Learning como unha especialización dos SXC para un propósito específico con funcionalidades propias.

Algúns teóricos dividen o e-Learning en tres ramas diferentes:

- computer aid instruction (CAI)
- computer-managed instruction (CMI)
- computer supporter learning resources (CSLR)

O primeiro termo abrangue a porción de produtos de e-Learning que proporcionan ensino como titoriais, simulacións e exercicios. O segundo termo refírese aos produtos de e-Learning que teñen funcións de avaliación, seguimento e guía de estudo. Finalmente, o terceiro termo cobre os aspectos do e-Learning que dan soporte ao desempeño, a comunicación e o almacenamento. Esta clasificación refírese só a partes do conxunto total representado polo e-Learning.

### ***23.2.3 Plataformas de e-Learning***

Na práctica, para levar a cabo un programa de formación baseado en e-Learning, faise uso de plataformas ou sistemas de software que permitan a comunicación e interacción entre profesores, alumnos e contidos. Existen principalmente dous tipos de plataformas:

- LMS (Learning Management Systems), utilizados para impartir e dar seguimento administrativo aos cursos en liña.
- LCMS (Learning Content Management Systems), empregados para a xestión dos contidos dixitais. Seguen o concepto básico dos SXC, que é a administración de contidos, pero enfocados ao ámbito educativo.

Ás veces a diferenciación entre ambas é só funcional e en lugar de constituír dúas ferramentas software diferentes ofrécense nunha mesma aplicación, que en España se coñece polo nome de Plataforma Tecnolóxica ou de Teledocencia.

Entre as ferramentas máis utilizadas para os ambientes ou sistemas e-Learning están, como xa se dixo anteriormente, os sistemas de administración de aprendizaxe ou LMS, tamén amplamente coñecidos como plataformas de aprendizaxe. Un LMS é un software baseado nun servidor web que prové módulos para os procesos administrativos e de seguimento que se requiren para un sistema de ensino, simplificando o control destas tarefas. Os módulos administrativos permiten, por exemplo, configurar cursos, matricular alumnos, rexistrar profesores, asignar cursos a un alumno, levar informes de progreso e cualificacións. Tamén facilitan a aprendizaxe distribuída e colaboradora a partir de actividades e contidos preelaborados, de forma síncrona ou asíncrona, utilizando os servizos de comunicación da internet como o correo, os foros, as videoconferencias ou o chat.

O alumno interactúa coa plataforma a través dunha interface web que lle permite seguir as leccións do curso, realizar as actividades programadas, comunicarse co profesor e con outros alumnos, así como dar seguimento ao seu propio progreso con datos estatísticos e cualificacións. A complexidade e as capacidades das plataformas varían dun sistema a outro, pero en xeral todas contan con funcións

básicas como as que se mencionaron. Entre as plataformas comerciais máis comúns atópanse Blackboard e WebCT, mentres que as máis recoñecidas por parte do software libre son Moodle e Claroline.

#### **23.2.4 Vantaxes**

O e-Learning permite superar algunhas das barreiras existentes nos sistemas de ensino asistido por ordenador. Algunhas delas son:

- Elimina as distancias e favorece a mobilidade dos alumnos.
- Aumenta o número de destinatarios que poden seguir un curso simultaneamente.
- Permite flexibilidade horaria.
- Permite alternar diversos métodos de ensino.
- Favorece a interacción entre alumnos. Está demostrado que a non presenza física minimiza a timidez e favorece o establecemento de comunicación entre os alumnos, especialmente na adolescencia.
- Anonimato.
- Seguimento e tutoría do progreso do alumno a través das canles de comunicación establecidos.
- Posibilidade de escoller entre gran variedade de materiais, cursos e especialidades.
- Minimiza os custos de formación continua na empresa.
- Favorece a convivencia familiar para alumnos con responsabilidades familiares ao seu cargo.

Ademais de polas vantaxes enumeradas, interveñen outros factores que favorecen a implantación de sistemas e-Learning:

- **Factores económicos:** Alcánzase unha mellor relación custo-beneficio na produción e desenvolvemento aproveitando a reutilización de compoñentes tecnolóxicos e materiais de aprendizaxe. É un factor interesante á hora de aumentar os niveis de formación en países en desenvolvemento, cun alto ritmo de crecemento económico e con grandes necesidades de traballadores cualificados.
- **Alta dispoñibilidade de recursos dixitais:** As grandes empresas multinacionais necesitan distribuír materiais de aprendizaxe a sitios xeograficamente dispersos, para que estean dispoñibles en calquera momento desde calquera lugar. A existencia dun gran número de recursos dixitais libres e gratuítos na internet (imaxes, clips de audio e vídeo, animacións, etc.) favorecen a súa reutilización e aproveitamento por parte das grandes empresas (ou terceiros, como pode ser unha empresa especializada na creación de cursos ou implantación de sistemas de e-Learning) para a creación de cursos a través de sistemas e-Learning.
- **Penetración social:** A alta penetración na sociedade das novas tecnoloxías en xeral e da internet en particular, favorece a aceptación de novas vías de información e de comunicación.
- **Axudas estatais:** Os programas de subvencións por parte do Estado, as comunidades autónomas e o Fondo Social Europeo, incentivaron a creación e desenvolvemento dun sector empresarial dedicado á formación en liña. Estas subvencións fixeron posible a aparición de programas como os de Formación Continua de traballadores, que contribúen á adaptación dos traballadores ás máis novas tecnoloxías.

### **23.2.5 Inconvenientes**

Algúns inconvenientes no emprego de sistemas de e-Learning son:

- **Preparación do estudante:** É necesario un esforzo para asegurar que os estudantes teñen as habilidades e coñecementos técnicos, así como o acceso ao hardware e software necesarios para completar satisfactoriamente o curso baseado nas TIC. Tanto a xestión do tempo e as habilidades metacognitivas están relacionadas coas actitudes e a motivación do estudante.
- **Persoal dedicado:** Do mesmo xeito que os estudantes, os profesores deben ter habilidades técnicas, coñecemento e acceso ao hardware e software, necesarios neste caso, para facilitar o deseño e desenvolvemento do curso baseado nas TIC. E deben ter un excelente manexo do tempo e a motivación para proporcionar asistencia e levar o seguimento do estudante. Non obstante algúns autores diferencian rol do profesor, encargado da selección de contidos, seguimento e asistencia ao alumno, do rol do técnico encargado do deseño e creación do curso e-Learning a partir dos contidos, obxectivos e metodoloxías, establecendo desta forma a necesidade de diferentes perfís.
- **Xestión da información:** Malia que se posúan unhas habilidades técnicas e un manexo do tempo excepcionais, tanto os profesores como os alumnos requiren de interfaces que reduzan as cuestións loxísticas e técnicas. O uso de boletíns e listas de distribución poden axudar a manexar a sobrecarga de información.
- **Equidade:** Non todos os usuarios contan coas mesmas facilidades de acceso á internet. A tecnoloxía incrementa as diferenzas entre os que teñen e os que non teñen tales posibilidades.
- **Largo de banda:** Este é un dos maiores inconvenientes desde hai unha década e que está desaparecendo rapidamente coa chegada de liñas de banda larga. Actualmente, en Europa, o largo de banda é aceptable e permite

transmitir con bos resultados audio e vídeo sincronizados sen os indesexables “saltos” de outrora.

### ***23.2.6 Estandarización***

Un dos principais problemas dos sistemas de e-Learning sempre foi reutilización dos contidos, de forma que estes poidan ser utilizados en sistemas diferentes, debido a que a maioría dos sistemas definían os seus propios formatos de almacenamento e procesamento dos contidos educativos, así como a forma de acceder e manexalos. Esta falta de acordo débese en gran medida á descoordinación no desenvolvemento de estándares para e-Learning na década pasada.

Hoxe en día existen multitude de sistemas destinados ao ensino, xa sexan simples xestores de contidos, xestores do proceso de aprendizaxe ou sistemas máis completos capaces de dar soporte a procesos administrativos, ofrecer ferramentas de autoría e edición de cursos, etc. Con todo, malia a variedade existente, a súa heteroxeneidade dificulta a compatibilidade entre eles. Non todos son de código aberto, algúns usan formatos propietarios e xeralmente non é posible reutilizar contidos e estruturas de aprendizaxe entre eles.

Estas incompatibilidades, xa sexan totais ou parciais, repercuten negativamente no custo asociado á implantación dun sistema de e-Learning, posto que no mellor dos casos, unha vez superado o tempo de aprendizaxe das distintas aplicacións do sistema, sería necesaria a readaptación de material xa existente para outros sistemas, ou no peor dos casos, crear devandito material desde cero. Unha especificación sobre aprendizaxe virtual asegura que o novo material siga funcionando exactamente igual independentemente da plataforma que se utilice, sempre que esas plataformas cumpran a mesma especificación.

### **23.2.7 Plataforma Moodle**

#### **23.2.7.1 Introducción**

Moodle é un acrónimo de Module Object-Oriented Dynamic Learning Environment. Consiste nunha plataforma que proporciona de forma integral mecanismos para a xestión de cursos. Moodle integra ademais as ferramentas necesarias para crear e xestionar comunidades virtuais orientadas á aprendizaxe en liña. Xa que logo, podemos clasificar Moodle como unha plataforma tecnolóxica de tipo LMS (Learning Management System).

Orixinalmente Moodle foi creado por Martin Dougiamas. Baseou o deseño da plataforma partindo de que o coñecemento se constrúe na mente do estudante en lugar de ser transmitido sen cambios a partir de libros. Existe tamén unha importante aposta polo modelo de aprendizaxe colaboradora. O propósito é construír un ambiente centrado no estudante que lle proporcione capacidade para xerar ese coñecemento, baseado nas habilidades e coñecementos propios dos titores ou profesores, en lugar de simplemente publicar e transmitir a información que se considera que os estudantes deben coñecer.

En conclusión, Moodle é un paquete de software para a creación de cursos e sitios web baseados na internet, orientado a dar soporte a un marco de educación construtivista. O sistema é multiplataforma e está rexistrado baixo licenza GNU/GPL.

En canto á arquitectura da plataforma, Moodle é unha aplicación web que se executa en servidores que soportan PHP e facendo uso de base de datos para a persistencia da información. Esa base de datos é única, e desde a versión 1.7 Moodle conta cunha capa de abstracción que lle permite seleccionar entre diversos motores de bases de datos, sendo MySQL e PostgreSQL as máis utilizadas.

#### **23.2.7.2 Principais características**

Moodle, como sistema englobado dentro dos xestores de contido, e á súa vez



como sistema específico de e-Learning, ten as seguintes características:

- Promove unha pedagogía construtivista social fundamentada no traballo colaborador, a realización de actividades e debates.
- A súa arquitectura e ferramentas son apropiadas para clases en liña, ademais de servir como complemento da aprendizaxe presencial.
- Ten unha interface de navegador de tecnoloxía sinxela, lixeira, e compatible.
- Para a súa posta en produción, unicamente é necesaria unha plataforma que soporte PHP e a dispoñibilidade dunha base de datos. Grazas á súa capa de abstracción, Moodle soporta os principais sistemas xestores de bases de datos.
- É unha plataforma segura. Todos os formularios son revisados e as testemuñas (cookies) cifradas.
- É adaptable e extensible. A maioría das áreas de introdución de texto poden ser editadas usando o editor HTML, tan sinxelo como calquera editor de texto.

### ***23.3 ACCESIBILIDADE E USABILIDADE***

#### ***23.3.1 Accesibilidade como calidade dos sistemas***

A accesibilidade é unha calidade dos sistemas informáticos vinculada ao campo da interacción entre humanos e ordenadores. Fundamentalmente céntrase na capacidade de acceso ao uso da aplicación ou sistema informático que é obxectivo por parte do usuario. No campo concreto das tecnoloxías web, accesibilidade fai referencia á capacidade de acceso á web e aos seus contidos por todas as persoas. A accesibilidade pretende facilitar o acceso a calquera tipo de usuario independentemente da discapacidade (física, intelectual ou técnica) que presenten. Tamén está relacionado con aquelas dificultades que se derivan do contexto de uso xa

sexan tecnolóxicas ou ambientais. Esta calidade está intimamente relacionada coa usabilidade dos sistemas.

Á hora de deseñar contidos, hai que ter en conta os factores de accesibilidade que permitirán que calquera tipo de usuario poida acceder en condicións de igualdade á información almacenada. Existen mecanismos e estándares actualmente que traballan sobre iso, e as tecnoloxías proporcionadas pola maioría dos SXC permiten estruturar os nosos contidos tendo en conta este tipo de facetas. Un caso concreto dáse cos sitios que teñen un código XHTML semanticamente correcto, permitindo proporcionar un texto equivalente alternativo ás imaxes e ás ligazóns. Isto supón que os usuarios cegos poidan utilizar lectores de pantalla ou liñas Braille para acceder aos contidos. O mesmo ocorre cando os vídeos dispoñen de subtítulos; usuarios con dificultades auditivas poderán entendelaos perfectamente.

Os sistemas de xestión de contido actuais permiten ademais certa personalización das características do sitio. Factores como o tamaño de letra ou as proporcións da interface comezan a ser personalizables por cada tipo de usuario, proporcionando axuda para que os usuarios con problemas visuais poidan lelos sen dificultade.

### ***23.3.2 Limitacións na accesibilidade***

Existen fundamentalmente catro tipos de limitacións na accesibilidade dos sitios web:

- Visuais: Abarcando un amplo abano de patoloxías e de distintos graos de deficiencia visual, que poden ir desde a baixa visión á cegueira total, ademais de problemas para distinguir cores.
- Motrices: Dificultade ou a imposibilidade de usar as mans, incluídos tremores, lentitude muscular, debido a enfermidades como o Párkinson, distrofia

muscular, parálise cerebral ou amputacións.

- Auditivas: Xordeira ou deficiencias auditivas.
- Cognitivas: Dificultades de aprendizaxe ou discapacidades cognitivas que afecten á memoria, á atención, ás habilidades lóxicas, etc.

### **23.3.3 Promovendo a accesibilidade**

A tarefa de promover a accesibilidade no contorno web corre a cargo do grupo de traballo Web Accessibility Initiative (WAI), que depende directamente do World Wide Web Consortium. En 1999 o WAI publicou a versión 1.0 das súas pautas de accesibilidade Web (WCAG). Co paso do tempo convertéronse nun referente internacionalmente aceptado ata que en decembro do 2008 as WCAG 2.0 foron aprobadas como recomendación oficial.

Estas pautas divídense en tres bloques orientadas especificamente para cada un dos principais perfís que forman parte dun proxecto de desenvolvemento web:

- **Pautas de accesibilidade ao contido na web (WCAG):** Están dirixidas aos profesionais do deseño e desenvolvemento web e proporcionan información e recomendacións sobre como facer que os contidos do sitio web sexan accesibles.
- **Pautas de accesibilidade para ferramentas de autor (ATAG):** Están dirixidas aos desenvolvedores do software que usan os *webmásters*, co obxectivo de proporcionar un mellor soporte para a construción de sitios accesibles.
- **Pautas de accesibilidade para axentes de usuario (UAAG):** Están dirixidas aos desenvolvedores de axentes de usuario (navegadores e similares), para que estes programas faciliten a todos os usuarios o acceso aos sitios web.

#### ***23.3.4 Usabilidade***

A usabilidade é outro atributo vinculado aos sistemas software, particularmente importante no campo da interacción home-computador. Actualmente a usabilidade está recoñecida como un importante atributo de calidade do software. Actualmente non chega con fabricar sistemas con alto rendemento e fiabilidade, senón que o obxectivo é crear sistemas que sexan cómodos e manexables, adaptados para os usuarios finais. No marco da usabilidade xerouse un importante centro de servizos no que empresas especializadas desenvolven as súas actividades fundamentalmente orientadas á asesoría nestes campos.

Nos proxectos de desenvolvemento de software en xeral, e nos orientados á distribución e xestión de contidos en particular, o concepto de usabilidade é de importancia capital. Á hora de distribuír contido a través da rede, o portal está aberto a todo tipo de usuarios. Esta faceta comparte importancia co concepto anterior de accesibilidade. Pero ademais, a usabilidade permite incrementar o atractivo, desenvolvendo sistemas sinxelos e intuitivos que permiten un fácil manexo e rápida aprendizaxe.

Desde un enfoque do deseño e avaliación de aplicacións software, falamos de usabilidade software como un conxunto de fundamentos teóricos e metodolóxicos que aseguran o cumprimento dos niveis de usabilidade requiridos.

#### ***23.4 W3C***

O World Wide Web Consortium, abreviado W3C, é o máximo organismo mundial que se encarga de xestionar e publicar as recomendacións e estándares asociados ao World Wide Web. É dicir, o obxectivo deste consorcio é estandarizar os protocolos e as tecnoloxías utilizados para construír a web, de maneira que o contido este dispoñible para a maior parte posible da poboación do mundo. As principais actividades ás que se dedica son, á coordinación dos diferentes grupos de traballo no ámbito da xeración de:

- Especificacións e estándares: sobre tecnoloxías asociadas ao WWW.
- Directrices: e recomendacións de desenvolvemento para boas prácticas.
- Ferramentas: que permitan validar a aceptación e cumprimento dos estándares e recomendacións propostas.

Está dirixida por Tim Berners-Lee, responsable do grupo de investigación que desenvolveu a URL, o protocolo HTTP (HyperText Transfer Protocol, Protocolo de Transferencia de HiperTexto), así como tamén da linguaxe de etiquetado HTML (Linguaxe de Marcado de HiperTexto) que son as principais tecnoloxías sobre as que se basea a web.

Creouse en 1994 no MIT, actual sede central do consorcio. O consorcio está formado por unha gran diversidade de membros e entidades cada unha das cales colabora nos ámbitos nos que o W3C exerce a súa función. Actualmente está integrado por tres tipos de figuras principais:

- Membros adscritos do W3C: garanten a fortaleza e o sentido do consorcio a través do investimento e a participación activa nas actividades do W3C. O W3C conta con máis de 400 organizacións membro provenientes de máis de 40 países, con intereses moi variados. Entre os membros do W3C inclúense provedores de produtos de tecnoloxía e servizos, provedores de contido, usuarios corporativos, laboratorios de investigación, organismos de estandarización e administracións, que traballan conxuntamente para alcanzar un acordo sobre a dirección que debe tomar a web.



- Equipo W3C (W3C Team): O equipo do W3C inclúe a máis de sesenta investigadores e enxeñeiros de todo o mundo que dirixen as actividades técnicas do W3C e xestionan as operacións do consorcio. A maioría dos compoñentes do equipo do W3C traballan nunha das tres institucións que albergan o W3C: O MIT/CSAIL, nos Estados Unidos; o ERCIM, as oficinas centrais en Francia; e a Universidade de Keio, en Xapón. Están coordinados polo director Tim Berners-Lee, o director de Operacións Steve Bratt, e un equipo de dirección, os traballadores do W3C:
  - Mantéñense informados sobre as novas tecnoloxías, as flutuacións do mercado e as actividades de organizacións relacionadas, con intención de orientar ao W3C adecuadamente.
  - Organizan as actividades do W3C para, así, cumprir o maior número de obxectivos dentro duns límites prácticos (tales como os recursos dispoñibles).
  - Promoven a cooperación entre os membros, á vez que buscan a súa diversidade, incentivan a innovación, e facilitan a súa activa participación.
  - Divulgan os resultados do W3C aos membros e á prensa, e promoven a súa aceptación na comunidade Web; vexa a lista de presentacións públicas realizadas polo equipo.
- Oficinas W3C (W3C Offices): O obxectivo das oficinas do W3C é traballar coas comunidades rexionais para potenciar a adopción das recomendacións do W3C entre os desenvolvedores, os creadores de aplicacións, e os difusores de estándares, así como fomentar a inclusión das organizacións máis importantes na creación de futuras recomendacións a través da súa adscrición ao consorcio.

### **23.5 BIBLIOGRAFÍA**

- *"SilverStripe: The Complete Guide to CMS Development"*. Ingo Schommer e 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](http://www.w3c.es), [www.w3c.org](http://www.w3c.org).

**Autor:** Francisco Javier Rodríguez Martínez

Subdirector de Sistemas Escola Superior Enxeñaría Informática Ourense

Colexiado do CPEIG

**24. MOTORES DE BUSCA.  
FERRAMENTAS  
COLABORATIVAS. CORREO  
ELECTRÓNICO. LISTAS DE  
DISTRIBUCIÓN. GRUPOS DE  
NOTICIAS DE REDE (NNTP).  
FOROS DE DISCUSIÓN. CHAT.  
SISTEMAS DE  
VIDEOCONFERENCIA.  
MENSAXARÍA INSTANTÁNEA.**



**Tema 24: Motores de busca. Ferramentas colaboradoras. Correo electrónico. Listas de distribución. Grupos de noticias de rede (NNTP). Foros de discusión. Chat. Sistemas de videoconferencia. Mensaxaría instantánea.**

---

## ÍNDICE

### **24.1 Motores de busca**

- 24.1.1 Spiders*
- 24.1.2 Directorios*
- 24.1.3 Sistemas mixtos (directorio e motor de busca)*
- 24.1.4 Metabuscadores*
- 24.1.5 Multibuscadores*

### **24.2 Ferramentas colaboradoras**

- 24.2.1 Características*
- 24.2.1 Groupware*
- 24.2.2 Workflows*

### **24.3 Correo electrónico**

- 24.3.1 Elementos do servizo de correo electrónico*
- 24.3.2 Enderezo de correo electrónico*
- 24.3.3 Proceso de envío de mensaxes*

### **24.4 Listas de distribución**

### **24.5 Grupos de noticias de rede**

### **24.6 Foros de discusión**

### **24.7 Chat**

### **24.8 Sistemas de videoconferencia**

### **24.9 Bibliografía**

## **24.1 MOTORES DE BUSCA**

Nos inicios, a internet comezaba a ofrecer unha gran cantidade de información, que dificilmente podía ser catalogada e referenciada. Isto supoñía un impedimento á hora de realizar buscas de información relativas a temáticas concretas, provocando unha alta ineficiencia a nivel xeral no uso da internet e o acceso á rede para a busca e/ou divulgación da información. Como solución para este problema xurdiron os motores de busca.

Os motores de busca, tamén coñecidos como buscadores, son sistemas software, que se encargan de localizar sitios web relacionados cun determinado conxunto de termos clave que lle subministran. En esencia, son un sistema informático que consulta os ficheiros das web que se encontran almacenadas nos servidores web. Para realizar esta tarefa, habitualmente utilizan unha peza de software especificamente deseñado para analizar a rede en busca de webs e obter información que permita clasificalas mediante termos clave ou ben utilizando árbores xerárquicas por temas.

A solución ofrecida polos motores de busca non é total, senón parcial. Isto débese a que en realidade non buscan na internet cada vez que realizamos unha consulta. A busca realízana nunha base de datos na cal almacenan referencias das páxinas accesibles xunto con datos concretos, metainformación, que serve para catalogalas. Esta información habitualmente recóllese a través dun programa (habitualmente robot) que é o que se encarga de realizar visitas periódicas por todo o contido dispoñible do web. Non existe unicidade nos criterios de selección para a agregar novas páxinas ás bases de datos dos motores de busca. O resultado é que cada base de datos contén información de moi diversa calidade, especificando os seus propios criterios de selección, e consecuentemente, establecendo categorizacións e resultados diferentes para cada busca en función do motor de busca co que esteamos a traballar.

A nivel xeral, pódense distinguir cinco tipos básicos de motores de busca, diferenciados entre si fundamentalmente polo tipo de información que albergan, ou os mecanismos que utilizan para realizar a referenciación das páxinas que ofrecen. Estes cinco tipos son os *spiders*, directorios, sistemas mixtos, metabuscadores e multibuscadores.

#### **24.1.1 Spiders**

Os *spiders*, tamén coñecidos como arañas web ou *crawlers*, son programas que revisan as páxinas web de forma metódica e automática. Habitualmente realizan copias das páxinas web visitadas para un procesado posterior que consiste en indexar esas páxinas en función do seu contido, determinado por conxuntos de termos clave, para proporcionar un sistema de busca posterior máis optimizado.

O funcionamento é simple. A araña iníciase cunha lista de URL ou páxinas que visitar. A medida que vai consultando as páxinas, vai engadindo todos os hipervínculos que se encontran nesas páxinas a unha lista de URL que visitará de forma recorrente en función dunhas regras establecidas. As visitas realízanse de forma periódica; polo tanto, é posible que en determinadas ocasións o contido non apareza totalmente actualizado. A orde en que se mostran os resultados da consulta está determinada por diversos factores que dependen de cada buscador en particular.

A gran maioría dos buscadores que se utilizan habitualmente entran dentro da categoría de arañas. Son sistemas custosos, que fan uso intensivo dunha gran cantidade de recursos.

Algúns exemplos de arañas son Google, Bing ou Hotbot

#### **24.1.2 Directorios**

Os directorios son un tipo de motores de busca cun funcionamento totalmente distinto das arañas. Os directorios son simplemente listas categorizadas de recursos, que se estruturan xerarquicamente. Esta estrutura organízase en forma de árbore, permitindo visualizar os contidos con diferente grao de granularidade, dende os máis xerais aos máis específicos.

En realidade estes motores non dispoñen de ningún software específico que analice os contidos web, senón que realiza as clasificacións e categorizacións do material en función dun conxunto de criterios seleccionados de forma manual. Isto implica que a tecnoloxía na que se basean sexa barata e sinxela, non obstante, o custo operacional é alto, xa que sempre se require de intervención humana.

Algúns exemplos de directorios son Yahoo! e Open Directory Project

### ***24.1.3 Sistemas mixtos (directorio e motor de busca)***

Os sistemas mixtos combinan características de directorios e motores de busca. Dispoñen habitualmente dalgunha peza software de tipo araña para realizar a análise da web, e ademais permiten engadir e presentar páxinas clasificadas en catálogos segundo o seu contido. A combinación destas características representa a tendencia actual nos buscadores máis importantes.

### ***24.1.4 Metabuscadores***

Os metabuscadores son un tipo de motores de busca que centran os seus resultados en buscas que realizan sobre outros buscadores. Isto significa que obteñen inicialmente un conxunto de resultados doutro buscador, e a continuación refinan eses resultados presentando unha selección propia.

Unha das principais vantaxes dos metabuscadores é que amplían o ámbito das buscas que realiza o usuario. Proporciona unha gran cantidade de resultados combinados en función dos criterios particulares de cada metabuscador. En moitas ocasións estes criterios de ordenación non resultan de todo claros.

Por outro lado, o problema principal é que os metabuscadores non distinguen entre as diferentes sintaxes dos buscadores, limitando a especificidade coa que os metabuscadores poden traballar para localizar información. Ademais, ao realizar as buscas en diferentes fontes (buscadores), a obtención de resultados adoita demorarse moito máis que ao utilizar outro tipo de motor de busca.

Alguns exemplos de metabuscadores son Metacrawler, Ixquick, Dogpile ou Metabuscador

#### ***24.1.5 Multibuscadores***

Os multibuscadores son un tipo de motores de busca similares aos metabuscadores, pero cunha diferenza notable; mentres que os metabuscadores non distinguen as diferentes sintaxes dos buscadores que utilizan para a obtención de resultados, os multibuscadores si o fan. Isto implica que poidan lanzar varias buscas en motores seleccionados respectando o formato orixinal dos buscadores.

Os multibuscadores son útiles para realizar buscas en diferentes buscadores ao mesmo tempo. A súa operativa difire dos buscadores normais, dado que non dispoñen de compoñentes software que analicen e almacenen contido, senón que o único que conteñen é un rexistro de buscadores e os criterios de adecuación das expresións de busca asociadas a cada buscador. Os multibuscadores non almacenan información de páxinas relativas a contido. Simplemente realizan a consulta axeitada a cada buscador dentro do seu rexistro, e realizan un filtrado das ligazóns repetidas, e aplican ademais criterios de selección como a relevancia de cada ligazón nos diferentes buscadores, para xerar finalmente unha lista de resultados. Un exemplo de multibuscador é

iniciodirecto.com.

## **24.2 FERRAMENTAS COLABORADORAS**

As ferramentas colaboradoras son aquelas que proporcionan os medios axeitados para que os usuarios finais poidan interactuar entre si e alcanzar metas comúns. Son aplicables a calquera campo de desenvolvemento. Habitualmente son coñecidos como sistemas colaboradores ou *Groupwares*. Estes sistemas dan unha maior énfase á utilización de ordenadores para a interacción das persoas. Baséanse na adopción dun espazo de traballo virtual e compartido denominado *Workplace*, definido como un sistema que proporciona procesamento de información e actividades comunicativas.

Existen diversas maneiras para clasificar os sistemas colaboradores, pero dentro deste eido adóitase utilizar unha clasificación básica que permite entender as interaccións principais entre persoas, coñecida como matriz de espazo e tempo. Esta matriz permítenos entender as interaccións principais entre os distintos tipos de taxonomías mediante as cales se pode clasificar un sistema colaborador, con respecto ao tempo e espazo.

O traballo colaborador en canto a tempo, pode ser sincrónico ou asíncrono:

- **Sincrónico:** os individuos que fan uso dos sistemas ou ferramentas colaboradoras fano ao mesmo tempo.
- **Asíncrono:** Os individuos que traballan fano en distintos instantes de tempo.

En canto ao espazo, o traballo en grupo divídese en dous tipos: no mesmo espazo de traballo ou en espazos distintos. Cando se fala de mesmo espazo de traballo, fai referencia ao mesmo lugar físico onde o grupo de persoas traballa, o cal á

súa vez pode darse no mesmo momento do tempo ou en momentos distintos. Do mesmo xeito os integrantes poden traballar en distintos lugares físicos ao mesmo ou distinto tempo.

Segundo esta clasificación, observamos que o traballo colaborador ten catro alternativas de reunións, as cales virían dunha mestura entre os tempos e espazos posibles de colaboración.

	<b>Mesmo tempo</b>	<b>Diferentes tempos</b>
<b>Mesmo lugar</b>	Interacción sincrónica cara a cara	Interacción asíncrona
<b>Diferentes lugares</b>	Interacción sincrónica distribuída	Interacción asíncrona distribuída.

Estas catro categorías móstrannos unha gama de colaboración posible na taxonomía espazo tempo:

- Colaboración sincrónica cara a cara: Dáse cando as persoas están a traballar ao mesmo tempo e no mesmo lugar. Este tipo de colaboración prodúcese usualmente nunha sala de reunións, podendo estar a traballar nun orzamento entre varias persoas ou no proceso de ensino e aprendizaxe dentro dunha sala de clases.
- A interacción asíncrona refírese aos procesos que acontecen nun mesmo lugar pero en distintos instantes. Isto pode realizarse a través dun ficheiro nunha oficina ou universidade.
- Na interacción sincrónica distribuída as persoas encóntranse en distintos lugares, pero están traballando ou interactuando ao mesmo tempo. Isto podería ser unha chamada por teléfono ou unha conferencia telefónica,

algún tipo de chat ou unha videoconferencia.

- Cando os participantes que están a realizar o proceso de colaboración están en diferentes lugares e cada un traballa nos tempos que máis lle acomode, entón dicimos que a colaboración se denomina asíncrona distribuída. Usualmente nesta área teñen lugar os sistemas que apoian a produción dun material final coa preparación de material individual, os sistemas de correos electrónicos e *workflow* (automatización dos procesos que se usan diariamente nunha empresa).

#### **24.2.1 Características**

As ferramentas colaboradoras en xeral comparten unha serie de características comúns, pero un sistema *Groupware* debe ter en conta polo menos catro aspectos fundamentais para o soporte eficiente dun proceso colaborador:

- Percepción ou conciencia de grupo
- Comunicación
- Coordinación
- Memoria de grupo

O concepto de percepción en sistemas colaboradores pódese ver como o contexto persoal de traballo baseado no entendemento das actividades dos demais membros do grupo. A ausencia de percepción deixa os participantes nun estado similar ao bloqueo dos seus sentidos, imposibilitando a súa interacción cos demais. A manipulación de artefactos nun sistema colaborador, especialmente en sistemas síncronos de tempo real, debe proporcionar información acerca das manipulacións realizadas polo resto de participantes neses artefactos. Esa información coñécese como "*feedback*" ou retroalimentación.



Tamén é necesario proporcionar diferentes mecanismos de comunicación (síncronos e asíncronos), que permitan crear as condicións axeitadas para que se dean os procesos de intercambio de información.

Por outro lado, débese garantir o acceso aos artefactos xerados, a súa creación e mantemento de forma cooperativa, previndo e evitando fallos de coordinación que leven a situacións como duplicación da información ou varios participantes intentando utilizar concorrentemente un recurso compartido.

### **24.2.1 Groupware**

O *groupware* é un tipo de software colaborador que axuda a grupos de traballo a realizar as súas actividades a través dunha rede.

As características máis importantes dos *groupware* son:

- Prover dun ambiente de colaboración, no que realmente se perciba que o traballo en grupo se leva a cabo.
- Manter a información nun único sitio común para todos os membros.
- Interactuar con outros usuarios, de forma escrita, voz ou vídeo.

Os *groupware* pódense clasificar en base a tempo e espazo. Sobre a base do tempo clasifícanse en sincrónicos e asíncronos; e sobre a base do espazo, poden estar no mesmo lugar ou en forma distribuída. As aplicacións típicas dos *groupware* sincrónicos (os cales soportan aplicacións en tempo real) son: encerados compartidos, teleconferencia, chat e sistemas de toma de decisións.

Alguns exemplos de aplicacións típicas dos *groupware* asíncronos son: correo electrónico, *newsgroups*, calendarios e sistemas de escritura colaboradores. Os

groupware estanse volvendo máis populares dentro das empresas, xa que resulta máis barato instalar unha intranet e comprar ou implantar un sistema de colaboración que estar a transportar persoal dun lugar a outro. Ademais cando se necesita tomar unha decisión urxente e as persoas están en diferentes partes do mundo, para cando se reúnan a decisión posiblemente xa non funcione, ou peor aínda que a empresa quebre; cos groupware isto non pasaría, xa que se poden tomar decisións sen importar a distancia entre cada membro do equipo.

### **24.2.2 Workflows**

Os *workflows* son sistemas que axudan a administrar e automatizar procesos de negocios. Un *workflow* pode ser descrito como o fluxo e control nun proceso de negocio. Entre os exemplos de proceso de negocios temos: procesamento de ordes, informes de gastos, procedementos de produción, etc. Cabe mencionar que os *workflows* son só un camiño para a información, para reducir tempo, diñeiro e esforzo na execución dun proceso de negocio. As funcións máis comúns que proporcionan os *workflows* son:

- Asignación de tarefas ao persoal.
- Aviso ao persoal de tarefas pendentes.
- Permitir a colaboración nas tarefas comúns.
- Optimización de recursos humanos e técnicos, aliñándoos á estratexia da empresa.

### **24.3 CORREO ELECTRÓNICO**

O correo electrónico, ou e-mail, está catalogado como un servizo de rede que lles proporciona aos usuarios a capacidade para enviar e recibir mensaxes e arquivos de forma rápida e eficiente a través de dispositivos dixitais. O sistema trata de representar unha analoxía co correo postal habitual, presentándose como unha alternativa para o envío de mensaxes de texto ou calquera tipo de ficheiro en formato dixital. Dado que o seu custo operacional é baixo e a súa eficiencia é elevada, o correo electrónico está actualmente a desprazar o correo postal orixinal.

A orixe do correo electrónico é anterior mesmo á rede internet. Os primeiros pasos para a creación do sistema de correo electrónico déronse no MIT contra 1961, cando se desenvolveu un sistema que permitía a varios usuarios, dende terminais remotos, ingresar nun *mainframe* no cal podían almacenar unha copia dos seus arquivos no disco. Este foi un dos pasos iniciais na implantación de mecanismos para o compartimento de información. En 1965 comezou a utilizarse un sistema baseado no almacenamento de mensaxes compartidas entre os usuarios dunha supercomputadora dando lugar ao primeiro sistema de correo electrónico utilizado. Posteriormente, en 1971, incorporouse ao sistema de mensaxaría o uso da arroba (@) como elemento para dividir o nome dos usuarios da máquina na que se encontraban aloxados.

### ***24.3.1 Elementos do servizo de correo electrónico***

Tecnicamente falando, o correo electrónico é un servizo proporcionado na internet, soportado polo protocolo SMTP (Simple Mail Transfer Protocol) e o protocolo POP (Post Office Protocol). Como en todo servizo, a arquitectura do sistema consta dunha parte clienta habitualmente utilizada polos usuarios para enviar e recibir correos, e unha parte servidora que proporciona os mecanismos axeitados para o almacenamento e transferencia dos correos entre os diferentes clientes. Os protocolos definen os esquemas de comunicación entre os clientes e os servidores para que as mensaxes se transmitan dun sitio a outro. O protocolo SMTP é o protocolo encargado

do envío das mensaxes, mentres que o protocolo POP é o encargado da recepción das mensaxes.

O **cliente de correo electrónico**, tamén chamado **Mail User Agent (MUA)** é un programa que basicamente permite xestionar as mensaxes recibidas así como recibir correos novos. Habitualmente faise referencia a cliente de correo electrónico, faise referencia a aplicacións *stand-alone* que proporcionan un amplo abano de funcionalidades para a xestión do noso correo. Non obstante, actualmente a maioría dos provedores de servizo de correo permiten o acceso a través dos navegadores web, proporcionando interfaces web a xeito de cliente para a consulta e xestión do noso correo electrónico. Existe unha gran diferenza respecto do funcionamento de ambas as dúas opcións; cando se utiliza un cliente de correo electrónico, todas as mensaxes dispoñibles descárganse no computador no que se estea executando ese cliente de correo electrónico. Non obstante, cando se accede á conta de correo a través das interfaces web, as mensaxes seguen almacenadas no servidor, sendo accesibles a través do cliente web, dende calquera ordenador que dispoña dunha conexión á internet.

Algúns exemplos de clientes de correo electrónico *stand-alone* son:

- **Microsoft Outlook:** Cliente privativo da compañía Microsoft. É o cliente de correo estándar de Microsoft, incluído no paquete Microsoft Office.
- **Mozilla Thunderbird:** Alternativa de software libre de Outlook, desenvolvido por Mozilla.

Algúns exemplos de provedores de servizo de correo web son Gmail, Hotmail ou Yahoo!.

En canto ao **servidor de correo electrónico** consiste nun conxunto de aplicacións informáticas situadas nun equipo servidor, xa sexa en rede local ou na internet, coa tarefa de realizar unha serie de procesos que teñen a finalidade de transportar información entre os distintos usuarios do servizo. O servidor de correo electrónico é o encargado de xestionar a todos os usuarios rexistrados no sistema

coas súas correspondentes identificacións (enderezos de correo electrónico) que servirán para poder interactuar entre si mediante o envío de correos.

O **servidor de correo electrónico**, dispón dunha peza software denominada Axente de Transferencia de Correo (MTA) ou Axente de Transporte de Mensaxes, que ten por obxectivo transmitir os datos dunha máquina a outra. En concreto, céntrase na parte de transferencia de datos entre distintos servidores, exercendo diferentes roles como servidor doutros servidores de correo, cliente doutros servidores de correo e como intermediario entre o cliente de correo que emite a mensaxe e outro servidor de correo externo.

Actualmente, a excepción das grandes corporacións que dispoñen da súa propia infraestrutura TIC, a maioría dos usuarios fan uso de servidores de correo electrónico que pertencen a algunha entidade provedora dese servizo. Existen diferentes empresas e entidades que ofrecen servizos de correo electrónico, tanto de forma gratuíta coma de pagamento. Os servizos de correo gratuíto son os máis coñecidos polos usuarios, e entre eles podemos destacar os servizos de Gmail, Hotmail ou Yahoo!. As entidades rexistradoras de dominio son as que habitualmente ofrecen servizos de correo electrónico asociados á conta de dominio contratada. En canto ás solucións software para a implantación dun servidor de correo electrónico, poden destacarse Microsoft Exchange Server para plataformas Windows ou Sendmail, Qmail, Zimbra e Postfix para Unix/GNULinux.

### ***24.3.2 Enderezo de correo electrónico***

O enderezo de correo electrónico é unha secuencia de palabras que teñen por obxecto identificar un determinado usuario dun servizo de correo de forma inequívoca. Este enderezo de correo representa o identificador mediante o cal o usuario pode enviar e recibir correos.

A sintaxe dun enderezo de correo é a seguinte:

- **Nome de usuario:** É conxunto de palabras escollidas polo usuario que habitualmente adoita coincidir co nome ou algún identificador da persoa ou usuario que utilizará a conta de correo. Pode conter letras, números e algúns signos.
- **@:** é o signo ou símbolo encargado de separar dúas partes importantes do enderezo de correo, concretamente o nome de usuario e o dominio.
- **Nome de dominio:** O nome de dominio na internet é unha identificación asociada a un dispositivo ou grupo de dispositivos. Habitualmente correspóndese co nome do provedor do servizo de correo.

### ***24.3.3 Proceso de envío de mensaxes***

Detállase a continuación o proceso de envío e recepción de correos electrónicos e os elementos e protocolos que interveñen entre un ordenador A e un ordenador B.

O ordenador co cliente A redacta un correo electrónico para o cliente B e envíallo. Ao realizar a operación de envío, o cliente de correo en A contacta co servidor de correo A a través do protocolo SMTP, transfírelle o correo e dálle a orde de envialo. Ao recibir a petición, o servidor de correo A verifica que o correo pertence a outro dominio. Para resolver a dirección á que lle ten que enviar o correo, realiza unha consulta a un servidor de DNS para saber quen é o encargado de xestionar o dominio asociado ao cliente B. Unha vez obtida a resposta, e resolto o servidor de correo B, o servidor de correo A comunícase con el a través do protocolo SMTP, enviándolle o correo emitido dende o cliente A, e quedando este correo almacenado no servidor B. Posteriormente, cando o cliente B decida consultar o correo, accederá

mediante o protocolo POP ao servidor de correo B e descargará as mensaxes almacenadas neste servidor que teñan por destinatario ao usuario de cliente B.

#### **24.4 LISTAS DE DISTRIBUCIÓN**

As listas de distribución, ou listas de correo electrónico son agrupacións de usuarios de correo electrónico. Mediante un software apropiado pódense configurar listaxes de enderezos de correo electrónico para o envío masivo de información a múltiples usuarios a un tempo. Cada lista de distribución de correo electrónico está á súa vez referenciada por un enderezo de correo electrónico. A grandes trazos, cada vez que un usuario autorizado emite un correo co enderezo da lista de distribución como destinatario, en realidade a lista reenviará o correo a todos os usuarios adscritos a esa lista.

As listas de correo electrónico son unha das ferramentas cada vez máis utilizadas nas organizacións para manter aos usuarios informados con noticias e información de interese. De forma habitual, é necesario que os propios usuarios se rexistren nesas listas das que están interesados en recibir noticias ou información.

As listas de correo electrónico están xestionadas polo propio servidor de correo, ou por software adicional específico para a súa xestión. Para a alta, baixa ou modificación dos datos dos usuarios, é habitual que os servidores de listas de correo electrónico poñan á disposición dos usuarios un ou varios enderezos de correo aos que enviar comandos. Ademais algúns servidores de listas de correo permiten diferentes modos de subscrición:

- Modo individual: o usuario da lista recibe todas as mensaxes que formen parte desta. Da mesma forma, se o usuario dispón dos privilexios necesarios, pode enviar correos á lista de distribución.

- Modo non correo: o usuario non recibe as mensaxes que se envían á lista pero pode enviar correos á lista. Habitualmente esta opción permite a consulta dos correos a través de interface web.
- Modo resumo diario: tamén chamado modo *digest*, consiste en que o usuario só recibe un correo diario que inclúe todas as mensaxes enviadas á lista de correo.

#### Tipos de listas de correo electrónico:

- Boletín electrónico: utilízase como medio unidireccional para a transmisión de información debido a que só poden enviar mensaxes á lista determinadas persoas encargadas da publicación e xestión dese boletín.
- Lista de debate: Neste tipo de lista, calquera subscritor pode enviar correos á lista de distribución, e o resto de usuarios poden contestalos do mesmo xeito. Desta forma pódense xerar debates e intercambios de información. As cadeas de correos van xerando fíos que poden ser contestados por calquera dos usuarios da lista.

Existen na internet diferentes servizos que permiten a creación de listas de correo electrónico de forma gratuíta, como por exemplo Google Groups, Yahoo! ou eListas.

No que atinxe á implantación, existen diferentes produtos baseados en software libre para a configuración e xestión do servizo de listas de correo, como por exemplo phpList, Sympa, Mailman e Gmane.



## **24.5 GRUPOS DE NOTICIAS DE REDE**

Os grupos de noticias son un servizo proporcionado na internet ao cal os usuarios poden subscribirse para participar de forma similar ás listas de correo. En esencia, os grupos de noticias serían similares a un taboleiro electrónico de noticias categorizadas xerarquicamente por temáticas. O contido dentro do servizo de noticias organízase como un gran número de grupos, nos que se agrupan os diferentes temas. O nome de cada unha dos grupos de noticias dispoñibles na rede consta dun conxunto de identificadores separados por puntos, habitualmente relacionados co dominio da entidade que xestiona o servidor de noticias, ou ben seguindo un estándar definido para as principais redes de grupos de noticias. Isto permítelle ao usuario subscribirse a un grupo ou grupos determinados que resulten do seu interese e recibir todas as mensaxes que o resto de usuarios envían a ese grupo.

Este funcionamento aseméllase bastante ao dunha lista correo, de feito comparten un obxectivo intrínseco que consiste na xeración de espazos de debate e foros de discusión sobre algún tema concreto. A diferenza é que coas listas de correo se reciben directamente as mensaxes no cliente de correo, mentres que coas *newsgroups* ou grupos de noticias cómpre conectarse a un servidor de noticias e extraer os grupos nos que o usuario estea interesado.

Unha vez que o usuario se rexistra nun grupo ou grupos determinados, pode agregar mensaxes ao sistema. Pode tamén publicar noticias que contesten ou repliquen outras noticias previas, formando fíos de debate. Para a xestión das noticias necesítase software específico para este servizo. Actualmente a maioría dos clientes de correo web veñen preparados para desempeñar esta función. As funcionalidades básicas que deben proporcionar son as de permitir seleccionar os grupos de interese para o usuario, lectura de noticias publicadas por outros e envío de noticias ao servidor.

Dada a cantidade de mensaxes que se xeran a diario nos grupos de noticias, é habitual que os servidores de noticias públicos dispoñan de mecanismo para evitar a

saturación dos seus sistemas de almacenamento. Unha delas consiste en estipular un tempo de vida determinado para as noticias que se van almacenando no sistema. Ao cabo dese período de vida, o contido é eliminado.

Os grupos de noticias clasifícanse xerarquicamente en función das súas temáticas, proporcionando unha axuda importante á hora de localizar os temas de interese.

## ***24.6 FOROS DE DISCUSIÓN***

Os foros son aplicacións web dinámicas que lles permiten aos usuarios o intercambio de opinións. Preséntanse como ferramentas de comunicación e intercambio de coñecemento. Están intimamente ligados cos sistemas de xestión de contidos, dado que comparten moitas das características destes últimos.

Habitualmente os foros dispoñen de sistemas integrados de xestión de usuarios e unha parte privada que permite configurar a ferramenta pasando pola configuración da aparencia ata a distribución interna de foros e subforos de discusión.

Na actualidade considéranse os foros como os descendentes modernos dos grupos de noticias. Mentres que para os grupos de noticias era necesaria a subscrición a un determinado grupo, e acceder ás mensaxes a través dun cliente asociado específico (habitualmente os xestores ou clientes de correo permíteno), para interactuar co foro, unicamente é necesario un navegador web. En función da configuración particular de cada foro, podería ser necesario que os usuarios se rexistren para poder participar.

A dinámica de uso do foro por parte dos usuarios é controlada habitualmente polo coordinador ou moderador. Neste sentido, existe nos foros unha estrita política de roles e permisos, que permite controlar a nivel de usuario as actividades vinculadas con cada rol. Este tipo de xestión de usuarios é común para a gran maioría de

aplicacións web que existen actualmente nas que o obxectivo principal é a participación dos usuarios.

Están considerados como complementos de sitios web, fundamentalmente baseados en xestores de contidos, ampliando as funcionalidades dos devanditos sitios mediante a introdución de ferramentas que lles permitan aos usuarios discutir ou compartir información relevante acerca da temática do sitio. Isto provocou o crecente desenvolvemento, dentro da comunidade de software libre, dunha gran cantidade de solucións para a posta en produción de foros de forma moi sinxela, xa sexa instalando aplicacións predefinidas e desenvolvidas nunha gran variedade de linguaxes orientadas ao web, ou ben en forma de módulos e complementos que poden ser integrados na maioría dos principais xestores de contido que existen no mercado.

Existe unha gran variedade de soportes dispoñibles para a implantación de foros. Habitualmente os paquetes desenvolvidos preparados para a instalación están desenvolvidos en linguaxes orientadas a desenvolvemento web como PHP, ASP, Perl, ou Java. A arquitectura deste tipo de aplicacións é similar á dos sistemas de xestión de contidos, dispoñendo dunha base de datos que asegura a persistencia do contido publicado no foro, así como o rexistro das configuracións e os usuarios autorizados no sistema.

Cada tipo de foro é diferente, no que se refire ás capacidades ou funcionalidades que pode ofrecer. Os máis simples limítanse unicamente á organización e publicación de mensaxes en forma de fíos, sobre os que os usuarios poden ir achegando novas anotacións. Os máis recentes inclúen avanzados sistemas de administración de contido e traen soporte integrado para a inclusión de contido multimedia.

Os exemplos máis habituais de sistemas de foros que se poden encontrar nunha alta porcentaxe de sitios en web son: phpBB, vBulletin, MyBB, SMF, YaBB, ou JavaBB. Como se comentou anteriormente, moitos sistemas de xestión de contidos integran os seus propios módulos con funcionalidade de foro, como é o caso de WordPress, Drupal ou Joomla!

## **24.7 CHAT**

O termo chat é un anglicismo que fai referencia á charla ou cibercharla. Utilízase para designar as comunicacións escritas realizadas en tempo real a través da internet entre dúas ou máis persoas. Pode realizarse a través de canles públicas, ou mediante canles privadas, dependendo do medio e protocolos que se utilicen. Este tipo de características determinan as diferentes tipoloxías de chat:

- **Webchat:** É un tipo de chat no que as mensaxes se transmiten a través de WWW. É un tipo de chat de doado acceso, dado que as interfaces están executadas como aplicacións web, accesibles dende calquera navegador. Resulta sinxelo de utilizar dado que existen unha gran cantidade de compoñentes visuais que axudan a personalizar rapidamente os estilos de escritura e visualización neste tipo de aplicacións de acceso aos webchats, o que o fai resultar atractivo para usuarios noveis. Non obstante o uso dos webchat está a decaer dado que as tarefas de actualización do contido da páxina que carga o webchat, así como a inestabilidade dalgúns navegadores fai que manter as conversacións en tempo real sexa difícil nalgúns ocasións.
- **IRC (Internet Relay Chat):** Representa a forma máis coñecida e antiga de chat que existe. IRC é un protocolo de comunicación en tempo real baseado en texto que permite comunicación entre usuarios sen necesidade de acordo previo de establecer a comunicación, é dicir, que dous usuarios que se encontren nunha canle poden comunicarse entre si sen necesidade de establecer unha comunicación previa. O IRC presenta un modelo cliente-

servidor onde as aplicacións cliente dos usuarios, que habitualmente son aplicacións *stand-alone*, se configuran e conectan contra un determinado servidor de IRC, permitindo establecer comunicación co resto de persoas que se encontran conectadas ao devandito servidor, ben mediante chat privado, ou a través de canles de libre acceso. Neste modelo de chat, existen axentes moderadores que interveñen na administración e control de todo o que sucede en cada servidor de IRC. O cliente máis habitual deste tipo de redes é o ***mIRC***.

- **Mensaxaría instantánea:** Pode considerarse outra modalidade de chat. En esencia é similar ao IRC, dado que a arquitectura deste tipo de sistemas que proporcionan mensaxaría instantánea se basea nun modelo cliente-servidor no cal aplicacións *stand-alone* se conectan contra o servidor e permiten enviar e recibir mensaxes doutros usuarios conectados ao servidor. Non obstante a gran diferenza radica en que nos sistemas de mensaxaría instantánea, para que dous usuarios se comuniquen, deberá de existir un contacto previo mediante o cal ambos os dous usuarios accedan a establecer a comunicación. A maioría destes sistemas contan coa súa propia rede que unicamente é accesible mediante o cliente propio desa rede, desenvolvido por unha entidade ou compañía concreta. Nese sentido, preséntase como un modelo de comunicación limitado e controlado que se está a comezar a adoptar nalgúns empresas e corporacións para establecer un mecanismo de intercambio de información de forma económica, controlada e fiable. Algúns sistemas de mensaxaría instantánea máis comúns son o MSN Messenger, Yahoo Messenger ou ICQ.

## **24.8 SISTEMAS DE VIDEOCONFERENCIA**

Os sistemas de videoconferencia teñen como principal característica permitir

comunicación simultánea e bidireccional de sinais de audio e vídeo, o que proporciona capacidade para manter reunións con persoas situadas en lugares afastados.

Este tipo de sistemas habitualmente integran capacidades que abranguen parte dos sistemas vistos con anterioridade xa que integran a capacidade de establecer comunicación escrita (chat) e xestión de mensaxaría instantánea. Ademais poden incluír capacidade para a transmisión de ficheiros e edición en ferramentas colaboradoras.

A base tecnolóxica dos sistemas de videoconferencia é a compresión dixital dos fluxos de audio e vídeo en tempo real.

En canto á categorización dos sistemas de videoconferencia, podemos clasificalos fundamentalmente en dous grandes grupos:

- **Sistemas de videoconferencia dedicados:** Dispoñen dos compoñentes hardware necesarios para realizar unha videoconferencia en remoto. Son sistemas de alta calidade, especiais para as circunstancias nas que se demanda unha alta fiabilidade e calidade dos datos transmitidos. Polo xeral, este tipo de dispositivos constan dunha cámara de vídeo de alta calidade e unha consola. Dentro deste tipo de sistemas podemos distinguir varios tipos de dispositivos hardware en función do obxectivo do sistema:
  - Grupos grandes: son dispositivos grandes, non portátiles, máis custosos utilizados para grandes salas e auditorios. Requiren de instalación e mantemento axeitados.
  - Grupos reducidos: non son portátiles, son máis pequenos e menos custosos, utilizados para salas de reunións pequenas. Requiren de instalación.
  - Videoconferencia individual: Trátase de dispositivos portátiles, destinados a usuarios individuais, teñen cámaras fixas, micrófonos e altosfalantes integrados na consola.
- **Sistemas de videoconferencia de escritorio:** Os sistemas de escritorio, ou sistemas de usuario, baséanse na combinación de parte software e hardware.

En canto a parte software, trátase dalgún cliente de mensaxaría con capacidade para realizar videoconferencia mediante a transmisión dunha cámara web e un micrófono conectado ao ordenador. En canto aos dispositivos hardware, simplemente serían necesarios unha cámara web e un micrófono. Na actualidade, practicamente a gran maioría dos sistemas de mensaxaría instantánea soportan videoconferencia. É o caso por exemplo dos clientes de MSN Messenger ou 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& worflkow. 1998.
- Ortega M. Velázquez Iturbide J.A. Paredes M., Fernández I. Escritura colaborativa e pdas: una propuesta de aprendizaje basada en resolución de problemas. 2003.
- Network Working Group. «[RFC 5321 - Simple Mail Transfer Protocol](#)»
- Mark Harrison (xullo 1995). *The USENET Handbook (Nutshell Handbook)*. O'Reilly.[ISBN 1-56592-101-1](#).
- Kate Gregory, Jim Mann, Tim Parker, and Noel Estabrook (xuño 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 (xullo 1995). *The USENET Handbook (Nutshell Handbook)*. O'Reilly
- Videoconferncing and Videotelephony. Richard Schphorst. Editorial Artech House. Norwood, 1996.

**Autor:** Francisco Javier Rodríguez Martínez



Subdirector de Sistemas Escola Superior Enxeñaría Informática Ourense

Colexiado do CPEIG

**25. WEB 2.0. WIKIS. BLOGS.  
COMUNIDADES VIRTUAIS.  
REDES SOCIAIS. SINDICACIÓN  
DE CONTIDOS. PODCAST.  
MODELOS DE TV NA INTERNET.  
SUITES DE OFIMÁTICA EN WEB.  
ALMACENAMIENTO EN WEB.  
ESCRITORIOS VIRTUAIS.  
MASHUPS. WIDGETS. MUNDOS  
VIRTUAIS. P2P. WEB  
SEMÁNTICA.**

**Tema 25. - Web 2.0. Wikis. Blogs. Comunidades virtuais. Redes sociais. Sindicación de contidos. Podcast. Modelos de TV na internet. Suites de ofimática na web. Almacenamento en web. Escritorios virtuais. Mashups. Widgets. Mundos virtuais. P2P. Web semántica.**

---

## **ÍNDICE**

### **25.1 Web 2.0**

### **25.2 Wikis**

### **25.3 Blogs**

### **25.4 Comunidades Virtuais**

### **25.5 Redes Sociais**

### **25.6 Sindicación de contidos**

#### *25.6.1 Fonte Web*

#### *25.6.2 Agregador de noticias*

#### *25.6.3 Formato RSS*

#### *25.6.4 Estándar Atom*

### **25.7 Podcast**

#### *25.7.1 Podcasting Vs. Streaming*

### **25.8 Modelos de TV na Internet**

#### *25.8.1 Características da televisión IP*

### **25.9 Suites Ofimáticas en Web**

#### *25.9.1 Feng Office*

#### *25.9.2 Google Docs*

#### *25.9.3 Office Web Apps*

### **25.10 Almacenamento en web**

#### *25.10.1 Dropbox*

##### *25.10.1.1 Funcionalidades de Dropbox*

### **25.11 Escritorios Virtuais**

#### *25.11.1 eyeOS*

### **25.12 Mashups**

### **25.13 Mundos Virtuais**

#### *25.13.1 Second Life*

## **25.14 P2P**

*25.14.1 Características*

*25.14.2 Tipos de redes P2P*

25.14.2.1 Redes P2P centralizadas

25.14.2.2 Redes P2P híbridas, semicentralizadas ou mixtas

25.14.2.3 Redes P2P puras ou totalmente descentralizadas

## **25.15 Web semántica**

*25.15.1 Definición de web semántica*

*25.15.2 RDF, SPARQL e OWL*

## **25.16 Bibliografía**

### **25.1 WEB 2.0**

O concepto de web 2.0 nace para describir aquelas aplicacións web que se centran no usuario, en contraposición á web tradicional (ou 1.0) que simplemente actúa como unha mera presentadora de datos. A web 2.0 fomenta a interacción co usuario, a interoperabilidade, e busca compartir información e a colaboración. Este concepto desenvolveuse principalmente mediante servizos web, redes sociais, wikis, blogs e sistemas de almacenamento de vídeos, entre outros.

Pódese entender a web 2.0 como a evolución dunha serie de aplicacións tradicionais noutras enfocadas ao usuario, non tanto dende un punto de vista tecnolóxico, senón de concepto e intención. Así, a través do concepto 2.0, certas aplicacións irán abandonando o escritorio e irán migrando á web, sempre baseándose na colaboración co usuario e a interactividade. Para permitir o uso do software en liña e outras aplicacións multimedia, a extensión da banda larga foi un factor fundamental.

A web 2.0 é unha actitude de compartir información, colaboración, interacción, cambio continuo e a creación dunha plataforma global.

A web 2.0 é unha reinterpretación da web, que describe os pasos para chegar a un modelo de comunicación colectiva máis participativa e innovadora.

Un dos principais cambios prodúcense na xestión dos datos. Na web 1.0, é a empresa a que xestiona a información, a través dunha rede de expertos, ou algún tipo de procesamento artificial. Pola súa banda, a web 2.0 é un concepto colaborador no que se espera que os datos sexan obtidos por medio dos usuarios.

En 2004, O'Reilly Media realiza unha conferencia sobre web 2.0, onde se comeza a

sentar as bases deste concepto. Dende o primeiro momento déixase claro que non se trata dun cambio tecnolóxico na web, senón un cambio na forma na que desenvolvedores e usuarios utilizan a web. Non obstante, Tim Berners-Lee, o creador da World Wide Web, cualificou o termo 2.0 como "labia", xa que, segundo el mesmo, a web xa contiña eses valores dende un principio.

Con anterioridade ao concepto 2.0, a maioría de aplicacións web eran portais estáticos, programados en linguaxe HTML (Hyper Text Markup Language), cunha periodicidade de actualización baixa, e con escasa interacción co usuario, que simplemente "consumía" contido. Unha primeira aproximación ao concepto 2.0 foron as aplicacións webs dinámicas, nas que as páxinas son servidas ao usuario dinamicamente a partir de contido obtido dunha base de datos.

Algúns expertos na web 2.0 manteñen que a web debe enfocarse á interacción e ás redes sociais, de modo que a web sexa un punto de encontro, e dependa do usuario.

Dale Dougherty, de O'Reilly Media, usa por primeira vez o termo "web 2.0" xunto con Craig Cline, de MediaLive, para ilustrar a idea de que a web se estaba a refundar. Unha das principais críticas do concepto 2.0 é que non existe unha definición formal. Dougherty argumentou o seu punto de vista con exemplos de aplicacións web 1.0 e 2.0. Así, o que DoubleClick era na web 1.0, éo AdSense na 2.0. E o que era Ofoto na web 1.0, éo Flickr na 2.0. Outros exemplos son Google (que mide o impacto dos sitios web mediante o número de enlaces a páxinas web, e non tanto por clics absolutos) ou dia (un proxecto colaborador a partir dunha gran cantidade de pequenos usuarios, en lugar dun reducido equipo de expertos).

Deste modo, en outubro de 2004 realízase a primeira conferencia sobre web 2.0, con Dougherty, Cline e John Battelle. Un ano despois realízase unha segunda conferencia, onde se une Tim O'Reilly para resumir os principais trazos da web 2.0. Entre eles, encontramos a innovación, o deseño para múltiples plataformas, e a importancia da

participación do usuario. Na web 2.0, a aplicación está orientada polo usuario, que é o que alimenta e modifica unha base de coñecemento da aplicación, a partir dun deseño interactivo e en rede (tal e como definiu Xavier Ribes en 2007).

Algunhas das características que definen a web 2.0 son:

- Permite o uso de aplicacións en liña, substituíndo potencialmente as aplicacións de escritorio, e dende un punto de vista multiplataforma. As aplicacións executadas en web son independentes do navegador e do sistema operativo dende o que se executan, o que facilita o desenvolvemento.
- Permite a transferencia de información e contidos entre aplicacións web.
- Permite unha experiencia de usuario simple, cunha curva de aprendizaxe rápida.
- Permite engadir novas funcionalidades dun xeito simple e intuitivo.
- Permite gradualmente a virtualización das estruturas sociais no mundo en liña.
- Fai que o papel do usuario gaña importancia, levándoo ata o rol de co-desenvolvedor, e fomentando un desenvolvemento colectivo. Pódese dicir que un elevado número de usuarios poden substituír nalgúns casos un reducido grupo de expertos.
- Fomenta a interoperabilidade das aplicacións web, a incrustación de código externo e o uso de API mesmo por usuarios non expertos. Neste punto é destacable a contribución da tecnoloxía RSS (Real Simple Syndication) que separa totalmente contido e presentación dos datos. RSS permite coñecer as actualizacións dun portal web sen necesidade de visitalo, e ademais fai posible crear sistemas de agrupación de información alimentado por distintas fontes (os chamados agregadores, como Google Reader). RSS baséase en XML, que foi outro actor importante na transmisión de información para a web 2.0.
- Fomenta a participación para a mellora continua da aplicación.

## **25.2 WIKIS**

Un wiki (do hawaiano "wiki wiki" = rápido) é un tipo de aplicación web que permite a edición dos seus contidos de forma concorrente, voluntaria e colaboradora por parte de usuarios, autenticados ou non, a través dun navegador web, e co obxecto de acumular coñecemento de xeito conxunto a xeito de repositorio centralizado. Os wikis baséanse no esforzo democrático e compartido sobre unha base de igualdade e facilidade: todo o mundo debe poder achegar novo contido.

Cada páxina de contido do wiki correspóndese cun nome unívoco e simple que facilita a súa comprensibilidade, así como a súa ligazón dende outras páxinas de wiki e portais externos. Ademais, existe unha linguaxe wiki que facilita a edición e creación de xerarquías, categorías, thesaurus e taxonomías por medio de enlaces internos. Isto crea unha estrutura descentralizada que fai que a navegación polos wikis sexa non lineal, xa que cada páxina contén numerosas ligazóns a outras páxinas.

A orixe dos wikis provén de Ward Cunningham, quen desenvolveu un servidor wiki como repositorio de patróns de deseño en Portland (Portland Pattern Repository) en 1995 (chamado WikiWikiWeb), e definiu o wiki como 'a base de datos en liña máis simple que podería funcionar'. Posteriormente, en 2001, Jimbo Wales e Larry Sanger usan un wiki como xerme do seu proxecto de enciclopedia Wikipedia, unha enciclopedia libre e en rede. Comezan utilizando o software UseMod, aínda que finalmente desenvolven un software propio, denominado Media Wiki, que se converteu nun estándar para outros wikis. Foi precisamente a Wikipedia, e outras enciclopedias colectivas, as que colaboraron no auxe dos wikis.

Cada artigo coescribese co resto da comunidade. Dentro da colaboración múltiple, o wiki posibilita un historial de actualizacións que actúa a xeito de control de versións



temporal e por usuario. Ao traballar como un repositorio, os wikis permiten volver a versións anteriores con facilidade. Normalmente non existe unha supervisión, e a edición baséase na negociación entre usuarios, pero a tendencia actual é que exista un reducido grupo de usuarios cun rol especial que revisa os contidos e fai posible manter a calidade nos contidos e evitar incoherencias e sabotaxes. Noutros casos requírese autenticación soamente para manter o historial de cambios e asinar os contidos.

Hoxe en día, a versión inglesa da Wikipedia é o wiki máis grande que existe. O resto de versións noutros idiomas, e outras aplicacións wiki máis específicas, contan con menor número de usuarios debido a que as súas comunidades son menos numerosas.

O que diferencia un wiki doutras aplicacións web de xestión de contidos é a súa rapidez para crear e modificar páxinas, así como a simplicidade e lexibilidade da súa interface. Isto fomentou o alto número de participantes nos proxectos wiki, destacablemente maior que noutros proxectos colaboradores web. Se ben o usuario posúe un alto grao de liberdade para editar contidos, existen equipos para que as páxinas wiki garden coherencia entre si, o que fai aumentar a calidade do repositorio. Estas estruturas predefinidas facilitan que a edición de contidos sexa o máis simple posible. Ademais, os wikis teñen normalmente un deseño sinxelo que non se adoita modificar.

Os wikis teñen un compoñente de altruísmo máis notable que outras aplicacións web. Se ben é colaborador, e o usuario fomenta a pertenza a unha comunidade con intereses comúns, o importante da colaboración é o ben común, e non tanto que un usuario destaque máis ou menos polas súas contribucións, xa que a autoría dos contidos rara vez é exclusiva. Non só iso, os contidos están en continua edición, de xeito indefinido, o que obriga á reflexión e aínda continua revisión das ideas.

É destacable a gran relación entre os wikis e o mundo educativo. Os wikis cambiaron

radicalmente o modelo de consulta de coñecementos, pasando das mastodónticas enciclopedias estáticas aos proxectos colaboradores actuais baseados en wikis onde o usuario xoga un papel fundamental.

Os software máis utilizados para o desenvolvemento de wikis son: MediaWiki, TikiWiki ou CitiWiki (en PHP), e JSPWiki ou XWiki (en Java), entre outros. A aplicación soamente define a presentación básica dos datos (estilos, ámbito...), pero a edición dos datos corre por parte dos usuarios.

### **25.3 BLOGS**

Un blog (ou weblog) é un sitio web de actualización frecuente que recompila artigos, presentando primeiro o máis recente, e que permite a interacción cos lectores por medio de comentarios sobre os artigos. O blog é cronolóxico (permite manter unha liña de tempo de publicación), é colaborador (poden publicar varios autores), e é interactivo (os lectores poden publicar os seus comentarios, de modo que o autor poida contestarlles para conformar un diálogo). O administrador do blog pode tomar distintas opcións de deseño, como non permitir comentarios, e administrar os artigos (borralos ou reordenalos).

A temática do blog é variada, sendo a súa motivación primixenia actuar a xeito de diario persoal ou bitácora. Dende aquela, hainos corporativos, xornalísticos, educativos, etc. O blog que se dedica esencialmente á publicación de fotografías denomínase fotolog ou fotoblog (e videoblog no caso de vídeos). Unha práctica habitual é proporcionar un gran número de ligazóns que amplíen a información para cada entrada. En ocasións as entradas permiten que se lles faga *trackback* (unha ligazón inversa) para coñecer quen ligou a entrada dende outro sitio web.

As entradas do blog adoitan agruparse en categorías, e é frecuente a práctica de indicar palabras clave ou etiquetas para facilitar a busca por contido. Os blogs tamén proporcionan arquivos e índices mensuais e anuais que permiten unha navegación ordenada por data. Así mesmo, é habitual que as entradas proporcionen facilidades para ser compartidas noutros blogs, ou por correo electrónico, así como por sindicación de contidos, mediante o uso de tecnoloxía RSS ou Atom.

Gran parte do auxe dos blogs débese á súa facilidade de mantemento e ás numerosas alternativas gratuítas dispoñibles. Non son necesarios grandes coñecementos técnicos para administrar un blog, e nin sequera para crealo, o que os achegou ao gran público. Ademais, como calquera outro sitio web, un blog pode ter publicidade e xerar ingresos.

Existen principalmente dous tipos de solucións blog: as que proporcionan unha solución completa de software e aloxamento web gratuíto (como Blogger ou LiveJournal), e as que simplemente proporcionan software que precisa ser instalado nun sitio web (como WordPress). Este último é un tipo específico de xestor de contido (SXC).

## **25.4 COMUNIDADES VIRTUAIS**

Unha comunidade virtual é aquela na que os vínculos, interaccións e relacións non teñen lugar nun espazo físico, senón nun espazo virtual como a internet.

As comunidades virtuais xorden coa internet e obteñen o seu modelo das comunidades non informáticas, existentes dende moito antes. A primeira comunidade virtual data dos anos 70, aínda que o seu maior desenvolvemento se produce nos 90, volvéndose, neste momento, accesibles ao público en xeral, grazas ao nacemento da

World Wide Web (WWW) e a expansión de ferramentas como os chats, correo electrónico ou mensaxaría instantánea. Ata este momento, as comunidades estaban restrinxidas ao ámbito científico e a expertos en informática.

Os usuarios sen acceso á internet implantaron e popularizaron o uso do sistema do taboleiro de anuncios (BBS ou Bulletin Board System), que se trataba dun sistema que funcionaba mediante un acceso mediante modem telefónico a unha central (o BBS), o cal podía basearse nunha ou varias liñas de teléfono. Nos BBS podíanse manter conversas, intercambiar arquivos, publicar comentarios, etc. Nesta época as comunidades eran independentes, e o máis habitual era que os usuarios particulares empregasen os seus propios equipos domésticos para proporcionar servizo con ata un único modem de entrada.

Actualmente, as comunidades virtuais evolucionaron, converténdose nunha ferramenta moi útil dende o punto de vista empresarial. Isto débese a mellora que ofrecen ás organizacións na súa dinámica de traballo interno, nas relacións cos clientes ou no incremento da eficiencia dos seus procedementos.

Dende o punto de vista social, as comunidades virtuais permítenlles aos usuarios relacionarse cos demais, adquirindo así un carácter socializador.

Estímase que no ano 2000 máis de 40 millóns de persoas participaban en comunidades virtuais, as cales podemos caracterizar da seguinte forma:

- Asociación virtual de persoas
- Existe un propósito determinado que é a razón de ser da comunidade virtual
- Existe un gran desexo de interacción entre os usuarios para satisfacer unhas necesidades ou desempeñar uns roles concretos
- Existen sistemas que avalían e miden as interaccións e favorecen a cohesión entre os membros

O principal inconveniente ao que se enfronta o desenvolvemento das comunidades

virtuais é a problemática da organización interna destas, que adoita ser moi difícil de establecer e xestionar. En moitos casos, é demasiado custoso crear a estrutura da comunidade co que se pode chegar a perder o verdadeiro propósito da creación desta.

Unha comunidade virtual queda definida dende 3 puntos de vista:

- Comunidade virtual como lugar: localización onde os individuos poden manter relacións económicas ou sociais.
- Comunidade virtual como símbolo: os membros dunha comunidade desenvolven un sentimento de pertenza a unha estrutura maior.
- Comunidade virtual como virtual: a pesar das similitudes entre as comunidades físicas e as virtuais, unha comunidade virtual desenvólvese principalmente nun ámbito virtual que non pode ser asimilable cunha localización física.

## **25.5 REDES SOCIAIS**

O concepto de rede social, está estreitamente ligado co de comunidade virtual, entendéndose unha comunidade virtual como un caso máis específico de rede social.

Unha rede social é unha estrutura de nodos onde distintos actores, que poden ser individuos ou organizacións, están conectados mediante unha serie de relacións baseadas en propiedades comúns. Unha rede social aséntase sobre certo tipo de relacións, económicas, laborais, familiares, políticas, deportivas, etc.

Unha rede social é distribuída cando a súa localización non está limitada a un sitio en concreto senón que se distribúe a nivel xeográfico. No caso dunha rede social, é lóxico pensar que non todos os actores participantes nesa rede se encontren localizados nun

único espazo.

Unha rede social apóiase no uso dalgunha tecnoloxía de comunicación que lles permite aos distintos usuarios interactuar entre si. Neste caso, o máis habitual é empregar a internet como tecnoloxía subxacente, non obstante, tamén existen redes sociais baseadas en tecnoloxías móbiles e mesmo en tecnoloxías non dixitais como o teléfono, o fax ou o correo postal.

Actualmente as redes sociais oríéntanse ao redor dun sitio web que lles ofrece aos usuarios unha serie de servizos, como son chat, mensaxaría instantánea, carga de imaxes, vídeos, grupos de debate, etc. Un dos servizos que teñen unha maior importancia son os do "software social", que abrangue todas aquelas aplicacións que simulan procesos sociais do mundo real. O exemplo máis habitual é a simulación do efecto "amigo dun amigo", neste caso a aplicación localiza os amigos dos nosos amigos para poder así facilitar o contacto con novos usuarios.

Dentro das redes sociais máis empregadas hoxe en día, podemos citar Facebook, Youtube, Twitter, Myspace, Orkut, Hi5 etc.

## **25.6 SINDICACIÓN DE CONTIDOS**

Antes de definir que é a sindicación de contidos, é necesario aclarar que aínda que a expresión correcta é "redifusión web", o termo "sindicación web" está moi expandido no seu uso, especialmente no que se refire a contidos web, aínda que esta redifusión se pode levar mediante calquera medio de comunicación.

A sindicación de contidos (sindicación web ou redifusión web) consiste no reenvío ou redistribución de contidos dende un sitio web de orixe ata outro sitio web receptor, o cal á súa vez se pode ver como un emisor dos contidos, posto que estes deixan de

estar limitados aos usuarios do sitio web inicial. Esta redifusión de contidos faise habitualmente mediante unha licenza ou contrato entre os sitios web de orixe e destino.

Os contidos que se redistribúen adoitan codificarse en XML, aínda que isto non é obrigatorio e pode empregarse calquera outro formato soportado por http.

Existen dúas familias máis destacadas en canto a formatos de redifusión web, que son RSS e Atom. De feito, actualmente o termo RSS (Really Simple Syndication) empezouse a usar indistintamente para referirse a calquera dos 2 formatos de fontes web, o propio RSS ou Atom.

Para poder ler unha fonte web é necesario realizar unha subscrición mediante un agregador, o cal mostra os novos contidos que fosen publicados polo provedor da fonte web subscrita.

### **25.6.1      *Fonte Web***

Unha canle web ou fonte web (Web feed) é un medio de redistribución de contidos web, que se emprega para lles subministrar información aos subscritores de xeito actualizado, os cales, deben contar cun programa "agregador" para acceder a todas as fontes ás que están subscritos dende un mesmo lugar.

Como xa comentamos anteriormente, os dous principais formatos de fonte web son RSS e Atom, ambos os dous escritos en XML.

### **25.6.2      *Agregador de noticias***

Un lector RSS ou agregador de noticias (eventualmente só agregador) é unha aplicación que permite establecer unha subscrición a fontes de noticias en formatos Atom, RSS e outros derivados de XML/RDF. A función do agregador consiste en reunir

todas as noticias e contidos publicados nos sitios con redifusión escollidos e mostrarllas de xeito unificado ao usuario, de tal forma que o usuario poida saber que webs incorporaron ou modificaron contidos dende a última lectura, e en cada caso, cal é o contido delas.

Os lectores RSS volvéronse máis populares coa implantación de XML e a web semántica, e hoxe en día existe un gran número de blogs e sitios web que ofrecen as súas actualizacións, que son administradas e agregadas nun único lugar, grazas a ferramentas como as de Google Reader, Netvibes, etc.

### **25.6.3      *Formato RSS***

RSS é un formato XML para syndicar contidos web que se emprega para difundir información aos usuarios subscritos a unha fonte de contido. Este formato caracterízase por permitir a distribución de contidos sen necesidade de empregar un navegador, xa que se utiliza un agregador de contidos RSS, pero aínda así, é posible empregar o navegador para ver os contidos RSS.

De feito, as últimas versións dos navegadores permiten visualizar os RSS sen necesidade dun agregador.

Este formato, desenvolveuse especificamente para aqueles sitios que se actualizan de forma habitual e mediante o cal se pode compartir a información e ser empregada noutros sitios web.

### **25.6.4      *Estándar Atom***

Atom fai referencia a 2 estándares relacionados entre si:

- Protocolo de publicación Atom (AtomPub ou APP): protocolo baseado en http para crear ou actualizar recursos en web.
- Formato de redifusión Atom: ficheiro en formato XML usado para redifusión web.



Para crear un contido que poida ser tratado con agregador ou por outro sitio web que volve difundir os contidos da fonte, o propietario do sitio web pode empregar un software específico como un sistema de xestión de contidos, o cal publica unha fonte web de artigos recentes nun formato estándar e lexible polos ordenadores.

O formato Atom foi desenvolvido como unha alternativa a RSS. Atom xorde pola incompatibilidade existente entre algunhas versións do protocolo RSS. O formato de redifusión Atom publicouse como un "estándar proposto" de la IETF con RFC 4287, mentres que o protocolo de comunicación se publicou como RFC 5023.

## **25.7 PODCAST**

*Podcasting* consiste en distribuír arquivos multimedia, xeralmente audio ou vídeo, mediante un sistema de redifusión que lles permita establecer subscricións aos usuarios, os cales empregan un programa de descarga para poder visualizar o contido no momento que se desexe. Tamén existe a posibilidade de descargar os contidos sen unha subscrición previa. O *podcasting* é un tipo de sindicación onde os arquivos que se redistribúen son de contido multimedia.

Ao principio o *podcasting* referíase exclusivamente ás retransmisións arquivos de audio, aínda que máis tarde se estendeu o concepto para facer referencia tanto a audio como a vídeo de xeito indistinto.

O contido dos podcasts é moi diverso, sobre tecnoloxía, política, noticias, contidos educativos, etc. En función do produtor do podcast a súa complexidade, número de participantes e estrutura varían significativamente. Algúns aseméllanse a programas de radio, con varios participantes e diversas opinións, e outros parécense máis a

comunicados ou monólogos dunha única persoa, cunha duración que xeralmente é máis curta.

Os podcasts adoitan ser accesibles dende o sitio web en que foron colocados. Existen blogs que permiten realizar podcasting mediante o uso de plug-ins gratuítos. Ademais estes arquivos tamén se poden descargar.

### **25.7.1      *Podcasting Vs. Streaming***

Antes da aparición do podcasting, a forma habitual de transmitir contidos multimedia era o *streaming* ou webcasting. Mediante este sistema, provedores de contidos como cadeas de televisión ou radios empregaban o streaming para emitir dende un servidor central.

Podcasting e streaming presentan certas diferenzas, as máis destacadas:

- Con streaming non se produce a descarga do ficheiro senón que este se reproduce en modo fluxo mentres se está a descargar. Cando remata a reprodución, o ficheiro non se almacena no equipo receptor. Isto presenta a vantaxe do aforro de espazo de almacenamento, non obstante, sempre que se queira ver ou oír novamente o arquivo volverá ser descargado e non pode ser reproducido se non existe unha conexión á internet.
- Con streaming é necesario acceder ao sitio web onde está a canle desexada e indicar que a reprodución do contido debe iniciarse mediante algún tipo de ligazón, botón, etc. Non obstante, con podcasting, cando o contido está dispoñible, este descárgase de xeito automático e pode ser escoitado en calquera momento.
- O streaming presenta máis problemas de compatibilidade entre os distintos

sistemas empregados que o podcasting.

- O streaming é máis sensible a problemas de conexión á internet ou de sobrecarga do servidor xa que a descarga se produce mentres se está a reproducir o arquivo.

### **25.8 *MODELOS DE TV NA INTERNET***

A televisión IP (IPTV) supón unha nova forma de comunicación audiovisual que consiste na retransmisión de material audiovisual pola internet. Para a retransmisión destes contidos emprégase o protocolo TCP/IP, ademais este tipo de televisión caracterízase por ter programación para todos tipos de usuarios e contidos específicos que poden ser seleccionados na televisión polos propios usuarios.

Este modelo de televisión supón un avance ao modelo de televisión habitual e é considerado como un dos avances máis interesantes e prometedores que a tecnoloxía IP favoreceu.

Mediante a rede IP a programación das diversas canles de televisión chega a todos os televidentes, este proceso realízase mediante as funcións seguintes:

1. Os sinais de vídeo orixinais dixitalízanse e convértense en paquetes de datos IP.
2. Este contido, convertido a IP, almacénase para a súa redistribución, así como para a súa dispoñibilidade futura.
3. Estas tramas de paquetes transpórtanse a través dunha rede IP.
4. Os sinais son recibidos nun equipo residencial que ten por función volver converter os paquetes IP en sinais de televisión estándar.

Debido á gran robustez dos equipos de redes cos que se conta actualmente, o servizo da televisión IP pode ofrecerse cunha alta calidade, funcionalidade e un bo nivel de servizo.

### **25.8.1      *Características da televisión IP***

- Soporte para definición estándar e alta definición (HDTV)
- Nivel de interactividade completo. O equipo receptor ao ser un dispositivo IP, mantén unha conectividade bidireccional, o que permite ao usuario servizos como:
  - Videoconferencia
  - Acceso a contas bancarias
  - Compra en liña dos produtos que se estean a anunciar no momento
  - Navegación pola internet a través do dispositivo de TV
- Posibilidade de visualizar dende o principio programas xa iniciados, e mesmo programas transmitidos con anterioridade.
- Reprodución a cámara lenta, posibilidade de poñer en pausa e retroceder a reprodución, nunha retransmisión en vivo.
- Servizo de videogravadora virtual, que permite gravar directamente ou de forma programada calquera programa.
- Servizo de vídeo baixo demanda, pódese seleccionar o programa que se desexa visualizar e a súa reprodución iníciase inmediatamente.
- Guías de programación interactivas, con filtros por diversos factores como horario, tipo de programa, contido, etc.

Con todo isto, o paradigma de televisión tradicional cambia radicalmente ante o desenvolvemento da televisión IP, por exemplo, o sistema de publicidade que se emprega na televisión IP é distinto ao que se presenta na televisión tradicional, onde se producen uns cortes da programación habitual, de duración variable, onde se incorporan as cuñas informativas; non obstante, na televisión IP a publicidade aparece

simultaneamente e de forma continuada aos contidos que esteamos a visualizar.

Este modelo de televisión foi moi impulsado polas novas tecnoloxías da internet, pero a súa expansión será aínda maior, polo crecente desenvolvemento desas tecnoloxías e polos requisitos que esixe esta televisión, que se limitan a unha conexión á internet, actualmente moi estendida. Ademais, este modelo de televisión, permite visualizar o contido que o usuario desexa, no momento e formato elixido.

## **25.9 SUITES OFIMÁTICAS EN WEB**

Unha suite ofimática é un conxunto de ferramentas que se utilizan habitualmente en ámbitos de oficina para o traballo con documentos de calquera tipo. Normalmente inclúense nestes paquetes un editor de textos, un xestor de follas de cálculo, un xestor de bases de datos, un programa de creación de diapositivas de presentación etc. Tradicionalmente todas as suites ofimáticas eran ferramentas de escritorio. Actualmente existen distintas versións de suites ofimáticas pero en web, ás que se accede mediante o uso dun navegador.

### **25.9.1 Feng Office**

Feng Office é unha aplicación libre de tipo Web Office, antes coñecida como OpenGoo. Trátase dunha sistema completo que proporciona funcionalidades para crear, publicar, colaborar e compartir documentos.

Feng Office permite crear e traballar entre outros, sobre:

- *Documentos*: permite aloxar documentos de todo tipo e editar directamente algúns deles.
- *Listas de tarefas*: permite a creación de listas de tarefas asignadas a distintos

usuarios, con opcións de notificación, categorización, etc

- *Correo electrónico*: permite centralizar a xestión das distintas contas de correo.
- *Calendario*: permite establecer reunións e unha xestión das actividades diarias.
- *Axenda*: permite realizar unha xestión de contactos.

Esta aplicación pode funcionar baixo un modelo SaaS (Software as a Service), onde os servidores do proveedor a través dun navegador nos permiten traballar coa aplicación, pero tamén é posible realizar unha instalación da aplicación nun servidor propio, neste caso os requisitos deste sistema pasan por un servidor web Apache, PHP e MySQL como base de datos.

### **25.9.2      *Google Docs***

Google Docs & Spreadsheets, é un programa web gratuíto que permite crear e traballar sobre uns documentos de xeito individual ou en grupo.

Google Docs componse de:

- Procesador de textos
- Follas de cálculo
- Programa de presentación sinxelo
- Editor de formularios

Entre as vantaxes de Google Docs, encóntrase o feito de que pode ser usado tanto en liña coma sen conexión. Nesta modalidade desconectada, os cambios que se introduzan nos documentos serán actualizados de forma automática en canto a conexión coa internet se restableza.

Ademais recentemente incorporouse compatibilidade entre Google Docs e os dispositivos móbiles, de tal forma que se poida non só acceder aos documentos senón tamén editalos.

### **25.9.3      *Office Web Apps***

Office Web Apps é a solución de Microsoft para as suites ofimáticas na web. É unha versión gratuíta baseada no conxunto de aplicacións de Microsoft Office.

Office Web Apps, componse de:

- Word Web App
- Excel Web App
- PowerPoint Web App
- OneNote Web App

Estas aplicacións permiten acceder aos documentos a través do navegador, así como compartir arquivos e traballar sobre eles de forma colaboradora.

## **25.10 ALMACENAMENTO EN WEB**

Un servizo de almacenamento de arquivos en liña (servizo de aloxamento de arquivos ou centro de medios en liña) é un servizo de aloxamento en liña co propósito de facilitar o almacenamento de contido estático, como arquivos, documentos, etc. Por norma xeral este tipo de servizos prové de accesos a través de diversas interfaces, web, ftp, etc.

### **25.10.1      *Dropbox***

Dropbox é un servizo de aloxamento de arquivos na nube, que permite almacenar e sincronizar arquivos entre distintos ordenadores e mesmo con distintos usuarios.

Como característica principal cabe destacar que é un sistema multiplataforma e que presenta versións tanto gratuítas como de pagamento.

O funcionamento é moi sinxelo, cada ordenador cliente instala un software que lles permite aos usuarios desprazar calquera contido a unha carpeta designada, a cal se integra no sistema de arquivos do sistema de que se trate. Despois de situar un arquivo nesa carpeta, ou de modificalo, este sincronízase na nube e con todos os demais ordenadores onde estea instalado o cliente Dropbox dese usuario. O acceso aos arquivos da carpeta de Dropbox tamén se pode realizar a través da web e mesmo ser compartido por varios usuarios. Aínda que Dropbox funciona como un servizo de almacenamento, o seu propósito céntrase máis na sincronización e o compartimento de arquivos.

#### **25.10.1.1 Funcionalidades de Dropbox**

- Historial de revisións: os arquivos borrados da carpeta Dropbox poden ser recuperados dende a web ou dende calquera dos ordenadores sincronizados.
- Historial do documento: pódese acceder ao historial dun documento, de tal forma que se pode traballar sobre este, sen que isto afecte ás versións preexistentes.
- Optimización da conexión: ao modificar un arquivo nunha carpeta Dropbox, o sistema só cargará as partes do documento que foron modificadas cando se produza a sincronización.

### ***25.11 ESCRITORIOS VIRTUAIS***

Un escritorio virtual consiste nun servizo de virtualización aplicado sobre un escritorio tradicional. Neste caso o escritorio do usuario execútase nun servidor, onde as ordes dese usuario se transmiten en liña ao servidor, o cal envía de volta os resultados



desas accións.

A virtualización de escritorio é relativamente recente e describe a separación do contorno que percibe o usuario, que engloba os seus datos e programas, da máquina física na que estes se almacenan e executan. Neste caso, o usuario pode ter un sistema completo e empregar adicionalmente o escritorio virtual para certo tipo de tarefas, ou mesmo, o usuario pode contar cun sistema sinxelo tipo terminal, onde toda as tarefas do usuario se realizan directamente contra o servidor.

### **25.11.1    *eyeOS***

eyeOS é un sistema libre e multiplataforma que se basea no estilo que teñen os escritorios nos sistemas operativos tradicionais, e inclúe a estrutura dun sistema operativo así como certas aplicacións ofimáticas como procesador de textos, calendario, navegador, xestor de arquivos, etc.

Este sistema diferénciase doutros en que non necesita de ningún software adicional para poder usalo, posto que todo o acceso se realiza mediante un navegador web. Recentemente, o sistema foi adaptado para poder utilizarse en dispositivos móbiles.

### **25.12 MASHUPS**

Un *mashup* é unha aplicación ou páxina web que usa e combina funcionalidades e datos dunha ou máis fontes para crear novos servizos. Implica unha integración rápida e sinxela, xeralmente con API abertos e fontes de datos, para producir resultados enriquecidos. Tómanse unha serie de datos existentes e transfórmanse noutros cun valor engadido que son máis útiles tanto a nivel persoal como profesional. Como principais características dos *mashup* pódese destacar a visualización, a

combinación e a agregación.

Os mashup compóñense de 3 partes:

- Proveedor de contidos ou fonte de datos. Os datos están accesibles a través dun API e mediante distintos protocolos como RSS.
- Sitio *mashup*: aplicación web que ofrece un servizo a partir de distintas informacións que non son súas.
- Navegador web: é a interface coa que o usuario interactúa co *mashup*.

Un erro moi frecuente é confundir os contidos embebidos cos que existen nun *mashup*. Un sitio que permite embeber por exemplo un vídeo ou un arquivo de son, non é un *mashup*, xa que non existiu ningún tipo de procesado nestes datos que permita incrementar o valor que estes teñen para o usuario.

Existe distintos tipos de *mashups*:

- *De consumidores*: é o máis coñecido. Intégranse datos de diversas fontes e accédese a través dunha interface sinxela. Exemplo: Google Maps.
- *De datos*: mestúranse datos de tipo similar de distintas fontes. Exemplo: combinación de múltiples *feeds* RSS nun único.
- *Empresariais*: integra datos de fontes tanto externas coma internas. Exemplo: incorporar maior información a un informe estratéxico mediante datos existentes nalgún rexistro oficial.
- *De negocio*: é unha combinación dos 3 anteriores.

### **25.13 MUNDOS VIRTUAIS**

Os mundos virtuais podemos velos como un tipo de comunidade virtual, que simula un mundo artificial, o cal pode estar inspirado ou non na realidade. Neste mundo

virtual os distintos usuarios mediante os seus avatares (personaxes ou representantes do usuario no mundo virtual, caracterizados como gráficos en 2D ou 3D) poden interactuar entre si e con outros obxectos presentes no mundo virtual. Para poder definilo como un mundo virtual, é necesario que ese mundo teña unha liña temporal activa, persistente e dispoñible as 24 horas. A interacción que se establece entre os usuarios dun mundo virtual é habitualmente en tempo real.

Aínda que actualmente a maioría dos mundos virtuais ten un propósito recreativo, existen moitos mundos con propósito e formas diferentes.

- *Entretenemento (Social):*
  - MMORPG (massively multiplayer online role-playing games): Videoxogo de rol multixogador masivo en liña.
  - MMOFPS (massively multiplayer first-person shooter)
  - Metaverso: moi similar a MMORPG; consiste en contornos 3D completamente inmersivos.
  - MMORLG (massively multiplayer online real-live games)
  - Xogos sociais: a súa principal intención é facilitar a interacción entre personaxes que xeralmente xa se coñecen.
- *Educativo:*
  - MMOLE (massively multilearner online learning environments)
- *Profesional (Simuladores):*
  - Simuladores de voo
  - Reprodución de contornos especialmente custosos ou difíciles de simular

### **25.13.1      *Second Life***

Second Life (SL) é un metaverso accesible de forma gratuíta na internet, no que os usuarios adoitan empregar uns programas chamados *viewers* para acceder ao sistema, no cal os usuarios interactúan a través de avatares.

Os usuarios de SL poden explorar o mundo, interactuar con outros usuarios,

relacionarse, participar en actividades, comerciar, etc. Para poder acceder a SL é necesario crear unha conta, a cal dá acceso directo a un avatar 3D personalizable.

### **25.14P2P**

Unha rede P2P (Peer-to-peer, rede de pares ou rede punto a punto) é unha rede de ordenadores na que todos ou algúns dos aspectos funcionan sen que existan clientes nin servidores fixos, senón unha serie de nodos que actúan como iguais entre si, onde cada un deles é á vez cliente e servidor.

Este tipo de redes permite o intercambio directo de información entre os ordenadores que están conectados. Habitualmente para compartir ficheiros de calquera tipo, aínda que tamén se emprega para telefonía VoIP.

#### **25.14.1 Características**

A continuación detállanse algunhas características das redes P2P:

- *Anonimato*: é importante que o autor dun contido, o seu lector, editor e o servidor que o almacena sexan anónimos
- *Descentralización*: por definición os nodos P2P son iguais e a rede descentralizada. Ningún nodo é imprescindible para o funcionamento da rede.
- *Robustez*: ao tratarse de redes distribuídas, a robustez tamén se ve incrementada xa que en caso de se producir un fallo, ao existir unha réplica dos datos en múltiples destinos, a información desexada sempre se pode encontrar, ao non depender dun servidor central.
- *Seguridade*: consiste en identificar e evitar nodos maliciosos, así como o contido potencialmente perigoso, etc. Os mecanismos de seguridade máis

destacados neste caso son: caixas de area, reputación, comunicacións seguras, comentarios sobre os ficheiros, cifrado multiclave, etc.

- *Escalabilidade*: canto maior número de nodos estean conectados a unha rede P2P mellor será o funcionamento. Cando se incorporan novos nodos, cos seus recursos, os recursos totais do sistema aumentan.

## **25.14.2      *Tipos de redes P2P***

### **25.14.2.1    Redes P2P centralizadas**

Este tipo de rede caracterízase por:

- Arquitectura monolítica onde todas as transaccións se fan a través dun único servidor, o cal almacena e distribúe os nodos onde se almacenan os contidos.
- Todas as peticións dependen da existencia do servidor.
- Administración dinámica.
- Privacidade dos usuarios limitada.
- Falta de escalabilidade.

### **25.14.2.2    Redes P2P híbridas, semicentralizadas ou mixtas**

Este tipo de redes caracterízase por:

- Existe un servidor que atende peticións pero non almacena información.
- O servidor administra os recursos, enrutamentos e comunicación entre nodos.
- Os nodos son os encargados de almacenar a información.
- O servidor central recoñece a información que desexa compartir cada nodo.
- Pode existir máis dun servidor que xestione os recursos compartidos.
- Os nodos poden seguir en contacto directo entre eles en caso de que o servidor ou servidores caian.

### **25.14.2.3 Redes P2P puras ou totalmente descentralizadas**

Este tipo de redes caracterízase por:

- Son as máis comúns e versátiles posto que non necesitan de ningún tipo de xestión central.
- Redúcese a necesidade de usar un servidor central.
- Cada nodo é á vez cliente e servidor.
- As conexións establécense entre usuarios, coa axuda dun terceiro nodo que permite ligar esa conexión.
- Non existe un enrutador central.

## **25.15 WEB SEMÁNTICA**

A web influíu moito no modo de comunicación dos últimos tempos e se ben ten multitude de vantaxes, como o acceso a millóns de recursos independentemente da nosa localización, tamén existen dificultades como son a sobrecarga de información e a heteroxeneidade das fontes de información, o que nos leva a un problema de interoperabilidade.

Coa web semántica estes problemas soluciónanse, permitindo que os usuarios deleguen certas tarefas no software. Grazas á incorporación de maior "semántica" á web, o software é capaz de procesar o contido, combinalo, realizar deducións, etc.

### **25.15.1 Definición de web semántica**

A web semántica (semantic web) baséase na idea de incorporar metadatos ontolóxicos e semánticos á web. Esta información adicional describe o significado, contido e relación entre os datos. Ademais debe ser proporcionada de xeito formal para que poida ser avaliada automaticamente por equipos de procesamento. Ao

enriquecer a web con máis significado, pódense obter solucións a problemas comúns na busca de información.

A web baséase fundamentalmente en documentos HTML, o que non é demasiado versátil á hora de categorizar os elementos que configuran o texto. A función da web semántica é resolver estas deficiencias de tal forma que se poidan describir os contidos dunha web, mediante tecnoloxías como RDF, OWL, ademais de XML. Este tipo de tecnoloxías achega descripcións explícitas dos distintos recursos incorporando unha serie de etiquetas interpretables polos xestores de contidos, de tal forma que sexa posible a interpretación dos documentos, tratamento da súa información, etc.

### **25.15.2     *RDF, SPARQL e OWL***

A web semántica, para realizar unha axeitada definición dos datos, emprega fundamentalmente RDF, SPARQL e OWL.

- *RDF*: proporciona información sobre os recursos da web, de forma simple e descritiva.
- *SPARQL*: é a linguaxe de consulta de RDF. Permite realizar buscas sobre os recursos da web semántica.
- *OWL*: é un mecanismo que permite desenvolver vocabularios específicos que se poidan asignar aos recursos. Proporciona unha linguaxe para definir ontoloxías que se poden usar a través de distintos sistemas.

As ontoloxías encárganse de definir os conceptos empregados para describir e representar unha área de coñecemento, inclúen as definicións de conceptos básicos e a relación entre estes.

### **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  
Colexiado do CPEIG





## **26. SISTEMAS DE INFORMACIÓN XEOGRÁFICA. ARQUITECTURA DOS SISTEMAS DE INFORMACIÓN.**

## Tema 26: Sistemas de información xeográfica

---

### **ÍNDICE**

#### **26.1 Introducción**

#### **26.2 Conceptos básicos**

##### *26.2.1 Xeorreferenciación*

###### *26.2.1.1 Xeorreferenciación directa*

###### *26.2.1.2 Xeorreferenciación indirecta ou discreta*

##### *26.2.2 Modelo de datos*

###### *26.2.2.1 Modelo ráster*

###### *26.2.2.2 Modelo Vectorial*

#### **26.3 Arquitectura dun SIX**

##### *26.3.1 Clasificación dos SIX*

#### **26.4 ÁMBITOS de Aplicación**

##### *26.4.1 Demografía*

##### *26.4.2 Xestión e planificación urbana*

##### *26.4.3 Xestión de instalacións*

##### *26.4.4 Aplicacións de xestión e inventario de recursos*

##### *26.4.5 Xestión catastral*

#### **26.5 Proveedores e Usuarios de Información Espacial**

#### **26.6 Infraestruturas de Datos Espaciais**

##### *26.6.1 Principios das IDE*

##### *26.6.2 Compoñentes das IDE*

###### *26.6.2.1 Datos*

###### *26.6.2.2 Metadatos*

###### *26.6.2.3 Servizos*

#### **26.7 Bibliografía**

## **26.1 INTRODUCCIÓN**

Como información espacial (xeográfica, xeorreferenciada ou xeodatos) referímonos a todo tipo de información relativa a sucesos ou elementos para a cal se inclúe unha referencia á súa localización, a cal está situada sobre ou nas inmediacións da superficie da Terra. O xeito de referenciar a posición destes elementos ou estes sucesos pode realizarse de distintas formas, mediante un simple enderezo postal, con coordenadas xeográficas (lonxitude e latitude) ou con coordenadas cartesianas nalgún sistema de referencia cartográfico.

A maior parte da información en formato electrónico almacenada actualmente en sistemas de todo tipo é información espacial ou que podería selo. O porqué deste auxe da información espacial encontrámola nunha serie de características que xustifican o interese de asociar a unha información a referencia da súa localización.

Por unha parte temos a calidade da información espacial para a súa representación en forma gráfica e simbólica mediante mapas. Os mapas son un sistema de comunicación que foi utilizado dende as primeiras civilizacións e co que está familiarizado practicamente todo o mundo. Ademais os mapas tiveron grande importancia ao longo da historia militar, económica e política das nacións, polo que foron considerados sempre como un recurso clave ao desenvolvemento do cal se dedicaron importantes esforzos.

Por outra parte, a capacidade que posúe a información espacial para integrar conxuntos de información que doutra forma serían inconexos, mediante a aplicación das relacións espaciais de coincidencia, proximidade ou inmediatez inherentes a esa localización espacial. Esta característica é probablemente a que maior potencial lle outorga á información espacial, constituíndo a base da análise espacial.

A primeira manifestación dos sistemas de información xeográfica podémola encontrar, como se comentaba anteriormente, nos mapas, non obstante, xa en épocas máis recentes, as contribucións das tecnoloxías da información no ámbito da cartografía foron moi importantes. Pódense destacar aqueles avances destinados á mellora dos procesos de produción cartográfica, as orientadas á explotación e análise da información cartográfica.

No tocante á produción cartográfica, actualmente cóntase con técnicas moi depuradas para a produción de mapas en todas as súas fases, dende a captura de datos (fotogrametría aérea, imaxes de satélite, teledetección, telemetría láser, GPS, etc.), ata os diferentes procesos que compoñen a fase de elaboración da cartografía. Estas técnicas permitiron non só notables melloras na calidade, diversidade e flexibilidade dos produtos cartográficos, senón que fixo posible dispoñer de información cartográfica moi actualizada

No tocante á análise da información xeográfica é necesario destacar en primeiro lugar as importantes limitacións prácticas que presentan os mapas tradicionais para a súa utilización en análises mediante técnicas manuais. A superación destas limitacións foi a motivación inicial para o desenvolvemento dos sistemas de información xeográfica, SIX (ou GIS de acordo coa terminoloxía anglosaxona), que se converteu na outra gran rama de contribucións das tecnoloxías da información no ámbito da cartografía.

O desenvolvemento dos primeiros SIX datan de finais dos anos 60 e supuxo un gran cambio na utilización da información espacial que se facía ata ese momento. De feito as técnicas e metodoloxías de análise espacial da información, que ata o momento foran pouco examinadas pola excesiva complexidade asociada aos tratamentos manuais, víronse paulatinamente melloradas e en moitos casos empezou a ser posible a súa utilización co procesamento automatizado da información espacial en formato dixital.

Un sistema de información xeográfica está orientado á captura, manipulación, recuperación, análise, representación, etc, de información xeorreferenciada, aquela

na que a posición espacial ocupada polos obxectos do mundo real que se modelizan forma parte inherente a esa información.

Os SIX gozan de grande aceptación dende as súas primeiras implantacións o cal se debe en boa medida á súa capacidade para construír modelos orientados á resolución de problemas cun universo de discurso que se caracteriza por ter un compoñente espacial.

Estas primeiras realizacións foron impulsadas principalmente por organizacións con responsabilidades na xestión de recursos con implantación territorial como son ordenación do territorio, recursos naturais, censo, defensa, etc.

Dende estas primeiras implantacións, nos anos 60, ata a década dos 80, o desenvolvemento dos SIX produciuse dunha forma relativamente lenta debido sobre todo á capacidade e ao custo da tecnoloxía dixital dispoñibles naquel momento. Dende a segunda metade dos 80 prodúcese un grande auxe, tanto en diversificación das áreas de aplicación desta tecnoloxía coma na oferta de produtos comerciais, o que lles outorgou gran popularidade e difusión aos SIX en todo tipo de organizacións.

Actualmente a evolución caracterízase por unha serie de factores que impiden unha plena estabilidade do sector:

- Evolución das tecnoloxías nas que se apoian os SIX, como son, xestores de bases de datos, procesamento paralelo, visualización, etc.
- Alto grao de relación entre os SIX e a internet, que está en permanente evolución.
- A tecnoloxía dispoñible oríéntase a implantacións que non aproveitan o seu potencial.
- Restricións institucionais que aínda impiden o acceso e utilización da información cartográfica de que se dispón en todos os ámbitos.

## **26.2 CONCEPTOS BÁSICOS**

### **26.2.1 Xeorreferenciación**

A xeorreferenciación é o proceso polo cal se identifica unha determinada posición na superficie terrestre ou nas súas inmediacións. Dise que unha información é ou está xeorreferenciada cando mediante algún procedemento se asociou a esa información a posición do elemento ou suceso ao que se refire ela.

A posición é o que distingue a información espacial de calquera outro tipo de información, polo cal é de grande importancia o método utilizado para especificar esa posición, sobre todo cando se deben combinar informacións espaciais de diferentes procedencias que puideron utilizar procedementos de xeorreferenciación distintos.

Existen dúas técnicas para asociar a posición a unha información: *a xeorreferenciación directa e a indirecta (ou discreta).*

#### **26.2.1.1 Xeorreferenciación directa**

A xeorreferenciación directa baséase na utilización de coordenadas para definir posicións. O sistema de coordenadas xeográfico é o máis sinxelo a nivel conceptual, segundo o cal, para definir a posición dun punto se utilizan a lonxitude e latitude del. Este é un procedemento moi sinxelo que se complica notablemente cando o que queremos localizar é unha distancia ou unha superficie e non un punto, posto que entran en xogo procedementos de trigonometría esférica. Por iso, é moi habitual a utilización de sistemas de coordenadas cartesianas definidos para un determinado sistema de proxección.

Entre os sistemas de proxección válidos para todo o globo terráqueo, tamén denominados globais, o máis utilizado é o correspondente á proxección *Universal Transversal Mercator (UTM)*.

Este sistema de proxección é o que empregan a maioría de organismos cartográficos, tanto nacionais coma internacionais, ademais, case todos os receptores GPS proporcionan coordenadas UTM. Os principais problemas deste sistema de proxección radican no traballo con datos de diferentes fusos ou no emprego de latitudes moi altas.

Á península Ibérica correspóndenlle os fusos UTM 29, 30 e 31 (ás Illas Canarias correspóndelles o fuso 28).

A xeorreferenciación directa é de tipo continuo, é dicir, pódese situar unha posición coa precisión que sexa necesaria, por contraposición á xeorreferenciación discreta que só permite referenciar un número finito de posicións no espazo.

#### 26.2.1.2 Xeorreferenciación indirecta ou discreta

A xeorreferenciación indirecta ou discreta consiste no uso de nomes, topónimos, etc. para indicar a posición dun lugar e mesmo se este descriptor non existe, empréganse construcións léxicas de aproximación partindo dun lugar si referenciado, como poden ser, "ao lado do colexio", " máis alá do banco", "preto do teatro", etc. En moitos casos as coordenadas destes lugares de referencia si son coñecidos e contamos con mecanismos o suficientemente accesibles para obter a posición desexada.

A referencia deste tipo máis empregada é o enderezo postal, asociado a multitude de rexistros de información a pesar das súas limitacións de localización e que é de grande utilidade en aplicacións onde por exemplo a escala que se necesita non é moi detallada

#### **26.2.2 Modelo de datos**

O modelo de datos é o mecanismo polo cal se realiza a representación dos obxectos do mundo real no sistema de información.

Os modelos de datos utilizados variaron pouco dende os inicios dos SIX, sendo, o modelo de datos ráster e o modelo de datos vectorial, os máis utilizados.

- Modelo de datos ráster: pártese dunha concepción da realidade, ou parte dela, e represéntase como algo continuo, polo que esa realidade ten asociada unha distribución dos valores que toma en cada posición (ou nun conxunto discreto de posicións seleccionadas).
- Modelo de datos vectorial: a abstracción do mundo real conduce á distinción dunha serie de obxectos diferenciáveis, relevantes para o problema en cuestión, que son os representados no sistema.

Independentemente do modelo empregado, o seu desenvolvemento debe levarnos, tras sucesivas abstraccións nas fases de deseño lóxico e físico, a conseguir a representación dos elementos de información que se empregan nun SIX:

- Xeorreferencias: información posicional.
- Información relativa ás características dos obxectos modelizados: información temática.
- Información sobre as relacións espaciais existentes entre os obxectos: información topolóxica.
- Información sobre as relacións de tempo: información temporal. Este tipo de información é moi importante en certo tipo de problemas, se ben xeralmente se trata como un atributo adicional.



O tipo de modelo de datos que se seleccione condicionará todas as operacións que poidan ser realizadas con el, se ben existen moitos sistemas comerciais que permiten a combinación de ambos os dous, o cal pode ser conveniente no tratamento de determinado tipo de problemas.

#### *26.2.2.1      Modelo ráster*

O modelo de datos ráster ten a súa orixe nas técnicas de captura de datos temáticos e xeográficos a partir de imaxes de satélites e de fotografía aérea (técnicas de teledetección). Estas técnicas comparten moitos puntos coas tecnoloxías de tratamento de imaxes.

A rexión que se vai modelar considérase dividida seguindo unha matriz ou malla rectangular de celas (píxeles) xeralmente cadradas e de igual tamaño<sup>1</sup>. A cada unha destas celas asígnaselle o valor da propiedade ou atributo que se vai representar, o cal se determina sobre a base dunha convención preestablecida, por exemplo, o valor que toma o atributo no centro da cela, nun dos vértices ou o valor medio na cela, etc. Este valor podería ser o nivel de gris nunha escala de 256 valores, a temperatura media de certo lugar, as precipitacións nunha rexión, etc.

Un conxunto de datos de tipo ráster de grande utilidade e importancia é o modelo dixital de características relevantes para a súa resolución. Na práctica, é corrente manexar ata varias decenas, ou mesmo centos de capas. Por exemplo, para representar os niveis de vermello, verde e azul dunha imaxe RGB sería necesario utilizar 3 capas, unha para cada cor, en cada píxel da imaxe.

De acordo con isto, os obxectos reais que se representan son os segmentos do terreo correspondentes ás celas, ou máis concretamente, o valor do atributo que se está a

---

<sup>1</sup> O tamaño da cela denomínase resolución.

representar nese segmento do terreo. Hoxe en día é habitual obter imaxes de grandes extensións de terreo con resolucións de 50 x 50 cm ou mesmo inferiores.

No modelo de datos ráster non existe unha representación explícita de entidades físicas do mundo real, non se representan explicitamente os edificios, nin os ríos, por exemplo. É por isto, que este modelo non é útil para a representación de información topolóxica, é dicir, do tipo "un elemento é contiguo a" ou "un elemento está sobre" outro. Este modelo tampouco garda explicitamente a posición das celas, xa que, se se coñece a orientación da malla de celas respecto a unha referencia, a secuencia de varrido (filas e columnas) e as coordenadas xeográficas dunha delas, pode obterse a xeorreferencia de calquera cela.

As técnicas de organización e compresión que se empregan para o almacenamento interno da información que se asocia a cada capa son moi relevantes e buscan un equilibrio entre o volume de información e a eficiencia do acceso a ela. Existen moitas técnicas, a máis elemental de todas elas, consiste en percorrer a imaxe seguindo a secuencia de varrido e almacenar os valores dos atributos en sucesivas celas. O problema desta técnica radica na súa ineficiencia.

Para solucionalo, adóitanse empregar técnicas de compactado de datos, como son, Run Length Encoding (RLE) na cal se almacenan pares (L,V), onde L é o número de celas contiguas en que repite o valor V do atributo.

Outras técnicas máis complexas baséanse en estruturas de datos orientadas á indexación espacial e á compresión de datos, denominadas *quadrees*. Nestas técnicas, realízase de xeito recursivo unha división da información inicial en cuadrantes cada vez menores aos que se aplican procedementos de compresión.

Unha técnica de compresión cada vez máis utilizada é a baseada en *wavelets*, que aínda que implica certa perda de información, a suple ao conseguir uns niveis de compresión moi elevados.

Nun SIX tipo ráster, as funcionalidades de tratamento de información máis habituais son as que se mencionan nas categorías seguintes:

- *Operacións locais nunha capa:*
  - Recodificación de capas: asignar novos códigos para un atributo a partir dos xa existentes.
  - Filtrado(resaltado ou suavización): obtense unha nova capa a partir doutra dándolle a cada cela un valor que se obtén dos valores das celas veciñas.
  - Determinación de pendentes e rumbos de máxima pendente: a partir dun modelo dixital do terreo (MDT), represéntase o atributo de elevación (cota) dos puntos situados nunha matriz regular de tamaño preestablecer.
  
- *Operacións de presentación:*
  - Xeración de lendas.
  - Determinación de isoliñas (curvas de nivel).
  - Determinación de perspectivas con *drapping*: representación da capa correspondente a un atributo concreto sobre unha vista tridimensional obtida partindo dun MDT.

- *Operacións de mantemento de datos:*
  - Intercambio de datos con outros sistemas.
  - Intercambio de datos con outros formatos.
  - Remostraxe: cambiar o tamaño e orientación das celas para facelas compatibles cos datos de entrada ou para cambiar de escala.
  - Vectorización: conversión da información ráster a vectorial.

A estrutura de datos que se obtén tras a realización das operacións é a capa, que representa a variación espacial dun único atributo como a sucesión de valores tomados por ese atributo nas sucesivas celas. Polo tanto, para un problema será preciso representar tantas capas como atributos sexan de elevacións.

*Operacións con varias capas:*

- Superposición (*overlay*): obtéñense novas capas a partir de dúas ou máis capas existentes mediante operacións booleanas ou aritméticas con elas.
- Cálculo de corredores: determinar zonas que distan dunha determinada característica menos dun valor dado.
- Determinar concas visuais: zonas vistas dende un ou varios puntos dados.

*Agrupación de celas:*

- Determinar zonas de celas contiguas co mesmo valor de atributo.
- Cálculo de áreas, formas, distancias, perímetros, etc.

#### 26.2.2.2 Modelo Vectorial

No modelo vectorial, utilízanse tres principios xeométricos para representar as entidades xeográficas. Estas bases xeométricas son:

- O punto é a entidade básica de representación de entidades con posición, pero acéptase que carece de dimensión.
- O arco representa as entidades unidimensionais e defínese mediante vórtices ou nodos.
- O polígono utilízase para as entidades bidimensionais e defínese mediante os arcos que o delimitan.

Cada entidade xeográfica que se representa mediante o modelo vectorial ten asignado un identificador único no sistema. O devandito identificador permite referenciar as entidades en calquera momento e vinculalas cos seus atributos alfanuméricos (información temática).

Para especificar a definición xeométrica empréganse as coordenados dos puntos e vértices a partir dos que se definen as distintas entidades. Podemos falar polo tanto dunha xeorreferenciación continua, sen que a resolución supoña un impedimento como pasaba no modelo de datos ráster.

Ao contrario do que sucede no modelo ráster, no que se representan todas as posicións do espazo que se estuda, no modelo de datos vectorial só se almacena a información das entidades territoriais relevantes, o que supón un achegamento ao modelo de razoamento espacial que se emprega habitualmente.

A pesar disto, a diferenza máis relevante entre este modelo e o ráster é a capacidade que ten para expresar as relacións espaciais que existen entre as entidades (información topolóxica), que son as que lle outorgan ao modelo a capacidade semántica precisa para representar o coñecemento territorial. Non obstante, esta

vantaxe na representación espacial tamén implica un aumento na complexidade deste modelo en comparación co modelo de datos ráster.

Os primeiros SIX baseados no modelo vectorial almacenaban de forma separada a información xeométrica e topolóxica da información correspondente aos atributos. Para a información asociada aos atributos empregábanse SXBD relacionais convencionais e para a información xeométrica e topolóxica empregábanse estruturas de datos e ficheiros de tipo propietario, deseñados para optimizar o rendemento das operacións a realizar, recaendo no sistema SIX o peso do mantemento das relacións entre todos eles. Este tipo de arquitectura denomínase modelo xeorrelacional.

Dada a mellora no rendemento dos SXBDR xa non existe motivo para manter esta separación, polo que actualmente se tende a que todos os datos cos que traballa un SIX se almacenen en BD relacionais convencionais, ou quizais ampliados mediante extensións xeográficas. As bases de datos que se empregan son normalmente de propósito xeral e externas ao propio SIX, dando lugar ás chamadas bases de datos xeoespaciais (Geodatabases).

Este novo enfoque no almacenamento dos datos espaciais resultou un pilar fundamental na evolución dos SIX nas organizacións, xa que se cubriu o espazo existente entre os sistemas orientados a proxecto ou departamentais e os sistemas de información espacial de alcance corporativo.

As principais funcionalidades dos modelos de datos vectoriais son:

- Conversión entre diferentes formatos.
- Análise espacial: estudos baseados nos operadores espaciais habituais como son inmediatez, superposición, proximidade, etc. Os operadores (booleanos ou aritméticos) empréganse sobre os atributos das entidades das capas iniciais.

- Acceso á base de datos e recuperación da información das entidades que satisfán unha serie de cláusulas, que poden formularse tanto en termos tanto espaciais como dos seus atributos temáticos.
- Medida de áreas, perímetros e distancias.
- Análises estatísticas: correlacións espaciais, análise de patróns, etc.
- Presentación de resultados.

Se ben tanto o modelo vectorial coma o ráster teñen as súas vantaxes e os seus inconvenientes e aínda que se admite de forma global que cada modelo se adecúa máis a un tipo distinto de problemas, tamén existen solucións híbridas que permiten a combinación de ambos os dous modelos.

- Os modelos ráster son máis axeitados para problemas que admiten algún tipo de formulación analítica.
- Os modelos vectoriais adecúanse mellor a problemas de xestión que admiten unha formulación mediante polígonos, redes, etc.

Como evolución do modelo de datos vectorial, temos o modelo de datos orientado a obxectos no que o elemento central é o conxunto de elementos xeográficos e as relacións entre eles. Cada obxecto xeográfico é un paquete que integra xeometría, métodos e propiedades. Os obxectos xeográficos do mesmo tipo agrúpanse en clases, onde cada un destes obxectos sería unha instancia da clase. A definición da clase inclúe tamén as relacións topolóxicas e xeográficas ou espaciais.

### **26.3 ARQUITECTURA DUN SIX**

Nos primeiros desenvolvementos dos SIX encontramos principalmente sistemas software pechados de gran tamaño e complexidade (SIX monolítico), que eran utilizados principalmente por grupos de usuarios reducidos cun nivel de especialización bastante elevados, ademais, orientábanse a tarefas moi concretas e xeralmente presentaban pouca ou ningunha integración con outros sistemas. Actualmente os sistemas diferéncianse moito destes iniciais, son cada vez máis habituais e sinxelos, non requiren de usuarios expertos para o seu manexo e permiten a integración da información con outros sistemas.

Nun sistema SIX podemos falar de arquitecturas de 3 capas, así temos:

- Capa de presentación: incorpora todas as funcionalidades que permiten a interacción entre o usuario e o sistema, para acceso o acceso á información e presentación de resultados. Habitualmente isto tradúcese nunha GUI que facilita o acceso ás ferramentas da seguinte capa ou tamén nunha aplicación externa que poida acceder a determinadas funcións de xeoproceso.
- Capa de proceso: abrangue unha serie de ferramentas diferentes que integran o núcleo do SIX.
- Capa de xestión de datos: centraliza o acceso aos datos, que poden localizarse en distintos almacéns. Ademais, integra tamén moitas das funcións que se encargan de proporcionar transparencia sobre os detalles dos datos: sistemas de proxección, formatos, transformación de coordenadas, etc.



Para realizar estas capas funcionais podemos ter os mesmos ou diferentes sistemas físicos, tendo unha gran cantidade de posibilidades. Se se fai unha desagregación completa, cada unha destas capas residirá nun ou máis servidores diferentes, adaptado ás necesidades específicas do contorno de implantación do SIX.

No mercado dos SIX comerciais, estanse a asumir cada vez mais unha serie de estándares de facto que foron xurdindo nos últimos anos debido ás tecnoloxías de compoñentes (Java Beans, .NET...) e de plataformas interoperables de obxectos distribuídos (SOAP, CORBA). Estas tecnoloxías, permiten construír novos SIX de forma extensible e integrando funcionalidades proporcionadas por diversos provedores.

Dende a perspectiva dos almacéns de datos, téndese cada vez mais ao uso dos sistemas posrelacionais, que permiten integrar en sistemas relacionais tradicionais algunhas características das BDOO e mesmo inclúen extensións espaciais do modelo multimedia do estándar SQL3.

Por outro lado, o avance no campo das telecomunicacións, e máis en concreto da internet, cun gran potencial tanto para a transmisión de grandes cantidades de información e acceso a datos, favoreceu a expansión das arquitecturas de xeoproceso baseadas en servizos web.

Os servizos web permiten concibir e desenvolver sistemas que integran, cun mínimo nivel de axuste, información e servizos de xeoproceso interoperables de múltiples fontes e en distintos formatos aos que se accede nun ámbito de rede distribuído.

Estas novas arquitecturas pretenden satisfacer o desexo da comunidade SIX de dispoñer dun acceso ilimitado e en calquera momento a información actualizada e interoperable. A dispoñibilidade deste tipo de servizos está a facilitar unha expansión do intercambio e da difusión electrónica da información espacial.

Por outra parte, este crecemento na implantación de produtos e servizos de información cartográfica na rede establece os principios para o asentamento real dun contorno no que sexa posible o intercambio de información xeográfica e servizos de xeoproceso. Cabe destacar tamén a acción tan importante que nesta liña está a desenvolver o consorcio OpenGIS, no que se aglutinan os principais entes involucrados no sector da información espacial e todos os sistemas e tecnoloxías que a soportan (usuarios, universidades, administracións, industrias software...). O propósito destes colectivos é elaborar de forma consensuada, especificacións de interfaces interoperables no campo das tecnoloxías da información espacial.

Dende a creación de OpenGIS, a mediados dos anos 90, foron xa moitas as realizacións prácticas nas que tomou parte e as súas especificacións son estándares de facto no ámbito das tecnoloxías da información espacial. Ademais, en moitos casos estes estándares son a base para a formulación de estándares internacionais.

Por exemplo, os dous seguintes, son servizos web que xa foron enteiramente especificados:

- Servizo de entidades vectoriais: facilita información relativa á entidade ou entidades que se encontran almacenadas nunha capa vectorial e que reúnen as características especificadas durante a consulta.
- Servizo de mapas en web: xera mapas no formato desexado para ser visualizados nun navegador ou outro tipo de cliente sinxelo. Estes mapas serán a resposta a algunha consulta con certos parámetros realizada previamente.

Podemos concluír que as arquitecturas dos SIX tenden a ser distribuídas, interoperables e en rede, apoiadas sobre estándares abertos da internet.

### **26.3.1 Clasificación dos SIX**

De acordo coa funcionalidade que integran e o tipo de problema que pretenden resolver, podemos distinguir os seguintes grupos de sistemas de información xeográfica.

1. *SIX profesional*: enfócanse cara a usuarios cun alto nivel de especialización e formación neste campo. Integra todas as funcións que se poden necesitar nun SIX a nivel de recompilación e edición de datos, administración de BD, análise e xeoproceso avanzado e todas as ferramentas específicas que poidan ser necesaria para mantemento da información.
2. *SIX de sobremesa*: enfócanse cara á explotación e utilización da información. Incorpora ferramentas de análise da información, ademais de mecanismos avanzados para a presentación de resultados como son informes, gráficos, mapas, etc. Presentan unha gran facilidade de manexo, co cal os usuarios non necesitan ser expertos no ámbito, ademais as ferramentas que integran son potentes e facilitan o acceso avanzado á información.
3. *Visualizadores SIX*: trátase de ferramentas sinxelas que se centran exclusivamente na visualización da información, de distintos tipos e formatos.
4. *WebGIS*: trátase de proporcionar o acceso a datos cartográficos e ás funcionalidades (servizos) dos SIX a través da rede. Cada vez máis téndese cara á estandarización deste tipo de servizos liderado por OpenGIS.

5. *SIX de compoñentes:* coa expansión no campo da enxeñaría de software dos desenvolvementos baseados en compoñentes, alcanzouse a posibilidade de incorporar funcionalidades espaciais en todo tipo de aplicacións (captación espacial de aplicacións), o que supón un novo impulso para a xeneralización do uso da información espacial a novos campos nos que se poden realizar interesantes sinerxías.
6. *SIX de dispositivos móbiles:* apóiase no uso de PDA e teléfonos intelixentes. Estes dispositivos teñen capacidade abonda como para soportar case todas as funcións dun sistema tradicional.

## **26.4 ÁMBITOS DE APLICACIÓN**

Os produtos SIX comerciais son cada vez máis comúns e populares, polo que recoller todas os ámbitos posibles de aplicación é unha ardua tarefa. Non obstante, no seguinte listado preséntanse os máis destacados ou onde o número de desenvolvementos é maior.

### **26.4.1 Demografía**

Nesta categoría recóllense todas as aplicacións que, se ben poden ser de natureza moi diversa, comparten o feito de que utilizan características demográficas e socioeconómicas, e a distribución espacial delas para a toma de decisións.

Os datos nos que se apoian este tipo de sistemas adoitan proceder de rexistros estatísticos confeccionados por algún organismo (oficial ou non).

As aplicacións dentro desta categoría adóitanse centrar na mercadotecnia, avaliación do impacto dun servizo, selección de lugares para o establecemento de negocios ou servizos, etc.

### **26.4.2 Xestión e planificación urbana**

Esta categoría oríentase a actividades propias de xestión municipal como son a xestión de servizos de infraestrutura (iluminación, rede de sumidoiros, mobiliario urbano, etc.), a xestión do tráfico, a xestión de taxas e licenza, a localización para instalacións e servizos comunitarios, etc.

Este tipo de sistemas adoita manexar escalas grandes e úsase como base o rueiro do concello en cuestión. Ademais este tipo de aplicacións adoita empregar un modelo de datos de tipo vectorial.

### **26.4.3 *Xestión de instalacións***

Nesta categoría agrúpanse os desenvolvementos orientados a compañías de subministracións e servizos, como son electricidade, auga, ferrocarril, etc. As aplicacións tipo deste grupo pasan pola xestión do mantemento, a relación co cliente (notificacións de cortes de subministración), deseño de instalacións, etc.

Estes sistemas caracterízanse por:

- A precisión necesaria adoita ser elevada.
- Existe unha forte estrutura en rede, necesaria para a realización de análises.
- Establécense conexións con bases de datos externas.
- Existe unha xerarquía de compoñentes da rede.

### **26.4.4 *Aplicacións de xestión e inventario de recursos***

Nesta categoría inclúense campos como a xestión forestal, a planificación agraria, a avaliación do impacto ambiental, a xestión do territorio, a do patrimonio natural e a do medio.

Normalmente manexan escalas pequenas con diversas calidades nos datos e mesmo sen contrastar. Estas aplicacións usan modelos de datos tanto vectoriais como ráster.

#### **26.4.5 Xestión catastral**

Esta categoría oriéntase á xestión da propiedade inmobiliaria e pola súa importancia adquiriu un termo específico: sistemas de información territorial (SIT).

No noso país contamos co sistema de información catastral, que conta con datos e descrições das propiedades tanto do ámbito urbano coma do rústico.

### **26.5 PROVEDORES E USUARIOS DE INFORMACIÓN ESPACIAL**

De xeito tradicional foi o sector público o encargado da construción da infraestrutura cartográfica dun país. Ademais das moitas consideracións que xustifican este feito, hai que ter en conta tamén que son as propias administracións públicas as principais consumidoras desta información espacial.

Por exemplo, algunhas das actividades para as que as administracións fan uso da información espacial son:

- Protección civil
- Rexistro catastral
- Censos estatísticos e electorais
- Xestión de recursos naturais
- Protección do medio
- Inventario do patrimonio
- Xestión dos dominios públicos

- Planificación de infraestruturas
- Organización territorial

Ademais destas, existen moitos outros servizos públicos cunha clara implicación territorial, como son os servizos sociais e asistenciais, servizos educativos e de saúde pública, etc.



## **26.6 INFRAESTRUTURAS DE DATOS ESPACIAIS**

Unha IDE (infraestrutura de datos espaciais) é un sistema informático integrado por un conxunto de recursos (catálogos, servidores, programas, datos, aplicacións, páxinas web,...) dedicados a xestionar información xeográfica (mapas, ortofotos, imaxes de satélite, topónimos...), dispoñibles na internet que cumpren unha serie de condicións de interoperabilidade (normas, especificacións, protocolos, interfaces,...) que permiten que un usuario, utilizando un simple navegador, poida utilizalos e combinalos segundo as súas necesidades.

O establecemento dunha IDE nun ámbito local, rexional, estatal ou global require do acordo dos produtores, integradores e usuarios de datos espaciais do ámbito territorial no que se establece. Este acordo debe considerar tamén as IDE definidas, ou en definición, noutros ámbitos territoriais superiores, cara ás cales deberá converxer.

A xustificación do establecemento dunha IDE, esta ligada a dúas ideas fundamentais:

- A necesidade de xeito doado, cómodo e eficaz dos datos xeográficos existentes. A información xeográfica foi ata agora un recurso de custosa produción e difícil acceso por varios motivos: formatos, modelos, políticas de distribución, falta de información...
- A oportunidade de reutilizar a información xeográfica xerada nun proxecto para outras finalidades diferentes, dado o alto custo da súa produción.

### **26.6.1 Principios das IDE**

Todas as iniciativas para o establecemento dunha IDE inclúen uns principios comúns:

- Marco institucional: o establecemento de acordos entre os produtores de información xeográfica, especialmente entre os produtores oficiais, para xerar e manter os datos espaciais fundamentais («Framework data») para a maioría das aplicacións baseadas en sistemas de información xeográfica.



- Estándares: o establecemento de normas ás que se deberá axustar a información xeográfica, os intercambios desta e a interoperación dos sistemas que a manexan.
- Tecnoloxía: o establecemento da rede e mecanismos informáticos que permitan buscar, consultar, encontrar, acceder, subministrar e usar os datos espaciais ou xeográficos; como por exemplo permitir incorporar os metadatos organizados en catálogos e ofrecelos na rede a través de servidores.
- Política de datos: O establecemento das políticas, alianzas e acordos de colaboración necesarios para aumentar a dispoñibilidade de datos espaciais e compartir os desenvolvementos tecnolóxicos.

## 26.6.2 **Compoñentes das IDE**

### 26.6.2.1 Datos

Na actualidade existe un consenso internacional que clasifica os datos espaciais que poden manexar as IDE en:

#### **26.6.2.1.1 Datos de referencia**

Son aqueles datos xeorreferenciados fundamentais que serven de esqueleto para construír ou referenciar calquera outro dato fundamental ou temático. Constitúen o marco de referencia que proporciona o contexto xeográfico a calquera aplicación.

Cumpren a función de ser a información xeográfica de referencia utilizada como base común que permite mesturar e integrar datos de aplicacións de todo tipo ao ser o vínculo ou nexo de unión.

A iniciativa europea INSPIRE definiu os temas que deben ser considerados como datos de referencia, nos Anexos I e II na Proposta da directiva pola que se establece unha infraestrutura de información espacial da Comunidade (INSPIRE):

- Sistema de coordenadas.
- Cuadrículas xeográficas.

- Nomes xeográficos.
- Unidades administrativas.
- Redes de transporte.
- Hidrografía.
- Lugares protexidos.
- Elevación.
- Identificadores de propiedade.
- Parcelas catastrais.
- Cuberta terrestre.
- Ortoimaxes.

#### **26.6.2.1.2 Datos temáticos**

Son os datos propios de aplicacións específicas que explotan a información xeográfica cunha finalidade concreta. Inclúen valores cualitativos e cuantitativos que se corresponden con atributos asociados aos datos de referencia como por exemplo: vexetación, xeoloxía, clima, tráfico, contaminación, etc.

#### **26.6.2.2 Metadatos**

A estrutura e o contido dos metadatos deben estar baseados nunha norma aceptada e amplamente utilizada. Un dos beneficios das normas é que son froito da experiencia e do consenso, xa que foron desenvolvidas e revisadas por un grupo internacional de expertos que achegaron unha considerable diversidade cultural e social. En particular, as normas ISO19100 relativas á información xeográfica proporcionan unha base dende a que se poden desenvolver perfís ou particularizacións da norma, nacionais e sectoriais.

Na actualidade existen diferentes normas e perfís dentro do campo dos metadatos que é interesante mencionar:

- ISO 19115 "Geographic information - Metadata"

Norma internacional de metadatos pertencente á familia ISO 19100 desenvolvida polo Comité Técnico 211, pertencente á Organización de Estandarización Internacional (ISO) que proporciona un modelo de metadatos e establece un conxunto común de terminoloxía, definicións e procedementos de ampliación para metadatos. Foi adoptada como Norma Europea polo CEN/TC287 e como Unha Norma Española por AEN/CTN148 "*Información Geográfica*", polo que está dispoñible en castelán.

- [Núcleo español de metadatos "NEM"](#)

Recomendación definida polo grupo de traballo de la IDEE, establecida en forma de perfil de ISO19115. É un conxunto mínimo de elementos de metadatos recomendados en España para a súa utilización á hora de describir recursos relacionados coa información xeográfica. Está formado pola ampliación do núcleo (Core) da norma ISO 19115 de metadatos, cos ítems de ISO19115 necesarios para incluír os elementos do Dublin Core Metadata, a descrición da calidade e os elementos requiridos pola Directiva marco da Auga.

- Dublin Core Metadata Iniciativa

A iniciativa Dublin Core Metadata é un foro aberto dedicado ao desenvolvemento de estándares na liña dos metadatos. Ten como actividades principais a formación de grupos de traballo, conferencias globais e talleres e desenvolvemento de prácticas no campo dos metadatos. Esta iniciativa definiu 15 elementos básicos e esenciais para describir un recurso calquera (ficheiro, mapa, libro..) e na actualidade é a iniciativa de metadatos máis utilizada. Para máis información consultar a páxina web <http://dublincore.org/>

### 26.6.2.3 Servizos

Moito máis axeitado que concibir unha IDE como algo baseado nos datos xeográficos dispoñibles é pensar que unha IDE é en realidade un conxunto de servizos que ofrecen unha serie de funcionalidades que resultan útiles e interesantes a unha comunidade de usuarios, de forma que a énfase se pon nos servizos, na utilidade. Establécese un xogo novo con regras novas; dende o punto de vista das IDE, ao usuario non lle interesa xa tanto descargarse os datos no seu sistema, senón obter directamente as respostas que necesita e que un servizo lle ofrece.

Os servizos IDE ofrecen funcionalidades accesibles vía a internet cun simple navegador ou *browser* sen necesidade de dispoñer doutro software específico para iso.

- Servizo de mapas en web (WMS)

O seu obxectivo é poder visualizar información xeográfica. Proporciona unha representación, unha imaxe do mundo real para unha zona requirida. Esta representación pode provir dun ficheiro de datos dun SIX, un mapa dixital, unha ortofoto, unha imaxe de satélite... Está organizada nunha ou máis capas que se poden visualizar ou ocultar unha a unha. Pódese consultar certa información dispoñible e as características da imaxe do mapa. Unha especificación do Open Geospatial Consortium (OGC) establece como debe ser un WMS estándar e interoperable, que permita superpoñer visualmente datos vectoriais, ráster, en diferente formato, con distinto sistema de referencia e coordenadas e en distintos servidores.

- Servizo de fenómenos en web (WFS)

Ofrece o poder acceder e consultar todos os atributos dun fenómeno (*feature*) xeográfico como un río, unha cidade ou un lago, representado en modo vectorial, cunha xeometría descrita por un conxunto de coordenadas. Habitualmente os datos proporcionados están en formato GML, pero calquera outro formato vectorial pode ser válido. Un WFS permite non só visualizar a información tal e

como permite un WMS, senón tamén consultala libremente. Unha especificación Open Geospatial Consortium establece como debe ser un WFS estándar e interoperable.

- Servizo de coberturas en web (WCS)

É o servizo análogo a un WFS para datos ráster. Permite non só visualizar información ráster, como ofrece un WMS, senón ademais consultar o valor do atributos ou atributos almacenados en cada píxel. Unha especificación Open Geospatial Consortium establece como debe ser un WCS estándar e interoperable.

- Servizo de nomenclátor (*Gazetteer*)

Ofrece a posibilidade de localizar un fenómeno xeográfico dun determinado nome. Defínese como un servizo que admite como entrada o nome dun fenómeno, coas posibilidades habituais de nome exacto, comezando por, nome incluído... e devolve a localización mediante unhas coordenadas do fenómeno en cuestión. Adicionalmente, a consulta por nome permite fixar outros criterios como a extensión espacial na que se desexa buscar ou o tipo de fenómeno dentro dunha lista dispoñible (río, montaña, poboación...). Se hai varios que cumpren a condición de busca, o servizo presenta unha lista dos nomes encontrados con algún atributo adicional para que o usuario poida elixir o que desexa. Evidentemente este servizo necesita dispoñer dun conxunto de nomes con coordenadas. Unha especificación Open Geospatial Consortium establece como debe ser un Servizo de nomenclátor estándar e interoperable.

- Servizo de *Geoparser*

Un servizo de *Geoparser* analiza palabra por palabra un texto dixital dado, efectúa comparacións cun conxunto de nomes xeográficos dado e crea os vínculos ou enlaces necesarios para que exista unha referencia permanente no texto orixinal

aos fenómenos xeográficos aludidos. Transforma o texto orixinal nun hipertexto con vínculos xeográficos. Este servizo baséase e utiliza un servizo de nomenclátor.

- Servizo de catálogo (CSW)

Un servizo de catálogo permite a publicación e busca de información (metadatos) que describe datos, servizos, aplicacións e en xeral todo tipo de recursos. Os servizos de catálogo son necesarios para proporcionar capacidades de busca e invocación sobre os recursos rexistrados dentro dunha IDE. Unha especificación Open Geospatial Consortium establece como debe ser un Servizo de Catálogo estándar e interoperable.

- Descritor de estilo de capas (SLD)

Esta especificación da OGC describe un conxunto de regras de codificación que lle permite ao usuario definir estilos de simbolización das entidades personalizados. É recomendable ler esta recomendación xunto coa última versión da especificación WMS.

Os servizos OGC poden ser encadeados e combinados nun xeoportal, ofrecendo por exemplo a posibilidade de buscar un fenómeno por nome (nomenclátor) e visualizar o resultado sobre uns datos de referencia (WMS); localizar un produto seleccionando algunhas características (catálogo) e visualizalo na pantalla (WMS ou WCS). Tamén é posible basearse nun servizo OGC para implantar servizos que ofrezan funcionalidade adicional, por exemplo desenvolver un servizo de camiño mínimo por estrada baseado nun WFS que acceda a todos os atributos dun conxunto de datos de poboacións e estradas.



## 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

Colexiado do CPEIG





## **27. ARQUITECTURA DAS REDES INTRANET E INTERNET: CONCEPTO, ESTRUTURA E CARACTERÍSTICAS. A SÚA IMPLANTACIÓN NAS ORGANIZACIÓNS.**

## **TEMA 27. ARQUITECTURA DAS REDES INTRANET E INTERNET: CONCEPTO, ESTRUCTURA E CARACTERÍSTICAS. A SÚA IMPLANTACIÓN NAS ORGANIZACIÓNS.**

### **27.1. INTRODUCCIÓN E CONCEPTOS**

### **27.2. INTERNET**

### **27.3. INTRANET/EXTRANET**

### **27.4. IMPLANTACIÓN DE REDES EN ORGANIZACIÓNS**

### **27.5. ESQUEMA**

### **27.6. REFERENCIAS**

### **27.1. INTRODUCCIÓN E CONCEPTOS**

Unha rede son dous ou máis nodos comunicados entre si. A partir de aí, a rede pode aumentarse en calquera número de nodos e conectarse a outras redes. **Internet** é unha rede de alcance mundial que conecta as diferentes redes físicas dun xeito descentralizado como unha rede lóxica única.

No mundo da informática un nodo pode ser calquera compoñente dunha rede, dende dispositivos de interconexión a equipos ou estacións de traballo, ou calquera outro tipo de cliente como equipos portátiles e dispositivos móbiles.

Por debaixo destas redes ademais teremos diferentes tipos de redes físicas, que tomarán diferentes medios e tecnoloxías. Internet proporcionará un mecanismo de comunicación común baseado na familia de protocolos TCP/IP, de maneira que calquera destas redes que implemente ou acepte esta familia de protocolos poderá comunicarse coas demais.

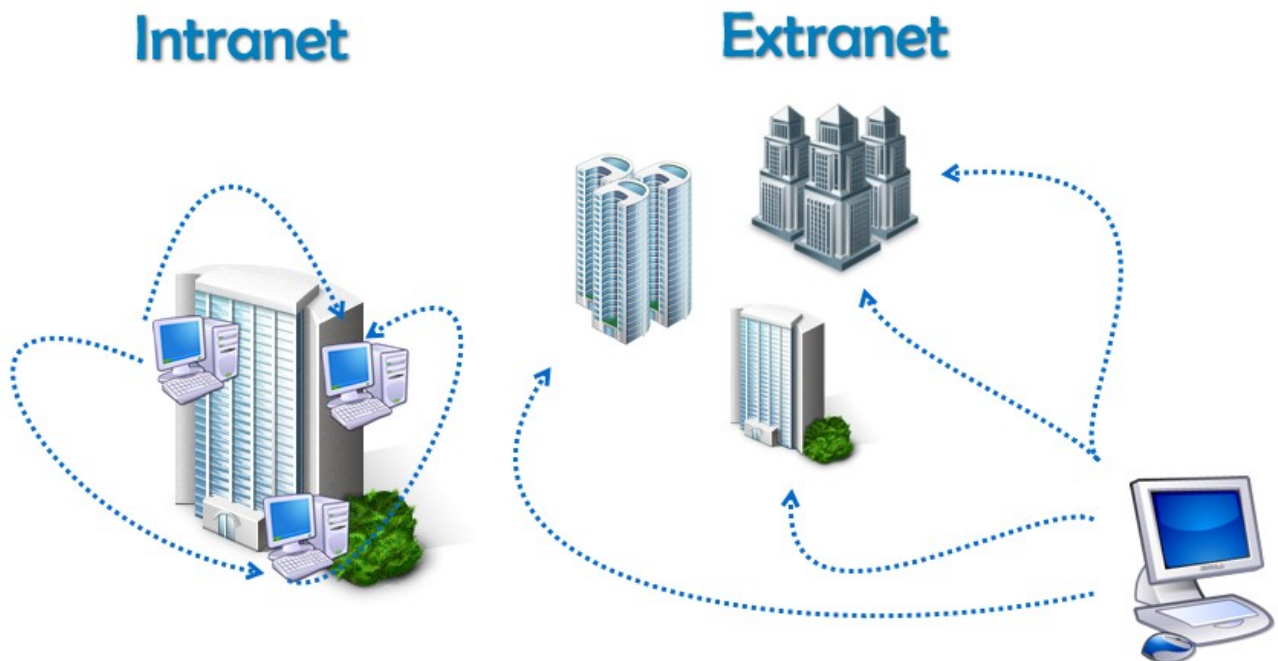
De entre todos os servizos que proporcionar Internet o buque insignia é o World Wide Web (WWW, ou a Web) o conxunto de protocolos que permite a consulta de arquivos de hipertexto ou páxinas web emprazados en

diferentes sitios de aloxamento ou sitios web.

Unha **Intranet** é unha rede interna a unha organización ou institución, que ten por obxecto proporcionar un conxunto de servizos accesibles exclusivamente dende a rede local ou un conxunto de redes illadas do exterior a través de Internet.

A idea principal dunha Intranet é que os seus servizos sexan só accesibles polos usuarios da organización ou institución, dun xeito privado. Estes servizos poden incluír servidores web, servidores de correo electrónico, sistemas de xestión de arquivos, contidos e utilidades de comunicación ou mensaxería.

Estendendo este concepto a Internet, cando os servizos están dispoñibles cara fóra, pero só para os usuarios da organización ou institución estarase falando dunha **Extranet**. No caso da Extranet establécese un mecanismo de seguridade ou autenticación dos usuarios para garantir que pertencen á organización ou institución. En consecuencia unha Extranet non será nin unha Intranet nin un sitio de Internet senón a publicación dos servizos dunha Intranet a través da Internet mediante un sistema de autenticación dos usuarios da organización ou institución.



**Figura 1: Intranet e Extranet**

## **27.2. INTERNET**

### **27.2.1. CARACTERÍSTICAS BÁSICAS**

Internet ten as súas orixes a finais da década dos 60, sendo unha evolución da rede experimental ARPANET (Rede da Axencia de proxectos de investigación avanzada), desenvolvida polo departamento de Defensa dos EUA.

A idea orixinal era dispoñer dunha rede na que en caso de acontecer danos ou a desaparición dalgún nodo ou punto da mesma a rede permanecera activa entre os nodos ou elementos restantes, garantindo así a supervivencia da información e o funcionamento do medio de comunicación. A partir deste concepto pode entenderse o funcionamento distribuído e completamente descentralizado que posúe o sistema actualmente, de xeito que cada nodo individual ten a mesma importancia e

peso no conxunto á hora de dar servizo ou comunicarse cos demais.

Posteriormente desenvolveuse sobre a rede un software básico de control da transmisión de información que terminaría por dar lugar á **familia de protocolos TCP/IP**. Esta familia de protocolos representa un conxunto de normas e estándares que definen o mecanismo de comunicación entre os diferentes nodos da rede. Calquera rede física que implemente ou dea soporte a este conxunto de protocolos poderá comunicarse con outras redes que tamén o fagan. A partir dun destes protocolos, podemos especificar outro dos factores fundamentais que explican o funcionamento desta rede o concepto de **Enderezo IP** (Protocolo de Internet). Este enderezo representa o enderezo ou nome de cada nodo da rede, sendo un identificador único para cada un deles. Os enderezos IP compóñense de catro cifras numéricas separadas por puntos que toman valores entre 0 e 255. Por exemplo: 192.168.1.1. Por mor de aumentar o rango de enderezos deseñouse o **IPv6** que pasa a valores de 128 bits, con oito grupos de catro díxitos hexadecimais, por exemplo: FEDC:BA98:7654:3210:FEDC:BA98:7654:3210.

Enderezo IP	Significado
::	Ausencia de enderezo
0:0:0:0:0:0:0:0	Ausencia de enderezo
::1	Loopback
::1.2.3.4	Compatible con IPv4
::ffff:0:0	Enderezo Ipv4 mapeado
Ff00::	Multicast
FF01:0:0:0:0:0:0:0:101	Multicast

**Táboa 1: Exemplos de enderezos Ipv6.**

Como este tipo de identificación pode resultar difícil de lembrar emprégase en conxunción o Sistema de Nomes de Dominio (**DNS**). Neste sistema diferentes nodos da rede fan as funcións de tradutores entre enderezos IP e nomes de Dominio, sendo estes varias palabras separadas por puntos, por exemplo [www.xunta.es](http://www.xunta.es), indicando en última instancia a zona ou tipo de organización á que pertence o sitio, neste caso España, co acrónimo 'es', a continuación a organización, institución ou mnemotécnico, neste caso 'xunta', e por último o usuario ou protocolo, neste caso 'www'.

Por último outro concepto fundamental é o de **clientes e servidores**. O obxectivo da rede será dobre comunicar e dar servizos. Neste caso podemos distinguir tres tipos de nodos:

1. **Servidores**. Proven de servizos á rede, tales como contidos web, correo electrónico, vídeo, xestión das comunicacións, seguridade, etc...
2. **Clientes**. Nodos que representan o equipo de traballo dun usuario final, o cal fai uso dun dos servizos da rede que lle proporciona un servidor.
3. **Elementos de interconexión**. Son nodos específicos de comunicación, encárganse de xestionar as comunicacións, retransmitir e dirixir as mensaxes.

O modelo de Internet pode aplicarse sobre redes máis pequenas, de menos equipos e unha extensión menor. A idea de Internet é unha rede global, con servizos e comunicación a escala mundial. Abstraendo funcionamento e protocolos, poden facerse rede máis pequenas cun servizo reducido ao seu ámbito. A partir disto temos a clasificación habitual das redes, que inclúe:

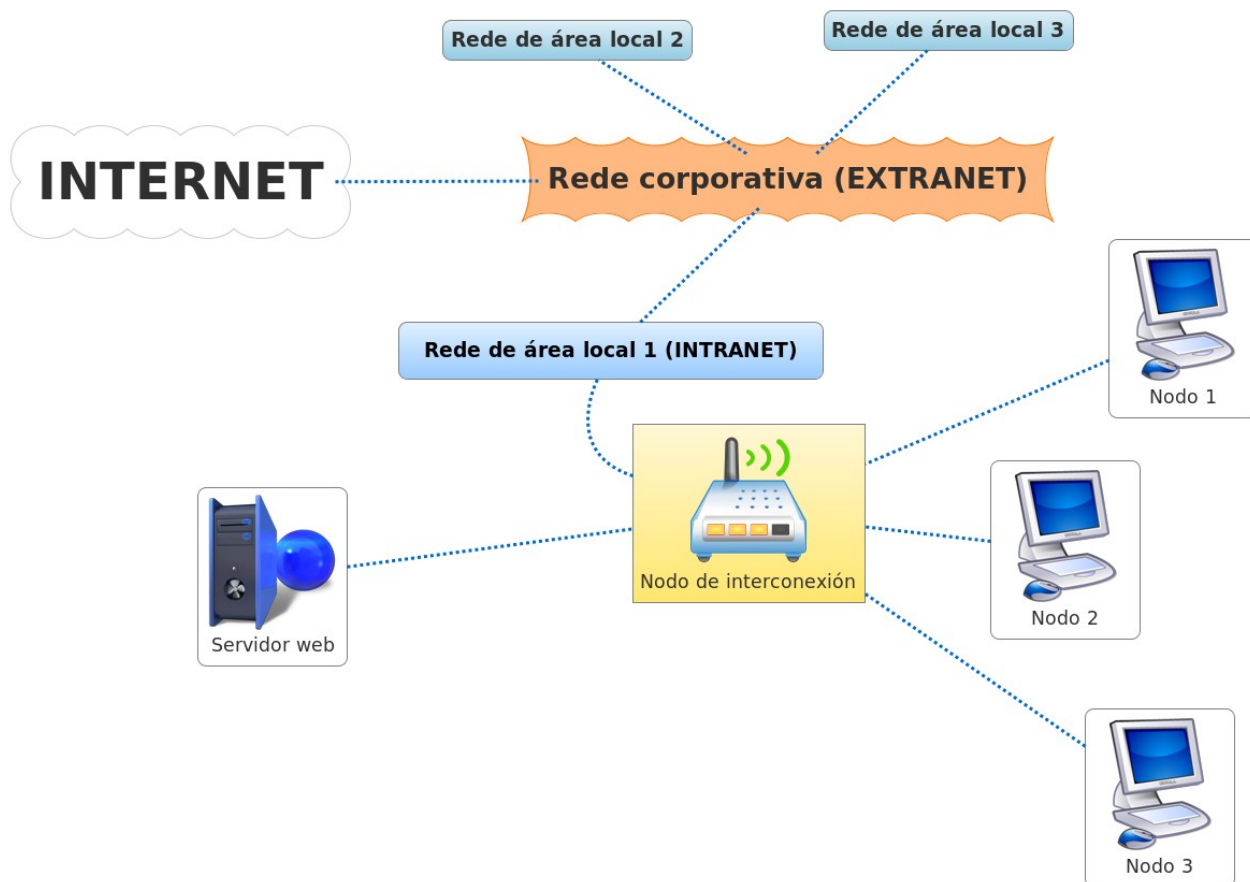
1. **Redes de área local**. (En inglés *Local Area Network* ou LAN). Interconexión de varios computadores e elementos de interconexión limitada fisicamente a un edificio ou contorno de arredor de 200



metros - 1 Quilómetro. Exemplos destas redes serían as redes corporativas ou institucionais dentro dun mesmo edificio, como pode ser a rede interna dunha Consellaría, e por norma xeral inclúen ademais servizos de Intranet.

2. **Redes de área metropolitana.** (En inglés *Metropolitan Area Network* ou MAN). Interconexión de varias computadores e elementos de interconexión nun área extensa, como pode ser unha cidade, provincia ou comunidade autónoma. Exemplo deste tipo de redes sería a rede corporativa da Xunta de Galicia. Por norma xeral este tipo de redes incorporan servizos de Intranet/Extranet.
3. **Redes de área ampla.** (En inglés *Wide Area Network* ou WAN). Interconexión de varias computadores e elementos de interconexión en distancias de 100-1000 Quilómetros. Exemplo deste tipo de redes sería a propia rede Internet.

Na seguinte figura, podemos ver un exemplo de rede de área local, con algúns elementos básicos. Diferentes equipos de traballo, conectados por nodos de interconexión e con algún servizo como o proporcionado polo servidor web. Esta pequena rede pode atoparse integrada nunha rede de maior alcance con servizos de Intranet e como medio de comunicación co resto do mundo a través de Internet.



**Figura 2: Exemplo de rede de área local conectada a unha rede corporativa e a Internet.**

### 27.2.2. TIPOS DE CONEXIÓN A INTERNET

Para conectar outra rede ou equipo cliente, xa sexa un ordenador de sobremesa, portátil, teléfono móbil, PDA , etc..., á rede Internet o primeiro paso será dispoñer dun **provedor de acceso ou ISP** (en inglés *Internet Service Provider*, provedor de servizos de Internet). Trátase de empresas que proporcionan e xestionan a conexión á rede aos seus clientes, empregando diferentes tecnoloxías. Por normal xeral os ISP proporcionan un hardware de conexión á rede específico e pode que un software para xestionalo.

Entre as tecnoloxías de conexión máis empregadas hoxe en día dispoñemos





de:

1. **RTC.** A rede telefónica conmutada, que emprega a mesma rede que os teléfonos fixos en Galicia. Neste caso se trata dun soporte analóxico polo que para enviar datos dixitais haberá que mudalos empregando un dispositivo denominado **Módem** (modulador - demodulador), ou variantes máis avanzadas con maiores características como a enrutación ao estilo dos **Módem-Routers**. Deste xeito un usuario que queira acceder a Internet precisará dispor dunha liña telefónica e un Módem ou Módem-Router. Estes dispositivos poden ser internos, como acontece normalmente nos dispositivos portátiles ou externos. Neste último caso a conexión co equipo de traballo realizarase conectando o dispositivo por un cable/porto (P.ex.: USB) ou con conectividade sen fíos. Actualmente esta tecnoloxía atópase nun estado practicamente obsoleto, debido a que non pode transmitir datos e voz á vez e que a súa velocidade máxima é moi baixa (arredor de 56 Kbps).
2. **ADSL.** A liña de aboado dixital asimétrica convirte a liña telefónica nunha liña de alta velocidade debido a que aproveita toda a potencia dos fíos establecendo tres canles independentes:
  - a) Canle de alta velocidade para transmitir datos.
  - b) Canle de alta velocidade para recibir datos.
  - c) Canle de alta velocidade para voz.

Deste xeito permítese que a través da mesma liña se envíen datos e voz á vez. O concepto de asimétrica ven de que as velocidades de subida e baixada de datos son diferentes sendo máis altas as velocidades de baixada, nunha interpretación de que as necesidades dos usuarios van neste senso. O hardware empregado neste caso serán Módem-Routers, proporcionados por un ISP. As velocidades de descarga acadadas son moi superiores ao RTC, indo de 512 Kbps a un máximo teórico para VSL (unha

evolución da ADSL de moi alta taxa de transferencia) de 55 Mbps, se ben os provedores en Galicia proporcionan bastante menos.

3. **Sen fíos.** Aínda que en orixe as redes sen fíos foron deseñadas para redes de área local actualmente tamén se empregan para posibilitar accesos a Internet. Baseados no conxunto de estándares Wi-Fi (en inglés *Wireless Fidelity*) chegan a acadar velocidades de arredor de 54 Mbps chegando ao máximo teórico de 600Mbps. O hardware necesario neste caso será un Router Wi-Fi sen fíos que faga as funcións de punto de acceso (en inglés *hotspot*) e no equipo de traballo unha antena receptora integrada nunha tarxeta de rede (interna ou externa).
4. **Cable.** Redes baseadas en tecnoloxías de fibra óptica o que implica que precisa unha liña de transmisión desta tecnoloxía. O hardware empregado é similar ao da ADSL, pero neste caso será un Cable-Módem o encargado de xestionar a comunicación, aínda que o termo Cable-Router sería máis axeitado neste caso, pois a xestión é máis avanzada ca no caso do Módem. As velocidades son moi elevadas, esta tecnoloxía tamén resulta moi cara en contrapartida, chegando a 10 Gbps de máximo teórico con 1 Gbps habituais. De cara ao usuario e en Galicia, o ancho de banda é moito menor, os provedores máis habituais acostuman a proporcionar velocidades similares ás da ADSL.
5. **Satélite.** A conexión vía satélite emprégase en emprazamentos con pouca infraestrutura onde non é posible aplicar as tecnoloxías anteriores, como ADSL ou Cable. En Galicia recórrase a este tipo de tecnoloxías en zonas do contorno rural ou zonas de alta montaña. Esta tecnoloxía ten un custe moi alto, pero presenta unha ampla cobertura. O hardware necesario require a instalación dunha antena



parabólica e na oferta habitual dos ISP proporcionan 2 Mbps de subida e baixada.

6. **Módem Móbil.** As últimas tecnoloxías desenvolvidas para teléfonos móbiles como GSM, GPRS, ou UTMS/3G permiten que os operadores ofrezan aos usuarios servizos de Internet ben directamente dende o **dispositivo móbil** ou ben conectando outro equipo de traballo á rede a través do mesmo. Empregan un protocolo específico denominado WAP (en inglés *Wireless Application Protocol*) e as velocidades de conexión varían dependendo da tecnoloxía de 56 Kbps a 2 Mbps coas tecnoloxías de última xeración. O hardware básico é un teléfono móbil que soporte estas tecnoloxías, podendo precisar algún elemento de conexión extra para conectalo con outros equipos de traballo.
7. **PLC.** (Do inglés *Power Line Communication*) Esta tecnoloxía ofrece conexión a Internet a través da rede eléctrica. Como a ADSL esta tecnoloxía aproveita unha infraestrutura de cableado xa existente para ampliar os canais empregando medias e altas frecuencias. Require hardware específico, os denominados **Módem PLC**. Acada velocidades de ata 134 Mbps, e a pesar de que o ancho de banda é mesmo superior ao da ADSL e a infraestrutura de cableado eléctrico pode ser mesmo superior que o telefónico, en Galicia o uso desta tecnoloxía está moi pouco estendido.

### 27.2.3. SERVIZOS DE INTERNET

O fin último de acceder a Internet ou a outra rede é facer uso dos **servizos** que se atopan nela, e que veremos a continuación:

#### 1. WWW

No caso de Internet o servizo máis empregado é a Rede global mundial ou **WWW** (siglas en inglés de *World Wide Web*), trátase dun sistema de publicación e intercambio de información distribuído que relaciona uns contidos con outros a través de ligazóns. Este sistema estendeuse rapidamente grazas á súa facilidade de uso.

Neste contexto xorde o **Hiperligazóns**, que ven sendo un texto ou outro obxecto que contén unha ligazón premendo nas cal se accede a outra información emprazada noutra zona do documento ou noutro documento distinto. Esta funcionalidade permite relacionar uns documentos con outros, ou o que é o mesmo uns nodos con outros formando un rede denominada arañeira (en inglés *web*), de aí que cada documento pasara a denominarse páxina web. Cando se trata de texto as ligazóns soen aparecer resaltados en cor azul e subliñados, e mesmo pode cambiar o estilo do punteiro do rato para que non pasen desapercibidos.

Os documentos denominados páxinas web, son documentos en linguaxes estándar como HTML ou XML que poden incluír diferentes tipos de información: texto, hiperligazóns, gráficos e outros elementos multimedia. Estas páxinas web alóxanse en servidores web distribuídos por todo o mundo no que se coñece como **sitios web**. Cando o servidor se atope conectado á rede a conxunción de enderezos IP e nomes de dominio permitirá acceder aos documentos do sitio e visualizalos mediante uns programas denominados **navegadores** de Internet. Este tipo de programas implementan o protocolo HTTP que funciona sobre a familia de protocolos TCP/IP encargándose de xestionar a comunicación entre o cliente e o servidor web. Para acceder ao enderezo dunha páxina web podemos facelo tanto mediante ligazóns como directamente dende a barra de enderezos do navegador sen máis que inserir directamente nela o nome ou enderezo web do sitio.

Os enderezos web serven para identificar os recursos da rede, e denomínanse **URL** (en inglés *Uniform Resource Locator*) ou localizador uniforme de recurso. As URL poden ser da forma: <https://www.xunta.es:80/ruta/index.htm> tendo os seguintes compoñentes:

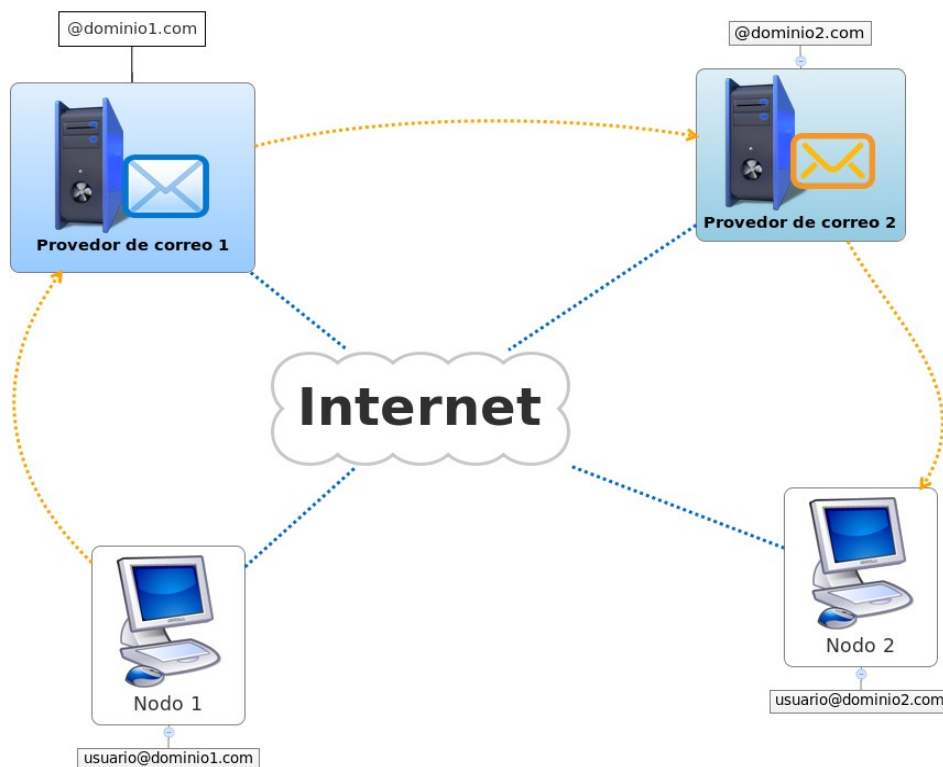
- a) O protocolo da rede que se emprega para recuperar a información do recurso especificado, neste caso 'https', sendo un dos máis habituais xunto a 'http', 'ftp', 'mailto', 'file', ou 'ldap'. Normalmente o protocolo HTTP é opcional na maioría dos navegadores xa que se trata do protocolo máis utilizado.
- b) O nome de dominio, ou servidor co que se comunica, neste caso '[www.xunta.es](http://www.xunta.es)'.
- c) O porto de comunicación que emprega ese protocolo no servidor, neste caso ':80', sendo este opcional pois os protocolos acostuman levar un porto asociado por defecto.
- d) A ruta do recurso no servidor, (en inglés *path*), neste caso '/ruta'.
- e) O nome do arquivo aloxado nesa ruta ou directorio, neste caso '*index.htm*'.
- f) Outros campos como parámetros ou propiedade propias de determinados protocolos.

## 2. Correo electrónico

O servizo de **correo electrónico** (e-Correo) proporciona os mecanismos para facilitar o envío e recepción de mensaxes que poden incluír texto e outras achegas a modo de arquivos multimedia. Neste servizo identifícase cada usuario cunha conta que levará o seu nome de usuario para o dominio dese servidor de correo seguido do símbolo '@' (arroba) e o nome de dominio (DNS) dese servidor. Por exemplo: [usuario@xunta.es](mailto:usuario@xunta.es). O acceso ao correo electrónico pode facerse con dous sistemas diferentes, ou ben accedendo cun correo web ou ben cun cliente de correo electrónico. No

**correo web** (en inglés *webmail*) accédese dende un navegador a unha páxina de administración do correo, que require a autenticación do usuario e permite facer as operacións como en calquera outro sitio web. Neste caso é idéntico a calquera outro servizo *www*, é dicir emprega os protocolos HTTP ou HTTPS segundo o nivel de seguridade do servidor. Non require software adicional e calquera equipo que teña instalado un navegador permitirá acceder a un servidor de correo remoto.

A alternativa é empregar software a modo de clientes de correo electrónico específicos que permiten conectar un software de xestión de correo co servidor a través dos protocolos de correo **POP3** ou **IMAP**. Estes dous protocolos permiten obter e enviar mensaxes de correo dende e cara un servidor remoto. A diferenza entre ambos protocolos é que POP3 atópase máis orientado cara a recepción de correo que para o envío, co cal ao conectarse descarga todas as mensaxes ao equipo cliente e as elimina do servidor, mentres que o protocolo IMAP as mantén. En liñas xerais IMAP proporciona máis funcionalidades que POP3, sendo un pouco máis complexo polo que non se atopa implantado en todos os servidores de correo. Para especificar como deben encamiñarse os correos empréganse os **Rexistros MX** (en inglés *Mail eXchange Record*), recursos DNS que indican os servidores de correo por prioridade. O MTA (en inglés *Mail Transfer Agent*) solicita o Rexistro MX perante unha petición DNS encamiñando posteriormente o envío. Existen moitos riscos de seguridade asociados aos correos, ademais da posibilidade de envío de virus, Hoax ou troianos, algúns servidores permiten o envío aberto ou Open Relay.



**Figura 3: Funcionamento do correo electrónico.**

### **3. Transferencia de arquivos (FTP)**

O servizo de transferencia de arquivos ou FTP (en inglés *File Transfer Protocol*) é un protocolo que define os estándares para o servizo de transferencia de arquivos a través de Internet. Trátase dun sistema cliente-servidor ao estilo dos anteriormente comentados onde un equipo cliente pódese conectar cun servidor de arquivos remoto para descargar ou enviar un ou máis ficheiros independentemente do sistema operativo do equipo cliente. Coma acontecía co correo electrónico pode xestionarse dende un navegador empregando o servizo *www*, ou ben cun cliente FTP que faga transparentes e usables as diferentes funcionalidades do servizo. Unha conta de usuario especial é a que ten como usuario e contrasinal 'anonymous' que se emprega para acceder a servidores FTP anónimos ou públicos, trátase dun estándar de facto para permitir acceder a calquera persoa aos contidos dun directorio público dun servidor FTP. Ampliacións

deste protocolo no eido da seguridade dan lugar á evolución a **SCP** (en inglés *Secure Copy*) e **SFTP** (en inglés *SSH File Transfer Protocol*) ambos engaden a seguridade **SSH** (en inglés *Secure Shell*) no primeiro limitado a transferencia de arquivos e no segundo con máis opcións.

#### **4. Conexión ou acceso remoto (Telnet)**

Este servizo permite o acceso remoto a outro equipo a través da rede e traballar con ela dende o noso equipo a través dunha consola coma se estiveramos conectados directamente a ela, coma un usuario desa máquina. **Telnet** é o protocolo de rede que permite realizar este tipo de comunicacións, que precisan que no servidor remoto estea activado o servizo de Telnet para aceptar as comunicacións. Require unha conta de usuario e contrasinal para o servidor de Telnet, que en moitos casos pode coincidir cun usuario do equipo remoto. Os problemas de seguridade das versións iniciais do Telnet arranxáronse coa súa evolución a **SSH** unha nova versión do sistema con técnicas de cifrado e con novas funcionalidades. Como ocorría co Telnet, SSH é tanto o nome do protocolo coma o do programa que o implementa, e como acontecía co FTP e co correo electrónico existe software de xestión que facilita ao usuario a conexión vía Telnet ou SSH. A posibilidade de estar nunha computadora mentres se traballa en outra resulta moi útil para tarefas administrativas, sobre todo para os administradores de rede ou para situacións de teletraballo.

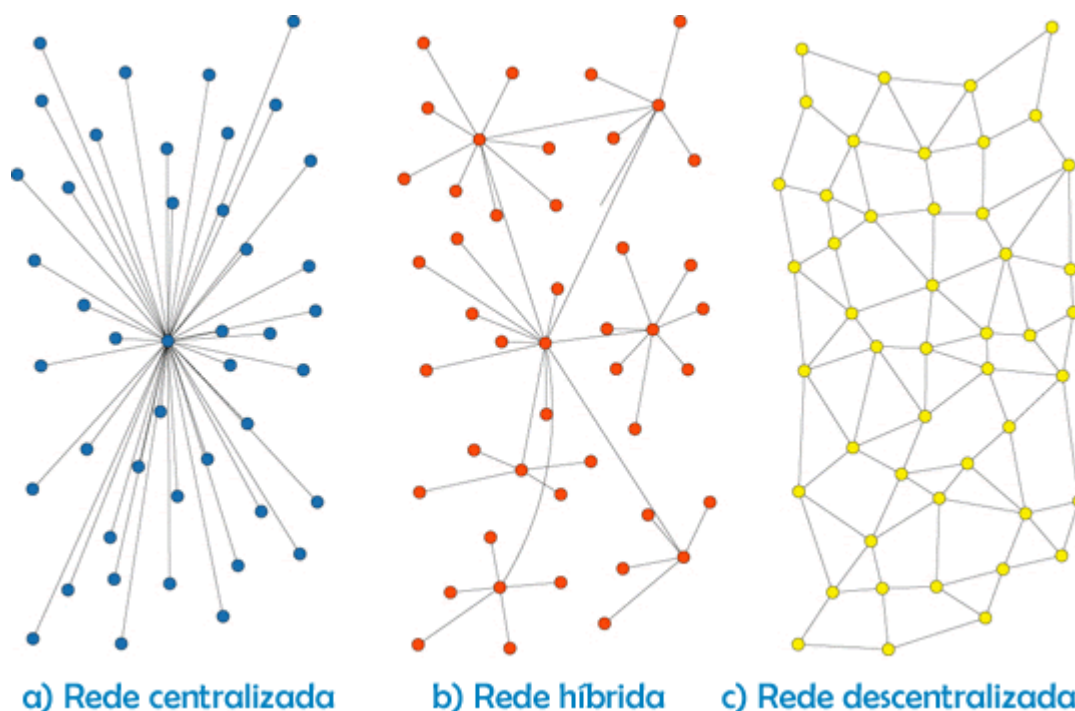
Un paso máis alá, os **terminais en modo gráfico** permiten ademais de texto amosar imaxes, co cal accederíamos dende o noso equipo a un escritorio idéntico a como o veríamos se nos atopáramos fisicamente no equipo remoto. Os clientes deste servizo empregan os protocolos RDP ou X11 segundo o sistema operativo, para sistemas Windows e Unix/Linux respectivamente.



## **5. P2P**

O servizos P2P teñen a súa orixe no concepto das redes entre iguais (en inglés *peer-to-peer*). A característica principal deste tipo de redes é que todos os nodos que participan na rede teñen o mesmo peso na mesma, todos actúan como clientes e como servidores. Trátase de subredes dentro da Internet establecidas a partir dun determinado software de xestión para P2P. Nun principio estas redes podían ter nodos centrais para xestionar as comunicacións se ben a base do intercambio de arquivos seguía sendo distribuída. Cada nodo, equivalente a un usuario conectado á rede P2P comparte os seus recursos con todos os demais nodos, se ben o xeito máis habitual é o de compartir arquivos en ocasións permiten realizar cálculos de custe elevado ou procesamentos de datos masivos con orientación científica. Segundo dispoñan de nodos centrais podemos falar dos seguintes tipos de redes:

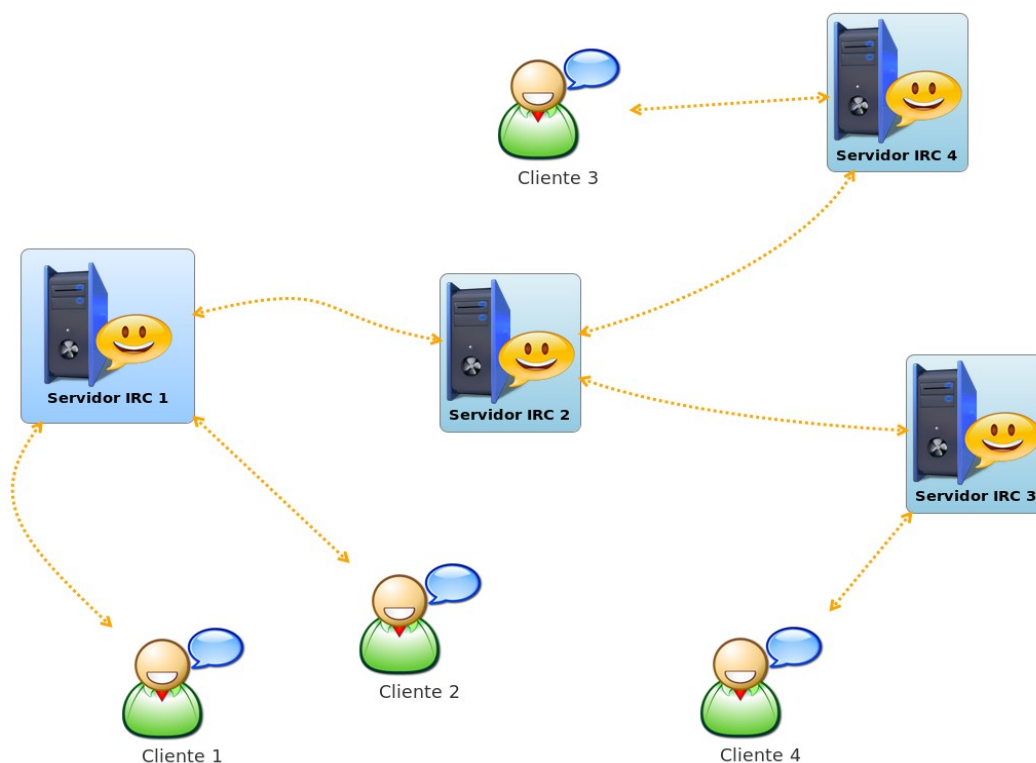
- a) Redes P2P centralizadas, en forma de estrela cun servidor central que monopoliza a xestión e administración da rede.
- b) Redes P2P híbridas, onde ademais do nodo central existen nodos de segundo nivel que centralizan a xestión de subredes.
- c) Redes P2P descentralizadas, onde todos os nodos son clientes e servidores co mesmo peso.



**Figura 4: Topoloxías habituais das redes P2P.**

## 6. Conversa (Chat)

Este servizo permite que dous ou máis usuarios conectados simultaneamente a Internet sosteñan conversas interactivas en tempo real. O IRC (en inglés *Internet Relay Chat*) é o protocolo de comunicación baseado en texto que sustenta o servizo. As conversas teñen lugar nos denominados canles de IRC de maneira que cada canle pode soste unha conversa paralela entre dous ou máis nodos calquera da rede. Existen múltiples clientes que como ocorría cos servizos anteriores facilitan o uso do servizo aos usuarios. Nas súas orixes permitía unicamente o envío de mensaxes de texto, pero evolucionou ata permitir o envío de arquivos, transmisión de voz e vídeo e mesmo conexión de escritorio remota.



**Figura 5: Exemplo dunha rede IRC.**

#### **27.2.4. MOTORES DE BUSCA**

Outra característica de Internet froito da gran cantidade de información que almacena sería a existencia dunhas ferramentas denominadas **Motores de busca** (en inglés *browser*). Estas ferramentas buscan os arquivos almacenados nos servidores web e os indexan para poder proporcionar resultados de buscas de palabras chave nos mesmos nun tempo óptimo. Os motores de busca empregan un **robot** (ou simplemente *bot*) que fai as funcións de rastrexador da web. Periodicamente este robot recolle información sobre os sitios e páxinas web que recorre dende un punto de partida ás ligazóns de cada documento que percorre. Deste xeito pode descubrir novos documentos nun sitio sempre e cando estean vinculados dende outros documentos xa atopados do sitio. En determinadas ocasións podemos non desexar que o documento sexa incorporado aos buscadores,

polo que poderemos perante código HTML indicarlle ao robot que salte ese documento. A información que recolle un robot inclúe o texto e parte do código da páxina web, non podendo interpretar imaxes, animacións ou vídeos non sendo a través da súa descrición. Para que un sitio web pase a existir cómpre dalo de alta en polo menos un dos buscadores, abondando con incluír a páxina principal do sitio sempre e cando o resto de páxinas estean ligadas dende ela.

A partir da información recollida polo robot elabórase un **índice** ou catálogo de documentos orientado a facilitar a busca de información. Con cada nova busca a información de rastreo deberá actualizarse e consecuentemente tamén o índice ou catálogo, incorporando as novas páxinas descubertas, eliminando as que foron borrados así como os cambios de cada documento.

De cara ao usuario o motor de busca proporcionará unha **interface de busca** vía web ou cliente software onde a partir dun termo inserido daralle como resultado as ligazóns atopadas que mellor se correspondan por orde de relevancia. Os factores chave do resultado dun buscador serán por tanto o tempo de resposta, optimizado grazas ao índice e a relevancia ou adaptación dos resultados aos termos empregados na busca.

Por norma xeral os buscadores implementan os seus propios algoritmos de relevancia ou **posicionamento**, que establece un peso para cada páxina en función do número de visitas, número de páxinas que a enlazan, aspectos comerciais, valoración dos usuarios e un longo etcétera. No resultado dunha busca aparecerán primeiro as páxinas que teñan un maior posicionamento ou relevancia.

### **27.3. INTRANET/EXTRANET**

En liñas xerais unha Intranet compórtase igual que Internet, sendo unha

Internet limitada ao ámbito da organización para a que da servizo, é dicir unha Internet privada. Unha Intranet sería unha Internet que restrinxe o acceso aos sistemas de información. A efectos de alcance e servizos poderemos dispor das mesmas posibilidades en cada tipo de rede. No tocante ao seu funcionamento tamén é idéntica ao de Internet, cada equipo ou nodo tamén disporá dun enderezo IP, pero neste caso non se corresponderá cos enderezos IP de Internet senón que será un enderezo IP privado, para uso interno. Se parte dos equipos atópanse abertos a Internet pasaremos a falar de Extranet, podendo convivir ambas na mesma organización.

Noutra variante unha Extranet pode comunicar dúas Intranets con distinta localización xeográfica establecendo por exemplo unha Rede privada virtual ou **VPN** (en inglés *Virtual Private Network*) que define unha rede privada lóxica sobre unha rede pública. Existen varias arquitecturas de VPN:

- 1) **VPN de acceso remoto.** Conecta directamente os usuarios a rede a través de Internet tendo en conta tanto só que o usuario se autentica de maneira correcta.
- 2) **VPN punto a punto (Tunneling).** Require un servidor VPN que responde ás conexións a través de Internet e crea un túnel VPN, que consiste en enmascarar un protocolo de rede sobre outro. Deste xeito pódense transmitir os paquetes con protocolos cifrados como SSH.
- 3) **VPN LAN.** Nesta solución non se emprega Internet para o acceso remoto senón que se fai sobre a propia rede da organización. En redes sen fíos, permite establecer un nivel de seguridade engadido onde ademais dos protocolos de seguridade da Wi-Fi se inclúen as credenciais de seguridade do túnel VPN.

Particularizando e concretando os servizos que ofrece Internet podemos definir unha serie de **servizos** básicos que pode proporcionar unha

Intranet/Extranet:

**a) Acceso a sistemas de información**

- ✓ Acceso a documentación: manuais, publicacións, guías e formularios internos.
- ✓ Acceso a sistemas de información e bases de datos corporativas.
- ✓ Consulta e edición de informes, formularios e listaxes.
- ✓ Axenda, calendarios e planificación de traballo en grupo.
- ✓ Acceso a información de contacto da organización.
- ✓ Páxinas de novas e ligazóns de interese.

**b) Recursos compartidos**

- ✓ Acceso a recursos compartidos: conexión a Internet, impresoras, escáners, etc...
- ✓ Acceso a sistemas de intercambio de arquivos.
- ✓ Buscadores de recursos e información.

**c) Fluxos de traballo**

- ✓ Xestión de usuarios e perfís.
- ✓ Acceso a aplicacións/equipos remotos.
- ✓ Acceso a repositorios de versións.
- ✓ Acceso a aplicacións de xestión e control de incidencias.
- ✓ Soporte a traballadores móbiles ou tele-traballadores.

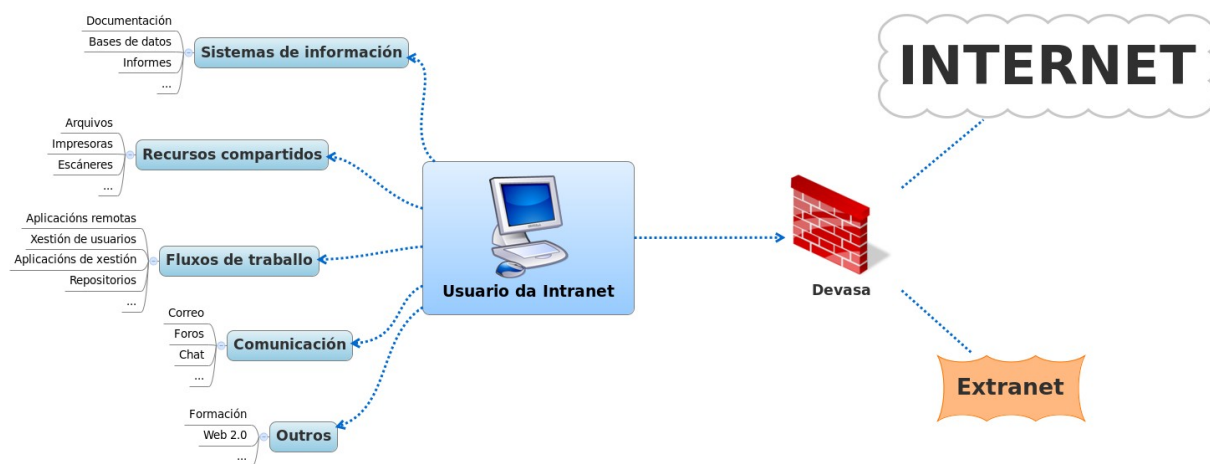
**d) Comunicación**

- ✓ Servizos de mensaxería interna, correo electrónico, foros e videoconferencia.

**e) Outros**

- ✓ Realización de actividades de formación.
- ✓ Acceso a ferramentas da Web 2.0: portais, blogs, wikis, redes

sociais, etc...



**Figura 6 : Servizos básicos dunha Intranet/Extranet.**

Para poder soportar esta longa lista de servizos unha Intranet debería estar dotada dos seguintes **compoñentes** básicos:

## **1. Soporte e infraestrutura de rede.**

O modelo máis sinxelo de Intranet sería dous equipos dunha organización conectados en rede. A partir de aí a rede pode medrar tanto como requira a organización, podendo incluír calquera número de redes, subredes, equipos e elementos de interconexión. A implantación disto equivalería á dunha rede LAN, sendo preciso definir unha topoloxía, un conxunto de tecnoloxías (Ethernet, Fibra óptica, Wi-Fi, etc...), dispositivos de interconexión e de seguridade e unha política de asignación de enderezos IP e nomes de dominio DNS. Nun paso máis alá habería que estender a rede cara o exterior no caso de que se queira definir parte da mesma como Extranet, tendo en conta tamén este conxunto de características. A este respecto hai que ter en consideración o Plan de Direccionamento e Interconexión de Redes de Área Local na Administración (2010), o cal establece os rangos de asignación de enderezos IP. Para a Xunta de Galicia establece o seguinte



**rango:**

<b>10.179.0.0 - 10.180.0.0</b>	<i>Xunta de Galicia</i>
------------------------------------	-------------------------

Así como outras **recomendacións**, tales como:

- ✓ Cada entidade ou organismo pode xestionar independentemente os seus plans de numeración IP pero seguindo o plan para evitar enderezos duplicados cos outros organismos.
- ✓ Empregar máscaras de rede de 24 bits, para ter redes de 254 nodos por segmento, co cal teríamos a máscara 255.255.255.0 independentemente da situación física do nodo.
- ✓ A asignación do grupo de bits para o *Host* realizárase de xeito ascendente para permitir subredes nas zonas aínda non asignadas.
- ✓ Empregar valores de enderezos IP baixos para servidores e equipos de comunicacións.
- ✓ Valores por riba dos anteriores para equipos de usuarios, ordenadores persoais e estacións de traballo.
- ✓ Seguir o plan de numeración en cada subrede.
- ✓ Manter ao día a documentación dos cambios que se producen no mesmo.

## **2. Servidores.**

Os servidores serán os provedores de servizos na Intranet/Extranet atopándonos diferentes requirimentos hardware e software segundo a función que van desempeñar. Segundo o seu perfil dentro da rede atopamos dous tipos:

- a) **Servidores adicados.** Invisten toda a súa potencia en dar servizo á



rede, adicando todos os seus recursos a tal función.

- b) **Servidores non adicados.** Funcionan tanto como servidor como estación de traballo, repartindo os seus recursos nas dúas funcións.

Por outra banda atendendo ao tipo de servizo que proporcionan, poderían clasificarse do seguinte xeito:

- 1) **Servidores de arquivos.** Almacenan arquivos e directorios e xestionan o acceso aos mesmos por parte dos usuarios da Intranet. En sistemas avanzados proporcionan información de versións, permisos e servizos de transferencia, sincronización, replicación e soporte de protocolos SMB/NetBIOS, CIFS, NFS e FTP así como funcionalidades de integración do estilo de Samba.
- 2) **Servidores de impresión.** Controlan as impresoras, fax ou escáneres en rede, realizando tarefas de xestión de colas, asignación de prioridades e detección de erros, con soporte para protocolos IPX/SPX, LDP, IIP, CUPS ou vía Socket.
- 3) **Servidores de comunicacións.** Realizan a xestión das comunicacións de telefonía, voz sobre IP (VoIP) ou videoconferencia. Sistemas avanzados inclúen contestadores automáticos e sistemas de resposta robótica paralela automática. Deben soportar diferentes protocolos como TCP/IP, IPX, PPP, SLIP/CSLIP, SNMP, LAT ou NetBEUI.
- 4) **Servidores de correo.** Almacenamento e xestión de mensaxes exclusivo para usuarios da Intranet/Extranet, con soporte para SMTP, IMAP, POP3 e seguridade SSL/TLS.
- 5) **Servidores de mensaxería instantánea.** Xestionan as comunicacións de *Chat* ou conversa instantánea entre os usuarios da Intranet/Extranet con soporte IRC, MUC, SIMPLE, MNP ou XMPP.
- 6) **Servidores de rede.** Realizan funcións de interconexión das redes e subredes que forman a Intranet/Extranet. Xestións de cachés (en inglés *proxy*), encamiñamento, servizos de devasa (en inglés *firewall*

), NAT, DHCP, etc...

- 7) **Servidores de acceso remoto.** Xestionan a conexión remota de equipos dende outras localizacións con protocolos XDMCP, NX, RFB ou RDP. Optimizan a elevada carga do uso de aplicacións e escritorios de maneira remota e incorporan mecanismos de autenticación avanzados.
- 8) **Servidores de aplicacións.** Permite que os clientes traballen con aplicacións de custe de implantación/configuración elevado ou cunha alta demanda de recursos de maneira remota. As solucións máis habituais baséanse nas plataformas JEE, .NET, PHP e Coldfusion.
- 9) **Servidores de copias de seguridade.** Permiten manter un sistema de control de almacenamento de copias de seguridade de datos ou servidores en discos duros redundantes ou cintas, en ocasións noutras localizacións pero adicados ou SAN. O obxectivo destes sistemas é restaurar o sistema a un estado funcional e seguro logo dun erro, caída ou desastre que provoque a perda da funcionalidade da rede, convertendo as redes locais en NAS. Actualmente coa mellora das conexións van gañando forza os *backups* na nube.
- 10) **Servidores de Bases de datos.** Proven os servizos de acceso ás Bases de datos así como a xestión das mesmas dende ordenadores con máis recursos que as estacións de traballo. Resulta habitual a súa comunicación con outros servidores para proporcionar servizos conxuntos. Algúns dos exemplos máis representativos son Oracle, DB2, SQL Server, MySQL e PostgreSQL.
- 11) **Servidores web.** Soportan o servizo de contidos web a nivel interno controlando o acceso ás páxinas e documentos HTML e XML. Os dous exemplos máis representativos son Apache e IIS.
- 12) **Outros.** Calquera outro servizo de importancia para a Intranet/Extranet debería ter un servidor adicado especializado que destinara todos os seus recursos á xestión e soporte dese servizo.

Alguns destes servizos poderían ser o control e xestión de usuarios (Servidores LDAP), servidores de informes, control de versións, etc...

### **3. Control de Seguridade**

En todas as redes e sistemas de comunicación é importante adicar recursos ao control da seguridade, principalmente nas partes visibles dende fóra, é dicir as partes da Extranet, pero tampouco hai que esquecer as partes propias da Intranet. A maior parte da seguridade recae sobre as **devasas**, que filtran as comunicacións co exterior, restrinxen aplicacións e controlan os enderezos IP e físicos das máquinas segundo unha serie de regras e filtros de control. Así mesmo dispoñen de ferramentas de monitorización e rexistro que permiten facer seguimentos e auditorías da rede.

Por outra banda, pódese restrinxir a comunicación co exterior empregando equipos de interconexión ponte que dean servizo ao resto da rede. Estes dispositivos de **xestión de caché**, fan a función de repetidores na rede, pero illan aos equipos internos e permiten centralizar e reforzar a seguridade e o control neste equipo, en lugar de en toda a rede. Os equipos pasarela deberían incluír todos os servizos básicos como Web, FTP ou mensaxería instantánea.

A seguridade debe contemplarse tamén nos **clientes**, aínda que unha correcta xestión nos servidores protexe por extensión aos equipos de traballo. Cómpre prestar especial atención ao control dos usuarios de cada equipo, controlar accesos físicos, xestión de contrasinais, e dotalos dun software antivirus axeitado. En ocasións pode ser necesario controlar o acceso dos usuarios ao mesmo equipo distinguindo en diferentes perfís usuario/administrador ou máis segundo as necesidades da organización.

### **4. Administración da rede.**

O papel de administrador da rede resulta fundamental para asegurar o correcto funcionamento e seguridade do sistema, ademais de para dar soporte e participar da resolución de incidencias.

Mención especial merece o control das comunicacións que se realizan entre os usuarios, tendo especial coidado con temas como correos masivos ou SPAM, envío masivo ou non autorizado fóra da organización. Entre as labores ou **funcións** do administrador ou administradores atoparíamos:

- ✓ Establecemento e mantemento de políticas de xestión de usuarios e roles, permisos e accesos.
- ✓ Mantemento e soporte físico do hardware da rede.
- ✓ Configuración e mantemento de devasas, antivirus e cachés, así como calquera outro equipamento ou software de conexión da rede.
- ✓ Avaliación da calidade do servizo.
- ✓ Realización de auditorías periódicas de control e avaliación da seguridade e rendemento.
- ✓ Atención aos usuarios, soporte e resolución de incidencias.
- ✓ Documentación do deseño e descrición da rede, configuracións de servidores e protocolos de restauración/recuperación da rede en caso de erro ou desastre.

## **27.4. IMPLANTACIÓN DE REDES EN ORGANIZACIÓNS**

Cando as organizacións conectan a súa rede e servizos con Internet teñen varias alternativas:

**1) Integrar por completo a rede corporativa en Internet.** Deste xeito cada equipo da organización pasa a ser un nodo de Internet, con enderezos IP de Internet. Dende calquera localización poderase ter acceso aos servizos e equipos da rede directamente, sen restricións. Esta solución

plantexa riscos de seguridade, xa que o conxunto da rede queda exposto a ataques dende o exterior, e cada nodo convértese nun potencial punto feble.

**2) Integrar parcialmente a rede e equipos.** Neste tipo de solucións a maioría da rede aparece oculta ao exterior, fóra de Internet, para evitar os riscos de seguridade. Dende o exterior pódense ver algúns servidores da organización e do mesmo xeito dende a rede se pode acceder a servidores externos, pero restrinxido os servizos e comunicacións. Cando a integración é parcial pódese falar de redes dos tipos Intranet e Extranet. Partindo disto xorden outras moitas cuestións, número de usuarios, distribucións físicas que abarcará a rede, servizos que se implantarán, e un longo etcétera. Resulta obvio que o primeiro paso da implantación dunha Intranet/Extranet será a **planificación**. Na planificación abordaranse os seguintes puntos:

### **1. Plantexamento de obxectivos.**

Os **obxectivos** da rede quedará definidos polo seu alcance. Habería que realizar tarefas tales como:

- ✓ Estimación do número de usuarios e a súa posible evolución.
- ✓ Determinar o emprazamento da rede e posibles subredes, situación de posibles redes externas e as necesidades de comunicación coas mesmas.
- ✓ Considerar os sistemas de información e necesidades de acceso aos mesmos, tendo en conta tamén os fluxos e procesos internos.
- ✓ Definir os servizos que se proporcionarán na Intranet/Extranet polo miúdo, con estimacións de carga predicións da súa evolución futura, etc...

A partires dos obxectivos pode irse elaborando a lista de **requisitos** da Intranet/Extranet, como paso previo ao deseño da rede. A documentación en ambos puntos debería ser o máis completa posible.

## **2. Selección de tecnoloxías**

Nun segundo paso tomando os obxectivos e requisitos habería que seleccionar as tecnoloxías máis axeitadas tanto a nivel de hardware, físico, como de software. A nivel físico acostuma a optarse por redes Ethernet, pero poden ser precisas redes sen fíos, así mesmo cada rede precisaría diferentes elementos de interconexión dependendo da tecnoloxía e o mesmo para clientes e servidores. Dende sistemas operativos a software de xestión e control de cada servizo, xestores de contidos e outros propósitos, debería seleccionarse atendendo ás necesidades especificadas polos obxectivos e requisitos sen esquecer outros aspectos como custes, a existencia e dispoñibilidade de soporte para cada tecnoloxía e complexidade de instalación, configuración e mantemento.

## **3. Definición dos recursos necesarios.**

Unha vez seleccionadas as tecnoloxías que tomarán parte no deseño da selección habería que definir o número de **recursos** necesarios para a implantación. Isto inclúe, número, tipo e software dos equipos clientes e o mesmo para os equipos de interconexión da rede e o servidores. Este paso sería o **deseño** da rede en si, dende o cableado á lista completa de software necesario. Segundo as particularidades da Intranet/Extranet podería ser preciso o desenvolvemento de software a medida, o cal habería que incluír tamén nesta fase do deseño.

## **4. Definición de políticas de seguridade.**

Paralelamente haberá que establecer e documentar os protocolos e políticas de seguridade como:

- ✓ A asignación de contas de usuario e contrasinais e usuarios dos equipos e servidores, así como caducidade e revisión do cambio de

contrasinais nas mesmas.

- ✓ Equipos que comunican co exterior e que precisan máis seguridade e equipos que pertencerán á DMZ (zona desmilitarizada).
- ✓ Filtros de aplicacións, de enderezos IP e enderezos físicos.

A continuación viría a **implantación** en si, sendo o recomendable establecer un período de proba e realimentación previo para ofrecer un produto de maior calidade.

### **1. Período de proba.**

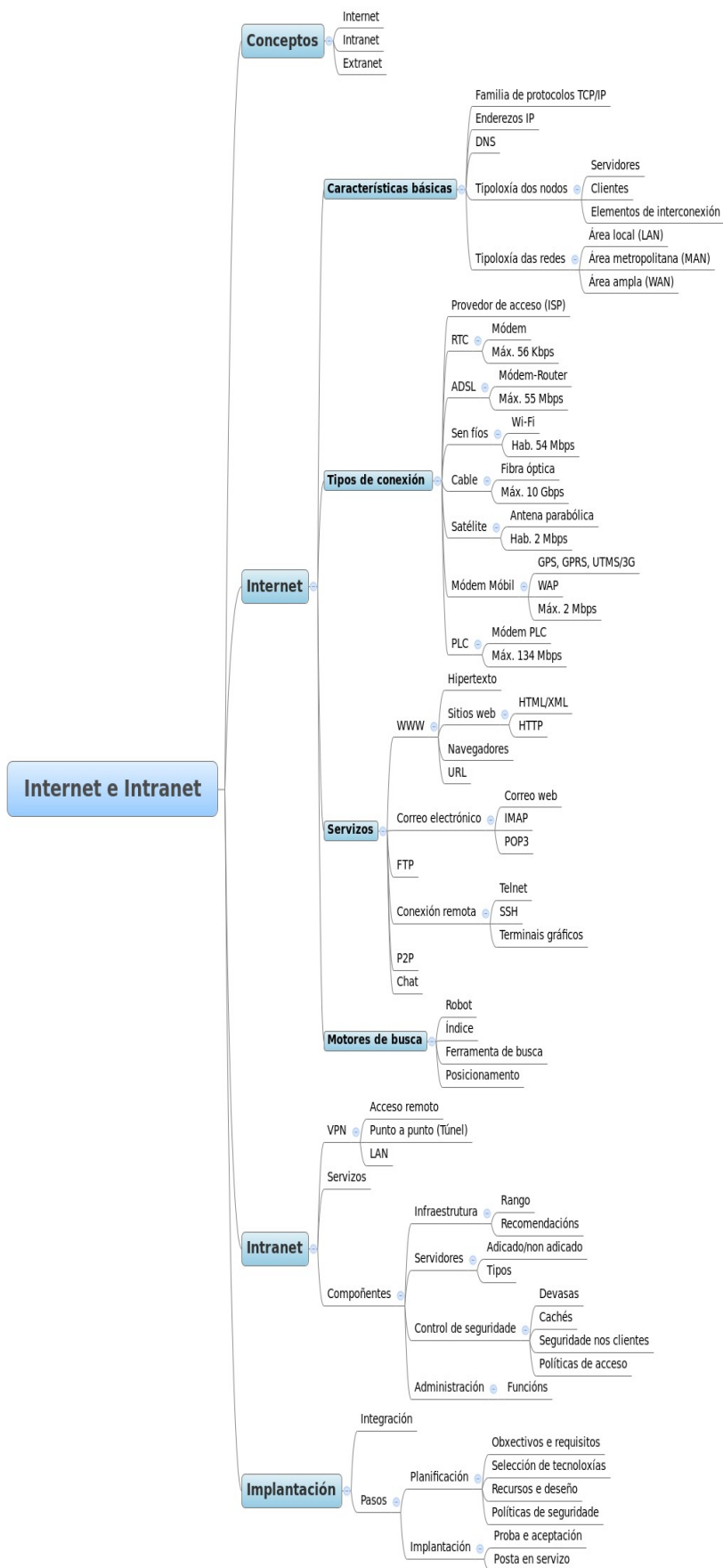
Durante este período realizaranse probas completas do funcionamento da Intranet/Extranet. Deberían incluírse casos de proba para os diferentes servizos e as comunicacións entre as diferentes subredes e redes externas. Coa calidade como obxectivo habería que realizar probas máis complexas como probas de carga, buscando os picos de demanda de recursos, e casos de ataques de seguridade controlados. Todo elo mentres se realiza a monitorización e posteriores probas de auditoría do sistema permiten elaborar un informe completo dos límites e deficiencias da rede, útil para detectar puntos febles que arranxar antes da posta en servizo.

### **2. Posta en servizo.**

Logo das sucesivas probas e unha vez obtidos resultados de aceptación pode levarse a cabo a posta en servizo definitiva da Intranet/Extranet, abríndoa a todos os usuarios. Nos primeiros momentos da posta en servizo cómpre realizar a monitorización e auditoría os sistemas do mesmo xeito que se fixo durante o período de proba pois neste primeiro momento poderán detectarse problemas e debilidades reais que puideron pasar desapercibidas durante as probas controladas realizadas anteriormente.

## **27.5. ESQUEMA**





## **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 e O. U.**

**Colegiado del CPEIG**



**28. MODELO DE CAPAS:  
SERVIDORES DE APLICACIÓNS,  
SERVIDORES DE DATOS,  
GRANXAS DE SERVIDORES.  
INTEGRACIÓN DE CONTIDO,  
SON, IMAXE E ANIMACIÓN.  
SCRIPTS DO CLIENTE.**

## **TEMA 28. MODELO DE CAPAS: SERVIDORES DE APLICACIÓNS, SERVIDORES DE DATOS, GRANXAS DE SERVIDORES. INTEGRACIÓN DE CONTIDO, SON, IMAXE E ANIMACIÓN. SCRIPTS DO CLIENTE.**

### **28.1. INTRODUCCIÓN E CONCEPTOS**

### **28.2 MODELO DE CAPAS: SERVIDORES DE APLICACIÓNS, SERVIDORES DE DATOS, GRANXAS DE SERVIDORES.**

### **28.3 INTEGRACIÓN DE CONTIDO, SON, IMAXE E ANIMACIÓN.**

### **28.4 SCRIPTS DO CLIENTE.**

### **28.5. ESQUEMA**

### **28.6. REFERENCIAS**

### **28.1. INTRODUCCIÓN E CONCEPTOS**

Nunha rede formada por equipos informáticos os **nodos** acostuman realizar tres **funcións** diferenciadas:

1. Facilitar a comunicación e interconexión dos nodos da rede.
2. Proporcionar servizos ou información a outros nodos.
3. Realizar funcións de equipo de traballo, facendo uso das comunicacións, servizos e información dispoñible.

Neste contexto os nodos ou equipos que realizan as funcións de proporcionar servizo ou información ao resto denomínanse **Servidores** e os que fan uso dos servizos **Clientes**. Formando no seu conxunto o que se da en denominar **Arquitectura Cliente-Servidor**. Trátase dunha das arquitecturas máis estendidas nos contornos distribuídos, permitindo a heteroxeneidade nos clientes e un acceso transparente á información. Os servidores permanecen á escoita da rede en todo momento para atender

ás solicitudes ou demandas dos clientes.

O esquema de **funcionamento básico** seguiría o seguinte modelo:

1. O cliente solicita un servizo ao servidor a través da rede.
2. O servidor á escoita recibe a petición do servizo e a pon na cola de demanda.
3. O servidor obtén o resultado da petición.
4. O servidor envía a resposta da petición ao cliente a través da rede.
5. O cliente obtén o resultado e o procesa.

A partir destes conceptos básicos podemos extraer as **características básicas** da arquitectura Cliente-Servidor:

- a) **Servizos.** Son a base das peticións entre os clientes e o servidores, trátase de calquera entidade susceptible de ser demandada por un ou máis clientes.
- b) **Recursos compartidos.** Elementos e servizos da rede, tanto lóxicos (software, datos e información), como físicos (hardware, impresoras, unidades en rede, etc...).
- c) **Comunicación asíncrona baseada no envío de mensaxes.** Este tipo de arquitecturas empregan protocolos de comunicación asimétricos onde os clientes inician conversas e os servidores esperan que se estableza a comunicación escoitando a rede. Toda a comunicación se realiza mediante o envío de mensaxes e respostas.
- d) **Transparencia.** A localización, a organización lóxica e física, así como a implementación dos servizos resulta transparente aos clientes. O uso dos mesmos limítase a facer unha petición á rede e obter a resposta.
- e) **Escalabilidade.** Horizontal nos clientes á hora de permitir engadir novos nodos sen máis que engadilos á rede e vertical nos servidores, de xeito que administrando un único punto pode mellorarse a

potencia, o rendemento, o mantemento e a recuperación de erros.

Froito da escalabilidade desta arquitectura xorden as **granxas de servidores**, consistentes en empregar varios servidores á vez subministrando o mesmo servizo e repartíndose as peticións ou carga do sistema. A xestión dunha granxa de servidores será complexa debido á necesidade de balancear a carga para obter o maior rendemento posible.

Un dos servizos máis estendidos actualmente é o web ou **WWW**, (siglas en inglés de *World Wide Web*), trátase dun sistema de publicación e intercambio de información distribuído que relaciona uns contidos con outros a través de ligazóns. Neste servizo os clientes solicitan información a modo de páxinas web, tratándose de documentos en linguaxes estándar como HTML ou XML que inclúen diferentes tipos de información: texto, hiperligazóns, e elementos multimedia. Entre estes elementos multimedia atopamos:

- a) **Texto.** Distinguindo entre sen formato, con formato ou enriquecido (tipo de letra, tamaño, cor, cor de fondo, etc...) e hipertexto texto cun vínculo ou ligazón a outro texto ou documento.
- b) **Son.** Dixitalización da fala, a música ou outros sons.
- c) **Gráficos.** Representan esquemas, planos, debuxos vectoriais, etc... son documentos que se constrúen a partires dunha serie de primitivas: puntos, segmentos, elipses, etc... aplicándolles a continuación todo tipo de transformacións ou funcións: rotación, cambio de atributos, escalado, efectos, etc...
- d) **Imaxes.** Representacións fieis da realidade, como fotografías. Son documentos formados exclusivamente por píxeles, punto a punto e por tanto non se estruturan ou dividen en primitivas.
- e) **Animación.** Representación dunha secuencia de gráficos por unidade de tempo, para ofrecer a sensación de movemento. Así mesmo ofrece

posibilidades de interacción ante eventos.

- f) **Vídeo**. Representación dunha secuencia de imaxes por unidade de tempo, para ofrecer a sensación de movemento.

Documentos complexos agrupan diversos compoñentes multimedia nunha mesma páxina ou documento. Os sistemas de publicación actuais permiten que a **multimedia dixital en liña** poda transmitirse **en fluxo** (en inglés *streaming*), que se atopa dispoñible tanto en liña en tempo real coma baixo demanda. Neste modelo non é necesario descargar ou acceder á totalidade do documento para acceder aos contidos senón que se proporciona acceso directo a calquera parte do fluxo e reprodución dende ese punto.

Outra característica das páxinas web ou documentos HTML/XML é que poden incluír **código de script para os clientes**. Este código representa un guión ou secuencia de instrucións a xeito dun programa sinxelo. Este programa pode ser interpretado polo navegador do equipo cliente cuns permisos limitados no equipo e focalizados principalmente na páxina ou documento web no que se atopan incrustados ou dende o que son chamados. Existen diferentes tecnoloxías para estas linguaxes de *script* sendo as máis coñecidas: Javascript, Visual Basic Script, Flash, e a evolución de Javascript: AJAX, aceptados con maior ou menor fortuna polos navegadores actuais, moitas delas denominadas tecnoloxías RIA nun achegamento das aplicacións web ás aplicacións de escritorio.

## **28.2 MODELO DE CAPAS: SERVIDORES DE APLICACIÓNS, SERVIDORES DE DATOS, GRANXAS DE SERVIDORES**

A distribución dos sistemas de información foi evolucionando ao longo do tempo en función das demandas e crecemento das redes e o aumento da

complexidade das arquitecturas de rede.

### **28.2.1. Arquitectura nunha capa: Superordenador central.**

A arquitectura máis simple estaría formada por un **superordenador central** (en inglés *mainframe*) que centraliza toda a capacidade de procesamento e almacenamento da rede, tamén denominada monolítica. Neste modelo o acceso á información faise directamente a través da computadora principal ou ben a través de clientes lixeiros que se limitan a facer as funcións de terminais. Nesta arquitectura centraliza todo o custe de administración e mantemento adícase ao servidor central. Os terminais carecen de programas propios, e teñen recursos de memoria ou disco mínimos, podendo mesmo carecer de disco. Calquera instalación ou mellora no servidor repercute ao momento na rede de xeito que calquera programa instalado estará dispoñible para todos os clientes. Por contra, se temos en conta a sostibilidade do sistema en caso de caída ou erros no servidor central toda a rede vese afectada, do mesmo xeito que se un cliente sobrecarga o sistema todos os demais veranse afectados en canto a rendemento. Á súa vez os mainframes organizáanse segundo arquitecturas paralelas tipo **SNA** (en inglés *Systems Network Architecture*) cun deseño de rede con comunicación P2P a través de **APPN** (en inglés *Advanced Peer-to-Peer Networking*).

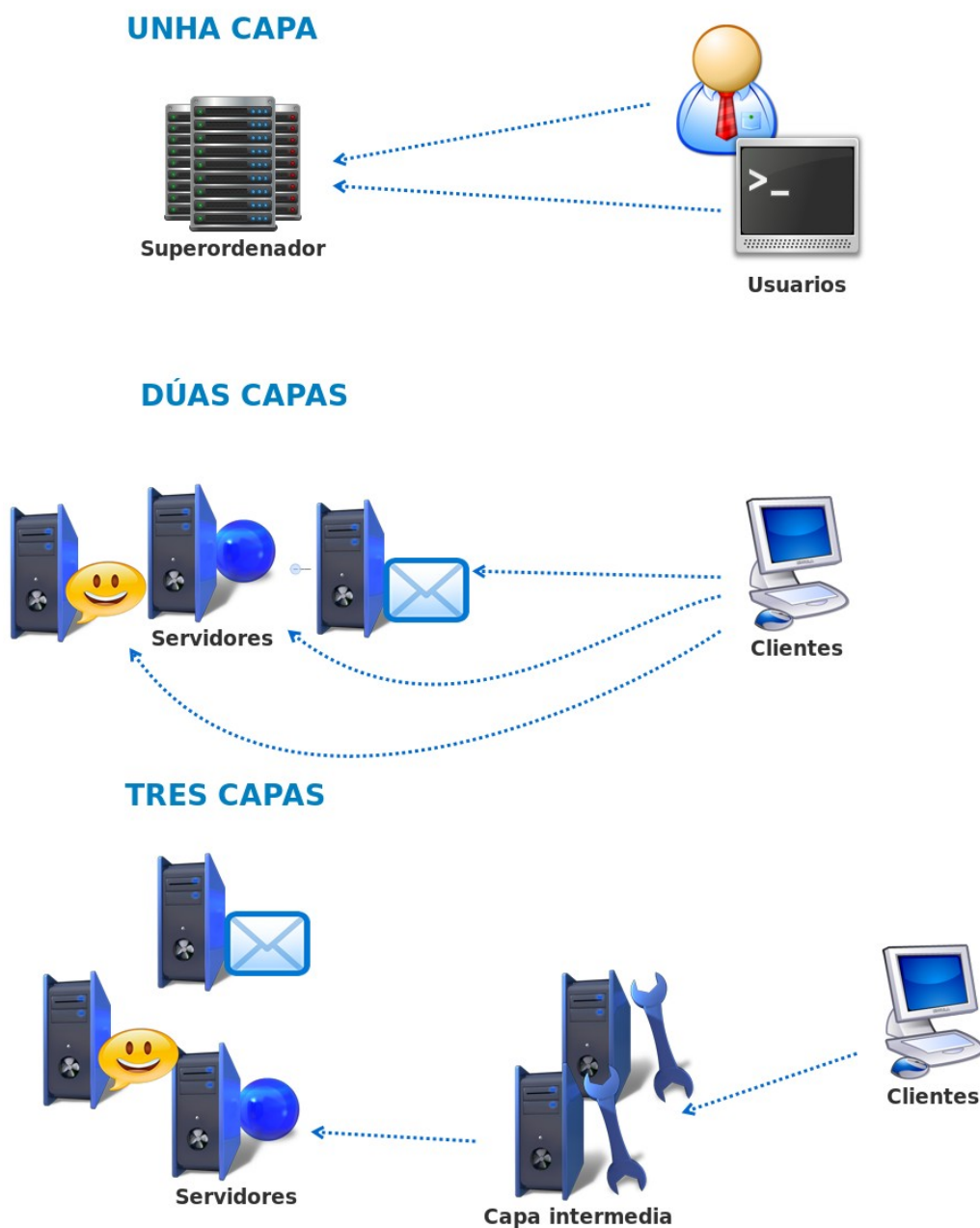
### **28.2.2. Arquitectura en dúas capas: Modelo Cliente-Servidor.**

Neste modelo o sistema se estrutura en dúas capas, unha capa a nivel de usuario que almacena e procesa parte da información e outra capa remota a nivel de servizos que almacena e da funcionalidade á totalidade de clientes da rede. Deste xeito conséguese descargar de parte da carga da rede aos servidores centrais e mantén a capa de servizos transparente aos usuarios coa posibilidade de escalar o sistema mellorando ou aumentando



o número de servidores sen que estes cheguen a notar o cambio en algo máis que o rendemento. Por contra, un modelo máis distribuído no tocante aos clientes obriga a un maior mantemento dos mesmos por parte dos administradores. Outro dos puntos a ter en conta é a consistencia dos datos entre cliente e servidor, de xeito que cómpre coordinar cada servizo por separado.

Nesta liña o uso de protocolos de comunicación soporta o uso efectivo por parte dos clientes dos servizos da rede permitindo a heteroxeneidade dos clientes sempre e cando os implementen.



**Figura 1: Arquitecturas en capas**

### **28.2.3. Arquitectura en tres capas: Granxas de servidores.**

Por mor dos inconvenientes dos sistemas dunha única capa, que obrigan a manter un servidor central de tamaño demasiado grande para un mantemento e rendemento eficientes, e de dúas capas, que obrigan a

manter cada servidor independente do resto para un único servizo, optouse polo establecemento dunha capa máis entre as de cliente e servidor.

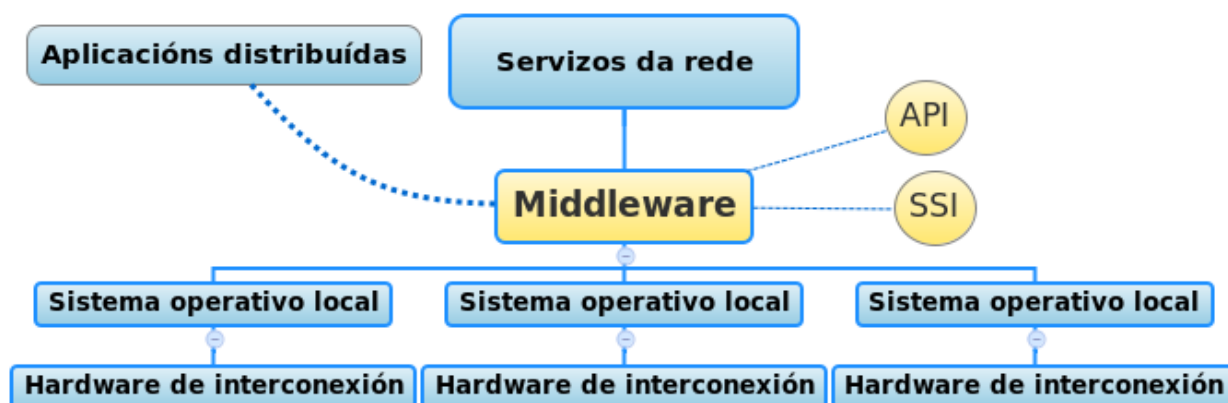
Nesta capa agrúpanse varios servidores nunha DMZ soportando o mesmo servizo dando lugar a unha redundancia que ten como vantaxes unha maior tolerancia a fallos e unha mellora de rendemento. A efectos da rede a granxa de servidores proporcionan un único servizo lóxico ou virtual integrado por calquera número de servidores físicos. Cada servidor da granxa debe ser unha réplica exacta do servidor lóxico en canto a datos e software instalado. Para escalar o sistema engádese á granxa un novo servidor réplica do virtual e aumenta a dispoñibilidade de recursos. O exemplo máis habitual de granxa de servidores é un servizo web, onde se por exemplo un servidor atende a mil usuarios e temos previstos picos de dez mil usuarios simultáneos poremos unha granxa de dez servidores, para atender o servizo e outros dous máis en previsión de caída dalgún ou picos puntuais aínda máis altos. A escalabilidade das granxas en función dos servizos ofertados define tipoloxías básicas como *Datacenters*, servidores de aplicacións, de importación, de *front-end* existindo elementos específicos para control de carga, Teredo ou de dominio, entre outros.

#### **28.2.3.1 Compoñentes intermedios: *Middleware***

Para dar o efecto de transparencia aos clientes, ese sistema require dunhas serie de compoñentes intermedios, é dicir que se atopan “polo medio” (en inglés *middleware*) das capas principais. Estes compoñentes se encargan de recibir e repartir as peticións dos clientes entre os servidores da granxa, coidar o balanceo de carga, o mantemento da sesión, etc... O ***middleware*** descríbese coma un condutor ou intermediario entre sistemas, dirixindo as peticións de datos e servizos a outros nodos da rede. Entre as súas principais características destacarían:

- a) Simplificar o desenvolvemento de aplicacións ao capsular comunicacións entre sistemas.

- b) Facilitar a interconexión dos sistemas de información con independencia da rede física.
- c) Mellorar a escalabilidade do sistema, aumentando a capacidade sen perda de funcionalidade.
- d) Mellorar a tolerancia a fallos do sistema, fiabilidade.
- e) Aumentar a complexidade de administración e soporte.



**Figura 2: O middleware nun sistema distribuído.**

Nun sistema distribuído o *middleware* é o software de conectividade que permite dispoñer dun conxunto de servizos sobre plataformas distribuídas heteroxéneas. Actúa coma unha capa de abstracción das funcións do sistema distribuído facendo transparente na rede os sistemas operativos e o hardware de interconexión das redes de comunicacións. Proporciona unha Interface de Programación de Aplicación (**API**) para a comunicación e acceso a aplicacións e servizos distribuídos. Por outra banda proporciona unha interface única de acceso ao sistema denominada **SSI** (do inglés *Single System Image*), a cal da ao cliente a sensación de acceder a un único servidor, o virtual.

Para garantir a heteroxeneidade na comunicación dos sistemas o *middleware* estruturase en tres **capas ou niveis de comunicación** separados:

- 1) **Protocolo de transporte.** Protocolos de comunicacións comúns á

capa de transporte da rede, como TCP ou UDP. Establecen niveis de seguridade, control de sesións, etc...

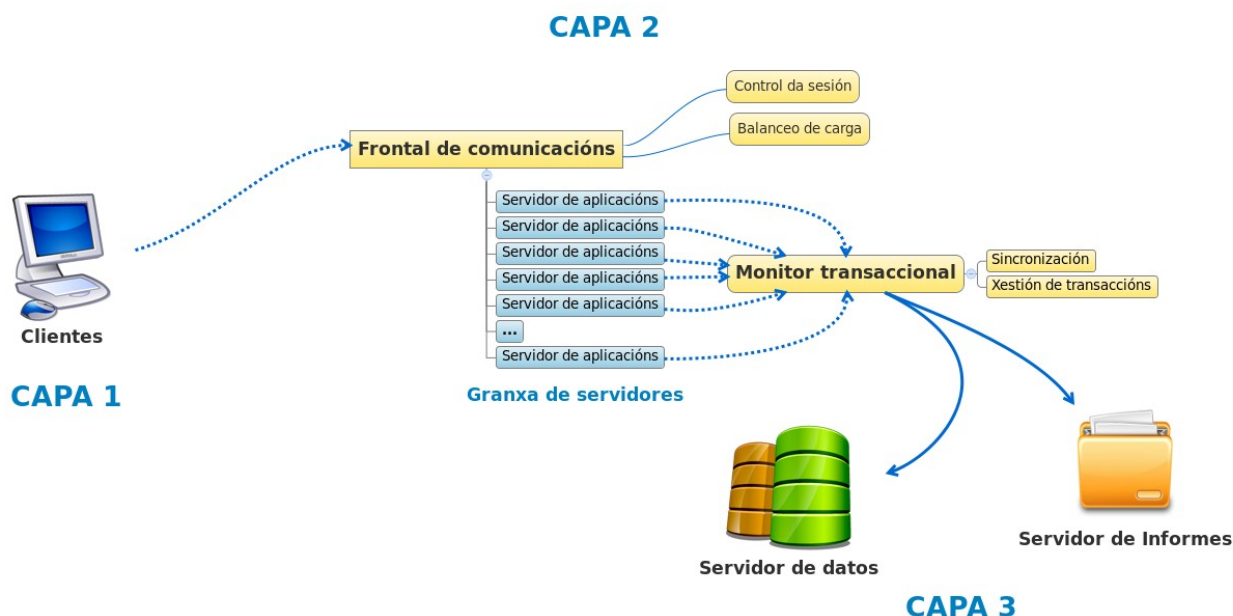
- 2) **Sistema Operativo en Rede ou NOS** (en inglés *Network Operating System*). Extensión do sistema operativo dos clientes que captura as peticións e as dirixe cara o servidor axeitado para devolver a continuación a resposta do mesmo ao cliente.
- 3) **Protocolo de servizo**. Protocolo específico do servizo ou aplicación no sistema Cliente-Servidor.

Os middleware acostuman a clasificarse segundo o tipo de comunicación que realizan no Sistema Operativo en Rede e aos parámetros que comunican (infraestrutura, acceso a datos, aplicacións, etc...), os **tipos de middleware** máis habituais serían:

1. **Chamadas a procedementos remotos** (en inglés *Remote Procedure Call* ou RPC). Os Clientes invocan directamente procedementos ou funcións de procesos que se executan en servidores remotos, permitindo distribuír a lóxica da aplicación remota a través da rede. As chamadas poden realizarse de maneira asíncrona ou síncrona. Mantén ao mínimo a información da sesión e en caso de ruptura da mesma o cliente reinicia a comunicación de cero.
2. **Publicación/subscrición**. Este middleware realiza unha monitorización do sistema detectando os servizos e procesos activos. Os compoñentes rexistran o seu interese en determinados eventos en cando estes eventos son detectados polo monitor envía esa información aos subscritores. A interacción é asíncrona recaendo por completo no servizo de notificación/monitorización.
3. **Middleware orientado a mensaxes** (en inglés *Message Oriented Middleware* ou MOM). A comunicación basease no envío de mensaxes

asíncronos por parte dos nodos (cliente, servidor, servizo ou aplicación). As mensaxes recóllense en colas priorizadas no nodo destino e almacénanse ata que poden responderse. O funcionamento do sistema é análogo a como funciona un servizo de correo electrónico.

4. **Middleware baseado en obxectos** (en inglés *Object Request Broker* ou ORB). Incorpora a RPC os paradigmas de orientación a obxectos. Define unha arquitectura cliente servidor onde os servizos devolven obxectos, sendo estes a unidade de comunicación. Os nodos piden os obxectos polo nome sendo estes entregados por un servizo de resolución de nomes. Exemplos de implementacións deste *middleware* serían: CORBA, RMI, COM, .NET Remoting, etc...
5. **Middleware de acceso a datos** (en inglés *Oriented Data Access Middleware*). Proporcionan a API transparente de acceso a datos agrupando a operación de manexo da conexión coas bases de datos. Exemplos deste tipo de API serían JDBC e ODBC. Por norma xeral realizan conexións síncronas e operacións transaccionais.
6. **Arquitecturas orientadas a servizos** (en inglés *Service Oriented Architecture* ou SOA). As funcionalidades ou procedementos se publican dende calquera servidor a modo de servizos. Os servidores publican o servizo e permanecen á escoita ata que chega unha petición, a procesan e devolven unha resposta ao cliente do servizo. Exemplos deste *middleware* son os Servizos Web e os Servizos CORBA.



**Figura 3: Granxa de servidores.**

As granxas de servidores complétanse con dous compoñentes fundamentais, funcións que de xeito xeral realiza o *middleware*:

1. **O frontal de comunicacións.** O frontal de comunicacións (en inglés *front-end*) é o punto de acceso único á granxa de servidores, simulando un único servidor lóxico. Aínda que cada servidor da granxa poida ter o seu propio enderezo IP o normal é que o frontal teña un propio e sexa esta a forma de que os clientes accedan a el, ou ben directamente ou ben a través dun nome de dominio (DNS).
  - ✓ **Balanceo de carga.** Consistir en dividir a carga de traballo dos clientes entre os servidores da granxa. Pode implementarse vía hardware, software ou unha combinación de ambas. Para facelo vía hardware o frontal de comunicacións debe dispoñer dun equipo específico, aínda que hai enrutadores que permiten esta funcionalidade.
  - ✓ **Control da sesión.** Se por mor do balanceo da carga diferentes

peticións dun mesmo cliente van cara servidores diferentes cómpre coordinar aos servidores no seguimento dunha sesión ou que poidan compartila.

- ✓ **Priorización.** En caso de ter peticións simultáneas o frontal debe ser capaz de atender primeiro aos clientes críticos ou de maior prioridade así como de asignar o procesamento das súas tarefas a aqueles servidores dotados de máis recursos.

2. **Os monitores transaccionais.** Os monitores transaccionais son os encargados de manter a consistencia dos datos e os procesos que se procesan simultaneamente nos servidores da granxa. Ten que garantir que unha modificación de datos froito dunha petición se realiza como unha transacción, é dicir, ou se realiza completamente ou non se realiza en absoluto. Cada transacción ten que ter lugar independente de que teña lugar outra simultánea, deben procesarse de xeito illado. As principais funcións serán:

- ✓ **A xestión das transaccións.** Encárgase de controlar a atomicidade e secuencialidade das transaccións, para garantir a consistencia de datos e operacións. A xestión de transaccións debe garantir o correcto funcionamento do sistema cando a carga de traballo ou o número de usuarios son moi elevados. Debe contemplar a posibilidade de erros nas aplicacións e caídas de elementos do sistema durante as transaccións, permitindo operación de volta atrás. Vista polo miúdo a xestión de transaccións constará de:

1. **Xestor de transaccións** (en inglés *Transaction Manager*). Controla o inicio de transacción, rexistra os recursos que precisa e xestiona as operacións de confirmación da transacción (en inglés *commit*) e de volta atrás e recuperación do estado inicial da transacción (en inglés



*rollback*).

2. **Xestor de rexistro** (en inglés *Log Manager*). Gardar os estado dos recursos que están uso por parte das transaccións, elaborando un historial de versións dos mesmos. Esta información é compartida polos distintos xestores de transaccións sendo o que permite garantir a consistencia dos recursos empregados.
  3. **Xestor de bloqueos** (en inglés *Lock Manager*). Xestiona o acceso simultáneo por parte de varios procesos aos recursos, permitindo bloquealos para evitar que dous ou máis accesos á vez dean lugar a inconsistencias. Así mesmo leva a cabo a detección de cando se libera un recurso e envía unha notificación ao xestor de transaccións.
- ✓ **Sincronización.** A sincronización das comunicacións resulta complexa neste modelo, xa que un cliente pode acceder a un servizo empregando diferentes servidores da capa intermedia, mesmo simultaneamente. Segundo o comportamento do servizo podemos atopar solucións síncronas, onde se espera sempre á resposta do servidor, simple pero con risco de bloqueo. Fronte as asíncronas onde se envía a petición e xa chegará a resposta, co cal non hai bloqueos, pero a resposta podería non chegar nunca sen máis opción que detectalo a través de tempos de espera esgotados.

#### **28.2.6. Arquitecturas en n-Capas.**

As arquitecturas en tres capas poden estenderse a n-capas cando na capa intermedia incorpóranse outros elementos de interconexión como distribuidores ou sistemas de devasa. Tamén pode dividirse a capa de servidores por servizos ou diferentes capas de acceso a datos ou presentación de información. A separación en capas é unha organización

lóxica do sistema co cal pode establecerse calquera número de capas segundo as necesidades do mesmo. Calquera especialización de servidores que se queira facer na rede e provoque un novo agrupamento podemos identificala cunha nova capa.

### **28.2.7. Arquitecturas para Rede entre iguais (P2P).**

Nos modelos distribuídos de igual a igual ou **P2P** (en inglés *Peer-to-Peer*), todos os equipos (agás os elementos de interconexión) teñen o mesmo rol dobre de cliente/servidor na rede. Fan uso de servizos e os proporcionan. Nesta arquitectura por tanto non se poden agrupar os nodos e perde sentido falar de capas. Estas redes non resultan óptimas para todo tipo de servizos, en moitos casos por exemplo á hora de funcionar como servidor web, requirirían un custe moi alto para control da consistencia do sitio web, mantemento e configuración do servidor, etc... por contra, en situacións onde os nodos caen a miúdo, por exemplo un servidor atacado continuamente, a redundancia de nodos garante que o sistema siga funcionando. Outros servizos como o intercambio de arquivos, ou o procesamento compartido presentan máis vantaxes á hora de empregar unha arquitectura deste tipo como solución de implantación. Os modelos máis habituais son centralizados, puros ou descentralizados ou híbridos, segundo o peso de cada nodo individual na rede ou da existencia de servidores con responsabilidade de control e xestión no modelo. A adaptación deste modelo por parte dos ISP da lugar a P2P híbridas de servizo denominadas P4P (en inglés *Proactive network Provider Participation for P2P*). Outros modelos similares serían os P2M, que actúan en arquitecturas híbridas empregando o correo electrónico como soporte do envío de datos.

A xestión deste tipo de redes realízase fundamentalmente vía software.

Neste caso o software deberá realizar as mesmas funcións xa vistas para a arquitectura de tres ou máis capas: frontal de comunicacións e xestión de transaccións. Por debaixo acostuman implementar servidores propios como Kademia, eDonkey, Gnutella, FastTrack, BitTorrent ou OpenNap entre outros.

## **28.2.8. SERVIDORES.**

### **28.2.8.1. Servidor web.**

Trátase de servidores que provén o servizo WWW a través do protocolo HTTP. En esencia trátase dunha aplicación executándose nun servidor á espera de peticións HTTP por parte dun cliente respondendo cos documentos solicitados xeralmente páxinas web e os obxectos que enlazan: imaxes, arquivos de *script*, animacións, etc... En funcións máis avanzadas estes servidores engaden seguridade a través de conexións encriptadas con protocolos tipo HTTP Seguro ou HTTPS. Por regra xeral, os servidores de aplicacións intégranse en arquitecturas de mínimo tres **capas**:

- 1) **Primeira capa.** Capa de interacción cos usuarios, principalmente a través de navegadores web.
- 2) **Capa intermedia.** Capa dos servidores web, que poden estar distribuídos nun modelo de granxa de servidores. Cada servidor incorporaría os módulos necesarios para seguridade, linguaxes de servidor interpretados, correo, mensaxería, acceso a datos e outras funcionalidades.
- 3) **Terceira capa.** Capa de servidores de acceso a datos, como servidores de arquivos, base de datos ou informes.

Entre os **servidores web de uso máis estendido** actualmente atoparíanse:

- ✓ **Apache.** Un dos máis utilizados, por se un servidor libre que ofrece prestacións a nivel doutras solucións propietarias ademais dunha grande facilidade de uso e configuración.
- ✓ **Internet Information Server (IIS).** Servidor propietario con soporte para aplicacións .NET ou ASP entre outras.
- ✓ **Outros:** Java Web Server, AOLServer, Cherokee, Tomcat, lightHttpd, etc...

Os servidores web poden dispoñer de módulos para a execución de programas de servidor interpretados, como son os das tecnoloxías Python, PHP, ASP, JSP, Tcl, ...

#### **28.2.8.2. Servidor de aplicacións.**

Os servidores de aplicacións son servidores web con capacidade de procesamento ampliada, podendo executar aplicacións e compoñentes de lóxica de negocio e recursos relacionados como o acceso a datos. Debido a isto permiten realizar o procesamento de aplicacións de cliente no propio servidor. Proporcionan soporte como *middleware* ou software de conectividade e para diferentes tecnoloxías de servidor. Por regra xeral, os servidores de aplicacións intégranse en arquitecturas de mínimo tres **capas**:

- 1) **Primeira capa.** Capa de interacción cos usuarios, principalmente a través de navegadores web.
- 2) **Capa intermedia.** Capa dos servidores de aplicacións, que poden estar distribuídos nun modelo de granxa de servidores. Un subconxunto dos servidores de aplicacións darán servizo aos usuarios/clientes mentres outro grupo encargárase de soportar a operativa común do dominio, como librarías ou aplicacións e servizos web dos que fagan uso as aplicacións para usuarios/clientes.
- 3) **Terceira capa.** Capa de servidores de acceso a datos, como

servidores de arquivos, base de datos ou informes.

O servidor de aplicacións acostuma ter integrado un servidor web, para xestionar de maneira independente o servizo WWW a través do protocolo HTTP.

Ademais deste servizo presenta un amplo conxunto de **ferramentas**:

- ✓ Servidor web integrado.
- ✓ Contedor de programas de servidor (en inglés *servlets*).
- ✓ Contedores de obxectos de lóxica de negocio (por exemplo EJBs).
- ✓ Sistemas de mensaxería.
- ✓ Software de conectividade con bases de datos.
- ✓ Balanceo de carga.
- ✓ Xestión de límites e colas de conexións (en inglés *Pool*) para bases de datos e obxectos.
- ✓ Etc...

En esencia un servidor de aplicacións realiza as mesmas funcións que un servidor web, pero cando a demanda de uso é grande e estamos ante un sistema complexo a solución pasa por empregar un servidor de aplicacións que ofrezca as seguintes **vantaxes**:

- ✓ **Centralización.** Centraliza nos servidores a administración e configuración da lóxica de negocio das aplicacións, de maneira que aspectos como o mantemento dos accesos a base de datos poden realizarse de xeito centralizado. Así mesmo cambios derivados de actualizacións, migracións ou recuperacións ante erros teñen lugar dende un único punto.
- ✓ **Seguridade.** Ao existir un único punto de acceso a datos pode reforzarse a defensa e os sistemas de control de erros nese punto, mellorando a súa xestión e protección.
- ✓ **Rendemento.** Como punto intermedio permite xestionar as peticións

dos clientes á Base de datos.

- ✓ **Escalabilidade.** Un mesmo servidor de aplicacións pode dar servizo a varios clientes, e por tanto aumentando o número de servidores mellórase o rendemento do sistema.

Entre os **servidores de uso máis estendido** actualmente atoparíanse:

- ✓ **Jboss, Glassfish.** Servidores de aplicacións libres baixo licenza GPL.
- ✓ **BEA Weblogic, IBM Websphere, Oracle Application Server.** Alternativas propietarias integradas en paquetes de aplicacións con funcionalidades de xestión e monitorización estendidas.
- ✓ **Tomcat, Internet Information Server (IIS), Jetty.** Proporcionan funcións parciais de servidores de aplicacións, co cal en ocasións se definen máis ben como contedores de programas de servidor.

### **28.2.8.3. Servidor de acceso a datos.**

Os servidores de acceso a datos ocuparían a última capa dos sistemas de información encargándose do acceso directo aos datos, existindo diferentes tipos segundo o sistema de información empregado para o seu almacenamento ou publicación:

- ✓ **Servidores de arquivos.** Neste tipo de servidores a información se almacena directamente en arquivos, por tanto a función destes equipos será a de permitir o acceso remoto aos mesmos dende os clientes ou outros servidores. Os protocolos máis habituais ofrecen servizo só dende redes locais pero en sistemas avanzados poden proporcionar servizos como FTP ou WebDAV para conexión remota a través de Internet. Actualmente o termo empregado para referirse a estes servidores é NAS (en inglés *Network-Attached Storage*), pero esta tan só sería a tecnoloxía máis habitual fronte a outras como DAS (en inglés *Direct Attached Storage*), baseada en SCSI ou SAN (en inglés *Storage Area Network*) baseada en fibra óptica. Non requiren

un software moi específico coma outros tipos de servidores senón máis ben soporte para diferentes protocolos e tecnoloxías. Por norma xeral acostuman a estar dipostos en [RAID](#) (en inglés *Redundant Arrays of Independent Disks*), equipos de almacenamento redundante.

- ✓ **Servidores de bases de datos.** Albergan un ou máis sistemas de xestión de bases de datos (en [inglés](#) *database management system*, ou DBMS), software de xestión que se encarga da comunicación entre as aplicacións e as bases de datos. Permiten realizar operacións de definición, manipulación e seguridade dos datos a través dunha API de comunicación coas aplicacións e un linguaxe estruturado de consulta como o SQL. Permiten accesos simultáneos aos datos, seguridade e xestión de transaccións.

Estes sistemas soen presentar ademais programas ou consolas de administración avanzadas para realizar as tarefas xerais de xestión da base de datos.

- ✓ **Servidores de informes.** Poden considerarse unha capa intermedia entre os servidores de datos e os de aplicación, onde se establecen servidores ou granxas de servidores que serven os datos en documentos predefinidos multiformato: follas de cálculo, PDF, XML, HTML, etc... O software deste tipo de servidores acostuma incorporar software de xestión para o servidor, e software de auto-edición de informes, para definir modelos de informes compostos de cabeceiras, imaxes, fórmulas, subinformes, etc... que se xerarán dinamicamente os informes a partir de consultas sobre os datos.

### CAPA DE USUARIO

### CAPA DE SERVIDOR DE APLICACIÓN



### CAPA DE ACCESO A DATOS

**Figura 4: Arquitectura en 3 capas con servidor web, de aplicación e base de datos.**

Entre os **servidores de uso máis estendido** actualmente atoparíanse:

- ✓ **Servidores de arquivos.** Non requiren xestores especializados pero si soporte software aos protocolos: CIFS, NFS, SMB, FTP, WebDAV, etc... Así como utilidades tipo Samba ou FreeNAS.
- ✓ **Servidores de bases de datos.**
  - ✓ De licenza libre: PostgreSQL, MariaDB, Firebird, SQLite, Apache derby, ...
  - ✓ Dual, dependendo do seu 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 CONTIDO, SON, IMAXE E ANIMACIÓN.**



O modelo máis habitual de integración de elementos multimedia a través de Internet é a través do servizo WWW, empregando a web. Neste servizo os clientes solicitan información a modo de páxinas web, tratándose de documentos en linguaxes estándar como HTML ou XML, baseados en etiquetas que se encargan de estruturar e referenciar os contidos do documento. Deste xeito poden incluírse diferentes tipos de información: texto, hiperligazóns, e elementos multimedia: son, imaxes, gráficos, vídeo e animacións, ademais de outros formatos ou tecnoloxías que á súa vez integran estes elementos.

Para reproducir a maioría de formatos básicos de imaxe, son e vídeo os navegadores soen dispoñer de compoñentes axeitados mentres que para os formatos e tecnoloxías específicos acostuman precisar de *Plug-Ins* ou complementos externos que precisan instalación e actualización independente do navegador. Segundo isto distingúirase por tanto dúas formas de integración multimedia:

- a) **Nativa.** Neste caso o elemento multimedia almacénase nun arquivo externo dun formato propio do tipo de elemento, se por exemplo trátase dunha imaxe en GIF ou JPG, e dende o documento HTML ou XML faise referencia ao arquivo a través do sistema de etiquetado. Case tódolos navegadores actuais, a excepción dos que son en modo texto, recoñecen estes formatos básicos co cal serán capaces a partir do arquivo de reproducir o contido e transmitilo de xeito correcto ao usuario.
- b) **Dependente.** Neste outro caso os elementos multimedia empregan tecnoloxías externas que requiren complementos ou *Plug-Ins* externos ao navegador que deben instalarse aparte para poder representar a información correctamente. Estas tecnoloxías fan as funcións de conector e especificado o seu contido a través do etiquetado HTML ou XML son capaces de aparecer como un elemento multimedia básico. Dentro destes conectadores destacarían os vídeos e animacións Flash e Silverlight, programas de cliente como

os controis Active X e os applets de Java, e documentos en formatos enriquecidos como o PDF.

Os sistemas de publicación actuais permiten que a **multimedia dixital en liña** poda transmitirse **en fluxo** (en inglés *streaming*), tanto de son (en inglés *Podcast*) coma de vídeo e videoconferencia. O mundo do vídeo en liña é dentro da multimedia un dos que presenta maiores problemas á hora de traballar en contorno web pois precisa máis recursos de almacenamento, ancho de banda para reprodución, problemas de conversión e mantemento de formatos de codificación (en inglés *codecs*).

Un último aspecto problemático é a sincronización de todos estes puntos nun proceso automático nun servidor, o que da lugar a solucións complexas e de pouca sostibilidade. As principais tecnoloxías que dan soporte a este tipo de arquitecturas multimedia son: Windows Media, ASF (en inglés *Advanced Streaming Format*), Quicktime, Real Media, VideoLAN e Flash Video.

<b>Elemento multimedia</b>	<b>Formatos de arquivo</b>	<b>Observacións</b>
<b>Son</b>	AAC, MP3, RealAudio, WMA, OGG, MIDI, WAV, AIFF, etc..	<i>Os catro primeiros producen perda de información na conversión.</i>
<b>Imaxe</b>	JPEG, GIF, BMP, TIFF, PNG, JPG, TGA, etc...	<i>O JPEG produce perda de información na conversión.</i>
<b>Vídeo</b>	AVI, MPG, QuickTime (MOV e QT), WMV, Ogg, RMVB, DIVX, Matroska, etc...	<i>Tan só algunhas tecnoloxías son axeitadas para fluxos de vídeo en liña.</i>
<b>Gráficos</b>	PNG, PSD, CDR, XCF, SVG, EPS, etc...	<i>Moitos pertencen exclusivamente ao programa de edición que os xera, agás SVG e PNG.</i>
<b>Animacións</b>	Flash (SWF), Silverlight (XAML), Javascript (JS), etc ...	<i>Agás Flash que comprime nun único</i>

		<i>arquivo os demais empregan outras tecnoloxías de definición abertas.</i>
<b>Documentos enriquecidos</b>	RTF, PDF, PostScript, etc...	<i>Levan incrustados outros elementos multimedia.</i>

***Táboa 1: Formatos de arquivo multimedia.***

O servidor de *streaming* permite que se poida ver parte do vídeo sen descargalo por completo grazas ao uso dun *buffer* que carga parte do arquivo previamente. Os formatos de vídeo empregados por tanto deben permitir estas reproducións parciais. O fluxo busca acadar o máximo que permita o ancho de banda e protocolos do sistema, parando a reprodución e esperando a que continúe a carga se a información dispoñible non abonda.

A existencia dun servidor de fluxo de vídeo ou *streaming*, posibilita os seguintes **servizos**:

- ✓ **Vídeo baixo demanda** ou **VoD** (en inglés *Video on Demand Media Streaming*). Neste modelo o vídeo, incluíndo o son correspondente e outros arquivos complementarios como subtítulos ou textos alternativos para tecnoloxías asistivas, atópase aloxado nun servidor específico e os usuarios solicitan o envío de información segundo precisen, en calquera punto do mesmo, co cal se produce unha resposta personalizada cun fluxo parcial a partir da posición solicitada. Os usuarios poden realizar diferentes interaccións (simultáneas), indo adiante, atrás ou situarse en calquera punto do vídeo. Con este sistema sempre se envía a información almacenada e se fai unha precarga de todo o vídeo a partir da posición solicitada, non sendo necesario dispoñer do arquivo ou arquivos completos para

a súa visualización.

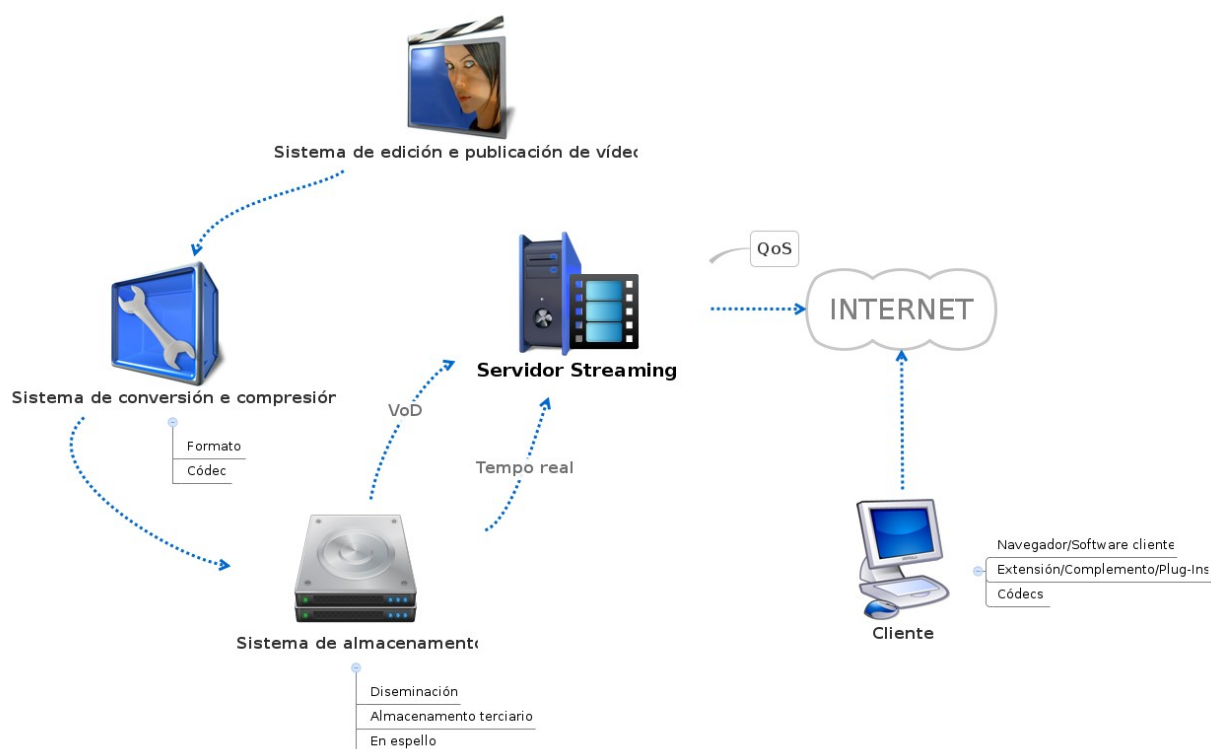
- ✓ **Vídeo en tempo real.** (En inglés *Live Media Streaming*). O contido se crea no mesmo momento da difusión a modo das videoconferencias. Trátase dun modelo orientado á multidifusión da información, producíndose un envío do fluxo de vídeo aos usuarios unha que o arquivo ou parte do mesmo pasa a estar creado no servidor. Non ten porque ser o mesmo fluxo para todos os clientes, senón que permite fluxos paralelos, coa posibilidade de pausas ou retrocesos, pero non avances.

Nunha **arquitectura de streaming**, deberían considerarse cando menos os seguintes elementos:

- ✓ **Sistemas de edición de vídeo.** Módulos de produción, compresión e conversión de vídeo en formatos aptos para *streaming*.
- ✓ **Sistemas de almacenamento** que permita alta capacidade de entrega, elevado espazo, tolerancia a erros e sistemas de copias de seguridade. En sistemas con moita demanda poden requirir técnicas de tipo:
  - **Diseminación de arquivos.** Emprega varios discos diseminando a información para permitir que o servidor acceda a eles en paralelo.
  - **Almacenamento terciario xerárquico.** Emprega diferentes soportes almacenando os arquivos máis demandados nos soportes de maior rendemento como discos, e os menos demandados en soportes como cintas, o cal permite reducir custes.
  - **Técnicas en espello.** Replica toda a información en diferentes discos separados en espello, co cal se aumenta tamén a tolerancia a erros.
- ✓ **Servidor de streaming.** Dispoñendo de liñas de alto ancho de

banda, con soporte de **Calidade de servizo** ou QoS (en inglés *Quality of Service*).

- ✓ **Cientes.** Con extensións ou complementos que soporten os formatos da arquitectura. O complemento fará unha función dobre, xestionar a precarga do vídeo e permitir a súa reprodución parcial segundo a información dispoñible.



**Figura 5: Arquitectura dun servidor Streaming.**

Mención especial requiren, respecto do almacenamento, as **bases de datos multimedia**, son sistemas xestores de bases de datos con orientación a obxectos, identificando cada tipo de elemento multimedia cun obxecto da base de datos. Existen varios tipos principais:

- 1) **Bases de datos referenciais.** Fan referencia polo miúdo a obxectos multimedia, incorporando información descritiva tanto sobre o elemento (título, autor, sinopse, ...) como información técnica (formato, duración, códec, ...)

- 2) **Bases de datos descriptivas.** Incorporan información descriptiva ou semántica do contido do elemento, como pode ser a descrición dun vídeo paso a paso, ou o texto alternativo dunha imaxe. O obxectivo destas solucións é dar cabida ás buscas semánticas e soporte de accesibilidade para tecnoloxías asistivas.
- 3) **Elementos multimedia integrados.** Os obxectos multimedia almacénanse como campos dentro da base de datos e non coma ficheiros externos, por norma xeral o tamaño dos campos das bases de datos relacionais atópase limitado en comparación coas necesidades dos elementos multimedia, pero a mellora de rendemento e eficacia do sistema poden facer necesarias este tipo de solucións. O exemplo máis habitual serían os bancos de imaxes e algúns tipos de xestores documentais.

Ademais da Web **noutros servizos** se pode realizar **integración multimedia** como son os de mensaxería instantánea e o correo electrónico. Para o caso do correo, o protocolo **MIME** (en inglés *Multipurpose Internet Mail Exchange*) desenvolveuse para permitir a integración de elementos multimedia nas mensaxes de correo, co obxectivo de realizar unha aproximación ao HTML. O funcionamento básico é asociar cada tipo de elemento multimedia a un tipo MIME (texto, imaxe, documento HTML) esta información permite aos navegadores e clientes de correo electrónico determinar con que tipo de contido se está a traballar para representalo correctamente co seu complemento ou *Plug-In* correspondente.

## **28.4 SCRIPTS DO CLIENTE.**

Os *scripts* do cliente son programas interpretados deseñados para

executarse nos navegadores co obxectivo de dotar ás páxinas de maior interactividade co usuario e dinamismo nunha aproximación ás aplicacións de escritorio. O **funcionamento básico** dun *script* consiste en interpretar unha serie de comandos a través dos cales pode modificar e manipular obxectos e reaccionar ante eventos da interface como respostas a periféricos (rato, teclado, etc...), ou cambios nos elementos do documento (botóns, elementos de formularios, etc...). Os seus usos básicos son validacións, manipulación de formularios, procesamento de funcións e carga asíncrona de datos.

Os *scripts* de cliente proporcionan as seguintes **vantaxes**:

- ✓ Modificar o contido da páxina sen recargala do servidor en función das interaccións co usuario.
- ✓ Modificar parámetros de configuración do navegador e outros elementos da páxina web.
- ✓ Mellorar a interacción entre o usuario e o documento, en xeral a usabilidade.

Por contra, presentan un serie de inconvenientes ou **desvantaxes**:

- ✓ Problemas de accesibilidade, pois complícase a posibilidade de presentar alternativas a usuarios que non soporten a tecnoloxía de *script*.
- ✓ Problemas de seguridade, pois toda a lóxica de interacción aparece sen protección descargada no equipo do usuario, co cal dispón do código fonte do programa de *script*.

As **tecnoloxías de *script*** máis empregadas son Visual Basic Script, Javascript, coa súa evolución AJAX e PerlScript. O principal problema á hora de seleccionar unha tecnoloxía cando se diseña unha páxina web é o soporte que recibirá por parte dos navegadores, pois hai que lembrar que as linguaxes de *script* serán en última instancia interpretados no

navegador.

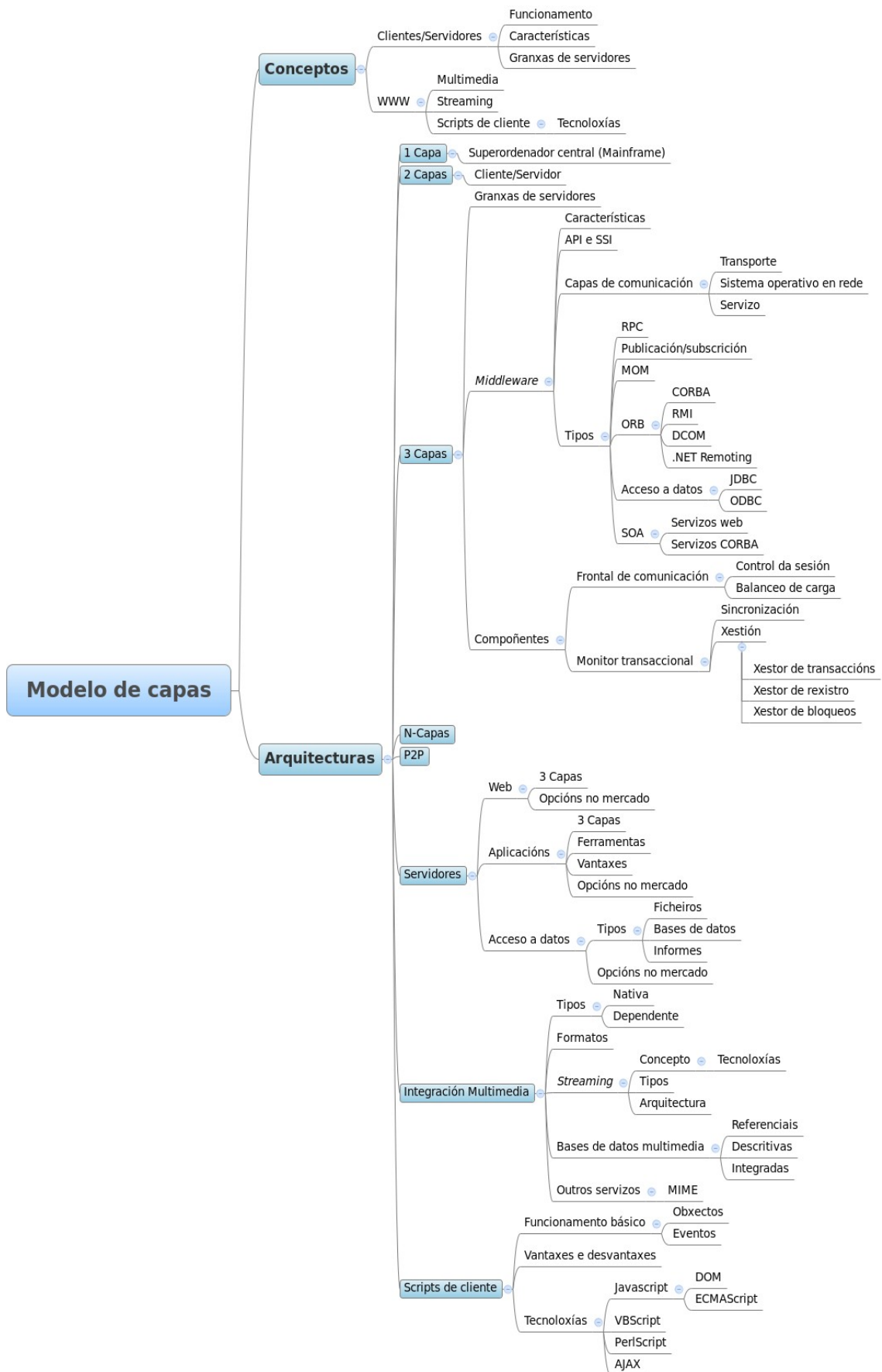
- a) **Javascript.** Baseado na linguaxe Java, é unha das linguaxes de script de uso máis estendido. É de sinalar, que ademais ten aplicación con outras tecnoloxías ademais da web coma en documentos PDF ou aplicacións de escritorio. Para permitir a interacción cos elementos dun documento web esta linguaxe dispón dunha API que implementa o DOM (en inglés *Document Object Model*) ou Modelo de Obxectos para a Representación do Documento, estandarizado polo W3C (en inglés *World Wide Web Consortium*). Nun intento por estandarizar esta linguaxe xorde o ECMAScript unha especificación da linguaxe aceptada como estándar ISO,
- b) **Visual Basic Script.** Similar ao Javascript no tocante a funcionamento e estrutura pero baseado en Visual Basic. Ten menor soporte dentro dos diferentes navegadores, agás no Internet Explorer.
- c) **PerlScript.** Baseado en linguaxe C o seu uso non está tan estendido coma as tecnoloxías anteriores aínda que ten menos limitacións. Debido a isto foi derivando cara linguaxe de servidor.
- d) **AJAX.** Acrónimo de Javascript Asíncrono e XML (en inglés *Asynchronous Javascript And XML*). Esta é unha tecnoloxía de *script* de cliente asíncrona, de xeito que pode realizar cargas de datos sen que afecten á recarga da páxina. AJAX é un conxunto de tecnoloxías que fai uso de:
  - 1) XHTML e follas de estilo en fervenza (CSS) para a estrutura e deseño dos contidos.
  - 2) A linguaxe Javascript como linguaxe de programación para funcións e definición do programa cliente.
  - 3) O obxecto *XMLHttpRequest* para intercambio de información asíncrona co servidor. Por tanto, cómpre que o navegador soporte



este obxecto, sendo empregado en ocasións o obxecto *Iframe*.

- 4) XML e DOM como estándares asociados para intercambio de datos e manipulación do documento.

## **28.5. ESQUEMA**



## **28.6. REFERENCIAS**

José Antonio Mañas.

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).

**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 E CONCEPTOS**

### **29.2 ARQUITECTURA WEB EN .NET**

### **29.3 ARQUITECTURA WEB EN J2EE**

### **29.4. ESQUEMA**

### **29.5. REFERENCIAS**

### **29.1. INTRODUCCIÓN E CONCEPTOS**

O desenvolvemento de aplicacións, servizos web e outros compoñentes software ten hoxe en día dúas vertentes principais, a plataforma .NET e a plataforma J2EE, ou JEE nome co que é coñecida actualmente ao cambiar de versión. A rivalidade entre estas dúas tecnoloxías é moi forte, pois proporcionan solucións similares fortemente soportadas polas compañías dun e do outro bando.

**.NET** é a plataforma de desenvolvemento proposta pola empresa Microsoft para o mundo dos servidores de aplicacións que funciona como ferramenta de deseño e programación ademais de proporcionar un amplo conxunto de utilidades estendidas de apoio ao desenvolvemento neste tipo de contornos. Pola súa banda **JEE**, (en inglés *Java Platform, Enterprise Edition*) ou Java EE, é unha evolución da plataforma Java para desenvolver e soportar compoñentes software segundo un conxunto de especificacións de xeito que poidan operar nun servidor de aplicacións, incluíndo tamén ferramentas de deseño e programación.

A pesar de que ambas plataformas perseguen o mesmo obxectivo, teñen unha serie de particularidades ou diferenzas que se ven acentuadas polas guerras comerciais entre as empresas que as soportan. Mentres JEE ten

soporte multiplataforma, .NET funciona unicamente baixo a familia de Sistemas Operativos Windows. Mentres JEE basease exclusivamente na linguaxe Java, en .NET permítense moitos linguaxes de alto nivel, aínda que na práctica os principais sexan C# e VB .NET. JEE leva máis anos de experiencia no mercado, mentres que .NET é máis recente. Así mesmo JEE presenta maior soporte en canto a solucións e posibilidades de software libre, que son moi escasas e de pouca calidade en .NET. Con JEE pódese instalar unha infraestrutura de alto rendemento de xeito completamente gratuíto.

## **29.2 ARQUITECTURA WEB EN .NET**

**.NET** é, segundo a empresa Microsoft, unha plataforma para o desenvolvemento de servidores, clientes e servizos. Representa un conxunto de tecnoloxías que teñen como núcleo principal o .NET Framework, un marco de desenvolvemento e compoñente software que pode instalarse en Sistemas Operativos da familia Windows (Windows 2003, Vista, Windows 7, ...). Existe unha versión adaptada para móbiles dispoñible en Windows Mobile. A norma ISO/IEC 23271 recolle un conxunto funcional mínimo que deben cumprir os produtos software desenvolvidos para que poidan funcionar dentro do marco de traballo. Esta e máis normas se recollen nos estándares:

- a) **Estándar ECMA-334.** Especificación da linguaxe C#. (2006).
- b) **Estándar ECMA-335.** Especificación da linguaxe de infraestrutura común (CLI). (2010).

Por contra, outros compoñentes coma ASP .NET, *Windows Forms* ou ADO .NET non se atopan estandarizados. Paralelamente, unha vez publicados os documentos de especificación da arquitectura .NET apareceu o **Proxecto Mono** co obxectivo de implementar o marco de traballo .NET Framework empregando código aberto, para a partir de aí desenvolver aplicacións para sistemas UNIX/Linux.

### 29.2.1 .NET Framework

Marco de traballo que proporciona o conxunto de ferramentas e servizos para o desenvolvemento de compoñentes software, aplicacións, servidores e servizos web. Pode dividirse en tres bloques principais:

- 1) O **Contorno de Execución Común** (en inglés *Common Language Runtime* ou CLR). Encárgase da xestión de código en execución, control de memoria, seguridade e o outras funcións relacionadas co Sistema Operativo.
- 2) A **Biblioteca de Clases Base** (en inglés *.NET Framework Base Classes*). Realizan a función de API de servizos a disposición dos desenvolvedores para tarefas como xestión de ficheiros, mensaxería, procesos en varios fíos, acceso a datos, encriptación, etc...
- 3) **Control de acceso a datos**, que permite realizar as operacións de acceso a datos a través de clases e obxectos do *framework* incluídos no compoñente ADO.NET.
- 4) O **Motor de Xeración da Interface de Usuario**, que permite crear interfaces para aplicacións de escritorio ou web empregando compoñentes específicos coma ASP.NET para web, *Web forms* para aplicacións de escritorio ou *Web services* para servizos web.

### 29.2.2 Contorno de Execución Común (CLR)

O Contorno de execución común ou CLR é o encargado de xestionar o código en tempo de execución. De xeito análogo á Máquina virtual de Java este contorno permite executar aplicacións e servizos web ou de escritorio en calquera cliente ou servidor que dispoña deste software. A diferenza da Máquina virtual de Java o soporte de .NET é multilinguaxe permitindo C++, C#, ASP .NET, Visual Basic, Delphi, e moitos outros. Ademais permite integrar e herdar compoñentes entre diferentes linguaxes, con maior ou menor fortuna á hora de sacar proveito de linguaxes antigas.



O contorno de desenvolvemento compila o código fonte en calquera das linguaxes soportadas a un código intermedio denominado **CIL** (en inglés *Common Intermediate Language*) de maneira análoga ao BYTECODE de Java. A esta linguaxe intermedia chégase empregando a especificación CLS (en inglés *Common Language Specification*) onde se especifican unhas regras necesarias para crear o código intermedio CIL compatible co CLR. Así mesmo, o CLR dispón de compiladores coma JIT (en inglés *Just In Time*) ou AOT (en inglés *Ahead Of Time*) adaptados a cada linguaxe.

**JIT** xera o código máquina real en cada máquina a partir dese código intermedio conseguindo independencia do hardware. Esta compilación faise en tempo de execución a medida que a aplicación ou servizo invoca métodos ou funcións. Para axilizar o procesamento este código máquina obtido en tempo de execución gárdase na memoria caché actualizándose tan só cando se produce algún cambio no código fonte, momento no se que se repite o proceso. Por contra **AOT**, compila o código antes de executarse co cal logra un maior rendemento en execución pero menos independencia da plataforma. No tocante a JIT acostuma a distinguirse entre:

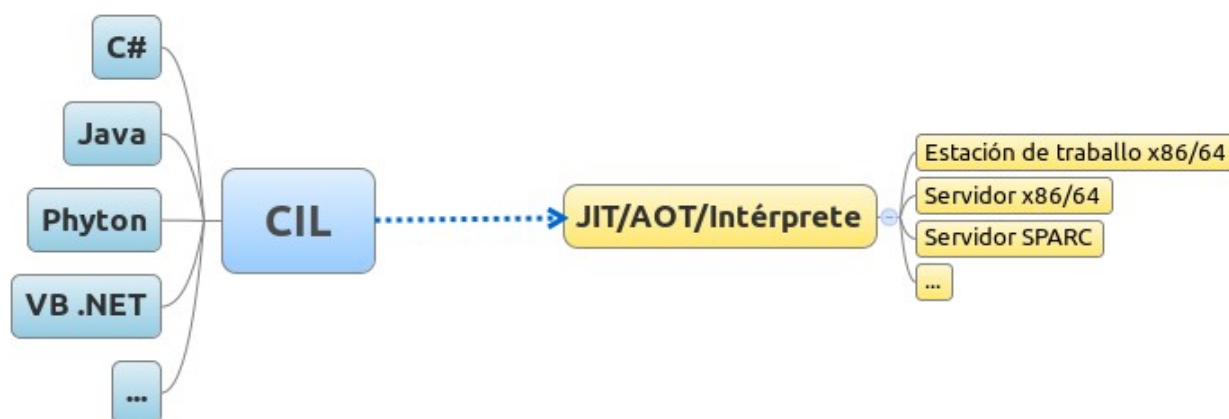
- 1) **Jitter estándar.** Compila o código CIL a nativo baixo demanda.
- 2) **Jitter económico.** Non optimiza, traduce cada instrución así precisa menos tempo e memoria de compilación.
- 3) **Prejitter.** Realiza unha compilación estática dun compoñente software completo.

As principais **vantaxes** deste modelo de compilación son:

- ✓ A **reutilización** de compoñentes escritos en diferentes linguaxes nunha mesma aplicación ou servizo web.
  
- ✓ **Modularidade** grazas á implementación do patrón Interface para cada compoñente ou librería xa que será accesible dende calquera

linguaxe a través da súa API (ASP, C#, Java, Python, etc ...)

- ✓ **Integración multilinguaxe**, xa que cada linguaxe cun compilador a CIL pode integrarse na plataforma co cal cada compoñente nesa linguaxe pode integrarse unha aplicación ou servizo web .NET.
- ✓ **Seguridade**. Polo illamento do código de usuario respecto dos accesos a datos e outras partes críticas do Sistema Operativo.



**Figura 1: Estrutura multilinguaxe do CLR**

O CLR cumpre ademais a función de proporcionar unha ampla gama de servizos ás aplicacións. A través da API de cada servizo os compoñentes web poden ter acceso a funcionalidades comúns, como:

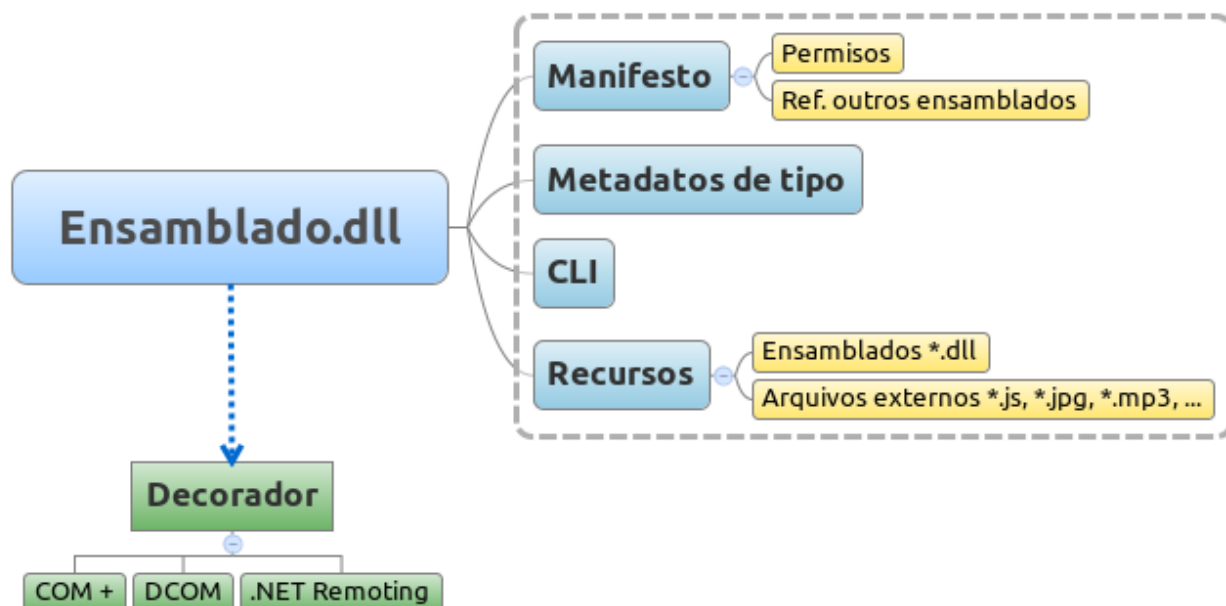
- a) **Seguridade acceso ao código ou CAS** (en inglés *Code Access Security*). Controla que tipo de operacións pode realizar un código segundo se identifique na sinatura do ensamblado ou na orixe do código. Así mesmo recoñece directivas de administración do sistema para compoñentes ou a nivel de *host*. Cando un compoñente trate de acceder a recursos protexidos do sistemas lanzarase o CAS para comprobar os permisos, pero a este nivel non se poden establecer comprobacións dinámicas, por exemplo contra Bases de datos.
- b) **Atributos de protección do *host* ou HPA** (en inglés *Host Protection Attributes*). Mantén unha lista de atributos protexidos, denegando o acceso ou modificación dos mesmos. Algúns destes



atributos serían *SharedState*, para estados compartidos, *Synchronization*, para permitir a capacidade de sincronizar procesos no *host* ou *ExternalProcessmgmt* que indica se os procesos no *host* se poden controlar externamente a través da API.

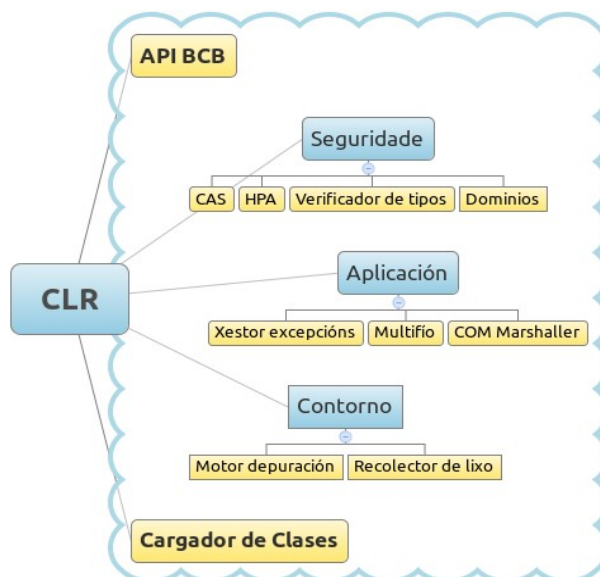
- c) **Dominios de aplicación.** Definen dominios illados de código para restrinxir o acceso dos compoñentes software, creando unha zona reservada para un subproceso. Por norma xeral o CLR crea para cada aplicación un dominio en tempo de execución pero pode precisar dominios específicos para compoñentes DLL ou externos.
- d) **Comprobación da seguridade de tipos.** Reserva espazos de memoria para cada obxecto segundo o especificado para o seu tipo. Cando o espazo é aleatorio ou queda algún oco fóra do espazo do obxecto, quere dicir que ese obxecto non ten seguridade de tipos. Coa compilación JIT realízase unha comprobación en tempo de execución para verificar se cada obxecto ten seguridade de tipos. Do mesmo xeito impide variables sen valores iniciais ou *cast* non seguros.
- e) **Cargador de clases.** Permite cargar en memoria clases e tipos de datos a partir da interpretación dos metadatos. Existe ademais a posibilidade de crear cargadores personalizados, aínda que só para Java, xa que por motivos de rendemento resulta máis óptimo empregar un ensamblado con outras linguaxes. Na compilación o cargador realiza a función de evitar código innecesario a través de funcións *stubs* que substitúe co código correcto baixo demanda.
- f) **Recolección de lixo** (en inglés *Garbage Collector*). Este servizo execútase de xeito continuo para buscar e eliminar de memoria os obxectos que non sexan referenciados ou rematen o tempo de espera de utilización.

- g) **Motor de interacción COM.** Realiza funcións de conversión de datos e mensaxes ou *marshaling* dende e cara obxectos COM, o que permite a integración con aplicación *Legacy*.
- h) **Motor de depuración.** Permite realizar un seguimento da execución do código aínda que mesture diferentes linguaxes.
- i) **API multifío** (en inglés *multithread*). Proporciona unha API e as clases necesarias para xestionar a execución de fíos paralelos.
- j) **Xestor de excepcións.** Realiza a xestión estruturada e integración con *Windows Structured Exception Handling* de excepcións aínda que o erro proveña de diferentes linguaxes nun mesmo compoñente e mesmo no código aínda non executado. Este código pode incluír excepcións SHE do tipo C++ ou resultados HRESULTS típicos de COM.
- k) **API da Biblioteca de Clases Base (BCB).** Interface coa BCB do marco de traballo que realiza a integración do código co motor de execución.



**Figura 2: Ensamblados.**

No .NET Framework cando se compila un programa ou aplicación web xérase un arquivo denominado **ensamblado** que contén o código compilado á linguaxe intermedia CLI e un manifesto con permisos e referencias a outros ensamblados, compoñentes software ou servizos web. Son paquetes ou librarías EXE ou DLL destinadas ao control de versións, seguridade e comprobacións de implementación polo miúdo. Os ensamblados levan unha indicación que define o contorno de execución no que se debe lanzar: COM+, DCOM, .NET Remoting, ...



**Figura 3: Servizos do CLR**

### 29.2.3 Biblioteca de Clases Base (BCB)

A Biblioteca de Clases Base é unha API de alto nivel para permitir acceder aos servizos que ofrece o CLR a través de obxectos nunha xerarquía denominada **espazo de nomes**. Agrupa as funcionalidades de uso frecuente permitindo a súa redefinición. Atópase implementada en CIL polo que pode integrarse en calquera outra linguaxe. É un conxunto de clases, interfaces e tipos valor que son a base sobre as que se crearán as aplicacións, compoñentes e controis do .NET Framework. Permite realizar operacións como: soporte para diferentes idiomas, xeración de números



aleatorios, manipulación de gráficos e imaxes, operacións sobre datas e outros tipos de datos, integración con APIs antigas, operacións de compilación de código adaptada ás diferentes linguaxes de .NET, elementos para interfaces de usuario, tratamento de excepcións, acceso a datos, encriptación, administración de memoria, control de procesos, etc...

Espazo de nomes	Utilidade e obxectos
<b>System</b>	Tipos básicos, táboas, excepcións, datas, recolector de lixo, etc...
<b>System.Collections</b>	Manipulación de coleccións como pilas, colas, <i>hash</i> , etc...
<b>System.Data</b>	Arquitectura ADO.NET (Obxectos <i>DataSet</i> , <i>DataTable</i> , <i>DataRow</i> , <i>DataRowView</i> , ...)
<b>System.IO</b>	Manipulación de E/S arquivos e outras orixes de datos
<b>System.Net</b>	Xestión de comunicacións de rede (TCP/IP, <i>Sockets</i> , ...)
<b>System.Security</b>	Xestión das políticas de seguridade do CLR
<b>System.XML</b>	Acceso e manipulación de datos en documentos XML con compatibilidade co W3C (Transformacións en <i>System.Xml.Xls</i> e serialización para servizos web en <i>System.Xml.Serialization</i> )
<b>System.Web</b>	Servizos para xestión de caché, seguridade e configuración para Servizos Web, estado das sesións e interfaces de usuario
<b>System.Web.Services</b>	Xestión dos requirimentos de Servizos Web
<b>System.Web.UI</b>	Controles para interfaces de usuario <i>HTMLControl</i> para mapeo de etiquetas HTML e <i>WebControl</i> para estruturar controis de usuario avanzados coma <i>DataGrids</i>
<b>System.Windows.Forms</b>	Creación da IU do cliente
<b>System.Drawing</b>	Acceso a funcionalidades gráficas básicas da GDI+ (Funcionalidades avanzadas en <i>System.Drawing.Imaging</i> , <i>System.Drawing.Text</i> e <i>System.Drawing.Drawing2D</i> )
<b>System.Reflection</b>	Acceso a metadatos sobre os ensamblados, módulos, membros, parámetros e outras entidades do código

	administrado
<b>System.JSON</b>	Proporciona compatibilidade baseada en estándares JSON, notación de objetos JavaScript (en inglés <i>JavaScript Object Notation</i> )
<b>System.Threading</b>	Manipulación de procesos e fíos de execución
<b>System.Text</b>	Proporciona clases para manipular a codificación de caracteres UNICODE e UTF-8 conversión de bloques de caracteres en bloques de <i>bytes</i> e viceversa
<b>System.Transactions</b>	Contén clases que permiten crear e administrar transaccións, admitindo participantes distribuídos, notificacións de fase e inscricións duradeiras
<b>System.Resources</b>	Proporciona clases e interfaces que permiten crear, almacenar e administrar recursos de localización
<b>System.Runtime.Remoting</b>	Proporciona a interface para acceso remoto e marco para a implantación de sistemas de compoñentes distribuídos
<b>Microsoft.CSharp</b>	Clases para realizar a compilación e execución de código en C# (O mesmo para outras linguaxes)

**Táboa 1: Principais espazos de nomes.**

#### **29.2.4 Control de acceso a datos.**

O control de acceso a datos, documentos XML e servizos de datos no marco .NET Framework recóllese na arquitectura ADO .NET, coma evolución do *ActiveX Data Objects*. A súa orientación principal é o acceso a datos do xestor de base de datos relacional *SQL Server*, orixes XML e orixes de datos vía obxectos OLE DB e ODBC. As **conexións** realízanse identificando os provedores de datos a través dos obxectos (Connection, Command, DataReader e DataAdapter). Unha vez establecida a conexión entra en escena o principal elemento do marco, o *Dataset* que recolle os **resultados** cargados a partir dunha orixe. Á súa vez pode particularizarse con outros elementos da base de datos con obxectos coma: *DataTable*, *DataRow*, *DataColumn* ou *Constraint*. Os **obxectivos** de deseño principais deste marco son:

- ✓ Soporte á tecnoloxía ADO previa.
- ✓ Integración con tecnoloxías baseadas en XML.
- ✓ Soporte a modelos de arquitectura multicapa.

Nas últimas versións incorpórase o **Marco de Entidades** (en inglés *Entity Framework*) que permite realizar Consultas Integradas nas Linguaxes (en inglés *Language Integrated Query*) ou **LINQ**.

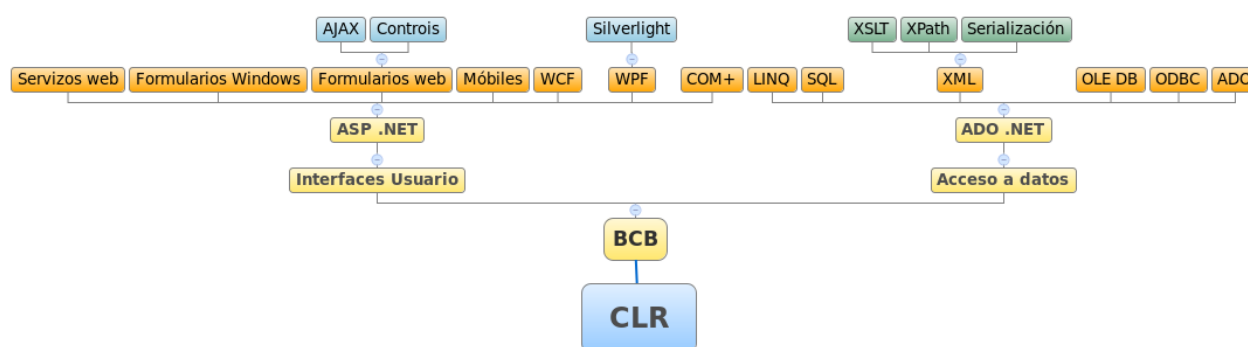
Este marco permitirá empregar LINQ sobre moitos compoñentes de acceso a datos novos: *LINQ to SQL*, *LINQ to DataSet* e *LINQ to Entities*. Asocia unha chave lóxica ás entidades, dotando ao modelo relacional ou conceptual de orientación a obxectos. Utilidades do marco de traballo coma **SQLMetal** permiten a xeración automática de clases a partir da base de datos ou documentos XML.

#### **29.2.5 Motor de Xeración de Interfaces de Usuario**

A parte do marco de traballo encargada da xeración de interfaces de usuario e servizos web sería a arquitectura ASP .NET. O conxunto de clases correspondentes agrúpanse nos espazos de nomes: System.Web, System.Web.Services, System.WebUI. As páxinas web desenvolvidas con ASP .NET teñen a extensión **ASPX** e son coñecidas con **Formularios Web** (en inglés *Web Forms*). Paralelamente a esta tecnoloxía de presentación atoparíamos **Formularios Windows** (en inglés *Windows Forms*) para aplicacións de escritorio e tecnoloxías para Móviles, sendo a primeira a máis empregada para aplicacións de servidor. No espazo System.Web.UI recóllense as dúas clases principais de controis os HTML para acceso directo ás etiquetas estáticas destas linguaxes e os controis web que incorporan código de servidor dinámico. A arquitectura recomendada emprega o modelo **Code-Behind** no que se crea un arquivo separado co código de servidor, a diferenza da arquitectura DNA para ASP anterior. Os



**Controis de usuario** (en inglés *User Controls*) seguen a mesma estrutura que os Formularios Web, pero derivan do espazo `System.Web.UI.UserControl`, e gárdanse en arquivos **ASCX**, que deberían seguir tamén o modelo Code-Behind. O marco incorpora tamén elementos para control do estado e a sesión así coma outros para seguridade, autenticación de usuarios, uso de roles, uso do servizo Indigo ou **WCF** (en inglés *Windows Communication Foundation*). Así mesmo, permite a integración con AJAX, a través da incorporación dun **Toolkit** na aplicación, ou **WPF** (en inglés *Windows Presentation Foundation*) baseado en XALM e marco para Silverlight.



**Figura 4: Arquitectura xeral**

### 29.2.6 Niveis lóxicos.

Nos modelos e solucións que propón esta estrutura establécense unha serie de servizos xenéricos presentes na maioría de aplicacións corporativas actuais. Esta división permite definir un deseño e unha arquitectura específicos para cada nivel, facilitando o desenvolvemento e soporte da aplicación.

1. **Servizos de usuarios.** Atópanse na primeira liña de interacción cos usuarios e proporcionan a interface de acceso ao sistema que deriva en chamadas aos compoñentes do nivel de Servizos corporativos. En ocasións considéranse dentro deste nivel procesos fóra das interfaces

de usuario, como procedementos de control ou automatizados que non requiren a presenza dun usuario.

2. **Servizos corporativos.** Encapsulan a lóxica corporativa proporcionando unha API das funcionalidades básicas do sistema. Isto permite abstraer os servizos de usuario da lóxica corporativa e manter diferentes servizos de usuario a partir das mesmas funcionalidades. Cada funcionalidade pode precisar dispoñer de varios servizos corporativos.
3. **Servizos de datos.** Sería a parte máis illada do usuario, proporcionando o acceso a datos e a outros sistemas ou servidores. Establecen diferentes API xenéricas das que poden facer uso os Servizos corporativos. Conteñen unha ampla gama de orixes de datos e sistemas de servidor, encapsulando regras de acceso e formatos de datos.

### **29.2.6 Solucións de integración.**

Coa tecnoloxía .NET existen tres principais plantexamentos de solucións arquitectónicas:

- 1) **SOA** (en inglés *Service Oriented Architecture*). Entende a comunicación entre aplicacións e compoñentes coma servizos, non necesariamente servizos web, demandados por clientes ou subscritores e proporcionados e publicados por provedores.
- 2) **MOA** (en inglés *Message Oriented Architecture*). A comunicación realízase por paso de mensaxes forzando un modelo SOA distribuído.
- 3) **EAI** (en inglés *Enterprise Integration Application*). Especifica unha serie de requirimentos de integración e comunicación en sistemas regulados polos patróns de integración Mediación e Federación, onde un sistema EAI fai funcións de *Hub* ou *bus* de comunicacións.

## **29.3 ARQUITECTURA WEB EN J2EE**

JEE representa un conxunto de especificacións para plataformas de desenvolvemento baseadas en linguaxe Java para servidores de aplicacións en arquitecturas de múltiples capas. O **JCP** (en inglés *Java Community Process*) é o organismo encargado de validar os requisitos de conformidade para cada plataforma e aceptala. As plataformas JEE constan dos seguintes compoñentes:

- 1) Un conxunto de especificacións.
- 2) Un test de compatibilidade ou CTS (en inglés *Compatibility Test Suite*)
- 3) Unha implementación de referencia para cada especificación.
- 4) Un conxunto de guías de desenvolvemento e boas prácticas denominadas JEE Blueprints.

As principais **especificacións** que inclúe JEE dan soporte a Servizos web, RPC baseado en XML, Mensaxería XML, despregues, servizos de autorización, conexión remota RMI, JSP, JSF, JSTL, Servlets, Portlets, Applets, JavaBeans, esquemas XML, acceso a datos JDBC, documentación Javadoc, transformacións XSL, etc...

O soporte multiplataforma do Java ten a súa base na **Maquina Virtual** (VM/JVM ou KVM/CVM para móbiles), unha plataforma lóxica capaz de instalarse en equipos con diferente hardware e Sistema operativo e interpretar e executar instrucións de código **Java bytecode**. A especificación da VM tamén se recolle como especificación pola JCP e do mesmo xeito están dispoñibles test de compatibilidade. A forma máis habitual para a VM é mediante un compilador JIT pero tamén permite interpretación. Do mesmo xeito permítese execución segura mediante o modelo das Java Applets. Programas de cliente que se executan nunha VM dentro do navegador logo de descargar vía HTTP código do servidor, que se executa nunha *Sandbox* moi restrinxida.

Os compoñentes software web e de negocio dentro desta tecnoloxía despréganse a través de **Contedores** (en inglés *containers*). Os contedores son implementacións de arquitecturas JEE que proporcionan os servizos do servidor de aplicacións aos compoñentes, incluíndo seguridade, acceso a datos, manexo de transaccións, acceso a recursos, control de estados, xestión do ciclo de vida e comunicacións entre outros. Antes de executarse un compoñente software debe configurarse coma un servizo JEE e despregarse dentro dun contedor. Os principais serían os contedores web para Servlets e JSP, os contedores EJB para compoñentes da lóxica de negocio, e contedores de aplicacións cliente e contedores de *Applets* para os programas de cliente e código de cliente para o navegador respectivamente.

Os principais **servizos** que proporciona JEE xunto coas súas respectivas API serían:

- 1) **HTTP e HTTPS**. Para control das comunicacións web e SSL a través destes protocolos. As API de servidor veñen dadas polos paquetes de clases Servlets e JSP e a de clientes no paquete Java.Net.
- 2) **JDBC** (en inglés *Java Data Base Connection*). API de acceso a datos en sistemas xestores de bases de datos relacionais vía SQL. Por un lado aporta a interface para ser empregada polos compoñentes software e por outra a interface para que os provedores poidan desenvolver os controladores específicos. As versións máis recentes son as JDBC 3.0 e 4.0, que inclúen os paquetes *java.sql* e *javax.sql*.
- 3) **JSTL** (en inglés *Java Server Pages Standard Tag Library*). Proporciona as funcionalidades de para etiquetas nas páxinas JSP.
- 4) **RMI-IIOP** (en inglés *Remote Method Invocation-Internet Inter-ORB Protocol*). Proporciona a API para permitir comunicacións en aplicación distribuídas a través de JAVA RMI, por exemplo para acceder a compoñentes EJB. Os protocolos máis habituais son JRMP, de RMI e IIOP, de CORBA.



- 5) **IDL** (en inglés *Java Interface Definition Language*). Permite a comunicación de clientes con servizos CORBA a través do protocolo IIOP, servizos SOAP ou RPC.
- 6) **JNDI** (en inglés *Java Naming and Directory Interface*). Proporciona o servizo de nomes e directorios, indicando o contexto de cada obxecto e as relacións entre eles. Divídese en dúas interfaces, a API de programación e unha SPI que permite conectar con provedores de servizos de nomes e directorios sendo os principais LDAP, CORBA e RMI.
- 7) **JAXP** (en inglés *Java API for XML Processing*). Soporta o procesamento de documentos XML que cumpra cos esquemas do W3C a través de DOM, SAX e XSLT.
- 8) **JMS** (en inglés *Java Message Service*). Proporciona a API de envío de mensaxes para comunicarse cun MOM (en inglés *Message-Oriented Middleware*), unha abstracción independente do provedor para comunicacións entre sistemas.
- 9) **JavaMail**. Proporciona a interface para controlar o envío e recepción de correos electrónicos. Pode soportar o formato MIME grazas á súa integración con marco de traballo JAF.
- 10) **JAF** (en inglés *Java Beans Activation Framework*). API que proporciona o marco de traballo para activación que soporta as peticións doutros paquetes.
- 11) **JTA** (en inglés *Java Transaction API*). Orientada cara o manexo de transaccións e a permitir a comunicación entre contedor e compoñentes do servidor de aplicacións coma os monitores transaccionais e os administradores de recursos.
- 12) **JAX-RPC** (en inglés *Java API for XML-based RPC*). Proporciona soporte para comunicacións remotas de tipo RPC entre clientes e servizos web cos estándares HTTP e SOAP. Soporta outros estándares coma

WSDL, así coma SSL e TTL para autenticación. O SAAJ (en inglés *SOAP with attachments API for Java*) engade a posibilidade de arquivos ou notas achegados coas mensaxes.

Cada compoñente denomínase **Módulo** JEE de xeito que unha aplicación estará formada por un conxunto de módulos sendo cada un un compoñente para un contedor. Existen tres tipos de módulos:

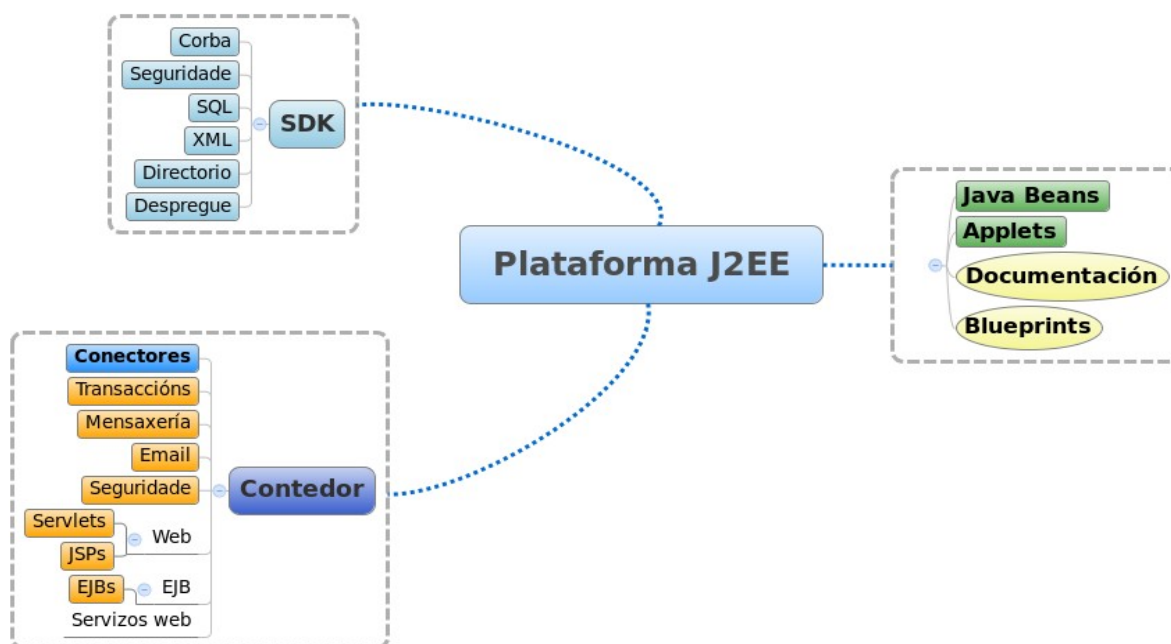
- 1) **Arquivos JAR** (en inglés *Java Archive*). Agrupación de arquivos Java e recursos segundo o formato ZIP. Empaquetan compoñentes EJB segundo a estrutura de directorios do código, engadindo unha carpeta especial, META-INF, con metadatos.
- 2) **Arquivos WAR** (en inglés *Web Application Archive*). Agrupan nun único arquivo unha aplicación web, incluíndo Servlets, arquivos JSP, contido estático e outros recursos web.
- 3) **Arquivos EAR** (en inglés *Enterprise Application Archive*). Agrupa nun único arquivo varios módulos dunha aplicación coma arquivos WAR ou compoñentes EJB e outras librarías en arquivos JAR empaquetados cos seus respectivos recursos. Así mesmo inclúese o descriptor de despregue da aplicación na carpeta META-INF.
- 4) **Arquivos RAR** (en inglés *Resource Adapter Archive*). Contén un adaptador de recursos de xeito análogo a un controlador JDBC e similar aos EAR, podendo ir contido nun arquivo deste tipo. O formato vén definido na especificación JCA (en inglés *Java EE Connector Architecture*).

De xeito xeral convén considerar á plataforma como JEE, se ben, existen diferentes **edicións**, sendo as principais:

- 1) **J2ME**. (en inglés *Java 2 Platform Micro Edition*). Para desenvolvemento de aplicacións para dispositivos móbiles, electrodomésticos e equipos PDA. Desenvolveuse mediante o JPC baixo a especificación JSR 68.

- 2) **J2SE**. (en inglés *Java 2 Platform Standard Edition*). Para desenvolvemento de aplicacións de uso xeral en estacións de traballo. Desenvolveuse mediante o JPC baixo diferentes especificacións segundo as versións existentes: 1.4, 5.0 e 6.
- 3) **J2EE**. (en inglés *Java 2 Platform Enterprise Edition*). Para desenvolvemento de aplicacións destinadas a servidores de aplicacións para dar soporte a sistemas distribuídos en N capas. Estandarizada polo JPC a partir da versión 1.4 acostuma a denominarse JEE.

Para cada edición pode distinguirse entre a SDK (en inglés *Software Development Kit*), co software e recursos destinados ao desenvolvemento de aplicacións e o JRE (en inglés *Java Runtime Environment*) co contorno e librarías principais para permitir a execución das aplicacións.



**Figura 5: Plataforma J2EE.**

### 29.3.1 Modelo de desenvolvemento

O modelo de desenvolvemento máis habitual na arquitectura JEE é un

modelo separado en múltiples capas sendo o habitual un mínimo de tres, pero podendo chegar a 5 ou 7 segundo a complexidade do sistema. O obxectivo é minimizar o solapamento entre elas para que os cambios e modificacións se limiten ao mínimo necesario co ideal de que se poida cambiar unha das múltiples capas sen ter que modificar o resto. Mellórase a sostibilidade, crecemento do sistema e a reutilización de compoñentes no mesmo e entre sistemas. Así mesmo permítese unha maior heteroxeneidade de clientes ou elementos de cliente e presentación ao modificar só a capa máis próxima ao usuario. O deseño do modelo é análogo a solucións en .NET pero a implantación diferente. As 5 capas máis habituais se describirán a continuación.

#### **29.3.1.1 Capa de cliente.**

Agrupa os elementos da interface de usuario máis próximos ao cliente. Exemplos destes elementos serían o código (X)HTML/XML e Javascript, os Applets, arquivos de recursos e tecnoloxías RIA. Os tipos de aplicacións cliente máis habituais serían os navegadores web, as aplicacións de escritorio e actualmente cobran forza as aplicacións para dispositivos móbiles. Un aspecto importante neste modelo e garantir que os EJB da lóxica de negocio sexan accesibles tan só dende interfaces remotas a través do patrón *SessionFacade*. A variedade de interfaces actual fai que aparezan *frameworks* de xeración dinámica dos mesmos baseados na linguaxe **XUL** (en inglés *XML User-Interface Language*), baseada en XML. Permite incrustar XHTML e outras linguaxes coma MathML ou SVG ademais de CSS. Existen varias alternativas de librarías XUL coma Luxor, XWT, Thinlets ou SwingML.

#### **29.3.1.2 Capa de presentación.**

Contén toda a lóxica de interacción directa entre o usuario e a aplicación. Encárgase de xerar as vistas máis axeitadas para amosar a información a través de formatos e estilos adecuados. Compóñense dunha serie de



Servlets e páxinas JSP que se encargan de devolver o código que irá á capa de cliente logo de comunicarse coa capa de lóxica de negocio para obter os resultados. Pode localizarse nunha aplicación de escritorio ou nun contedor web. Ademais de ensamblar as diferentes vistas, controla o fluxo de navegación e fai funcións de autenticación, permisos de acceso e autorización de usuarios, etc... O patrón máis habitual nesta capa será o MVC (en inglés *Model View Controller*). Entre as tendencias actuais atópanse implementacións deste modelo coma Swing o JFace para aplicacións de escritorio, mentres que dentro dos *frameworks* web atoparíanse Struts, JSF, Tapestry, Expresso e moitos outros. Sendo Struts unha especie de estándar de feito. Estes *frameworks* ademais incorporan outros servizos como etiquetas personalizadas JSTL para interfaces de usuario, manexo de XML, acceso a datos, modelos, filtros, etc...

#### **29.3.1.3 Capa de lóxica de negocio.**

Contén os compoñentes de negocio reutilizables EJB ou POJO, que representan o conxunto de entidades, obxectos, relacións, regras e algoritmos do dominio ou negocio no que opere o sistema. Nesta capa a solución POJO é unha opción sinxela que pode mesturar elementos das capas de integración e datos, mentres que os EJB distinguen os obxectos de sesión e as entidades, recomendado nos Blueprints de Sun, emprazando cada un na súa correspondente capa. O patrón básico nesta capa será o *SessionFacade* onde un único Bean de sesión encárgase de recibir as chamadas de cliente-presentación e dirixilas dentro do contedor de EJB illando esta capa.

De xeito análogo establécese o modelo dos Bean de mensaxería, que realizan comunicación asíncrona mediante JMS nun servidor MOM (en inglés *Messaging Oriented Middleware*), que pode ser un servidor externo ao servidor de aplicacións. Tamén funciona cun patrón Fachada centralizando as chamadas remotas.

#### **29.3.1.4 Capa de Integración.**

Agrupa os compoñentes encargados do acceso a datos, sistemas *legacy*, motores de regras de *workflow*, acceso a LDAP, etc... Poden realizar cambios de formato na información, pero transformacións máis complexas deberían realizarse na capa de lóxica de negocio, restrinxido esta á lóxica de acceso a datos ou DAO (en inglés *Data Access Objects*) e os encapsuladores de datos e entidades VO (en inglés *Value Object*). Os VO poden implementarse como POJO ou EJB de entidade. Como ocorría anteriormente no caso dos POJO gáñase en facilidade pero pérdense servizos e funcionalidades coma os de persistencia. Os EJB suman complexidade, pero melloran o rendemento en memoria. No tocante ao acceso a datos aparecen as seguintes alternativas:

- 1) **JDBC.** Para POJO ou Beans de entidade con control de persistencia. É unha solución sinxela, con poucas funcionalidade pero que fai uso dunha API de uso estendido.
- 2) **DAO.** Vai un paso máis alá que o JDBC incorporando interfaces para abstraer o acceso a datos e facelo independente da linguaxe do xestor. Cada interface terá unha implementación diferente para cada xestor de bases de datos.
- 3) **Frameworks de persistencia.** Fan as funcións de motores de correspondencia de obxectos a bases de datos relacionais definindo entidades e relacións vía XML. Realizan gran parte das funcións de acceso a datos automaticamente. As solucións de uso máis estendido son os *frameworks* Hibernate, iBatis, TopLink, JPA ou a través de EJB.
- 4) **JDO** (en inglés *Java Data Objects*). Sistema de persistencia estándar a partir dunha especificación JEE, engadindo ademais da correspondencia entre o modelo relacional e os obxectos a posibilidade de permitir definir os obxectos sobre a base de datos. As implementacións de uso máis estendido son OJB, XORM, Kodo JDO ou LiDO.

### **29.3.1.5 Capa de sistemas de información.**

Atópase integrada polos sistemas de bases de datos, ficheiros, sistemas 4GL, ERP, Data Warehouse, Servizos web e calquera outros sistema de información da organización. Nesta capa irían os conectadores para diferentes sistemas de información heteroxéneos e os propios recursos que integran os sistemas de información. As solucións máis habituais enuméranse a continuación.

- 1) **JCA** (en inglés *J2EE Connector Architecture*). Define unha interface de acceso común independente do sistema, coa mesma API para todos. Basease no concepto de adaptador de recursos, sendo cada adaptador un controlador específico para un sistema de información. As operacións básicas que define a especificación son: xestión das conexións de acceso a JCA, seguridade, transaccións, multiproceso, paso de mensaxes e portabilidade dentro dos servidores de aplicacións.
- 2) **JMS** (en inglés *Java Message Service*). O servizo de mensaxes Java emprega colas de mensaxes para o traspaso de información entre compoñentes software establecendo unha infraestrutura MOM con dous modelos de API, Punto a punto, entre dous únicos clientes ou Publicador/subscritor onde varios clientes segundo o seu rol envían ou len mensaxes.
- 3) **Servizos web**. Permiten a comunicación entre sistemas heteroxéneos a través do acceso á URL de aplicacións empregando protocolos baseados en XML como SOAP ou SAAJ. Os clientes acceden ao servizo a partir da súa interface definida perante WSDL (en inglés *Web Service Definition Language*) ou inserida nalgún rexistro de servizos web.



**Figura 6: Modelo de desenvolvemento en capas.**

### 29.3.2 Servidores de aplicacións.

O servidor de aplicacións será o encargado de soportar a maioría das funcionalidades e servizos da tecnoloxía JEE, sendo o núcleo desta arquitectura. Cando un servidor de aplicación implementa a tecnoloxía JEE ten que proporcionar todos os compoñentes definidos na especificación e por tanto calquera aplicación JEE poderá despregarse e executarse no devandito servidor.

O servidor de aplicacións disporá de diferentes contedores para Applets e aplicacións clientes, web e EJB, sendo estes últimos os que se encargarán de operar coa lóxica do dominio, xestión de transaccións, persistencia, control do fluxo, etc...

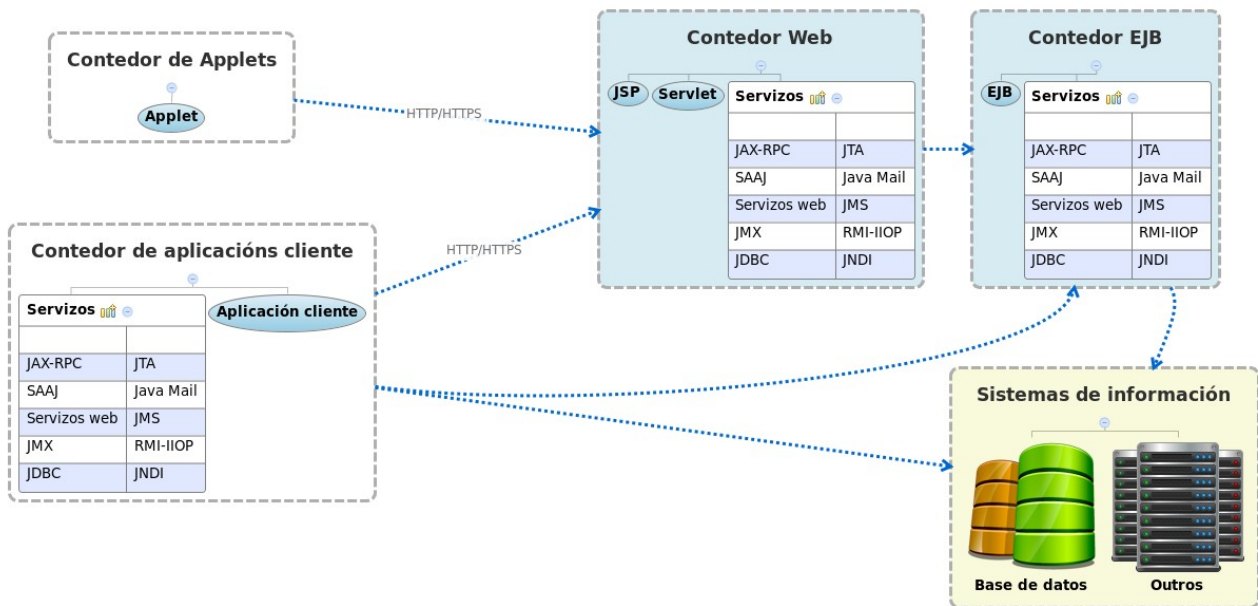
- a) **Tomcat.** Sen presentar tódalas funcionalidades dun servidor de aplicacións, este servidor libre de Apache incorpora o servidor web Apache e soporte para JSP e Servlets co contedor Catalina. Presenta diferentes módulos de soporte de aplicación como seguridade SSL, SSO, JMX, AJP, JSF, conector Coyote para peticións HTTP, soporte

para Comet, Recolector de lixo reducido así como ferramentas web para despregue e administración.

- b) **JBoss**. Un dos servidores de aplicacións libres de uso máis estendido composto por un Contedor de Servlets para JSP e Servlets e un Contedor de Beans. A diferenza de Tomcat implementa todo o conxunto de servizos especificados por JEE. Como contedor de Servlets emprega unha adaptación de Tomcat ou o contedor Jetty. Entre os módulos e funcionalidades que soporta destaca que permite a creación de *cluster*, soporte EJB, JMX, Hibernate, JBoss AOP para dotar a clases Java de persistencia e funcionalidade transaccional, sistema caché, JSF, Portlets, JMS, Servidor de correo, xestión de contidos foros e portais, entre outras moitas.
- c) **Geronimo**. Outro produto libre de Apache, compatible con JEE que inclúe JDBC, RMI, JM, Servizos web, EJB, JSP, Servlets e outras tecnoloxías. A principal característica deste servidor é que integra un gran número doutras solucións xa existentes: Tomcat e Embarcadero como contedores web, OpenEJB como contedor de Servlets, OpenJPA, Apache Axis, Apache CXF e Scout Apache para servizos web, Derby para o acceso a datos, e WADI para establecer clusters e balanceo de carga, entre outros.
- d) **JonAS**. Outra alternativa libre a JBoss, aínda que non soporta por completo JEE. Permite integración con Tomcat ou Jetty como contedores web e ten contedor de EJB. Entre módulos e servizos incorpora: Xplus, Hibernate, TopLink, OpenJPA, JORAM como implementación de JMS, varios protocolos RMI (IIOP, JRMP, IRMI), soporte LDAP, servizos web Axis e outros moitos.
- e) **Glassfish**. Alternativa libre de Sun, agora Oracle, que ten como base o *framework* para persistencia Toplink. Incorpora ademais módulos para soporte EJB, JAX-RS, JSF, RMI, JMS, servizos web, na liña dos anteriores, e novidades como Apache Félix, unha implementación de OSGi (en inglés *Open Services Gateway*) e Grizzly que fai uso da nova

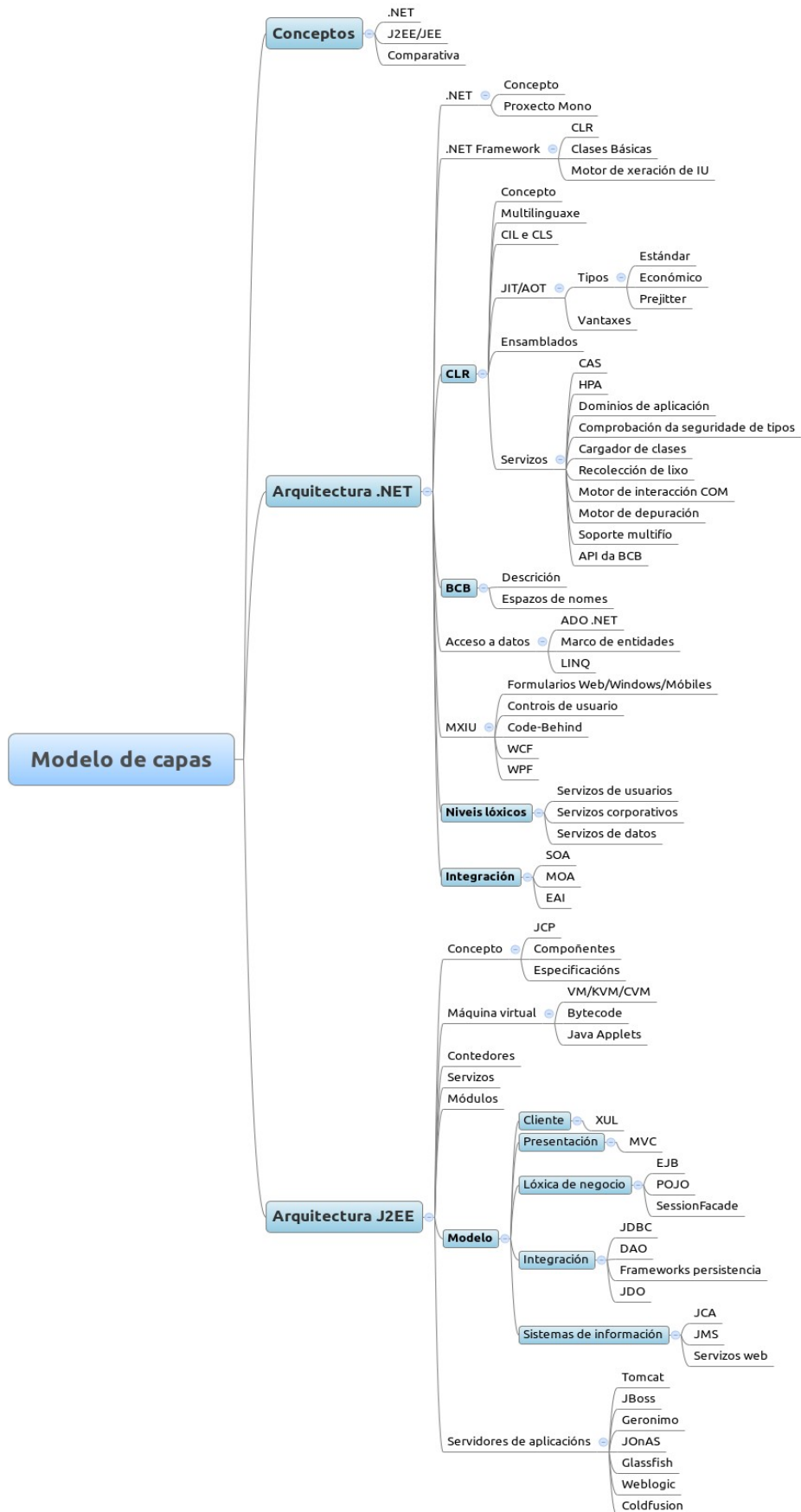
API de Java de E/S (NIO) para mellorar a escalabilidade.

- f) **WebSphere.** Alternativa comercial de IBM cunha versión de libre distribución. A versión libre, máis lixeira, basease no servidor Geronimo diferenciándose deste en que inclúe soporte para DB2, Informix, soporte RAC de Oracle e outras bases de datos así como mellores librarías para XML. Outras tecnoloxías serían: os Servlets SIP (en inglés *Session Initiation Protocol*) que utilizan elementos multimedia en tempo real, mensaxería instantánea e xogos en liña; o *framework* Spring; protocolos de seguridade Kerberos e SAML. A diferenza con outros servidores e que posúe ferramentas de administración máis avanzadas, sobre todo para sistemas en cluster e soporte para *mainframes*.
- g) **Weblogic.** Alternativa comercial de Oracle baseada en Glassfish, incorporando servizos do Weblogic server sobre a JVM JRockit. En concreto Weblogic Server proporciona os Servizos web Oracle WebLogic Server Services Web, a Application Grid coma solución de *grid* de datos, soporte de conectividade con Tuxedo (WTC), soporte de RAC para Oracle, SAML, unha API de integración con .NET a JMS.NET, Spring e o *framework* de diagnose WLDF.
- h) **Coldfusion.** Alternativa comercial de Adobe das máis valoradas actualmente, diferenciándose polo soporte a tecnoloxías RIA principalmente Flash. Implementa parte dos servizos JEE pero pode integrarse con outros servidores de aplicacións como WebSphere ou Jboss, podendo despregarse como aplicación Java. Ademais leva incorporado o servidor de aplicacións Adobe JRun. Destaca polo soporte en tecnoloxías AJAX, Flex, PDF, RSS, Flash Remoting, integración .NET e ferramentas de administración avanzadas.



**Figura7: Arquitectura J2EE**

## 29.4. ESQUEMA





## **29.5. REFERENCIAS**

Varios autores.

Biblioteca MSDN de Microsoft. (2003).

Jef Ferguson e outros.

La biblia de C#. (2003).

Benjamín Aumaille.

J2EE. Desarrollo de aplicaciones Web. (2002).

I. Singh, B. Stearns e outros.

Desingning 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. SERVIZOS WEB. TECNOLOXÍAS XML.**

## **TEMA 30. ARQUITECTURA SOA. SERVICIOS WEB. TECNOLOXÍAS XML.**

### **30.1 INTRODUCCIÓN E CONCEPTOS**

### **30.2 ARQUITECTURA SOA**

### **30.3 SERVICIOS WEB**

### **30.4 TECNOLOXÍAS XML**

### **30.5 ESQUEMA**

### **30.6 REFERENCIAS**

#### **30.1. INTRODUCCIÓN E CONCEPTOS**

Os sistemas actuais teñen unha grande complexidade debido á integración de múltiples compoñentes heteroxéneos. A comunicación e relación entre estes compoñentes é un dos grandes problemas actuais sendo **SOA** (en inglés *Service Oriented Architecture*) un dos actuais modelos de solución. Esta arquitectura entende a comunicación entre aplicacións e compoñentes coma servizos, non necesariamente servizos web, demandados por clientes ou subscritores e proporcionados e publicados por provedores. As arquitecturas para servidores de aplicacións de uso máis estendido coma .NET e JEE acostuman a definir unha **capa de integración** que agrupa os compoñentes encargados do acceso a datos, sistemas *legacy*, motores de regras de *workflow*, acceso a LDAP, etc... Para a comunicación dos compoñentes desta capa existen varias solucións coma JCA, JMS e servizos web, está última unha das máis aceptadas actualmente.

Os **Servizos web** permiten a comunicación entre sistemas heteroxéneos a través do acceso á URL de aplicacións empregando protocolos baseados en XML como SOAP ou SAAJ. Os clientes acceden ao servizo a partir da súa interface definida perante WSDL (en inglés *Web Service Definition Language*) ou inserida nalgún rexistro de servizos web.

O uso de XML convértese nun estándar de integración, sendo a base das comunicacións nesta capa, tanto para estruturar coma para almacenar e intercambiar información, estendendo o seu uso a outros ámbitos. As **tecnoloxías XML** son un conxunto de módulos que ofrecen servizos como: XSL/XSLT para deseño de documentos, Xpath como linguaxe de rutas para acceso a documentos, a linguaxe de consulta XQL, e outros como XLink ou XPointer.

### **30.2 ARQUITECTURA SOA**

SOA define unha arquitectura orientada a servizos que busca simplificar o modelo de integración de sistemas distribuídos heteroxéneos. Nesta arquitectura os compoñentes publican e invocan servizos na rede a través de mecanismos de comunicación coma JCA, JMS, SOAP, RPC ou Servizos web. Os servizos son funcionalidades da lóxica de negocio que poden invocarse de xeito remoto para obter un resultado. Defínense perante unha interface explícita, por exemplo a través de WSDL, independente da súa implementación empregando estándares de comunicación baseados en XML. SOA define tres **bases** fundamentais:

- 1) **Orientación ao intercambio de mensaxes.** A base do sistema é a comunicación entre os nodos do sistema.
- 2) **Abstracción de compoñentes.** Cada sistema redúcese á súa interface e o conxunto de servizos que define, co cal permite a integración entre calquera tipo de sistema.
- 3) **Metadatos.** Descricións e información asociada a servizos e mensaxes, mellorando as capacidade semántica do sistema.

A nivel lóxico os principais compoñentes nunha arquitectura SOA son:

- a) **Servizos.** Entidades ou funcionalidades lóxicas definidos en interfaces públicas, que poden ou non requirir autenticación.
- b) **Provedor de servizos.** Compoñente software que implementa un

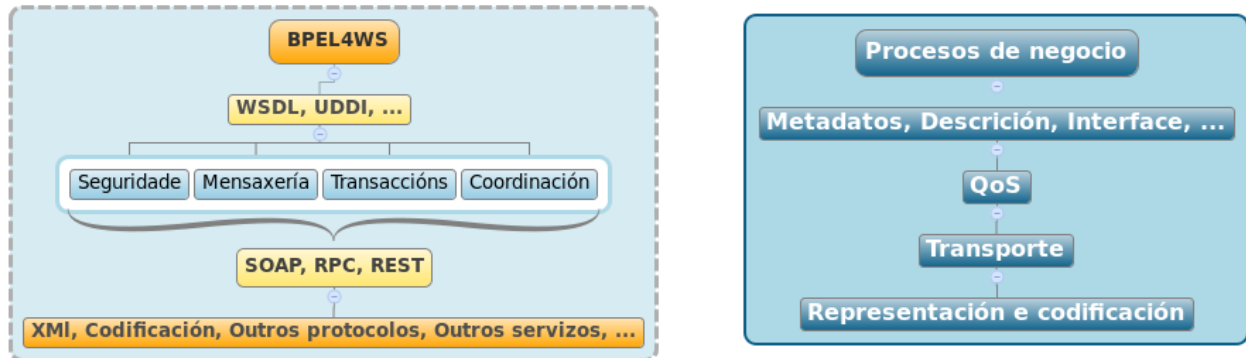
servizo e publica a súa interface.

- c) **Ciente de servizos.** Compoñente software que invoca un servizo dun provedor.
- d) **Localizador de servizos.** Provedor de servizos que rexistra as interfaces e permite aos clientes buscar no rexistro e acceder á súa localización.
- e) **Servizo de interconexión.** Provedor que comunica solicitudes de servizo a outros provedores.

O concepto de **BPM** ou Xestión de procesos de negocio (en inglés *Business Process Management*), está moi relacionado con SOA. BPM é un modelo de xestión centrado en procesos de negocio e de como integrar as súas funcionalidades en sistemas heteroxéneos. A partir da identificación e xestión dos procesos da organización pode implantarse unha solución BPM a través dunha arquitectura SOA. Froito desta idea aparecen solucións coma:

- ✓ **BPMN.** Notación para o modelado de procesos de negocio.
- ✓ **BPEL.** Linguaxe de execución de procesos de negocio con servizos web para a orquestración de servizos. Xeralmente se realiza unha conversión de BPMN a BPEL.
- ✓ **BPEL4WS.** Linguaxe de definición e execución de procesos de negocios empregando servizos web (en inglés *Business Process Execution Language for Web Services*). BPEL4WS é resultado da converxencia de WSFL (en inglés *Web Services Flow Language*) e XLANG, permitindo compoñer Servizos web coma servizos compostos denominados Servizos de negocio.

## Arquitectura SOA

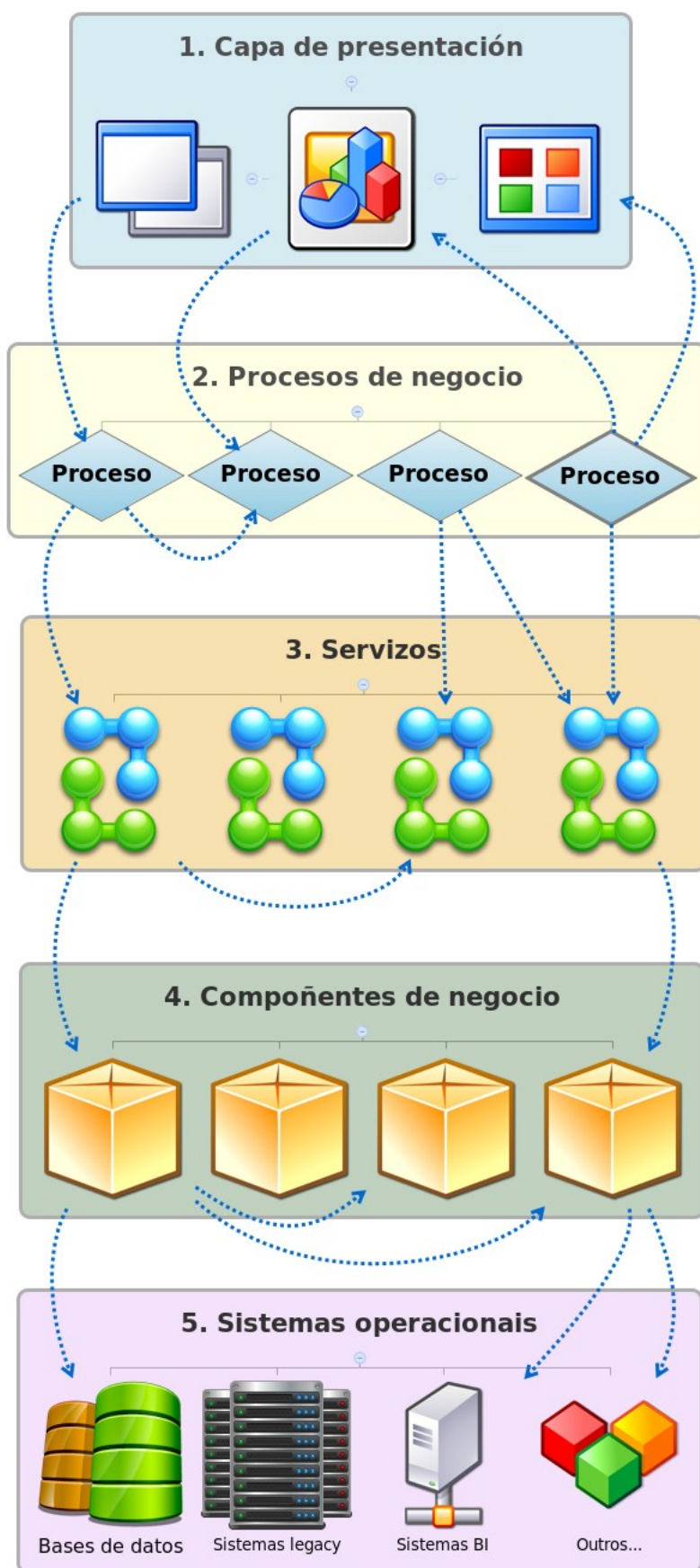


**Figura 1: Arquitectura SOA.**

A integración na arquitectura SOA dos BPM permite establecer o que se da en chamar **SOA Governance**, unha estrutura para a toma de decisións e establecemento de responsabilidades na organización a través da implantación de políticas, monitorización de servizos, incorporación de boas prácticas, principios arquitectónicos, mellora continua dos procesos de negocio, etc... en definitiva análise e deseño de solucións que permitan cumprir con éxito a implantación de SOA nunha organización.

A **nivel conceptual SOA** describe unha serie de guías ou patróns para servizos aliñados cun modelo de negocio. Un modelo conceptual de SOA permite definir un deseño en múltiples capas onde os servizos se relacionan con procesos de negocio e sistemas de información. A división máis habitual considera 7 capas diferenciadas, que se poden ver graficamente na Figura 2:

- 1) **Capa de Presentación.** Interfaces de usuario en sitios web, aplicacións e portais que invocan funcionalidades dos procesos de negocio.



6 Capa de Integración (ESB)

7 Capa de SOA Governance

- 2) **Capa de Procesos de negocio.** Representa os procesos e fluxos operativos ou workflows que invocan os clientes dende a capa de presentación ou orquestración de servizos. Os procesos por norma xeral representaranse con BPEL e implementarase con algunha ferramenta de transformación.
- 3) **Capa de Servizos.** Funcionalidades dos compoñentes da lóxica de negocio que se publican para uso dos clientes. Referéncianse a partir da interface sendo transparentes á súa implementación.
- 4) **Capa de Compoñentes de negocio.** Son os encargados de proporcionar as funcionalidades que se publicarán nos servizos así como calquera outra intermedia ou común ao sistema. A este nivel irían os servidores de aplicacións, outros servizos web, aplicacións, paquetes e librarías.
- 5) **Capa de Sistemas operacionais.** Neste nivel irían os sistemas de información da organización, sistemas *legacy*, sistemas CRM ou ERP, aplicacións de BI, etc...
- 6) **Capa de Integración.** Axiliza a integración de servizos a través de sistemas tipo Buses de Servizos Empresariais ou ESB, que realizan funcións de enrutamento, monitorización e administración, transformacións das mensaxes, etc... dentro da área de comunicacións.
- 7) **Capa de SOA Governance.** Realiza funcións de administración, monitorización e control da calidade do servizo en áreas como seguridade, dispoñibilidade e outros factores xerais non recollidos na capa de integración.

Existen **patróns de deseño** tomando como punto de partida esta arquitectura trátase de patróns para Servizos web e patróns **POSA** (en inglés *Service-Oriented Architecture Patterns*). Algúns dos principais son:

- **Service Oriented Architecture.** Patrón que define a arquitectura



SOA establecendo regras, relacións e dependencias entre os compoñentes do sistema. Permite buscar servizos dinamicamente con independencia da plataforma e sen requirir implementación, con transparencia. Este patrón é unha variante ampliada do **Broker Pattern** de POSA. Neste patrón un Servizo ou nodo intermedia axuda a localizar o servizo e pode obrigal a realizar todas as comunicacións a través del ou ben unha vez establecida deixar que esta sexa directa entre o cliente e o servizo.

- **Architecture Adapter.** Patrón xenérico que facilita a comunicación entre diferentes arquitecturas grazas á independencia de usar XML/SOAP e a xeración de clases proxy. Este patrón é implementado por *frameworks* para Servizos web como Apache Axis (Java).
- **Service Directory.** Facilita a localización de Servizos web a partir dunha especificación robusta das interfaces a través do catálogo UDDI de interfaces WSDL.
- **Service Factory.** Permite a selección de servizos do provedor illando o código de comunicación UDDI. Do mesmo xeito o patrón de estendido Service Factory Cache fai funcións de caché no servizo. Simplifica en parte a API do patrón Service Directory.
- **Service Facade.** Proporciona un servizo web controlador que actúe como punto de entrada da lóxica de negocio ou obxecto de fachada. Pode empregar simultaneamente outros mecanismos de comunicación coma CORBA.
- **Event Monitor.** Emprégase para notificar que un Servizo web de longa duración invocado remotamente completa a solicitude. Cando o Servizo non dispón de mecanismos de notificación cómpre establecer un intermediario.
- **Business Object.** Un BO engloba un concepto do dominio, equiparable a un VO para contornos distribuídos.
- **Business Process.** Un BP engloba un proceso da lóxica de negocio, representando a xerarquía formada polas diferentes implementacións



das súas funcionalidades e a interface do servizo.

- **Asynchronous Business Process.** Este patrón encárgase de xestionar a chamada e notificación de resposta ao cliente cando estas poden ser de longa duración.
- **Business Object Collection.** Agrupa diferentes procesos de negocio nun mesmo BOC.
- **Observer Services.** Basease nun rexistro de servizos onde o observador notifica ao cliente sobre eventos que derivados dos servizos nos que esta rexistrado.
- **Publish/Subscribe Services.** Evolución do patrón Observer Services incorporando un sistema de notificacións para substituír ao rexistro. Emprégase cando os servizos web non incorporan un sistema de notificación e precisan un intermediario.
- **Data Transfer Object.** Permite enviar múltiples obxectos nunha mesma chamada reducindo o número de conexións.
- **Partial Population.** Permite que os clientes seleccionen parte da información do mensaxe de resposta á solicitude de servizo buscando un mellor aproveitamento do ancho de banda.
- **Microkernel.** Separa un núcleo de funcionalidade mínimo de partes especificadas polo cliente.
- **Web Service Interface.** Proporciona unha interface que pode empregarse dende os clientes para invocar os métodos dun proxy de Servizo web xenérico en lugar de depender da clase proxy xerada a partir da WDSL.

REST (en inglés *Representation State Transfer*) representa un modelo de comunicación onde cada petición HTTP contén a información necesaria para responder á petición sen ter que almacenar o estado da sesión. En REST todo os servizos son recursos, identificados por URIs e se deseñan as súas representacións mediante XML, JSON ou microformatos. REST representa unha arquitectura SOA que non fai uso de Servizos web, SOAP nin RPC.

Actualmente dentro do marco da Web 2.0 xorde unha nova variante nas arquitecturas SOA, o concepto de **Mashup**, un sitio ou aplicación web que fai uso de contido doutras aplicacións ou servizos vía HTTP. Este contido é recuperado nun modelo de Servizos web a través da súa API pública evitando caer no Web Scraping. Para empregar os Mashups coma XML empréganse linguaxes específicos coma EMMML (en inglés *Enterprise Mashups Markup Language*). As arquitecturas Mashup constan de tres compoñentes:

- ✓ **Os provedores de servizos.** Orixes de datos que publican a través dunha interface os métodos de acceso aso mesmos e permiten a súa consulta vía Atom, RSS, REST, JSON, Bases de datos ou interfaces WSDL de Servizos web.
- ✓ **Aplicación ou Servizo web Mashup.** Proporciona un novo servizo a partir da información obtida dos provedores.
- ✓ **Cientes.** Usuarios finais, ou outras aplicacións ou servizos que fan peticións ao Mashup. Nos clientes acostuman a empregarse tecnoloxías RIA do tipo de AJAX ou Comet.

Outro concepto que se pode relacionar con SOA é o da **Nube** (en inglés *Cloud Computing*). A nube fundamentase en empregar a rede Internet para publicar servizos, que poden ou non requirir identificación. Na nube todo son servizos, aplicacións, bases de datos, redes, e xestiónanse e accédense como tal. A arquitectura da nube, estruturase habitualmente en tres capas:

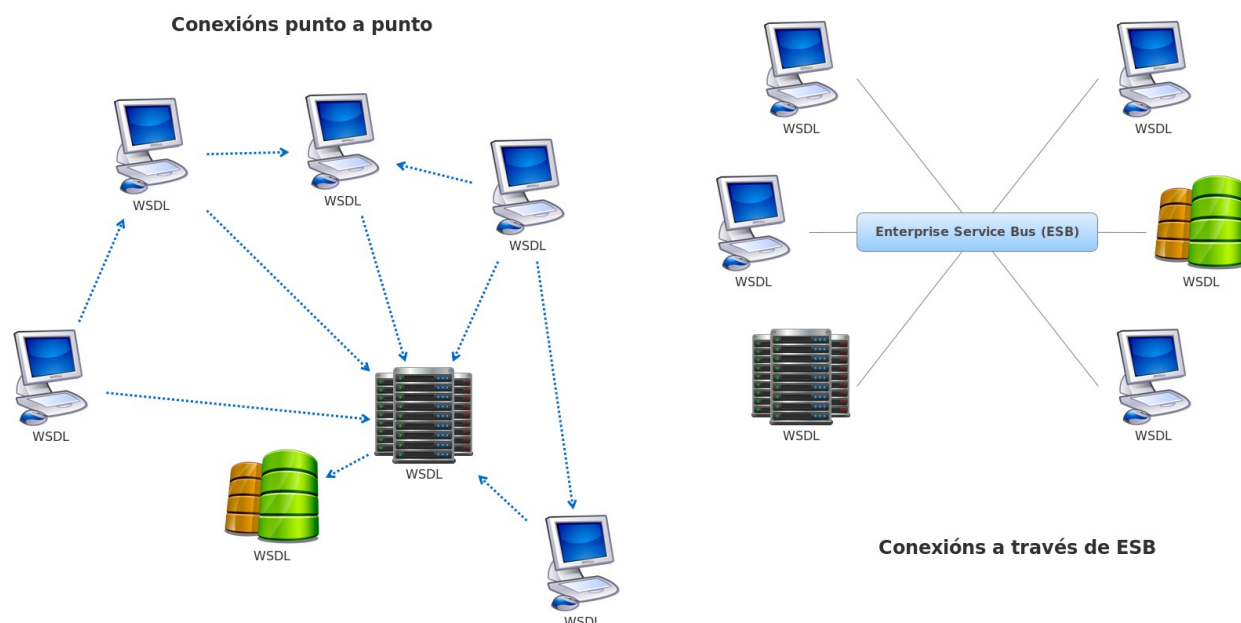
- 1) **Software como servizo** ou SaaS (en inglés *Software as a Service*). Sería o nivel máis alto, orientado aos usuarios e clientes finais. Incluiríanse as aplicacións propias e aplicacións de terceiros do estilo de Google Aps. A mesma infraestrutura do provedor serve a múltiples organizacións finais.
- 2) **Plataforma como servizo** ou PaaS (en inglés *Platform as a Service*). Serían a capa intermedia encargada de encapsular sistemas ou

*middleware* permitindo correr aplicacións sobre elas. Exemplos deste servizo serían Google App Engine ou Windows Azure. Deste xeito unha organización externa proporciona un servizo de infraestrutura e soporte para outras organizacións.

- 3) **Infraestrutura como servizo** ou IaaS (en inglés *Infrastructure as a Service*). Neste caso ofrécense servidores para computación, rede, almacenamento ou bases de datos a través de diferentes técnicas como por exemplo a través de máquinas virtuais.

O **Bus de Servizos Empresariais** ou ESB (en inglés *Enterprise Service Bus*) representa outras das características de SOA, aínda que non é imprescindible nunha arquitectura deste tipo. Trátase dun compoñente que fai abstracción do sistema de mensaxes da organización a través dun sistema único para todos os elementos dun sistema SOA. O ESB proporciona funcións de transformación, adaptación, conexión e enrutamento que poden ser implementadas en SOA. Nunha arquitectura SOA cun ESB todas as aplicacións e servizos conéctanse a un punto único e central que administra as comunicacións, realizando funcións de *middleware*. O ESB constrúese sobre tecnoloxías XML, XSLT, XPath, JMS ou propias de Servizos web. Fai uso de elementos denominados Contedores de Servizos ou Brokers que fan a función de servidores de comunicacións. Entre os servizos que proporciona se atopan:

- ✓ Funcionalidades de enrutamento, fraccionamento e combinación de mensaxes baixo a base dos patróns EIP (en inglés *Enterprise Integration Pattern*).
- ✓ Funcións de supervisión e control da calidade do servizo a través de Acordo de Nivel de Servizos ou SLA dos servizos.
- ✓ Funcións de monitorización, seguridade e mediación de protocolos.



**Figura 3: Bus de Servizos Empresariais (ESB).**

O Bus substitúe a comunicación directa entre dous aplicacións ou servizos, de xeito que a comunicación faise de xeito transparente a través do ESB. Emprega un sistema de mensaxería, como por exemplo Tibco, soportando varios MEP ou patróns de intercambio de mensaxes, así como colas para reenviar as peticións aos provedores de servizos e as respostas ás solicitudes aos clientes. Existen *frameworks* que recollen os compoñentes precisos para implantar un ESB como Mule ESB, este é un *framework* lixeiro destinado a mensaxería e control de eventos. Permite integracións con outros *frameworks* coma Struts ou Spring e soporta moitos compoñentes de servizo coma JMS, SOAP, BPEL, JBI (en inglés Java Business Integration), e outros.

Por último sinalar que as arquitecturas SOA poden completarse con módulos específicos segundo as necesidades da organización, como:

- ✓ **Seguridade.** Coa adopción de diferentes tecnoloxías, SSL, Kerberos, X.509, Sinaturas XML, Encriptación XML, XML Canonicalization, SAML



(en inglés *Security Assertion Markup Language*) ou XKMS (en inglés *XML Key Direction Specification*), que administra a chave pública ou PKI das infraestruturas.

- ✓ **Orquestración e coreografía de servizos.** Neste modelo a interacción entre servizos non se produce directamente senón que se define unha entidade que define a lóxica de interacción, facilitando a colaboración que será un servizo de control primario. En BPEL o servizo primario será un proceso BPEL, pero tamén se pode definir con BPEL4WS, WSFL ou XLANG. Mentres a orquestración precisa dun director de orquestra ou servizo central o modelo de coreografía establece interaccións punto a punto a partir de regras de colaboración xerais. Para a coreografía existen linguaxes específicas como WS-CDL (en inglés *Web Services Choreography Description Language*) que teñen definida a forma de representar as interaccións.
- ✓ **Xestión transaccional.** Existen varias tecnoloxías que coordinan as transaccións entres servizos autónomos. O BTP (en inglés *Business Transaction Protocol*) onde ningún dos servizos xestiona unha transacción, senón que esta se comunica a todos e deciden se se unen ou non, con comunicacións baseadas en XML nun formato propio. Outros mecanismos como WS-Transaction e WS-Coordination encárganse de xestionar transaccións levadas a cabo por varios servizos á vez, con protocolos SOAP e WSDL. Pola súa banda JEE dispón da especificación JAXTX para transaccións complexas co obxectivo de illar estas dos contedores.

### 30.3 SERVIZOS WEB

Os Servizos web son un dos modelos de implementación de SOA. Un Servizo web que proporciona un servizo vía web nunha rede a través dunha interface que lle permite recibir peticións e transmitir respostas. Para soportar este sistema se desenvolveron unha grande variedade de

protocolos e tecnoloxías. Os principais son o HTTP/HTTPS para peticións e respostas e o XML como formato de intercambio. Os principais **compoñentes** comúns aos servizos web serían:

- a) **SOAP** (en inglés *Simple Object Access Protocol*). O protocolo de comunicación, sobre a capa de transporte baseado en XML, que serve para invocar os servizos a través dun protocolo sendo os máis habituais HTTP ou SMTP, pero realmente é independente e permite outros como POP3 ou JMS. Permite tanto describir o contido da mensaxe e regras de codificación dos tipos de datos, coma aspectos de seguridade e transaccionalidade. Atópase estandarizado polo W3C, o que garante a comunicación entre sistemas heteroxéneos que o implementen.
- b) **UDDI** (en inglés *Universal Description, Discovery and Integration*). Directorio onde se publican os servizos proporcionando a información necesaria para permitir a súa invocación. Presenta dúas API que permiten aos servizos publicar as súas funcionalidades e aos clientes enviar as peticións e obter os resultados. Cada servizo publícase no UDDI proporcionando a URL da súa WSDL e meta-información. De xeito xeral enténdese que UDDI proporciona tres tipos de servizos: información xeral sobre os provedores dos servizos (páxinas brancas), categorías e clasificacións de servizos (páxinas amarelas) e as regras de negocio ou información técnica sobre os servizos (páxinas verdes).
- c) **WSDL** (en inglés *Web Services Description Language*). Linguaxe baseado en XML e XML Schema que permiten a descrición da interface dos Servizos web e que está estandarizado polo W3C. Nun documento WSDL defínense os tipos de datos, as mensaxes, os *endpoints*, os *bindings* e os servizos.
- d) **Serialización de datos**. Empréganse definicións de XML Schema para especificar como codificar os datos en conxunción coas regras

de codificación de SOAP. Aínda que o mecanismo máis habitual sexa o SOAP Document/Literal existen outros mecanismos coma: RPC/Encoding, Document/Encoding ou RPC/Literal.

Segundo o visto anteriormente para as arquitecturas SOA en xeral, pódense definir varios tipos de servizos segundo a súa complexidade, comezando polos de nivel básico aos de niveis máis complexos.

	<b>Servizos de nivel básico</b>	<b>Servizos de alta complexidade</b>
<b>Función</b>	Integración da funcionalidade dunha aplicación	Elemento chave dunha arquitectura SOA
<b>Protocolos e tecnoloxías</b>	SOPA, UDDI, WSDL	ebXML, BPEL, BTP, RossetaNet, Apache Axis, ...
<b>Tipo de contido</b>	Plano	MIME, PDF, ...
<b>Comunicacións</b>	Punto a punto	Multiparty, ESB, ...
<b>Mensaxería</b>	JMS, RPC, ...	Colaboración e <i>workflows</i>
<b>Transaccionalidade</b>	Non transaccional	Transaccional
<b>Seguridade</b>	SSL, autenticación, ...	Sinatura dixital, XML-encryption, Kerberos, ...

***Táboa 1: Complexidade dos servizos web.***

Segundo o tipo de comunicacións as APIs máis habituais son:

- API de mensaxería.** Clientes e servizos dispoñen de sistemas de mensaxería que lles permiten comunicarse en formato XML. Ao estar orientadas cara os sistemas de mensaxería presentan unha alta QoS.
- API de RPC.** A solución máis habitual, que emprega un compilador intermedio de WSDL para xerar o *stub* e o *skeleton* para cliente e



servidor respectivamente, tal e como acontece con CORBA. Este sistema é o que acostuman empregar os *frameworks* actuais como Apache Axis.

- c) **API para servidores de aplicacións (JEE/.NET).** Estas API veñen dispoñibles nas bibliotecas de clases de cada arquitectura, por exemplo en JEE dispónse de: JAXM (en inglés *Java API for XML Messaging*) para intercambio de mensaxes; JAX-RPC (en inglés *Java API for XML-based RPC*) , que permite enviar peticións remotas a terceiros e recibir resultados; e JAXR (en inglés *Java API for XML Registries*), que proporciona acceso a rexistros de negocio e mecanismos para compartir información .

O **proceso de implementación dun servizo web** consiste en implementar as funcionalidades do servizo a reutilizando as clases xeradas a partir dun WSDL ou dunha API (JAX-RPC, Axis, ...). Pódense aproveitar as ferramentas existentes nos IDE, ou outras máis específicas con Ant ou *WsdI2java*. Unha vez implementadas as clases coa lóxica do servizo xéranse as clases nun war e despréganse nun contedor de Servlets ou nun IIS. Sobre o modelo de programación empréganse diferentes variantes:

- a) **Estilo CORBA.** Xéranse todas as clases ao compilar empregando clases das API (Axis, JAX-RPC, ...)
- b) **Dynamic Proxy.** A interface WSDL créase ao compilar, pero o proxy no cliente só se compila en tempo de execución.
- c) **Dynamic Invocation Interface.** Tanto WSDL como cliente xéranse en tempo de execución. O cliente busca e invoca o servizo vía *broker*.

Outro dos factores a considerar é o tema da **seguridade** nos Servizos web, que pola propia natureza das arquitecturas SOA resulta un tema complexo. O principais elementos de seguridade no que respecta a JEE, aínda que

moitas serían extensibles a .NET serían:

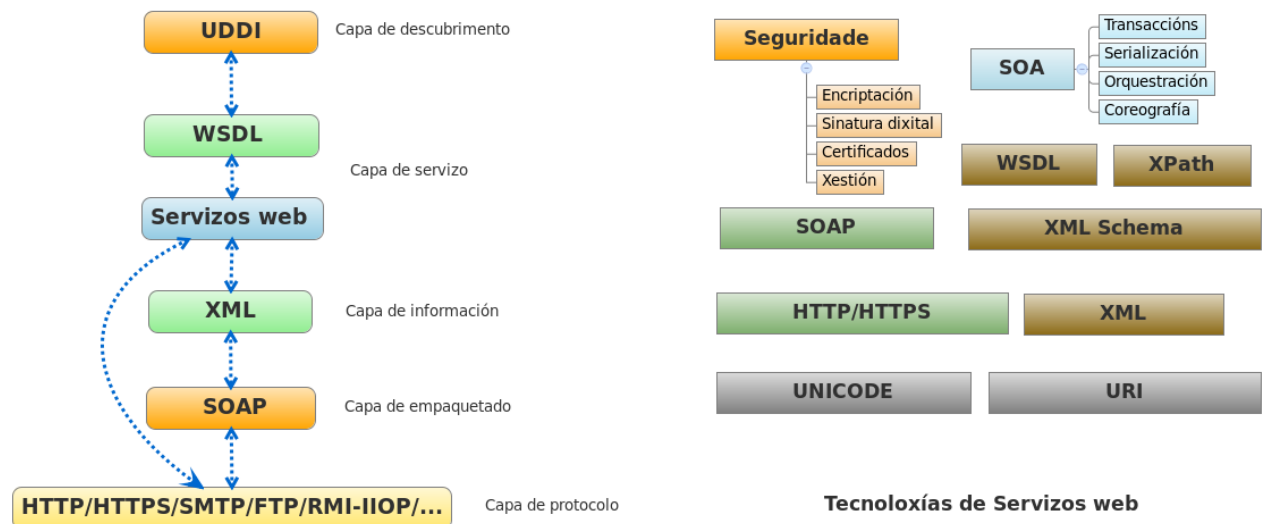
- ✓ Para JAX-RPC a **API XWS-Security** que facilita a integración de aspectos de seguridade.
- ✓ O estándar **XML-DigitalSignature** para sinatura dixital.
- ✓ O estándar **XML-Encrytion** para encriptación de mensaxería.
- ✓ **Certificados X.509** para autenticación.
- ✓ Bases de datos de certificados baseadas en **JKS** (en inglés *Java Key Store*).

Dentro da arquitectura os diferentes mecanismos integraríanse nivel a nivel do seguinte xeito:

- 1) **Nivel de transporte.** Autenticación básica, autenticación por certificado vía SSL/TLS. Codificación de usuario/contrasinal nos *stubs* e regras de seguridade para *endpoints*.
- 2) **Nivel de mensaxe.** Sinatura de contidos con certificados XML-DigitalSignature, certificados X.509 e encriptación.

Entre as **posibilidades** existentes para implementar Servizos web atópanse:

- ✓ APIs Java: JAX-RPC, JAXM, SAAJ (mensaxes SOAP como obxectos), JWS DL (Acceso a descrições WSDL), JAXR (Acceso ao UDDI), *framework* Apache Axis, ...
- ✓ .NET: ASP .NET, MS SOAP Toolkit, ...
- ✓ Outras tecnoloxías: NuSOAP para PHP, Axis para C++, ...



**Figura 4: Tecnoloxías de Servizos web.**

### 30.4 TECNOLOXÍAS XML

A linguaxe XML (en inglés *extensible Markup Language*) é unha metalinguaxe para etiquetado desenvolvido polo W3C. En SOA o XML representa o estándar para intercambio de información estruturada entre sistemas heteroxéneos. En esencia XML é unha linguaxe de marcas que permite a creación doutras linguaxes de marcas, con diferentes usos en SOA, cada unha destas linguaxes denomínase Aplicación XML e representa un modelo de datos de acordo a un esquema semántico.

O XML resulta máis estrito que outras linguaxes como HTML, admitindo varios mecanismos de validación ou corrección:

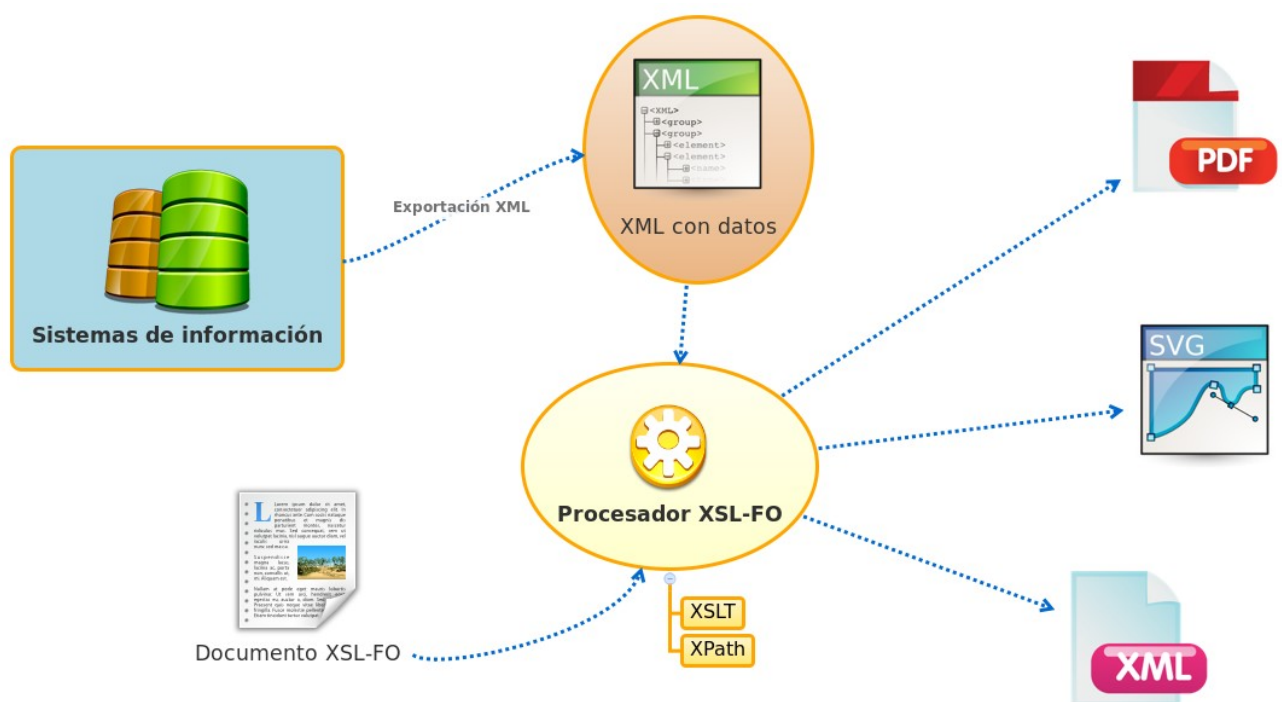
- ✓ **Formación.** Un documento XML denomínase “ben formado” cando segue as regras léxicas (tipo de caracteres, codificación, ...) e sintácticas (anidación correcta, marcas de apertura e peche de estrutura, ...) debidas.
- ✓ **Validación.** Un documento XML considérase “validado” cando

cumpre un conxunto de regras e restricións denominadas en conxunto gramática ou Esquemas XML (en inglés *XML Schema*). Existen varios formatos para gramáticas: os DTD herdados do SGML, os XML-Schema, que son recomendación do estándar polo W3C e outros máis específicos coma o XML Data.

As **tecnoloxías principais máis empregadas** do modelo XML en arquitecturas SOA veñen dadas por:

- ✓ **XML Schema.** Linguaxe de esquema para describir a estrutura e regras de validación dun documento XML. Diferenciase do DTD en que permite un grande número de tipos de datos. Os documentos de esquema son de extensión XSD (en inglés *XML Schema Definition*). A programación de esquemas basease nos espazos de nomes e os elementos e atributos que conteñen. Logo de validar un documento contra un XSD pódese expresar a súa estrutura e contido en termos do modelo de datos do esquema. Esta funcionalidade denomínase PSVI (en inglés *Post Schema Validation Infoset*), e permite transformar o documento nunha xerarquía orientada a obxectos.
- ✓ **XSL.** XSL funciona como unha linguaxe avanzada para crear follas CSS transformando e realizando outras operacións sobre documentos XML, dándolles formato. Á súa vez pode descompoñerse en tres linguaxes ou dialectos XML, todos recomendacións do W3C, que integran a familia XSL:
  - ✓ **XSLT** (en inglés *Extensible Stylesheet Language Transformations*). Estándar para documentos XML que permiten transformar documentos XML en base a modelos dunha sintaxe a outra permitindo estruturas de programación, funcionando a xeito de intérprete. As regras dos modelos defínense programaticamente e a principal capacidade desta linguaxe é que permite separar o contido da presentación, ou diferentes presentacións en documentos XML o que se adapta perfectamente aos modelos de

- separación en capas vistos.
- ✓ **XSL-FO** (en inglés *Extensible Stylesheet Language Formatting Objects*). Documentos XML que especifican formatos de datos ou obxectos para a súa presentación. A utilidade básica destes documentos é a presentación, co cal se complementan con XSLT na saída de datos das aplicacións. Permite a xeración de documentos multiformato: XML, (X)HTML e mesmo PDF. Existen procesadores específicos para este tipo de operacións coma Apache FOP.
  - ✓ **XPath ou XML Path Language**. Permite identificar partes dun documento XML, accedendo aos seus atributos e elementos coma se foran nodos, a través da construción de expresións que recorren e procesan un documento XML. En XSL permite seleccionar e percorrer o documento XML de entrada da transformación, pero por extensión ten outros moitos usos actualmente, servindo de base para outras linguaxes XML.



**Figura 5: Familia XSL.**



- ✓ **XPointer.** Recomendación do W3C que permite localizar puntos concretos ou fragmentos nun documento que expande as funcionalidades de XPath a través de rangos .
- ✓ **XLink** . Recomendación do W3C que define un mecanismo para engadir hiperligazóns en arquivos XML ou outros recursos, coa opción de navegar nos dous sentidos, con ligazóns bidireccionais ou varios arquivos enlazados, multiligazóns. En XLink todo na rede é un recurso, e se pode enlazar dende un localizador, definindo as relacións entre recursos con arcos. Así mesmo permite agregar a un vínculo información sobre si mesmo coma metadatos.
- ✓ **XQuery.** Linguaxe de consulta desenvolvido polo W3C para recuperar coleccións de datos XML, con moitas similitudes con SQL. Permite extraer e manipular información de documentos XML ou calquera outro sistema de información que permita representación vía XML como Bases de datos ou documentos ofimáticos. Emprega XPath para acceder aos documentos engadindo unhas expresións propias denominadas FLWOR. Así mesmo realiza transformacións de documentos XML e buscas de elementos textuais na web ou en recursos XML/(X)HTML. Nas arquitecturas SOA resultan especialmente útiles para recuperar información de Bases de datos e presentala a través de Servizos web.
- ✓ **XForms.** Linguaxe de definición de Interfaces de usuario desenvolvida polo W3C, centrada especialmente na parte de formularios web e a súa integración en documentos (X)HTML, ODF ou SVG. Aplícase o paradigma de separar o contido, propósito e estrutura. En aplicación do MVC incorpora un modelo declarativo de composto de regras e validación para datos e tipos de datos dos formulario, así como envío de parámetros; unha capa de vista

composta dos controis da interface de usuario; un controlador para orquestrar as manipulacións de datos, interaccións entre o modelo e a vista e envíos de datos. Outras evolucións desta tecnoloxía serían AJAXForms e XSLTForms, incorporando AJAX e XSLT a esta tecnoloxía. Por outra banda, existen outras linguaxes relacionadas coas interfaces de usuario que seguen dialectos de XML, moitas delas con capacidade para interactuar con XForms como: XAML, XUL, UIML, UsiXML, AUIML, ...

O grupo de tecnoloxías anteriores poderían definirse como linguaxes XML de propósito xeral. En moitas ocasións o XML emprégase de xeito concreto para representación de datos complexos ou con necesidades específicas para o noso dominio. Na táboa 2 recóllense algúns exemplos de linguaxes XML empregadas para representación ou adaptación de información a necesidades concretas, ben para contornos de traballo como XHTML e WML ou ben en dominios específicos como aplicacións de información xeográfica ou deseño gráfico.

	<b>Función</b>
<b>XHTML</b>	HTML con especificacións máis estritas para presentar unha maior compatibilidade coa web semántica e os outros estándares XML
<b>MathML</b>	Expresar formulacións matemáticas
<b>SVG</b>	Especificación para describir gráficos vectoriais e animacións
<b>SMIL</b>	Permitir a integración multimedia en XHTML e SVG
<b>WML</b>	Adaptación do HTML para móbiles e PDA
<b>VoiceXML</b>	Converter fala en XML a partir de gramáticas de recoñecemento de voz
<b>SSML</b>	Para fala sintética
<b>GML/KML</b>	Para sistemas de modelado e información xeográfica

	Función
<b>X3D</b>	Representación de gráficos en 3D
<b>EBML</b>	Para almacenar xerarquías de datos en formato binario de lonxitude variable

### ***Táboas 2: Linguaxes XML complementarias.***

O uso tan estendido do XML obriga a dispoñer de ferramentas que permitan o tratamento doado dos documentos, percorrer, manipular, procesar, etc... Moitas tecnoloxías dispoñen de *frameworks* específicos para **tratamento de XML**:

- ✓ **DOM** (en inglés *Document Object Model*). Especificación do W3C dunha API ([org.w3c.dom](http://org.w3c.dom)) para manipular documentos XML/HTML, acceder ao seu contido, estrutura e estilos, a través dun analizador sintáctico. DOM xera unha árbore xerárquica en memoria onde almacena todo o documento. A través dun procesador permítese acceder a calquera nodo da árbore, ou inserir/eliminar novos nodos. O principal inconveniente deste modelo é que precisa gran cantidade de memoria pola necesidade de cargar todo o documento, pero ten as vantaxes de ser moi sinxelo de implementar e de permitir a xeración de XML. Apoíase en tecnoloxías XSLT e Xpath. Frameworks como Xerces baséanse en DOM para tratamento de XML así como outros baseados en AJAX do tipo de JQuery, Prototype, Dojo, etc... Así mesmo existen alternativas recentes similares a DOM, deseñadas explicitamente para JEE que resultan máis doadas de empregar, JDOM ([org.jdom](http://org.jdom)) e DOM4J ([org.dom4j](http://org.dom4j)).
- ✓ **SAX** (en inglés *Simple API for XML*). API inicialmente para Java ([org.xml.sax](http://org.xml.sax)), pero que despois evolucionou a outras linguaxes coma C++, Perl, Python, ... , que dispón dun analizador que xera eventos ao acadar puntos chave do documento analizado. Percorre o documento de xeito secuencial a través dun administrador de eventos, o



DocumentHandler, evento a evento, co cal non precisa cargar o documento en memoria pero non permite volta atrás sen ir de novo ao inicio. Isto o fai moi axeitado para documentos de gran tamaño. Outros *frameworks* máis completos baséanse á súa vez en SAX, como: Xerces, Crimson, Piccolo ou Oracle XML Parser.

- ✓ **StAX** (en inglés *Streaming API for XML*). Define un analizador sintáctico de fluxo de datos integrado en JEE, con soporte para xeración de XML. Empréganse dous estilos de análise Cursor API e Iterador Event Iterator API, ambos baseados en iteracións para solventar as limitacións de SAX e DOM. Neste modelo o documento XML transmítese nun fluxo de datos onde o se vai solicitando o seguinte evento (*Pull*) co fin de optimizar recursos de memoria. Distínguese entre Streaming Pull Parsing onde o cliente só obtén os datos solicitados previamente (SAX) e o Streaming Push cando o analizador envía ao cliente datos do XML ao localizar un elemento.
  
- ✓ **JAXP** (en inglés *Java API for XML Processing*). API de Java (javax.xml.parsers e javax.xml.transform) que proporciona acceso a través de dúas factorías abstractas para traballar con instancias de analizadores DOM e SAX a través de diferentes implementacións, así como soporte para StAX, espazos de nomes e XSLT (Xalan). Tamén leva incorporado o analizador Crimson. Acostuma integrarse en contornos con Servizos web para agrupar nun mesmo *framework* todas as posibilidades de tratamento de XML.
  
- ✓ **JAXB** (en inglés *Java Architecture for XML Binding*) . API JEE (javax.xml.bind) que proporciona un conxunto de interfaces para analizar e xerar XML de xeito automático. A partires do modelo definido en XML realiza a xeración de clases Java equivalentes. O esquema acostuma definirse vía DTD, a partir do cal un desenvolvedor pode construír unha árbore de obxectos Java que se

corresponden co XML. Deste xeito evítanse as limitacións de memoria de DOM.

Paralelamente dispórase de compoñentes específicos para contornos baseados en **Servizos web** coma WSDL, os máis habituais serían:

- ✓ **SAAJ**. API (javax.xml.soap) de SOAP e SOAP con achegas (en inglés *SOAP with Attachments*) que permite enviar documentos XML e achegas en formato MIME que poden ser ou non XML. Acostuma empregarse a baixo nivel por outras API para operacións de mensaxería.
- ✓ **JAX-RPC**. API de JEE para facilitar o desenvolvemento de compoñentes software que fagan uso de XML para comunicacións a través de chamadas a procedementos remotos (RPC), na liña de IDL-CORBA e RMI. A diferenza destas alternativas JAX-RPC emprega XML como soporte a Servizos web. Permite correspondencia entre obxectos e estruturas XML. En arquitecturas SOA o JAX-RPC sería a tecnoloxía a través da que o cliente envía a petición de servizo. Por debaixo emprega SOAP, pero este nivel permanece transparente á API. As súas funcións abarcan: Mensaxería asíncrona, Enrutamento de mensaxes, Mensaxería con entrega garantida.
- ✓ **JAXR** (en inglés *Java API for XML Registries*). API de JEE para acceso a rexistros de servizos en estándares abertos como ebXML ou UDDI. Permite aos servizos a posibilidade de auto-rexistrarse. Así mesmo soporta o uso de consultas SQL para a busca de rexistro a través do obxecto SQLQueryManager. Fai uso de JAXM para mensaxería.
- ✓ **JAX-WS** (en inglés *Java API for XML Web Services*). Compoñente do servizo web base Metro, que sería evolución e ampliación de JAX-RPC e se atoparía integrado con JEE (javax.xml.ws). Fai uso de anotacións Java para describir elementos das clases, como metadatos e

permiten automatización de tarefas.

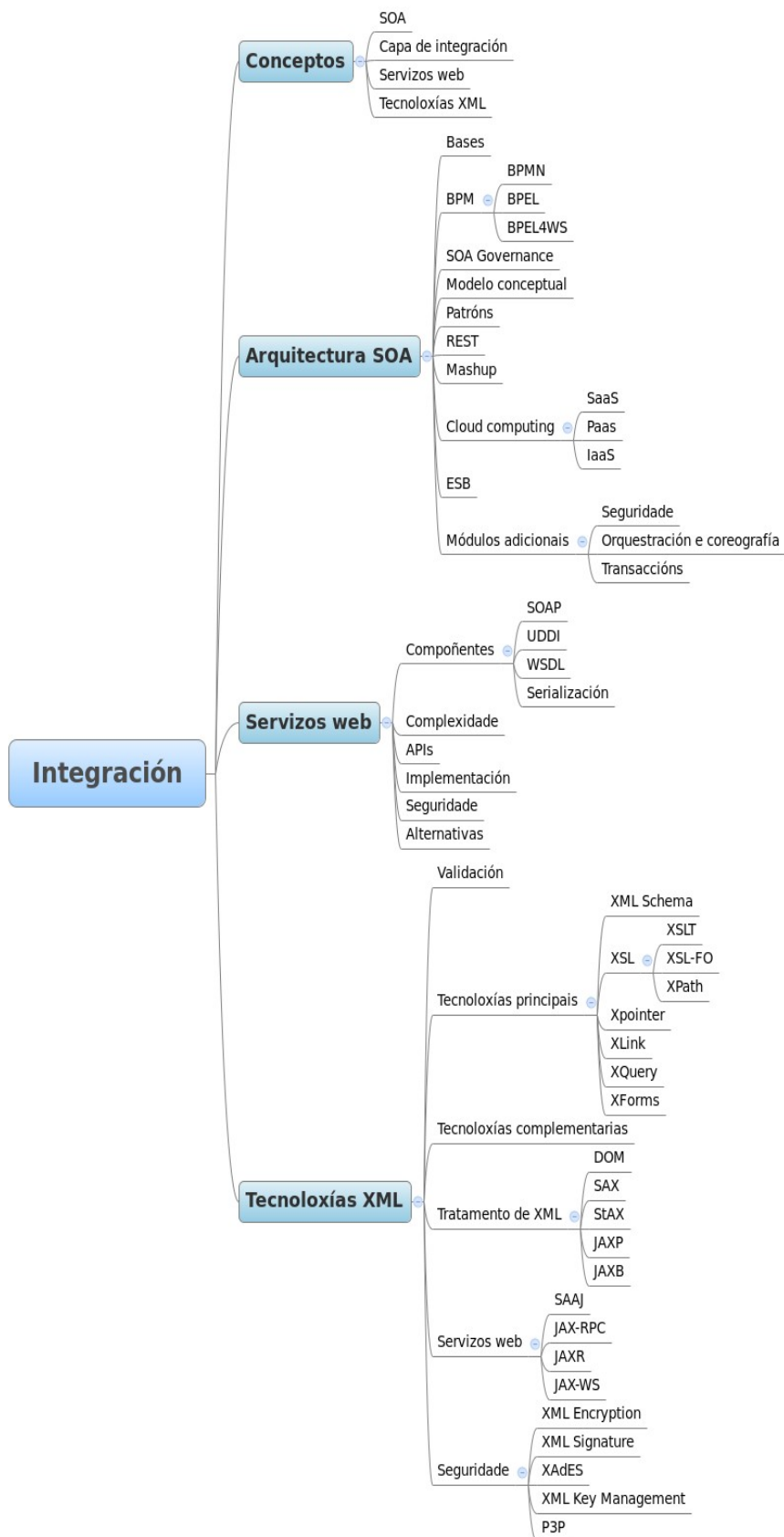
Por último dentro do ámbito da **seguridade**, existen unha serie de solucións derivadas da capacidade insuficiente ante arquitecturas SOA de TLS ou SSL. Deste xeito cómpre destacar as seguintes tecnoloxías:

- ✓ **XML Encryption.** A encriptación XML é unha recomendación do W3C que especifica o proceso para cifrar datos ou documentos completos e representar esa información encriptada nun documento XML. Permite supercifrado e soporta os algoritmos TripleDES, AES e RSA.
- ✓ **XML Signature.** Sinatura dixital que garante a integridade das partes nunha comunicación. Así mesmo proporciona autenticación de mensaxes, integridade de datos, soporte de transaccións sen repudio e sinaturas para calquera contido dixital ou XML. No documento engádese un elemento Signature que encapsula o contido da sinatura dixital incluíndo unha referencia ao obxecto asinado, a indicación do algoritmo de canonización, e o valor resultante da sinatura.
- ✓ **XAdES** (en inglés *XML Advanced Electronic Signatures*). Sinatura dixital avanzada XML, que engade un conxunto de extensións a XML Signature, permitindo por exemplo que as sinaturas sexan válidas durante longos períodos de tempo
- ✓ **XML Key Management.** Protocolo para distribuír e rexistrar chaves públicas e certificados evitando a complexidade de PKI. Está composto de dúas partes: X-KRSS ou rexistro de chave pública, un conxunto de protocolos que soportan o rexistro de pares de chaves; e X-KISS información de chave pública, que define un conxunto de protocolos para procesamento e envío de información asociada en identificada con XML Signature e cifrada con XML Encryption.
- ✓ **P3P** (en inglés *Platform for Privacy Preferences*). Especificación do



W3C que define un estándar de xestión de datos e de privacidade, así como un formato XML para expresar políticas de privacidade, co obxectivo de permitir aos usuarios se e como queren revelar información persoal.

#### **30.4. ESQUEMA**



### **30.5. REFERENCIAS**

Varios autores.

Web Services Architecture. W3C Working Group. (2004).

César de la Torre e Roberto González.

Arquitectura SOA con tecnología Microsoft. Buenas prácticas y diseño de aplicaciones empresariales. (2008).

Joan Ribas Lequerica.

Web Services. (2003).

Patrick Cauldwell e outros.

Servicios Web XML. (2002).

**Autor: Juan Marcos Filgueira Gomis**

**Asesor Técnico Consellería de Educación e O. U.**

**Colegiado del CPEIG**



# **31. PATRÓNS DE DESEÑO E FRAMEWORKS. MVC. JSF. ANTIPATRÓNS.**

## **TEMA 31. PATRÓNS DE DESEÑO E FRAMEWORKS. MVC. JSF. ANTIPATRÓNS.**

### **31.1 INTRODUCCIÓN E CONCEPTOS**

### **31.2 PATRÓNS DE DESEÑO E FRAMEWORKS**

### **31.3 MVC**

### **31.4 JSF**

### **31.5 ANTIPATRÓNS**

### **31.6 ESQUEMA**

### **31.7 REFERENCIAS**

### **30.1 INTRODUCCIÓN E CONCEPTOS**

Para moitos problemas de deseño que se repiten tanto en desenvolvementos software como en implantacións hardware existen solucións comúns de aplicación dentro do mesmo contexto. Estas solucións recorrentes denomínanse **patróns de deseño** e se basean no concepto de reutilización e aproveitamento de solucións xa existentes en problemas novos. Os patróns segundo o autor acostuman a dividirse en diferentes familias, sendo a clasificación máis habitual en patróns de deseño, de arquitectura e interacción. Á súa vez dentro dos patróns de deseño clasifícanse segundo creacionais, estruturais e de comportamento. Así mesmo defínense os patróns de programación como patróns específicos para linguaxes de programación ou sistemas concretos. Cómpre sinalar que nunha mesma solución ou deseño pode convivir calquera número de patróns que sexa necesario, xa que en moitos casos trátase de solucións parciais a problemas concretos non de solucións xerais. Fronte ao concepto de patrón xorde o de **antipatrón** que definen erros de deseño comúns ou problemas que se repiten a miúdo para axudar a identificalos. Os patróns e antipatróns poden definirse perante linguaxes de definición do estilo da



Linguaxe Unificada de Modelado ou **UML** (en inglés *Unified Modeling Language*), que soportado polo OMG é un dos máis empregados actualmente.

Nas aplicacións JEE e .NET un dos patróns de uso máis estendido é o Modelo Vista Controlador ou **MVC** (en inglés *Model View Controller*) que se basea na separación dunha aplicación en tres capas ou compoñentes diferenciados, interface de usuario, lóxica de negocio e sistemas de información.

Este patrón intégrase en **frameworks**, ou compoñentes software que implementan funcionalidades comúns a conxuntos de aplicacións, e que poden seguir os modelos de patróns de deseño. O patrón sería a solución de deseño abstracta e o *framework* unha implementación do mesmo concreta. Algúns *frameworks* como Struts representan o esqueleto dunha aplicación, con implementación do patrón MVC entre outros, aportando así directamente todas as funcionalidades precisas para o seu funcionamento interno. Se nunha mesma aplicación engadimos novos *frameworks* dispoñemos de funcionalidades engadidas. Deste xeito o *framework JSF* (en inglés *Java Server Faces*) proporciona, complementariamente a Struts ferramentas que facilitan o desenvolvemento de interfaces de usuario.

## **31.2 PATRÓNS DE DESEÑO E FRAMEWORKS**

As principais vantaxes do emprego de patróns en solucións software pasan por facilitar a comunicación interna entre compoñentes, aforrar tempo e outros recursos, mellorar a calidade das operacións de todo o ciclo de vida de desenvolvemento e facilitar a aprendizaxe. A día de hoxe é un feito consumado que a súa aplicación correcta reporta un beneficio directo en calquera desenvolvemento ou implantación.

### **31.2.1 Clasificación xeral**

Existen moitas clasificacións dos patróns, segundo o autor(es) pero a máis habitual fai referencia ao ámbito de aplicación do patrón tomando como referencia a enxeñaría do software:

- 1) **Patróns de deseño.** Proporcionan un esquema de aplicación en partes dun sistema software. Definen estruturas que resoven un problema de deseño de utilidade en diferentes aplicacións.
- 2) **Patróns de arquitectura.** Proporcionan un esquema ou organización estrutural para definir sistemas completos ou subsistemas incluíndo responsabilidades e relacións entre sistemas.
- 3) **Patróns de interacción.** Proporcionan un deseño de interface para aplicacións ou aplicacións web.
- 4) **Patróns de programación** (en inglés *Idioms patterns*). Patróns a baixo nivel para linguaxes de programación ou tecnoloxías específicas. Definen representacións de implementacións de compoñentes e relacións considerando funcionalidades propias de cada linguaxe.

### **31.2.2 Clasificación de patróns para tecnoloxías de servidores de aplicacións**

A maiores foron xurdindo patróns para outros ámbitos de aplicación, como programación multifío, fluxos de traballo para procesos de sistemas empresariais, arquitecturas SOA ou integración de sistemas. En definitiva, pode concluírse que o concepto de patrón pode estenderse a calquera problema que nos atopemos e o nivel de abstracción que precisemos na solución. Existen diferentes catálogos de patróns, sendo os máis coñecidos:

- ✓ **GoF**, (en inglés *Gang of Four*) para problemas de deseño. (1995).
- ✓ **POSA**, (en inglés *Pattern Oriented Software Architecture*) para solucións en arquitecturas SOA. (1996).



- ✓ **J2EE**, para solucións específicas desta tecnoloxía. (2003).
- ✓ **PoEAA** (en inglés *Patterns of Enterprise Application Architecture*). Para sistemas complexos en arquitecturas empresariais distribuídas en capas. (2003).
- ✓ **GRASP** (en inglés *General Responsibility Assignment Software Patterns*). Patróns xerais para asignación de responsabilidades e transicións. (2005).

En concreto para o ámbito dos servidores de aplicacións como .NET e JEE en canto a arquitectura e análise poden destacarse os seguintes atendendo ao seu nivel de utilización:

- a) **Patrón de análise Party (Grupo).** Agrupa as responsabilidades similares dos tipos de colectivos dunha organización nun supertipo. Emprégase para facilitar o modelado de estruturas en organización, sendo cada tipo unha organización, empresa, rol ou papel e almacenar os datos persoais de cada membro. Situacións especiais obrigan a adaptacións deste patrón como ocorre no Party Type Generalizations que permite a xeneralización de tipos de grupo que herdan dun subtipo, por exemplo para unha persoa ten varios roles a un tempo.
- b) **Patrón de análise Accountability.** Establece unha relación de responsabilidade entre dúas partes ou perfís. Cos tipos Accountability e Accountability Type permite expresar a clase de relación entre ambos. Pode facer uso do patrón Party para obter unha maior flexibilidade. Segundo sexan as relacións pode dar lugar a patróns máis complexos como Hierarchic Accountability ou Xerarquía de responsabilidade que engade restricións aos elementos de responsabilidade; ou que ten aplicación á hora de delegar tipos de responsabilidade a un subpatrón Party.
- c) **Patrón arquitectónico MVC** (en inglés *Model View Controller*).



Estrutura un compoñente software en 3 capas, o modelo coa lóxica de negocio, funcionalidades e sistemas de información, a vista coa interface de usuario e o Controlador que recibe os eventos da entrada e coordina as actividades da vista.

- d) **Patrón arquitectónico PAC** (en inglés *Presentation Abstraction Control*). Similar ao MVC este patrón define un sistema interactivo baseado nunha xerarquía de axentes cooperantes que realizan funcionalidades concretas. Divídese en tres capas: Presentación con interacción persoa-máquina, Abstracción coa lóxica e sistemas de información e o Control que centraliza as comunicacións entre axentes, procesa eventos externos e actualiza o modelo. A principal diferenza co MVC radica en que se poden facer diferentes axentes ou subsistemas de aplicación, operando de forma independente ou xerarquizada.
- e) **Patrón arquitectónico Capas** (en inglés *Layers*). Representaría a abstracción xenérica dos patróns anteriores a un sistema multicapa, orientado cara a distribución xerárquica de roles e responsabilidades. Permite aumentar ou diminuír o nivel de abstracción, máis ou menos capas, illando o mantemento e actualización de cada capa. Cada nivel ou capa ofrece servizos á capa superior e usa os da inferior.
- f) **Patrón arquitectónico Pipes and Filters**. Orientado tamén a arquitecturas SOA, neste modelo cada compoñente posúe un conxunto de entradas e saídas. Representa a lectura de fluxos de datos, transformándoos nun fluxo de saída sen ter que procesar toda a entrada, como ocorre nos modelos Streaming e de aí que se denominen Filtros aos compoñentes que reciben as entradas e tuberías ou condutos aos que encamiñan o fluxo cara a saída. Permite representar procesamentos en paralelo así coma execución concurrente.
- g) **Patrón arquitectónico Blackboard**. Proporciona un modelo de solucións aproximadas, cando non se pode aplicar unha solución

concreta. Permite reutilizar as fontes de coñecemento e un mellor soporte de cambios e mantemento da solución aproximada.

- h) **Patrón Microkernel.** Dentro dos patróns para sistemas adaptables, este modelo separa un kernel funcional mínimo do estendido para soportar sistemas software con requirimentos que cambian ao longo do tempo. Ideado para sistemas operativos, cada un deles sería unha vista do Microkernel central, permitindo que se poida estender o sistema de xeito doado.
- i) **Patrón Reflection.** Outro patrón sistemas adaptables que modela un mecanismo para mudar a estrutura e comportamento dun sistema dinamicamente. Establece dous niveis: Metadatos para que os software leve unha descrición de si mesmo e Lóxica de aplicación. Os cambios de comportamento poden reflectirse nos metadatos, pero isto pode pasar inadvertido.
- j) **Patrón arquitectónico Broker.** Orientado a arquitecturas SOA e sistemas distribuídos onde varios clientes fan peticións a un servidor ou servizo remoto. O axente Broker encárgase de coordinar a comunicación entre o cliente e o provedor do servizo. As principais vantaxes deste patrón son permitir a transparencia de localización do servizo, permitir cambios e ampliación de novos compoñentes sen que o sistema se vexa afectado, mellora da portabilidade e interoperabilidade con outros axentes Broker.
- k) **Patrón Publisher Subscriber.** Orientado a arquitecturas SOA e sistemas distribuídos insire unha capa entre clientes e servidores que se encarga de levar conta da comunicación de xeito transparente. Representa unha arquitectura de mensaxería sen acoplamento.

No tocante ao deseño, os principais patróns acostuman a agruparse en tres grandes categorías: Patróns creacionais, estruturais e de comportamento. Os **creacionais** incluírían:



- a) **Abstract Factory.** Prove unha interface que permite a creación de familias de obxectos dependentes ou relacionadas sen ter que especificar as clases completas. Exemplos deste patrón serían os Widgets e compoñentes de interfaces gráficas.
- b) **Builder.** Construtor virtual que separa a construción dun obxecto complexo da súa representación, de tal xeito que se obteñen diferentes representación nun mesmo proceso.
- c) **Factory Method.** Patrón que define unha interface para a creación de obxectos deixando que as subclases decidan que clase instanciar, facendo que o proceso de xeración do subtipo sexa transparente ao usuario.
- d) **Prototype.** Permite a creación de novos obxectos clonándoos dunha instancia dun obxecto xa existente.
- e) **Singleton.** Patrón de instancia única que asegura que dunha clase só existirá unha única instancia definindo un punto de acceso común á mesma.
- f) **Object Pool.** Patrón para a obtención de obxectos por clonación. Crease unha instancia dun tipo de obxecto da clase a clonar. Está pensado para casos onde a creación teña un custo moi alto e se permita a utilización de obxectos xenéricos do Pool.

Por outra banda, dentro dos **estruturais**:

- a) **Adapter.** Patrón que convirte a interface dunha clase noutra interface adaptada a necesidades específicas como determinados clientes ou interfaces requiridas por compatibilidade.
- b) **Bridge.** Ou patrón Handle/Body, separa unha abstracción da súa implementación de xeito que ámbalas dúas podan mudar de forma de maneira independente, sen que cambios nunha afecten a outra.
- c) **Composite.** Patrón que permite manipular obxectos compostos coma



se de un simple se tratase. Fai uso da composición recursiva e a estruturas en forma de árbore para poder presentar unha interface común.

- d) **Decorator**. Responde á necesidade de engadir funcionalidades a obxectos dinamicamente. Crea unha xerarquía de clases onde as fillas herdan da nais as funcionalidades e incorporan as súas propias.
- e) **Facade**. Proporciona unha interface común de acceso a un conxunto de interfaces dun sistema. Facilita o emprego do sistema interno con outras interfaces de alto nivel. Os clientes só poden comunicarse a través da interface única que fai de fachada.
- f) **Flyweight**. Permite eliminar a redundancia entre obxectos que presentan a mesma información. Factoriza os atributos comúns a estes obxectos nunha clase lixeira.
- g) **Proxy**. Proporciona un punto de control de acceso ou intermediario para o control doutro(s) obxecto(s). Presenta diferentes niveis de aplicabilidade:
  - ✓ *Proxy remoto*. Representa a un obxecto remoto de xeito local, codificando a petición e argumentos antes de enviala ao obxecto remoto.
  - ✓ *Proxy virtual*. Crea obxectos de alto custe baixo demanda, con posibilidade de caché da información dos mesmos limitando os custes de acceso.
  - ✓ *Proxy de protección*. Controla o acceso a obxectos remotos comprobando que os clientes dispoñen dos permisos necesarios.
  - ✓ *Proxy de referencia intelixente*. Análogo a un punteiro con operacións adicionais sobre un obxecto para temas de concorrencia, acceso a memoria, etc...

O último bloque serían os patróns de comportamento:

- a) **Chain of responsibility**. O patrón cadea de responsabilidade



permite establecer a liña que deben levar as mensaxes, denominada cadea de obxectos receptores, permitindo que varios obxectos podan capturar unha mensaxe, como pode ser unha excepción Java. Calquera dos receptores podería responder á petición segundo o criterio establecido.

- b) **Comando ou Orde.** Patrón que encapsula unha operación nun obxecto, de xeito que se poidan facer operacións estendidas como almacenamento e colas de peticións e soporte de accións de facer e desfacer.
- c) **Intérprete.** Define unha representación para a gramática dunha linguaxe xunto co seu intérprete.
- d) **Iterator.** Patrón co obxectivo de permitir percorrer obxectos compostos como poden ser as coleccións sen necesidade de contemplar aspectos de implementación ou representación interna dos mesmos. Define unha interface onde se ofrecen diferentes métodos para percorrer o obxecto complexo.
- e) **Mediador.** Define un obxecto que facilita a interacción entre outros de distinto tipo, coordinando a comunicación entre eles. O obxectivo é encapsular a interacción deses obxectos para evitar o acoplamento entre eles.
- f) **Memento.** Representa o estado dun obxecto ou sistema complexo para permitir o seu almacenamento e modificación, de xeito que se poida restaurar volvendo a estados anteriores no tempo.
- g) **Observador.** Permite definir unha dependencia dun a moitos, de xeito que eventos ou modificacións de estado disparen a notificación dos cambios a todos os obxectos ou sistemas dependentes.
- h) **Estado.** Emprégase para permitir que un obxecto cambie o seu comportamento no caso de modificarse o seu estado. Deste xeito diferentes clases poden representar a un mesmo obxecto ao longo do



tempo.

- i) **Estratexia.** Permite definir unha familia de algoritmos ou métodos de resolución, permitindo seleccionar dinamicamente cales aplicar e que deste xeito sexan intercambiabiles.
- j) **Template Method.** Define o esqueleto dun algoritmo para unha operación, delegando partes do mesmo ás clases concretas. Deste xeito as subclasses poden redefinir pasos concretos do método de resolución.
- k) **Visitor.** Representa un algoritmo ou operación realizada sobre a estrutura dun obxecto, permitindo a definición de novas operacións sen altera o tipo dos elementos sobre os que se realiza a operación.

Nunha última categoría poderían incluírse os patróns propias de linguaxes de programación ou tecnoloxías concretas, sendo os **patróns JEE**, a maioría Core J2EE Patterns, aqueles cun uso máis estendido dentro do mundo dos servidores de aplicacións e os servizos web:

- a) **Intercepting Filter.** Intercepta as peticións da capa de presentación antes ou despois do seu procesamento permitindo realizar operacións sobre os datos como auditorías, comprobacións de seguridade, conversións ou validacións. Permiten conectarse en fervenza e activar ou desactivar sen que afecte ao funcionamento xeral dunha aplicación. Permite diferentes estratexias como: Custom Filter, Estándar, Base Filter e Template Filter.
- b) **Front Controller.** Centraliza o control das peticións da capa de presentación, dirixíndoas cara o compoñente axeitado para validación de parámetros, invocación de elementos da lóxica de negocio, etc... Un controlador encárgase de recoller as peticións e factorizar o código repetitivo.
- c) **View Helper.** Prove unha clase que engloba código común, con aplicación tanto para a capa de negocio como para a de

presentación. Cada vista contén código para formato, delegando as responsabilidades de procesamento nas clases de axuda implementadas como Java Beans ou Custom Tags. Así mesmo poden almacenar modelos de datos intermedios facendo adaptacións previas do negocio, como conversións ou validacións, o lóxico pola separación en capas é que estas operacións non sexan moi complexas.

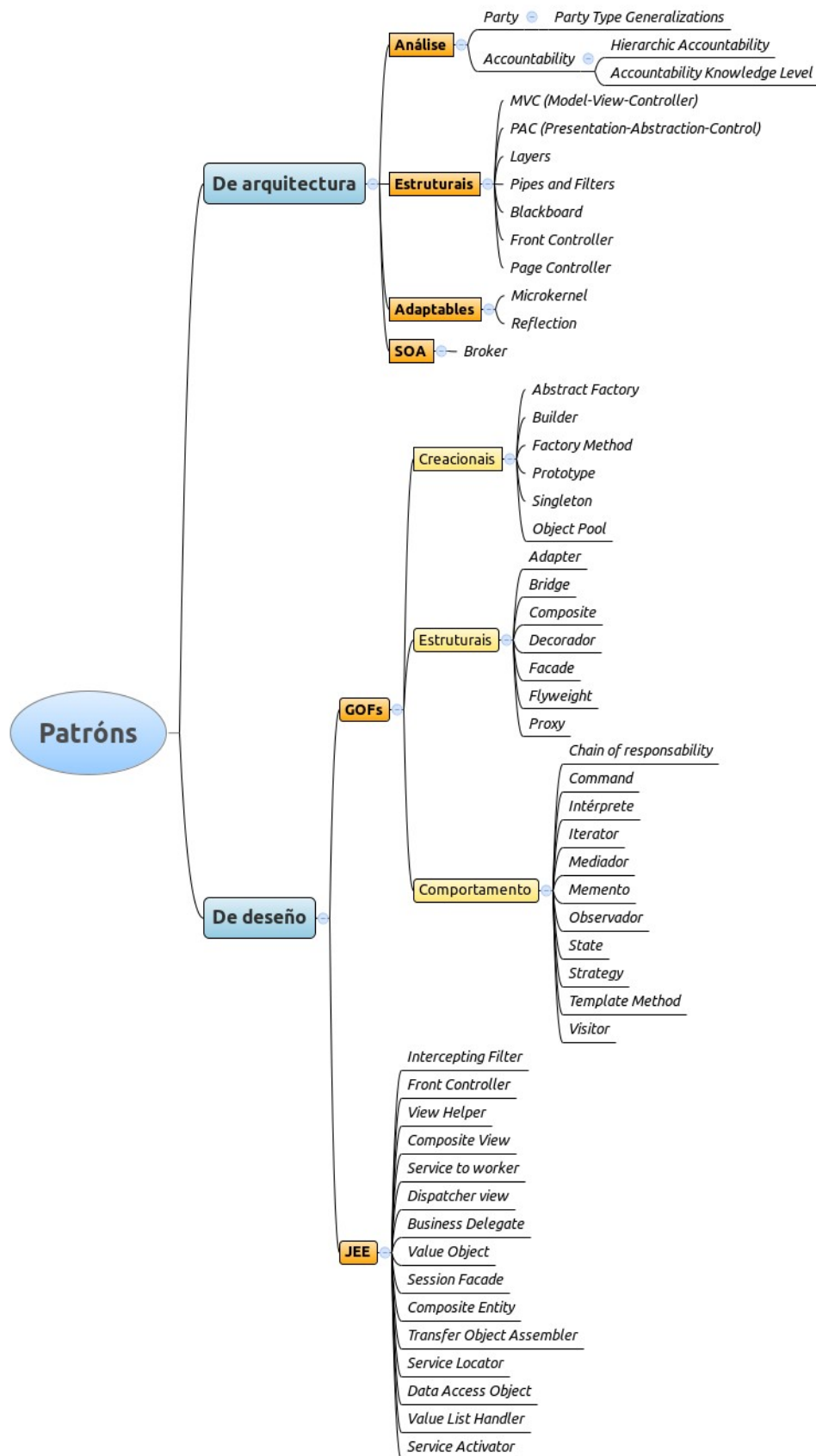
- d) **Composite View.** Define unha xerarquía de vistas compostas de diferentes vistas particulares permitindo modificar as partes en tempo de execución e a partir de modelos. Deste xeito inclúense dinamicamente as vistas concretas en vistas compostas da aplicación a través dos mecanismos que dispoñen para tal efecto JSP e Servlets.
- e) **Service to worker.** Agrupa varios patróns a modo de *framework* para permitir combinar un controlador (Front Controller), e un Dispatcher ou controlador de vistas (View Helper), para manexar as peticións dos clientes e xerar a presentación dinamicamente como resposta. Os controladores solicitan o contido aos Helpers que enchen o modelo de negocio intermedio.
- f) **Dispatcher View.** Cunha estrutura similar á do Service to worker, neste modelo tanto Controlador como Dispatcher teñen responsabilidades máis limitadas xa que lóxica de procesamento e control da vista son básicas.
- g) **Business Delegate.** Permite a abstracción a implementación de compoñentes complexos como EJB ou JMS da capa de presentación. Deste xeito poden crearse clases Proxy que almacenen e encolen as peticións podendo proporcionar control de prioridades, xestión de excepcións ou caché. O patrón emprega un compoñentes denominado Lookup Service, responsable de ocultar os detalles de implementación do código de busca dentro da lóxica de negocio.



- h) **Value Object (VO).** Encapsula un conxunto de datos que representan un obxecto ou entidade do negocio. Cando se solicita a un Bean un conxunto de información este pode crear o obxecto Value Object e encher os seus atributos para devolvelo ao cliente.
- i) **Session Facade.** Emprega un Bean de sesión como fachada para encapsular as interaccións dos compoñentes de negocio e ofrecer un servizo de acceso uniforme, a través dos interfaces requiridos unicamente a través dos casos de uso. Proporciona unha abstracción de alto nivel implementada a modo de Bean.
- j) **Composite Entity.** Permite ampliar os Beans de entidade cando estes son de pequeno tamaño, deste xeito poden aumentarse mantendo a compatibilidade. O abuso deste patrón considérase un antipatrón xa que pode dar lugar a estruturas moi complexas. Un Bean Composite Entity representa un grafo de obxectos, por tanto debe empregarse con coidado.
- k) **Transfer Object Assembler.** Simplifica o acceso aos sistemas de información a través dun conector común. Cada obxecto de negocio terá un Transfer Object (TO) cos detalles de acceso a datos (Beans, JDO, JDBC, ...) e un Bean de sesión funcionará como interface común.
- l) **Service Locator.** Emprégase para abstraer a utilización de JNDI a través dun obxecto Service Locator e para ocultar as complexidades da creación do contexto inicial, así como da busca e instanciación de EJBs a través dun punto de acceso común.
- m) **Data Access Object (DAO).** Emprégase un obxecto como medio de acceso a sistemas de información, en especial Bases de datos. Abstrae e encapsula as operacións relacionadas coa tecnoloxía de persistencia empregada (JDBC, JDO, LDAP, Beans, TopLink, Hibernate, iBATIS, etc...). Controla os parámetros de conexión, obtención de datos e almacenamento proporcionando unha interface de acceso

común.

- n) **Value List Handler.** Implementado coma Beans de sesión, encárgase de manexar a execución de consultas SQL, cachealas e procesar os resultados. Accede directamente a un DAO que se encarga á súa vez de facer a conexión co sistema de información e recuperación dos datos. Unha vez obtidos almacénaos como TO ou VO permitindo ao cliente percorrelos grazas á implementación do patrón Iterador.
- o) **Service Activator.** Proporciona un modelo para mensaxería asíncrona como JMS. O Service Activator recibe as mensaxes e localiza e chama aos métodos dos compoñentes de negocio que se van encargar de resolver a petición.





***Figura 1: Resumo dos principais patróns en arquitecturas de servidores de aplicacións.***

A implementación destes patróns non acostuma a facerse a medida senón que se recorre aos **frameworks**. Moi relacionados entre si, os *frameworks* representan unha arquitectura de pequeno tamaño que proporciona unha estrutura xenérica integrando diferentes patróns de xeito que poidan ser reutilizados ou integrados de xeito doado nas aplicacións. Nun *framework* os patróns teñen unha implementación concreta sobre a definición abstracta do patrón. En última instancia son un conxunto de clases e interfaces que cooperan para ofrecer un software reutilizable.

### **31.3 MVC**

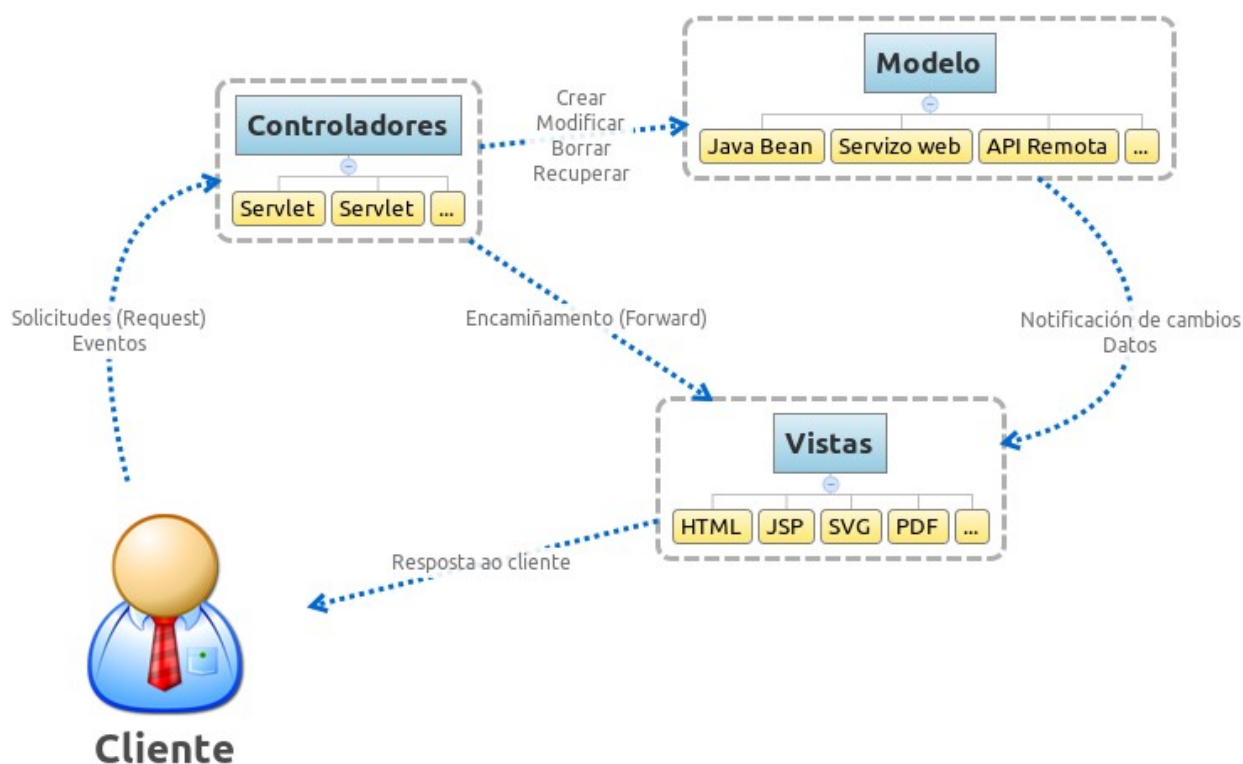
O patrón Modelo-Vista-Controlador é o máis empregado para estruturar unha aplicación atendendo a unha correcta separación en capas: entrada, procesamento e saída. As súas principais **vantaxes** son unha redución do acoplamento, facilidade de desenvolvemento, claridade no deseño, mellora no mantemento, maior escalabilidade, unha maior cohesión con cada capa fortemente especializada, e unha maior flexibilidade e axilidade nas vistas, permitindo a súa modificación dinámica, sincronización, aniñamento e a existencia de múltiples vistas.

As **capas** do modelo concrétanse en:

- 1) **Modelo** (en inglés *Model*). Encapsula tanto datos como as funcionalidades ou casos de uso. Ten que funcionar independentemente de calquera representación que tomarán os datos na saída e calquera comportamento que se especifique na entrada do sistema. A todos os efectos será unha caixa negra que

recibe peticións de devolve resultados, encargándose de manexar os datos e controlar as súas transformacións. Normalmente implementa os patróns DAO, VO e Fachada.

- 2) **Vista** (en inglés *View*). Capa na que se integran todos os compoñentes que afecten á interface de usuario. Recibe as peticións do usuario e as envía cara o controlador, obtendo deste as respostas. Permítense múltiples vistas do mesmo modelo, pero toda a lóxica de presentación debe ir nesta capa.
- 3) **Controlador** (en inglés *Controller*). Recibe peticións da vista, tales como eventos, refrescos, etc... que recolle cun xestor de eventos ou Handler e son traducidos a solicitudes de servizos ou casos de uso, enviando as peticións ao modelo. A miúdo implementan patróns como Comando ou Front-Controller para encapsular as accións.



**Figura 2: Modelo-Vista-Controlador con tecnoloxías JEE.**





Como patrón de arquitectura o MVC pode conter á súa vez os seguintes **patróns** de deseño:

- ✓ **Observador.** Para prover o mecanismo de publicación e subscripción que permita notificar cambios do modelo nas vistas.
- ✓ **Composite View.** Para permitir a creación de vistas compostas nunha xerarquía.
- ✓ **Estratexia.** Para levar conta da relación entre as vistas e os controladores, xa que permite modificar dinamicamente aspectos do control.
- ✓ **Factory Method.** Para especificar ao controlador unha vista coma predeterminada.
- ✓ **Decorador.** Para engadir funcionalidades adicionais ás vistas.
- ✓ **Proxy.** Para distribuír a arquitectura en diferentes emprazamentos e mellorar características de rendemento.

O modelo MVC impleméntase tanto en *frameworks* .NET (Windows Forms, ASP .NET, Spring .NET, Maverick .NET, MonoRail, ...) como en JEE (Struts, Spring, Tapestry, Aurora, JSF, etc..). Así mesmo é un modelo que se atopa estendido a moitas outras tecnoloxías coma PHP, Ruby, Perl, Python, etc ...

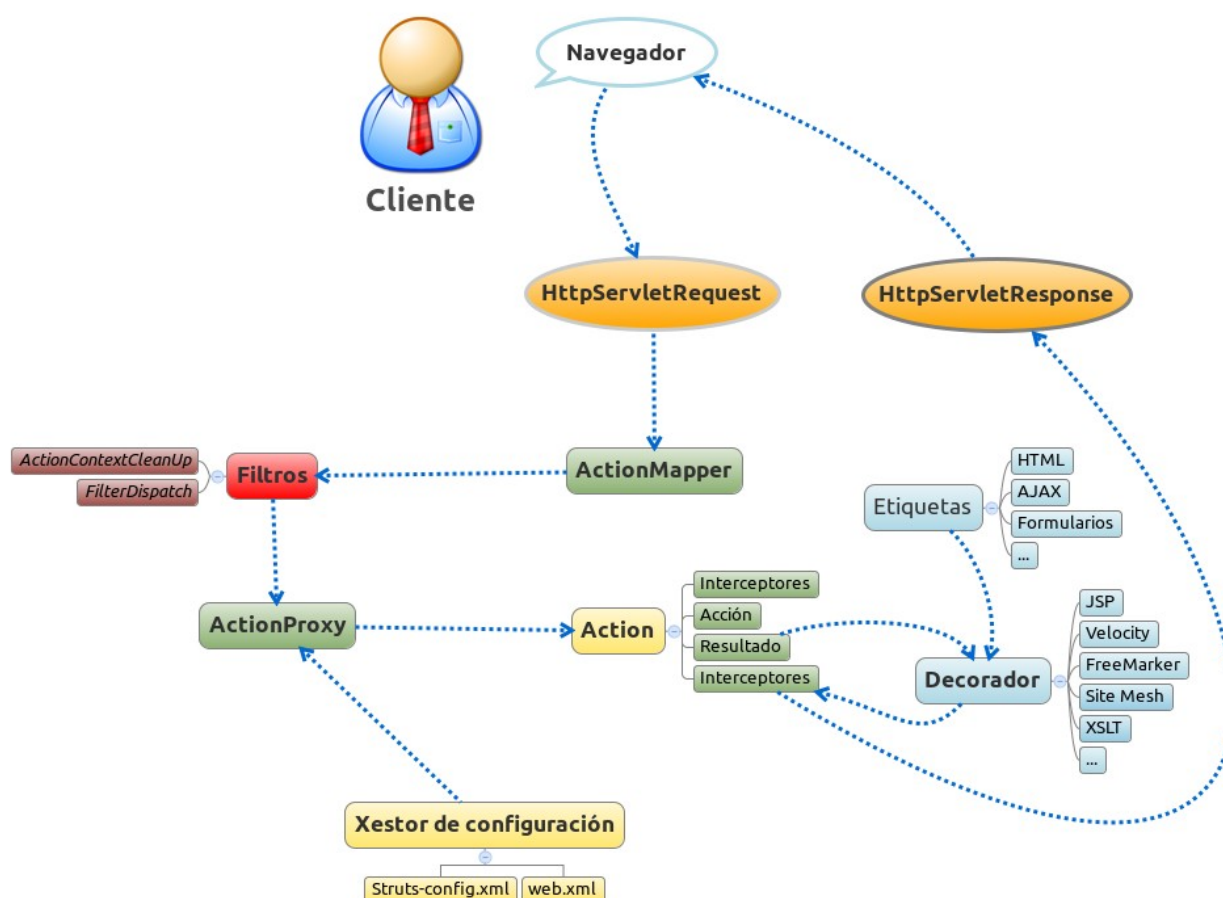
Os *frameworks* que implementan o MVC acostuman presentar unha serie de **características xerais**, comúns a todos eles e que inclúen:

- ✓ Implementación de diferentes patróns de deseño orientados á reutilización de deseño e código.
- ✓ Controis de validación de campos de formularios.
- ✓ Control de erros e excepcións.
- ✓ Mensaxería e localización de cadeas de textos.
- ✓ Librarías de etiquetas ou compoñentes (TagLibs, Widgets, etc...)
- ✓ Compoñentes da Interface de Usuario como etiquetado de compoñentes de formularios, pestanas, controis AJAX, etc...
- ✓ Presentación de información a través de listados e táboas con paxinación.

- ✓ Integración con *frameworks* co patrón Decorador ou baseados en modelos como Tiles, FreeMarker, Velocity, etc...
- ✓ Acceso datos en diferentes Sistemas de Información: Bases de datos, XML, etc...
- ✓ Abstracción de enderezos URL, Request e sesións.
- ✓ Autenticación e control de usuarios, roles e filtros.

Entre os frameworks que implementan o MVC destaca Apache Jakarta **Struts** (que ten unha evolución en Struts 2.0 ao fusionalo con WebWork), un dos máis empregados en tecnoloxías JEE e que resulta case un estándar de facto debido á súa integración noutros *frameworks* con máis funcionalidades. Emprégase para a implementación de aplicacións web baseadas en Servlets e JSP. Proporciona un conxunto de etiquetas JSP personalizadas (en inglés *Custom Tags*) que permiten encapsular funcionalidades na vista. Co modelo de Struts ten implantación directa o modelo MVC e outros patróns de deseño pre-construídos, permitindo a configuración directa de obxectos reutilizables perante a configuración de XML. Ademais proporciona as características anteriormente especificadas: validación, localización, modelos, etc...

Transporta automaticamente os datos inseridos polo cliente ata o controlador a través de Accións (en inglés *Actions*) mediante formularios ActionForms integrados no *framework* e vice versa para a súa presentación. Distingue entre unha parte común a calquera aplicación que faga uso do *framework* que fai de Controlador (ActionServlet) e outra parte configurable a través de arquivos de configuración en XML (struts-config.xml, web.xml, ...). A súa principal desvantaxe é non abarcar ata o nivel de acceso a datos, facendo que sexa necesario o emprego doutros *frameworks* especializados nesta capa para a elaboración de DAO, VO e outras operación complementarias.



**Figura 3: Funcionamento interno Struts/Struts 2.0.**

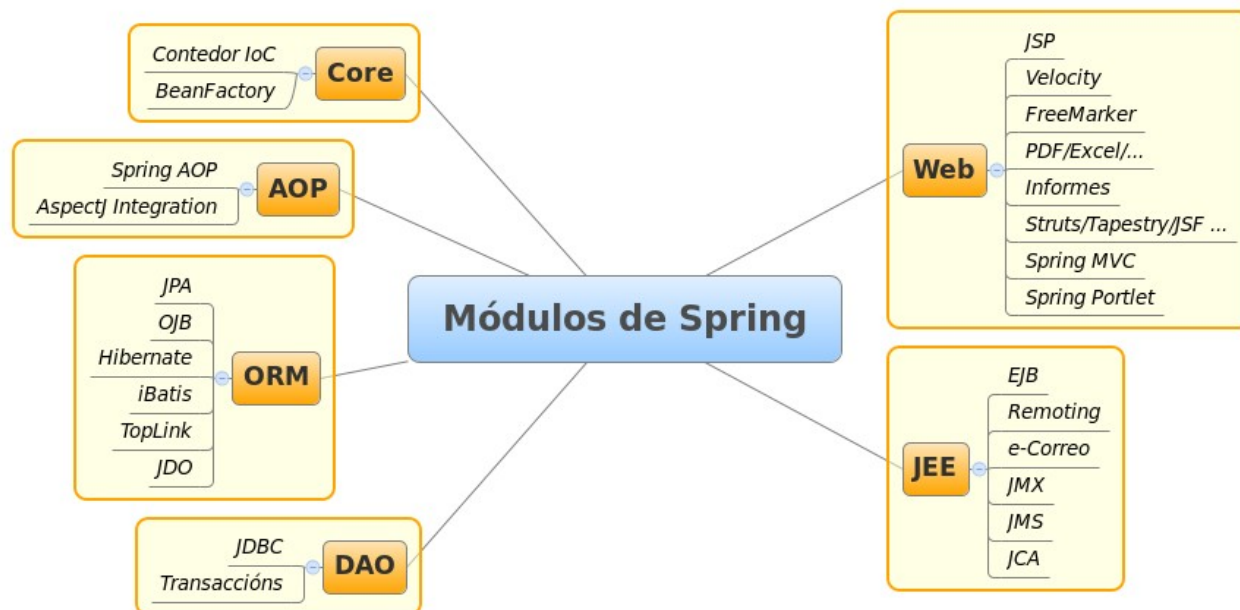
A principal alternativa a Struts sería **Spring** Framework, aínda que tamén permiten integración conxunta e con outros *frameworks* como JSF, Tapestry ou WebWork. Aínda que a súa orientación principal sexa a plataforma JEE, está dispoñible en .NET a través do *framework* Spring .NET. Ten soporte para JTA, JDO, JDBC e ODBC, e permite integración con terceiros como Acegi, Hibernate, iBatis e OJB. Como novidade permite programación orientada a aspectos ou AOP (en inglés *Aspect-Oriented Programming*) que busca empregar os servizos secundarios como seguridade, rexistro de log, manexo de transaccións, etc... das funcionalidades do modelo. Con AOP poden empregarse os servizos da aplicación de forma declarativa, ou perante arquivos XML de configuración ou mediante estándares JSR. Así mesmo realiza Inversión de Control ou IoC, que promove o baixo



acoplamento a partir da inxección de dependencias entre obxectos. As principais desvantaxes de Spring son que implica unha configuración complexa, xa que cada servizo leva o seu XML propio, aínda que existe a alternativa do JSR. O seu contedor non resulta lixeiro o que impide que teña aplicación práctica nalgúns contornos como poden ser os dispositivos móbiles.

A **arquitectura de Spring** está composta polos seguintes compoñentes:

- ✓ **Core.** O núcleo que aloxa o contedor principal ou BeanFactory.
- ✓ **Módulo AOP.** Prove a implementación de AOP, permitindo desenvolver interceptores de método e puntos de ruptura para desligar o código do modelo das funcionalidades transversais.
- ✓ **Módulo DAO.** Prove a capa de abstracción de acceso a datos e sistemas de información sobre os diferentes conectadores dispoñibles. Ademais prove de manexo de transaccións vía AOP e outros servizos.
- ✓ **Módulo ORM.** Prove integración para as distintas API de correspondencia entre obxectos e entidades de bases de datos con soporte de diferentes tecnoloxías e integración con *frameworks* de terceiros.
- ✓ **Módulo JEE.** Integración con aplicacións e servizos JEE.
- ✓ **Módulo Web.** Aporta compoñentes especiais orientados a desenvolvemento web e integración con *frameworks* alternativos como Struts ou JSF, ademais dunha implementación do paquete Spring MVC.

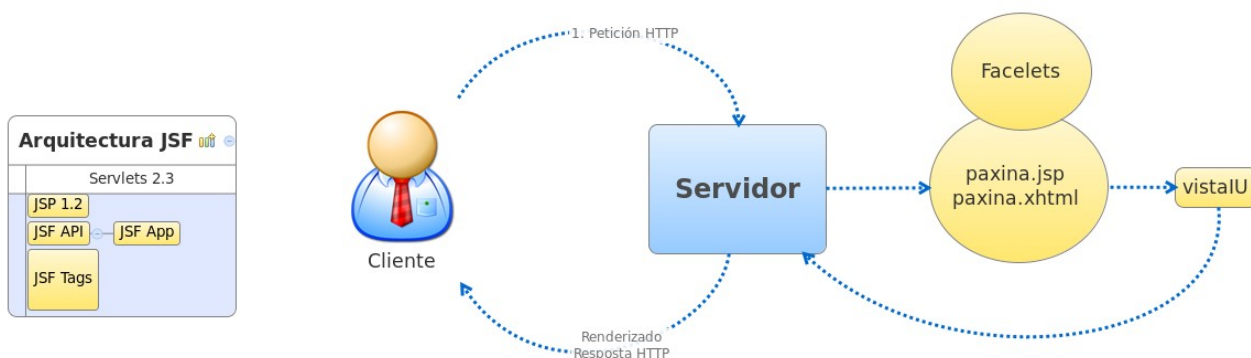


**Figura 4: Arquitectura de Spring.**

### 31.4 JSF

A tecnoloxía Java Server Faces proporciona un *framework* de interface de compoñentes de usuarios para o lado do servidor de aplicacións. Na súa base emprega JSP pero permite outras tecnoloxías para interfaces de usuario como XUL. Entres os **compoñentes** de JSF atópanse:

- 1) Un conxunto de APIs para representar e manexar compoñentes da interface de usuario. Entre as opcións que xestionaría atoparíanse control de estado e eventos, validacións de formularios, conversión de datos, control de navegacións e soporte de localización e accesibilidade.
- 2) Un conxunto de compoñentes da interface de usuario reutilizables.
- 3) Dúas librarías de etiquetas personalizadas (en inglés *Custom Tags*) para JSP.
- 4) Modelo de eventos para o lado do servidor.
- 5) Soporte para Managed Beans de control de eventos.



**Figura 5: Arquitectura JSF e funcionamento básico.**

Un dos compoñentes de JSF é o *framework* JavaServer **Facelets**, destinado á xestión de modelos (en inglés *templates*). As principais características deste *framework* son:

- ✓ Custe de tempo cero para o desenvolvemento de etiquetas de compoñentes da Interface de Usuario.
- ✓ Facilitade de creación de modelos de páxinas e compoñentes reutilizables.
- ✓ Soporte para UEL (en inglés *Unified Expression Language*) e validacións EL.
- ✓ Compatibilidade con calquera RenderKit.
- ✓ Intégrase plenamente con JSTL cousa que en JSF pode ocasionar problemas.
- ✓ Compilación máis rápida que con JSP.

Actualmente existen numerosas **implementacións** de JSF que poden complementar á especificación oficial JEE. Existe a posibilidade de combinar diferentes implementación nunha mesma aplicación, sendo as máis habituais:



- a) **MyFaces Tomahawk/Sandbox.** Desenvolvido por Apache proporciona un conxunto de compoñentes reutilizables compatibles coas especificacións JSF 1.1, JSF 1.2 e JSF 2.0.
- b) **Trinidad.** Subproxecto de MyFaces, a partir da inclusión dos compoñentes ADF Faces e outras melloras. Prove dos seguintes elementos: Unha implementación de JSF, varias librarías de compoñentes Widgets, a extensión MyFaces Orchestra e módulos de integración para outras tecnoloxías e estándares como MyFaces Portlet Bridge.
- c) **Tobago.** Outro proxecto baseado en MyFaces nunha aproximación do deseño de páxinas web ao de aplicacións de escritorio. Proporciona unha serie de compoñentes da Interface de Usuario como abstraccións do HTML. Presenta un conxunto de temas para clientes HTML con vistas independentes de HTML/CSS/Javascript.
- d) **ICEfaces.** Contén diversos compoñentes de interfaces de usuario enriquecidas baseadas en AJAX e compatibles con SSL, como editores de texto, reprodutores multimedia, etc... Soporta Facelets e Seam, ademais de ser compatible con Spring, WebWork e Tomahawk.
- e) **RichFaces.** Outro *framework* AJAX que inclúe ciclo de vida, validacións, conversións e xestión de recursos nas aplicacións. Soporta Facelets e Seam, ademais de ser compatible con Spring e Tomahawk.
- f) **Ajax4JSF.** Outra alternativa máis que proporciona un *framework* AJAX que inclúe ciclo de vida, validacións, conversións e xestión de recursos nas aplicacións. Soporta Facelets e Seam, ademais de ser compatible con Spring e Tomahawk. Inclúe os seguintes compoñentes:
  - ✓ *Ajax Filter.* Filtro de peticións para AJAX.
  - ✓ *Ajax Action Components.* Envían as peticións dende o cliente.
  - ✓ *Ajax Containers.* Interface que describe zonas dentro das JSP.

- ✓ *Javascript Engine*. Motor no lado do cliente que actualiza diferentes zonas das JSP en función da resposta AJAX.

### 31.5 ANTIPATRÓNS

Contrarios ao **concepto** de patróns, os antipatróns representan malos usos habituais, ou solucións que, sobre todo ao longo do tempo, presentan máis problemas dos que resolven, trátase en definitiva de malas prácticas. Existen dúas variantes principais, os que describen unha mala solución para un problema habitual e que produce consecuencias difíciles de arranxar ao longo do tempo; e aqueles que describen como poñer remedio a un problema e convertelo nunha boa solución. Por norma xeral os antipatróns vense como unha boa idea ao comezo, que falla de mala maneira á hora da súa implementación.

As **motivacións** ou razóns para ter en conta os antipatróns como caso de estudo atenden aos seguintes puntos:

- ✓ Permiten identificar solucións de risco para problemas habituais.
- ✓ Proven experiencia do mundo real para detectar problemas que se repiten ao longo do tempo, ofrecendo posibles solucións ou alternativas para as súas implicacións máis habituais.
- ✓ Proven dun marco común para a identificación e documentación dos problemas e deseño das solucións.

Como acontecía cos patróns, os antipatróns acostuman a agruparse en diferentes **categorías**, sendo as principais:

- 1) **Antipatróns de desenvolvemento software**. Definen problemas asociados ao desenvolvemento software a nivel de aplicación, ao



nivel dos patróns de deseño.

- 2) **Antipatróns de arquitectura de software.** Céntranse na distribución e relacións das aplicacións, servizos e outros compoñentes software a nivel de organización.
- 3) **Antipatróns de xestión de proxectos software.** Identifican escenarios críticos sobre a comunicación entre persoas e a resolución de problemas en equipos, vendo como afectan a un proxecto ou proceso software.

Así mesmo os antipatróns teñen aplicación en moitas outras áreas como metodoloxía, xestión da configuración, TDD, deseño web, accesibilidade, usabilidade, etc...

Dentro dos **antipatróns de desenvolvemento** software atopámonos entre os máis comúns:

- a) **Blob ou obxecto todopoderoso** (en inglés *God Object*). Emprégase un único obxecto, clase ou módulo para aglutinar un amplo conxunto de funcionalidades que deberían atoparse divididas. Con este patrón cáese nun código amplamente desorganizado e moi acoplado.
- b) **Fluxo de lava ou lava seca** (en inglés *Lava Flow*). Representa aqueles tipos de programación por impulsos ou erupcións de código, de xeito desestruturado, desorganizado e con pouca documentación. O sistema medra de xeito desproporcionado e pasado un tempo os bloques de código máis antigos considéranse metaforicamente solidificados no tocante á dificultade de solucionar calquera tipo de problema no que se atopen involucrados.
- c) **Descomposición funcional.** Deseño non orientado a obxectos, froito da migración dende linguaxes estruturadas a POO.



- d) **Poltergeists.** Ou clases pantasma debido ao descoñecemento dentro da aplicación de cal é o obxectivo dalgunhas clases, sendo en moitos casos súa única función transmitir información entre clases.
- e) **Martelo dourado.** Empregar a mesma solución para calquera problema que xorda, sen contemplar outras posibles alternativas.
- f) **Código spaghetti.** Fai referencia a código de aplicación cunha estrutura complexa e incomprensible con multitude de tecnoloxías mesturadas. A analoxía faise a partir das relacións entre o código que semellan un grande número de fíos mesturados e enrolados.
- g) **Programación copiar e pegar.** Solución na que en lugar de crear solucións xenéricas cópanse e adáptanse solucións xa existentes.

No tocante aos **antipatróns de arquitecturas** software destacan por ser os máis habituais:

- a) **Reinventar a roda.** Implementar compoñentes xa dispoñibles ou que poden aproveitarse con lixeiras modificacións. Dáse pola tendencia a facer todo un mesmo ou o descoñecemento da arquitectura e solucións dispoñibles no mercado ou alternativas de código aberto.
- b) **Vendor Lock-In.** Construír unha arquitectura dependente dun produto de terceiros, en especial cando se trata de software privativo. Ponse en perigo a escalabilidade do sistema e aumentan os custes de mantemento.
- c) **Illamento na organización.** Nunha mesma organización ou conxunto de sistemas créanse diferentes unidades illadas entre si que medran en paralelo solucionando problemas comúns de xeito



independente. Neste modelo pode medrar sobre maneira o custe de integración chegada a necesidade do mesmo.

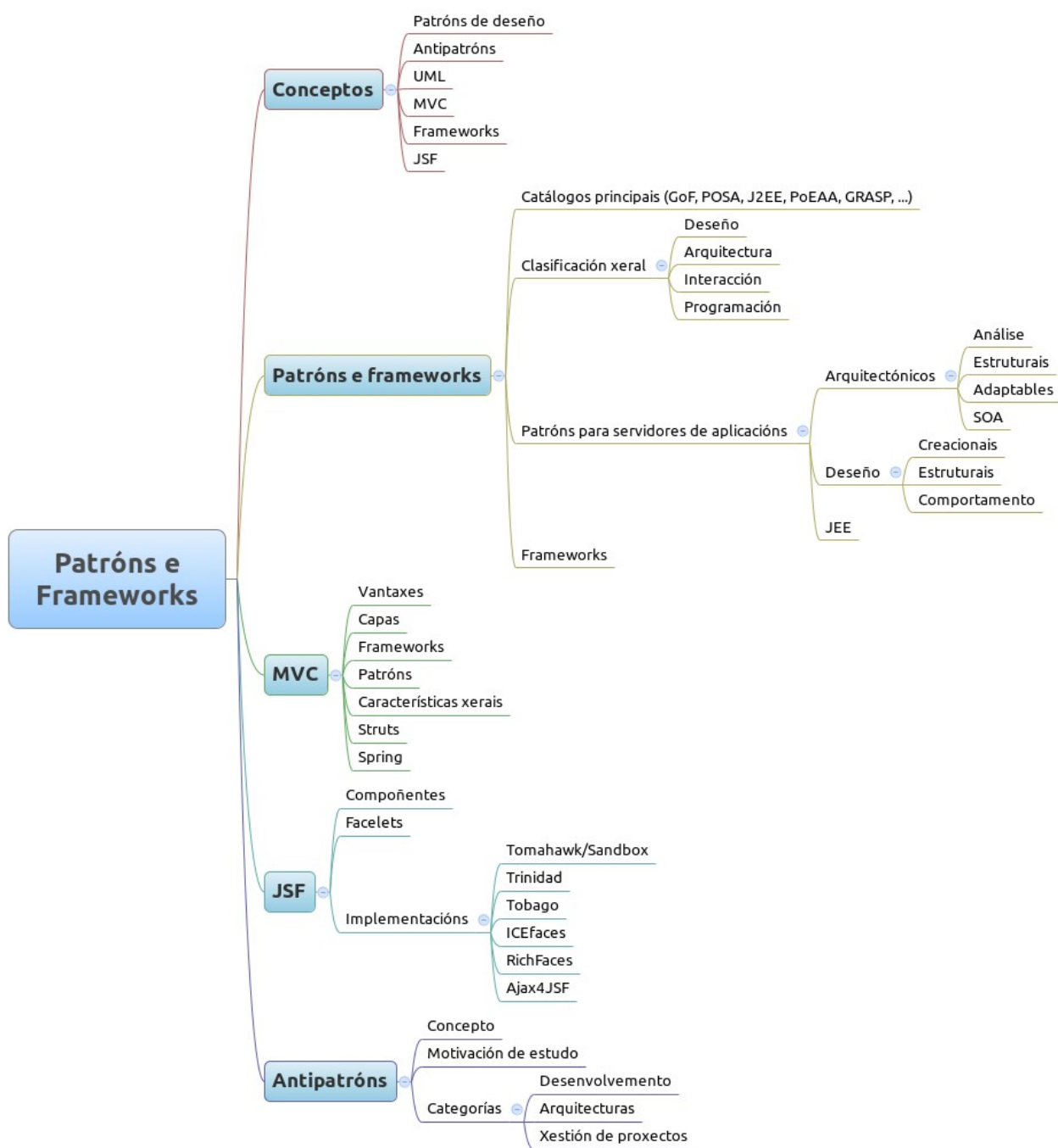
- d) **Deseño por comité.** Demasiadas persoas participan dos requirimentos do proxecto dando lugar a un deseño demasiado abstracto e excesivamente complexo por mor de contemplar demasiados puntos de vista particulares. Complícase a toma de requisitos dando a lugar a demasiadas reunións de longa duración, que dificultan e provocan erros ao longo de todo o ciclo de vida de desenvolvemento.
- e) **Arquitectura por implicación.** Non existe documentación da arquitectura do sistema, nin dos procesos, nin das tarefas automatizadas máis habituais.

No tocante aos **antipatróns de xestión de proxectos** software destacan por ser os máis habituais:

- a) **Parálise de análise.** Os procesos de análise e deseño prolóngase tanto que o proxecto remata morrendo nel sen chegar a implementarse. Son desenvolvementos opostos aos modelos baseados en prototipos e iterativos.
- b) **Morte por planificación.** Demasiada planificación e reunións sen chegar a concretar puntos de partida para o desenvolvemento. De novo son desenvolvementos opostos aos modelos baseados en prototipos e iterativos.
- c) **Persoas problemáticas** (en inglés *corncob*). Persoas difíciles de participar en equipos, ou con pouca capacitación ou aptitude, obstrúen, desvían e mesmo sabotan o desenvolvemento.
- d) **Xestión irracional.** A falta de decisión e capacitación sumado á nula planificación poden dar lugar á toma de decisións con posterioridade e desenvolvementos de urxencia.
- e) **Proxectos sen xestión.** Non se atende ao análise e o deseño, só a

implementación. Vanse arranxando incidencias segundo acontecen en modo pila, as últimas primeiro.

### **31.6 ESQUEMA**



### **31.7 REFERENCIAS**

Deepak Alur e outros.

Core J2EE Patterns. Best Practices and Design Strategies. (2003).

William Crawfor e Jonathan Kaplan.

J2EE Design Patterns. (2003).

Steven Metsker e William Wake.

Design Patterns in Java. (2006).

**Autor: Juan Marcos Filgueira Gomis**

**Asesor Técnico Consellería de Educación e O. U.**

**Colegiado del CPEIG**

## **32. APLICACIÓNS DA INTERNET ENRIQUECIDAS (RIA). ENXEÑARÍA DO SOFTWARE.**

## **TEMA 32. APLICACIÓNS DE INTERNET ENRIQUECIDAS (RIA).**

### **32.1 INTRODUCCIÓN E CONCEPTOS**

### **32.2 AJAX**

### **32.3 RIA PARA MULTIMEDIA E ANIMACIÓNS**

### **32.4 OUTRAS TECNOLOXÍAS RIA**

### **32.5 ESQUEMA**

### **32.6 REFERENCIAS**

### **32.1 INTRODUCCIÓN E CONCEPTOS**

As aplicacións de Internet enriquecidas ou **RIA** (en inglés *Rich Internet Applications*), son un conxunto de tecnoloxías que buscan achegar as interfaces das aplicacións web ás das aplicacións de escritorio dotándoas de novas funcionalidades, de aí a riqueza, e axilizando aspectos como as recargas de datos. Por norma xeral precisan dun *framework*, compoñente adicional ou *plug-in* no navegador que permitan a súa interpretación. Nas aplicacións RIA a maior parte da comunicación faise de maneira asíncrona en comunicacións transparentes ao usuario que evitan gran parte das recargas de páxinas para realizar actualizacións de datos. Fronte a estas vantaxes no tocante á usabilidade en canto a mellora das funcionalidades e actualizacións de datos a principal desvantaxe será a accesibilidade da páxina para usuarios que presenten dificultades de acceso á información na web.

Moitas destas **tecnoloxías** pertencen ao mundo do software propietario atopando gran dependencia respecto das compañías que as desenvolven. As principais tecnoloxías atópanse nas plataformas Flash, Flex e AIR de Adobe, Silverlight de Microsoft, OpenLaszlo, incontables *frameworks* AJAX e Javascript, e outras tecnoloxías como as xa maduras, Applets e Java WebStart e as emerxentes como XUL, JavaFX, GWT ou Bindows. Calquera



destas tecnoloxías localízase na capa de vista, usuario ou cliente como complemento á (X)HTML/CSS e intégranse coas tecnoloxías de servidores de aplicacións como .NET/JEE.

Dentro dos **casos de éxito** desta tecnoloxía, actualmente a maior parte das aplicacións e servizos web globais de maior uso dentro da Web 2.0 fan uso de tecnoloxías RIA nas súas interfaces, sendo Google Maps, Gmail, Flickr, Meebo, Orkut, e un longo etcétera.

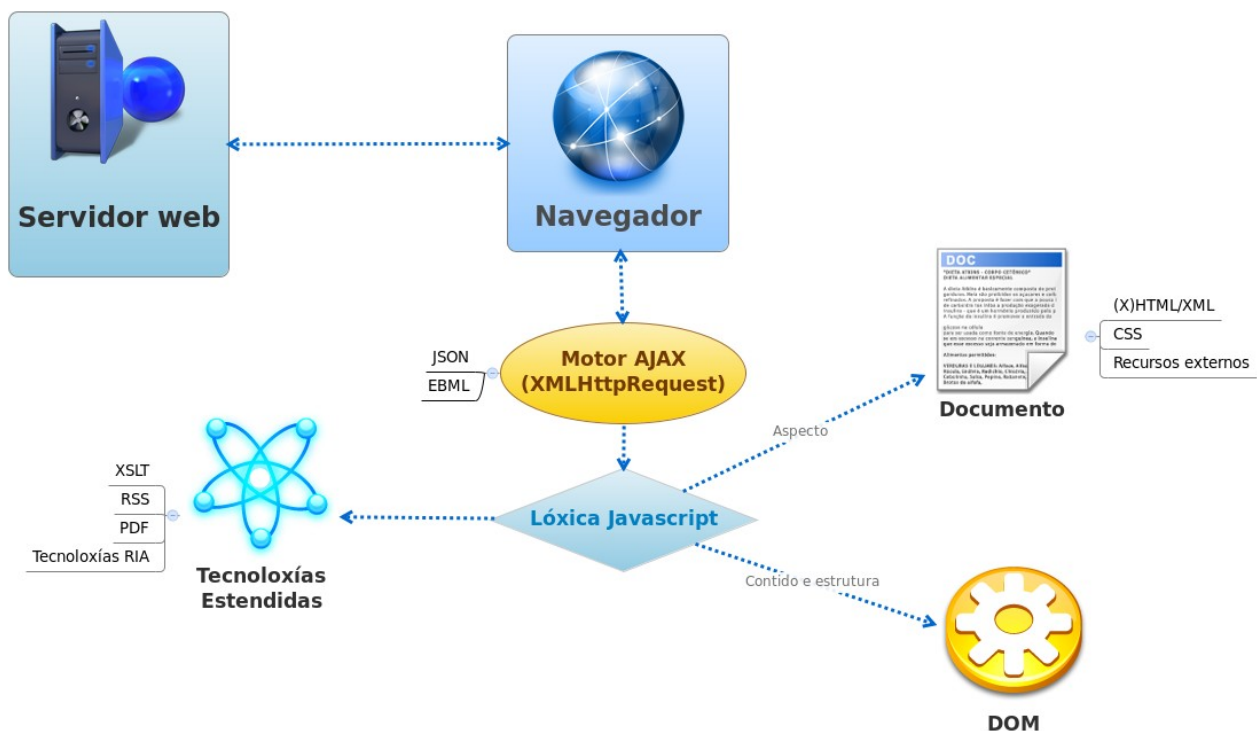
### **32.2 AJAX**

**AJAX** (en inglés *Asynchronous JavaScript And XML*), Javascript Asíncrono e XML, orixínase para aproveitar que a comunicación entre o usuario e a interface non é fluída permitindo realizar comunicacións asíncronas co servidor e realizar así un maior aproveitamento do ancho de banda e obter unha maior velocidade de resposta. Os datos cárganse nun segundo plano sen afectar á interface. AJAX non representa unha tecnoloxía en si mesma, senón que se trata da combinación dun grupo de **tecnoloxías** xa existentes:

- ✓ (X)HTML e CSS para o deseño das páxinas web.
- ✓ DOM (en inglés *Document Object Model*), ou Modelo de Obxectos do Documento, API que representa un conxunto de obxectos para manipular e modificar dinamicamente documentos (X)HTML e XML a través de linguaxes de Script como Javascript, JScript ou ECMAScript.
- ✓ Obxectos dos tipos Iframe ou XMLHttpRequest para intercambiar datos de maneira asíncrona co servidor.
- ✓ XML para os formatos de intercambio de datos e comunicacións a través de JSON ou EBML.
- ✓ Outras tecnoloxías para facilitar a implantación de solucións específicas como XSLT, RSS, PDF ou outras tecnoloxías RIA.
- ✓ Javascript para proporcionar o nexo común a todo o conxunto.

Como acontece coas tecnoloxías RIA en xeral, é requisito que o navegador teña **soporte** para o conxunto de tecnoloxías AJAX, doutro xeito habería que proporcionar unha alternativa HTML básica. Aínda así cada vez atópase soportado por un maior número de navegadores e non require a instalación de complementos.

O **funcionamento básico** de AJAX baséase no obxecto de comunicación asíncrona, por exemplo o XMLHttpRequest, que se instala cunha librería, *framework* ou motor AJAX no lado do cliente. O motor AJAX proverá os métodos para permitir a comunicación asíncrona de datos ademais de definir os compoñentes reutilizables AJAX coa definición do seu comportamento, e o contido e estrutura xeral do documento. O feito de realizar todas estas funcións dende o cliente de maneira asíncrona supoñen a gran mellora de rendemento de AJAX sobre o modelo tradicional de desenvolvemento web.



**Figura 1: Funcionamento básico de AJAX.**

A **refactorización** de aplicacións tradicionais ao modelo AJAX implica cambios na estrutura interna coa preserva das funcionalidades. A metodoloxía de refactorización habitual implica unha serie de cambios a pequena escala, para o que é ideal a programación orientada a obxectos. Estes cambios van dende:

- ✓ **Refactorización a nivel de método/clase.** En sistemas con pouco acoplamento, evitando por exemplo que se modifiquen os atributos das clases entre obxectos. Estes accesos múltiples poden integrarse nun nivel superior unha vez resoltas as dependencias do método/clase.
- ✓ **Creación de novas clases.** Defínense novas clases especializadas na arquitectura AJAX con responsabilidades e interfaces ben definidos.
- ✓ **Eliminación de clases intermediarias.** Elimínanse as delegacións en exceso entre clases do modelo tradicional en aplicación das consideracións sobre antipatróns de exceso de capas.
- ✓ **Compoñentes e etiquetado.** Diferentes compoñentes sobre todo da vista presentan funcionalidades comúns que se poden factorizar a través de compoñentes AJAX e etiquetados, para facilitar o mantemento e a reutilización.

Na actualidade existen infinidade de **frameworks e librarías AJAX**, incorporando compoñentes da vista, diferentes funcionalidades Javascript, elementos para comunicación asíncrona tanto no cliente coma no servidor e outros elementos para integración con outras tecnoloxías RIA. O obxectivo destes *frameworks* resúmese en facilitar o desenvolvemento de aplicacións web baseadas en AJAX, facendo fincapé en aspectos da capa de vista ou cliente. Os principais *frameworks* en canto ao seu uso máis estendido, son:



- ✓ **Prototype.** Pode ser o *framework* de uso máis estendido, tamén de código aberto dispón da extensión **Scriptaculous** para engadir animacións e efectos nos documentos, e JSON para intercambio de datos. Serve á súa vez a base de outros *frameworks* AJAX. Permite unha grande integración en aplicacións desenvolvidas con *Ruby on Rails* pero tamén pode operar de xeito independente. As súas principais características son:
  - a) **DOM Estendido.** Referencia áxil a obxectos DOM, como por exemplo empregando a función `$()` en lugar de `document.getElementById()`.
  - b) **Scriptaculous.** Aporta ao *framework* un construtor de obxectos DOM (*builder.js*), un repositorio de efectos visuais (*effects.js*, *slider.js*), funcionalidades de control de elementos (X)HTML (*dragdrop.js*, *controls.js*) e métodos para realizar test de verificación unitarios (*unittest.js*).
- ✓ **Dojo Toolkit.** Proxecto de software libre, actualmente co soporte de IBM e Sun entre outros, que contén varias APIs Javascript modulares e unha ampla coleccións de widgets para uso baixo demanda, agrupados nun sistema de paquetes ao estilo de JEE. Entre as súas principais características están a achega de:
  - a) **Compoñentes empacitados en Dijit.** Widgets para a estrutura das páxinas como menús, pestanas; específicos para calendarios, reloxos, gráficos, vectores 2D/3D, ordenación de táboas e paxinación; ademais de elementos para formularios e a súa validación, elementos HTML5 e compoñentes para mellorar a accesibilidade. Así mesmo presenta un editor de texto enriquecido e soporte drag & drop entre os seus compoñentes.
  - b) **Comunicación asíncrona.** Prove dunha capa de abstracción para a comunicación transparente entre o navegador e o servidor web que fai uso de elementos Iframes ocultos para o refresco de datos.



- c) **Almacenamento no servidor.** Implementa diferentes mecanismos de almacenamento de datos vía CVS, OPML, RDF ou o servizo web Del.icio.us.
  - d) **Soporte para outras tecnoloxías.** Permite integración con tecnoloxías RIA como as aplicacións AIR baseadas en Javascript a través de API e soporte para móbiles.
- ✓ **jQuery.** Outro proxecto de software libre, que neste caso busca simplificar o acceso a documento (X)HTML, o modelo DOM, a manipulación de eventos, utilidades, animacións e efectos. Permite a instalación a través dun paquete básico moi lixeiro (*jquery.js*) que pode ser ampliado a través de plug-ins coma JExpand, para táboas, e JQueryUI para widgets con efectos visuais, entre outros moitos. Entre as súas principais características atópanse:
- a) Integración na plataforma .NET e cos *frameworks* ASP .NET MVC e ASP .NET AJAX.
  - b) Soporte para CSS 3 e XPath.
  - c) Soporte para manipulación de (X)HTML E JSON.
  - d) Fai uso de programación non intrusiva.
  - e) Lixeiro e extensible.
- ✓ **Qooxdoo.** Colección de librarías Javascript multipropósito de código aberto, que como as vistas anteriormente permite control áxil a alto nivel de (X)HTML, CSS e DOM, ademais de proporcionar funcionalidades estendidas. A principal diferenza respecto as anteriores é que proporciona widgets de última xeración moi similares aos das aplicacións de escritorio. Entre as súas principais características atópanse:
- a) **Abstracción do navegador.** Establece unha capa intermedia



de abstracción do navegador coas especificacións necesarias para os principais tipos de navegadores definindo así unha interface estándar que mellora a compatibilidade sen necesidade de instalar *plug-ins* adicionais.

- b) **Administración de eventos.** Prove unha interface propia con métodos para rexistrar e eliminar eventos.
- c) Ferramenta de desenvolvemento de Interfaces de usuario.
- d) Soporte de internacionalización i18n e localización l10n que permite o formato de tradución baseado en arquivos .po.
- e) Prove *frameworks* para depuración de test unitarios e simulacións.

✓ **Mootools.** *Framework* de código aberto modulas e extensible que permite ao desenvolvedor seleccionar que compoñentes empregar para minimizar o peso final da librería no cliente. Presenta un compoñente para a incorporación de efectos avanzados e transicións, estreitamente relacionados con Flash sendo un punto forte a súa integración con esta outra tecnoloxía RIA. Prove dos seguintes compoñentes:

- a) **Core.** Núcleo de funcións básicas que empregan todos os demais compoñentes do *framework*.
- b) **Class.** Librería para instanciación e manipulación de obxectos.
- c) **Natives.** Extensións de funcións básicas Javascript.
- d) **Element e Effects/FX.** APIs para manexo de documentos HTML e aplicación de efectos sobre os seus elementos.
- e) **Remote.** Para intercambio de datos co servidor a través de peticións XmlHttpRequest, JSON ou Cookies.

✓ **ExtJS.** Conxunto de librerías derivadas da Yahoo! UI, actualmente



emprégase como extensión de JQuery e Prototype incorporando *widgets* especializados, en especial na representación de gráficas e *grids*. Existe ademais unha adaptación específica para GWT denominada ExtGWT, con moitas optimizacións para este contorno. Incorpora unha capa propia dentro dunha arquitectura MVC o que lle permite prover de flexibilidade no tocante aos estilos, facendo uso da extensión SASS (en inglés *Syntactically Awesome Style Sheets*), unha extensión de CSS3. Así mesmo prove de librarías que facilitan a integración con AIR e Spring como backend. Dentro dos compoñentes de datos dispón de varios lectores tanto para XML como JSON. A arquitectura xeral inclúe os paquetes Base e Core coas funcionalidades comúns; os Compoñentes da interface de usuario cos widgets e gadgets; Remoting para a execución de métodos no servidor vía RPC; os Servizos de datos para lectura de vectores, XML e JSON; e o *miniframework Drag and drop* para permitir soporte de arrastre entre os compoñentes do *framework*.

- ✓ **Rico.** Baseado en Prototype e orientado cara a Web 2.0 as principais achegas deste *framework* inclúen efectos de animacións que permiten realizar transicións que poden ser interrompidas, pausadas ou reiniciadas, permitindo o solapamento de animacións. Permite a creación de efectos cinematográficos e outros efectos visuais.

Así mesmo proporciona as funcionalidades básicas para soporte AJAX e estende parte do repertorio de Prototype con melloras.

- ✓ **DWR.** (En inglés *Direct Web Remoting*). Framework de código aberto orientado á integración de AJAX con aplicacións JEE a través de mecanismos de RPC como RMI ou SOAP. Permite executar código Java nun servidor de aplicacións como se estivera no navegador do cliente, invocando os obxectos como se foran locais. Consta de dous elementos principais: un *framework* Javascript no cliente e un Servlet



no servidor para procesar as peticións e xerar as respostas. O Javascript actuará como proxy das clases Java permitindo que nese código se inclúan as clases Java so servidor. Nunha chamada a un método dunha clase, DWR xera dinamicamente unha versión Javascript da clase AjaxService, invocada a través dun manexador de eventos que xestiona a interacción co servidor. Cando chega a resposta ao cliente invócase unha función *callback* para actualizar o contido do documento. Este método denomínase Reverse AJAX, soportando tres métodos básicos de envío de datos:

- 1) **Polling**. O navegador pregunta ao servidor en intervalos regulares se completou a petición.
- 2) **Piggyback**. O servidor espera á seguinte petición do navegador para darlle a resposta.
- 3) **Comet**. O servidor responde ao navegador de xeito planificado tipo Streaming nunha resposta Http longa.

Así mesmo, prove de dúas opcións de comunicación remota:

- 1) **DWR nativo**. Empregando un superconxunto de JSON onde o motor DW (*engine.js*) manexa as peticións e prepara a execución das chamadas ao servidor.
- 2) **JSON/JSONP**. API para JSON que facilita a integración con outros *frameworks* como Dojo, ExtJS ou JQuery.

No tocante ao tema da seguridade DWR contempla proteccións específicas contra ataques XSS (en inglés *Cross Site Scripting*) e CSRF (en inglés *Cross Site Request Forgery*).

- ✓ **SAJAX**. (En inglés *Simple AJAX Toolkit*). Ferramenta de código aberto que de xeito análogo a DRW permite realizar chamadas a métodos do servidor en PHP, ASP, Coldfusion, Ruby, Perl, Phyton e outras linguaxes dende Javascript no navegador, sen ter que recargar a páxina.

Prove dunha API para cada linguaxe de servidor, por exemplo *Sajax.php*,



que se inclúe no código deste para permitir a integración co Javascript do navegador.

- ✓ **GWT.** (En inglés *Google Web Toolkit*). *Framework* de desenvolvemento AJAX dentro de aplicacións Java. Este contorno permite que ao definir unha interface Java se traduza co compilador GWT de xeito transparente a Javascript e HTML. O principal obxectivo deste *framework* é integrar nun mesmo IDE o desenvolvemento da aplicación e da parte de interfaces de usuario con AJAX pero ademais prove doutras funcionalidades como compoñentes HTML dinámicos e reutilizables, protocolos de transferencia XML e JSON, internacionalización i18n, integración con JUnit incluso nas chamadas RPC e con Javascript a través de JSNI. A arquitectura de GWT estruturase nos seguintes elementos:

1. **Compilador Java a Javascript GWT.** Para aplicacións web xera automaticamente o código Javascript necesario para a interface Java definida.
2. **Hosted Web Browser.** Motor de execución de aplicacións Java sen traducilas a Javascript a modo de máquina virtual Java.
3. **Libraría de Emulación JRE.** Contén os principais paquetes Java de uso común soportadas por GWT.
4. **Libraría de clases de Interfaces de Usuario GWT.** Prove dun conxunto de compoñentes para interfaces de usuario.

A maiores destes *frameworks* existen infinidade de alternativas e librarías para temas específicos ou versións mais ou menos simples de propósito xeral, como:

- 1) **AjaxAC.** *Framework* PHP que emprega AJAX no cliente e se orienta á reutilización por dispor de clases moi simples.



- 2) **AJAX .NET Professional.** Librería AJAX para ASP .NET con funcionalidades básicas para controis de usuario e utilidades de uso xeral.
- 3) **ATLAS.** Tamén denominado ASP .NET AJAX, integra nun mesmo *framework* un conxunto de extensións para integrar AJAX en .NET, que inclúe a Microsoft Ajax Library .
- 4) **BAJAX.** Librería Javascript moi lixeira (<6k), para integrar AJAX da forma máis simple posible.
- 5) **Taconite.** *Framework* para desenvolvemento AJAX, que automatiza tarefas para xestionar o obxecto XMLHttpRequest ou a creación de contido dinamicamente.
- 6) **Spry Framework for Ajax.** Librería Javascript de Adobe para a integración de AJAX con orixes de datos XML, JSON e HTML para linguaxes de servidor como Coldfusion, PHP ou ASP .NET. Spry ofrece tres compoñentes principais: Datos, Widgets e Efectos.
- 7) **Tacos.** Librería que proporciona compoñentes, efectos, validacións e funcionamento AJAX para o *framework* Tapestry.
- 8) **XAJAX.** *Framework* AJAX para desenvolvemento en PHP, que permite dende o navegador chamar a funcións do servidor.
- 9) **Zephyr.** *Framework* AJAX para desenvolvemento en PHP5 baixo o modelo MVC. Prove dun motor de modelos, soporte para datos adoDB e outras opcións.
- 10) **ZK.** *Framework* para desenvolvemento de aplicacións Java que busca facer transparente a tecnoloxía Javascript. Os compoñentes da interface de usuario relaciónanse con compoñentes POJO no servidor. Recoméndase a integración con Spring, Toplink ou Hibernate e aporta proteccións contra ataques XSS, CSRF e DoS. Verase polo miúdo máis adiante.

### 32.3 RIA PARA MULTIMEDIA E ANIMACIÓNS

Conforme mellorou o ancho de banda das conexións foron en aumento as tecnoloxías RIA destinadas a mellorar as funcións multimedia, gráficos vectoriais, animacións e interactividade. A pioneira destas tecnoloxías foi Flash para posteriormente aparecer Flex, AIR, JavaFX, OpenLaszlo e Silverlight como principais alternativas.

#### 32.3.1 FLASH RIA

A plataforma Flash evolucionou de plug in no cliente (Flash Player) para a visualización de imaxes vectoriais e animacións, cara unha arquitectura RIA para dotar de novas funcionalidades ás interfaces web. Representa a primeira tecnoloxía RIA, sendo o marco que engloba diferentes tecnoloxías dentro do que se denomina Flash RIA. Dentro das Flash RIA atópanse as tres tecnoloxías principais soportadas por Adobe, e anteriormente Macromedia, as cales teñen o uso máis estendido:

1. **Flash.** Empaqueta de aplicación en arquivos SWF a modo de compoñentes.
2. **Flex.** A partir dun servidor de aplicacións JEE realiza a comunicación co SWF permitindo chamar a obxectos do servidor.
3. **AIR.** Para execución de aplicacións Flash no equipo do cliente sen necesidade de navegadores como intermediarios.

Alternativamente, existen outros provedores de tecnoloxías Flash RIA, entre os que se atopan:

1. **OpenLaszlo.** Moi similar a Flash pero cunha linguaxe de programación propia LZX.

2. **SnappMX**. Orientada cara servizos web.
3. **Zulu**. Permite desenvolver aplicacións conxuntamente co estándar XUL e Flash.
4. **XAMLON**. Permite desenvolver aplicacións Flash coa linguaxe de marcado XAML dentro da plataforma .NET.

A orientación principal de Flash a diferenza de AJAX é a de ser un complemento da interface de usuario estendendo determinadas funcionalidades, en especial no campo das animacións e da interacción co usuario. Os contornos de desenvolvemento de Flash están máis orientados cara a edición de animacións que cara o desenvolvemento web, pero foise abrindo camiño no campo da elaboración de widgets, soporte multilinguaxe, efectos 3D, control e validación de formularios. Permite integración con AJAX e Javascript pero dispón dunha linguaxe de *script* propia denominada **ActionScript**. Este *script* de programación orientada a obxectos segue o estándar ECMA-262, implementando E4X (en inglés *ECMAScript for XML*). Opera cun modelo de eventos baseado na especificación DOM, aínda que non o segue completamente. Lánzase nunha máquina virtual específica AMV2 (en inglés *ActionScript Virtual Machine*) aloxada no contorno de execución Flash Player. Por último destacar que permite conectividade con Servizos web e Bases de datos de maneira remota a través da clase *DataProvider*.

Como acontece na maioría de *frameworks* de desenvolvemento a plataforma Flash pode ampliarse con paquetes de librarías de terceiros, entre estas destacan:

- a) **SPL** (en inglés *Spelling Plus Library*). Para deseño de editores de texto enriquecido con corrección ortográfica.
- b) **Red5**. Servidor Flash de software libre.
- c) **Papervision3D**. Motor de xeración 3D de software libre.
- d) **As3corelib**. Paquete de librarías ActionScript 3 que contén clases e



utilidades de uso común. Inclúe codificadores de imaxe, serialización JSON, APIs para datas, Strings e outros tipos de datos e codificación de chaves MD5 e SHA 1.

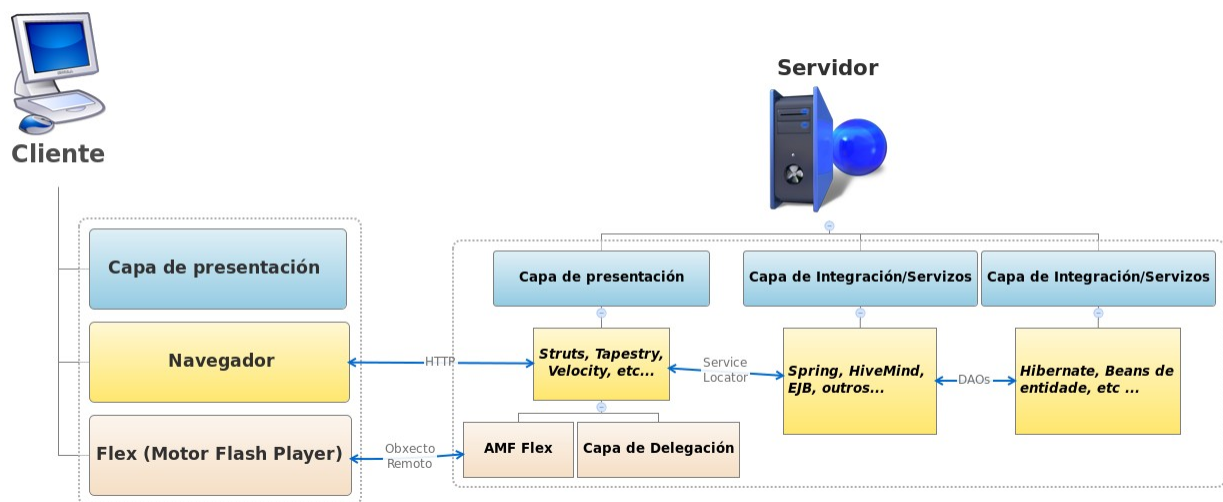
- e) **SWFObject**. Javascript para incrustar contido Flash en documentos (X)HTML
- f) **Tweener**. Para crear animacións e transicións directamente traballando con ActionScript.
- g) **Gaia**. *Framework* orientado cara a axilización do desenvolvemento Flash.

### 32.3.1 FLEX

Flex é a evolución de Flash ampliando o ámbito de desenvolvemento RIA con novas tecnoloxías e formatos. Diferenciase de Flash na súa facilidade de integración con tecnoloxías de linguaxes de servidor o que facilita o uso de patróns de deseño e que emprega MXML (en inglés *Macromedia eXtensible Markup Language*) para definir o aspecto e comportamento das interfaces de usuario. Como Flash soporte a linguaxe ActionScript e a súa plataforma incorpora librarías de compoñentes para interfaces de usuario específicas. Permite integración con outras tecnoloxías do lado do servidor como Servizos Web, REST ou AMF. As aplicacións Flex poden integrarse nun documento HTML de xeito que este pode actualizar dinamicamente a vista e enviar e recibir datos asincronamente co servidor de fondo, de xeito similar a AJAX.

Nas **comunicacións cliente servidor**, Flex no cliente comunícase co servidor vía HTTP, dispoñendo de tres API RPC: HTTPService, WebService e RemoteObject. Non acceden directamente a Bases de datos remotas senón que o fan a través de capas intermedias. A través de HTTPService solicita arquivos JSP ou XML cos datos en formato de variables String, formatos de intercambio XML, E4X ou obxectos ActionScript. No caso de devolver JSON

Flex dispón de librerías especializadas para serialización así como para SOAP. A través da API de RemoteObject permite realizar peticións **Flash Remoting** que devolven mensaxes binarias **AMF** (en inglés *Action Message Format*) sobre HTTP. Cando este formato ten aplicación obtense un maior rendemento que noutras tecnoloxías, como JSON ou SOAP.



**Figura 2: Integración de Flex en JEE.**

Así mesmo Flex permite intercambio de datos en tempo real perante dúas vías: **XML Socket** e **Socket Binario**. Co XML Socket créase unha conexión que permanece aberta mentres dure a comunicación, ou é pechada explicitamente. No Socket Binario o funcionamento é similar pero cliente e servidor non precisan intercambiar paquetes XML especificamente senón que envían os datos como información binaria, o que permite conectar con servidores de correo como POP3, SMTP e IMAP ou servidores de novas como NNTP.

No tocante á **seguridade** á hora de integrar Flex nunha aplicación JEE será a arquitectura desta a que impoña o modelo de seguridade, variando dende un *framework* de autenticación/autorización específico a un directorio LDAP, ou arquivos de configuración XML. A información de seguridade debe engadirse aos servizos BlazeDS e LiveCycle Data de xeito

que soliciten credenciais nas comunicacións co servidor.

Coma noutras tecnoloxías, en Flex están dispoñibles unha serie de **frameworks** multipropósito. Moitos deles tamén son válidos para AIR. Os máis empregados son:

- a) **Cairngorm**. Microarquitectura que aplica un pequeno conxunto de patróns de deseño (Service Locator, Front-Controller, ...) probados en conxunto. Céntrase en tres áreas chave: manexar accións de usuario, encapsular as interaccións con servidor e a lóxica de negocio e xestionar o estado do cliente representándoo na Interface de usuario.
- b) **Mate**. *Framework* orientado a eventos baseado en etiquetas, implementadas completamente en MXML. Implementa a idea de Inxección de dependencia, construíndo os obxectos para a continuación inxectar nas clases os datos. Os obxectos non solicitan a información pero esta lle é entregada polo sistema.
- c) **PureMVCFramework**. Como Cairngorm representa tamén unha microarquitectura cun pequeno conxunto de patróns de deseño, con MVC e Fachada como núcleos centrais, cada unha a través dun patrón instancia única.
- d) **Swiz**. *Framework* de control de inversión (Ioc), que prove metodoloxías para simplificar o manexo de eventos e as chamadas asíncronas a procedementos remotos. Emprega MVC pero a diferenza dos anteriores só no que respecta á estrutura de clases e non de directorios.
- e) **Parsley**. Conxunto de librarías ActionScript para correspondencia de obxectos e entidades, rexistro de depuración, inxección de dependencia, mensaxería e outras funcionalidades estendidas.

Para a integración con sistemas de información Flex prove do Servizo de xestión de datos dentro do Servizo LiveCycle Data. Neste servizo inclúese

sincronización de datos en tempo real entre cliente, servidor e outros clientes, replicación de datos, paxinación baixo demanda, e para aplicacións AIR sincronización de datos locais para conexións ocasionais das aplicacións.

### 32.3.3 SILVERLIGHT/MOONLIGHT

Complemento para navegadores que permite integrar na mesma extensión elementos multimedia, animacións e interactividade, de xeito similar ao WPF. Atópase baseado en XAML para a definición das interfaces de usuario, a partir das que invoca a métodos do servidor de aplicacións .NET. Permite a carga dinámica de XML co que se pode operar a través de DOM ao xeito de AJAX. Proporciona extensións Javascript e. As principais **características** do *framework* son:

- a) **WPF**. Inclúe un subconxunto de WPF que estende en gran medida elementos da Interface de Usuario.
- b) **XAML**. Definición da Interface de Usuario a través dunha linguaxe de marcado declarativa.
- c) **Integración** con Javascript e ASP .NET AJAX.
- d) Acceso a **obxectos do lado do servidor** .NET.
- e) Conexión con **servizos de rede** WCF, SOAP e ASP .NET AJAX, permitindo orixes de datos JSON, XML e RSS.
- f) Soporta **LINQ** para implementar o acceso a datos

A **arquitectura** de Silverlight se compón de 3 partes fundamentais:

- 1) **Framework de presentación básico**. Compoñentes e servizos orientados á Interface de usuario e a interacción co usuario, elementos multimedia e soporte XAML.

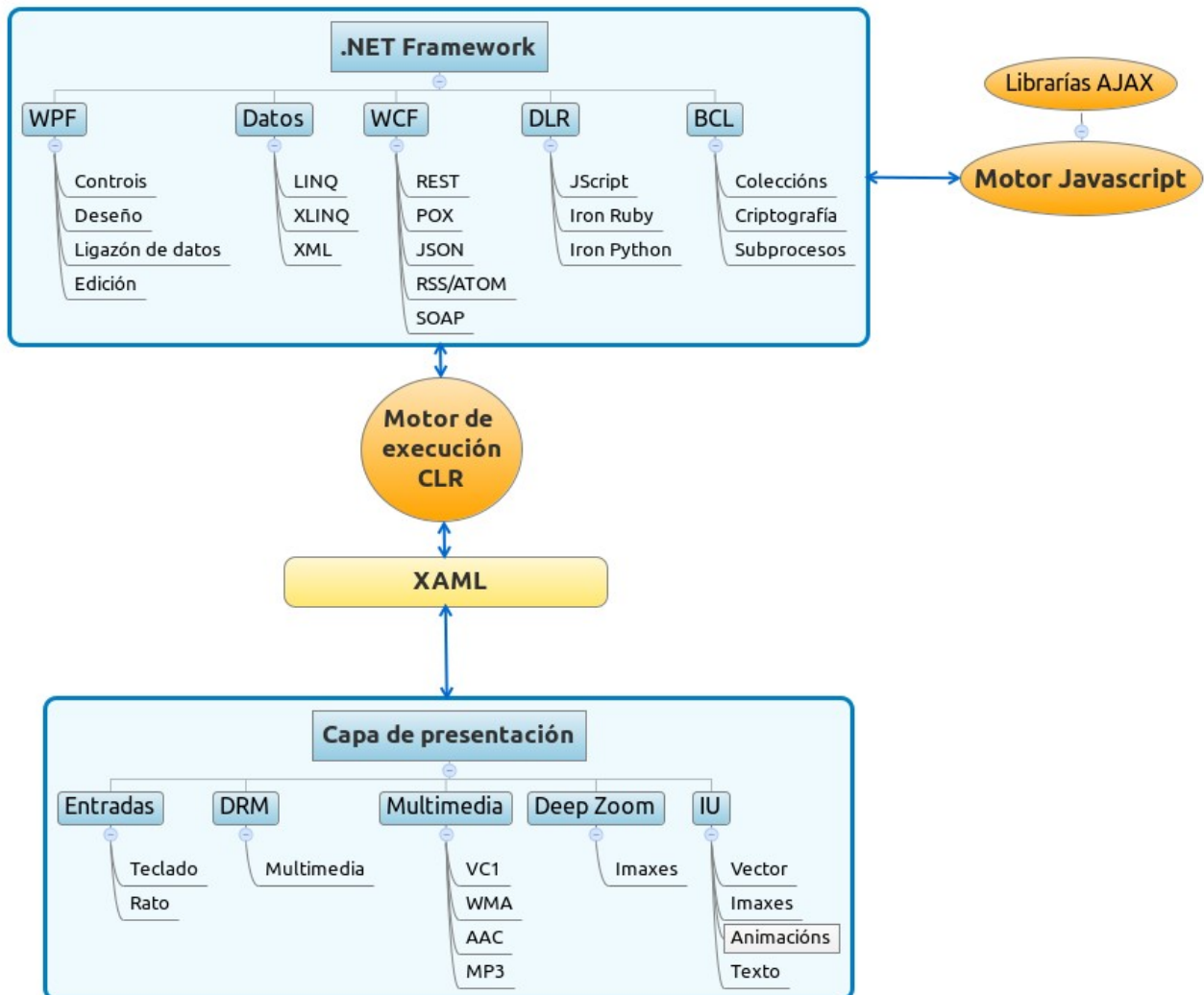




- 2) **.NET Framework para Silverlight.** Subconxunto de .NET Framework para Silverlight que contén compoñentes e librarías, recolector de lixo, WCF e CLR. Así mesmo inclúe os controis da Interface de Usuario, XLINQ, RSS/Atom, serialización XML e DLR (en inglés *Dynamic Language Runtime*)
- 3) **Compoñente de instalación e actualización.** Control de instalación e actualización da extensión.

Mención especial merece o apartado da **seguridade**, como acontecía con outras tecnoloxías RIA Silverlight incorpora políticas de seguridade específicas para:

- a) Seguimento do Ciclo de vida de seguridade de Microsoft SDL (En inglés *Security Development Lifecycle*)
- b) Evitación de ataques XSS.
- c) Illamento de código de arquivos de configuración XAP.
- d) Prover acceso seguro a recursos de rede.
- e) Servizos criptográficos para protección de datos de usuario.
- f) Sinatura dixital das aplicacións.



**Figura 2: Arquitectura Silverlight.**

### 32.3.4 JAVA FX

Java FX é unha plataforma que se compón de elementos web, multimedia e scripting xunto con tecnoloxías de servidor JEE para o desenvolvemento de aplicacións multiplataforma. Pode funcionar de maneira independente do navegador sempre que teña o equipo instalada unha máquina virtual Java compatible. Promove o concepto de “Perfil común” para tentar unificar todos os dispositivos que soporten JavaFX, de xeito que o mesmo modelo

de desenvolvemento se adapte a calquera contorno.

Os principais **compoñentes** de Java FX son:

- a) **JavaFX Script.** Linguaxe de programación declarativa, con tipos estáticos, que permite invocar métodos de calquera API de Java da plataforma.
- b) **Entorno de execución JavaFX.** Especializado para o dispositivo, Escritorio/Web, Mobile, ou TV.
- c) **Aplicacións JavaFX.** Independentes ou empaquetadas como arquivos JAR.
- d) **Ferramentas de desenvolvemento.** Inclúe o compilador para JavaFX Script, Plug ins para IDEs como Eclipse, e librarías especializadas para gráficos, multimedia ou Servizos web, entre outros.

A **arquitectura** de JavaFX presenta nun primeiro nivel:

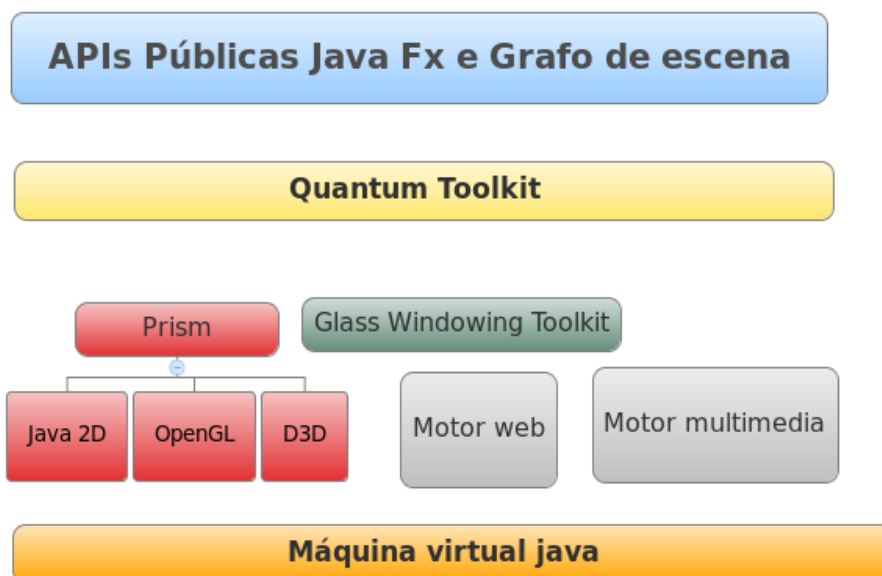
- 1. As **APIs públicas** de JavaFX. As principais funcionalidades destas APIs son permitir integración con outras linguaxes como JRuby, Groovy e Javascript, funcionalidades xenéricas e extensións para as interfaces de usuario.
- 2. **Grafo de Escena.** Neste grafo, definido na API *javafx.scene* represéntase nunha estrutura en árbore con nodos representando todos os elementos visuais da interface de usuario. Cada nodo pode levar os seus estilos, ademais de efectos, manexadores de eventos e control de estado.

Baixo eles atópase o motor de execución composto polos seguintes compoñentes:

- a) **Prism.** Motor gráfico de alto rendemento que soporta Java2D, OpenGL e DirectX.
- b) **Quantum Toolkit.** Xestiona as regras de procesos para

representación gráfica fronte ao manexo de eventos.

- c) **Glass Windowing Toolkit.** Sistema de control de ventás no nivel máis baixo da arquitectura gráfica de JavaFX. Prové dos servizos operativos nativos do sistema ademais de ser responsable de xestionar a cola de eventos.
- d) **Motores web e multimedia.** Inclúen APIs para soporte de medios visuais e de son. Así mesmo o motor web soporta os estándares HTML5, CSS, Javascript, DOM e SVG.



**Figura 3: Arquitectura JavaFX.**

## 32.4 OUTRAS TECNOLOXÍAS RIA

Se ben as tecnoloxías con anterioridade representan as solucións de uso máis estendido actualmente, existen outras multipropósito ou máis específicas que buscan facerse un oco no mundo das RIA. Dentro destas outras tecnoloxías, OpenLaszlo merece mención especial, se ben non

representa unha tecnoloxía en si, senón un conxunto de tecnoloxías, con algunhas adaptacións específicas.

### **32.4.1 OPENLASZLO**

OpenLaszlo é un *framework* e plataforma de desenvolvemento para aplicacións RIA con licenza GPL, precisando dun servidor propio para o aloxamento das aplicacións desenvolvidas. Unha mesma aplicación definida a través de dunha linguaxe de definición propia pode exportarse a diferentes formatos multinavegador e multiplataforma.

As aplicacións OpenLaszlo poden despregarse no servidor de aplicacións da plataforma, denominado **Despregue en modo proxy**, ou ben en modo **Despregue “SOLO”** con independencia do servidor, por norma xeral empaquetada nun arquivo SWF. Outra característica peculiar de funcionamento son as **Librarías dinámicas**, que permiten unha descarga “parcial” da aplicación, para obter unha carga inicial máis rápida, sendo o resto da carga da aplicación baixo demanda. Así mesmo a funcionalidade **Krank** permite cargar as aplicación OpenLaszlo máis rapidamente, realizando un preprocesamento da vista e *scripts* de inicialización.

OpenLaszlo aporta unha linguaxe declarativa propia, o LZX deseñado para describir as interfaces do usuario, ao estilo de XUL e XForms. Esta linguaxe incorpora un *framework* de etiquetas dividido en categorías como: elementos da interface, orixes de datos, efectos multimedia e accións. Emprégase conxuntamente con Javascript/AJAX sendo este último o encargado da interacción co usuario.

A plataforma OpenLaszlo incorpora os seguintes **compoñentes**:

- a) **Compilador**. Permite que unha aplicación definida perante a linguaxe declarativa LZX poida transformarse a Flash (SWF) ou



DHTML-AJAX. Así mesmo presenta unha serie de módulos específicos para:

- 1) **Compilación XML IU.** O compilador transforma as definicións da interface de usuario ao formato de saída especificado para a aplicación.
  - 2) **Compilación ECMAScript.** Clases e instancias LZX tradúcense a ECMAScript e controladores de eventos, transformándoas a Bytecode.
  - 3) **Compilación multimedia.** Codifícanse os arquivos en formatos de imaxe e son, así como as fontes TrueType en ficheiros OBJ para SWF ou XML.
- b) **Servidor.** Fai as funcións de aloxamento da aplicación e proxy, mantendo comunicación bidireccional cos back-ends a través de JAVARPC ou outros protocolos de servizos web. Así mesmo proporciona servizos de transformación de formatos, mensaxería, *streaming*, encriptación SSL e autenticación.
- c) **Contorno de execución ou LCF** (en inglés *Laszlo Foundation Class*). Inclúe compoñentes da interface de usuario, acceso a datos e servizos de rede. A LCF divídese en catro compoñentes principais:
- 1) **Data Loader/Binder.** O cargador e encargado de asociar e relacionar os datos. Dirixe o tráfico de datos incluíndo o fluxo de datos cara o cliente.
  - 2) **Sistema de eventos.** Permite unha programación baseada en eventos ao recoller os eventos detectados no cliente.
  - 3) **Layout & Animation System.** Sistema de animación e escenario da aplicación que ofrece todos os elementos para a parte gráfica da aplicación así como animacións e efectos.
  - 4) **Servizos para as aplicacións.** Con funcionalidades extra como contadores, sons, etc...



- d) **Framework.** Prove dunha extensa API para animacións, estrutura de aplicación, acceso a datos, comunicacións co servidor e definición da interface de usuario. Estruturalmente segue un modelo MVC, pero ampliable ás capas que sexan precisas para cada solución.
- e) **Servlet.** Trátase dun compoñente opcional para a aplicación que permite atender e dirixir peticións multimedia ou para servizos web como SOAP, JavaRPC ou XML-RPC. Fai funcións de caché e proxy para priorización e bloqueo de peticións así como de rexistro de trazas e auditoría.

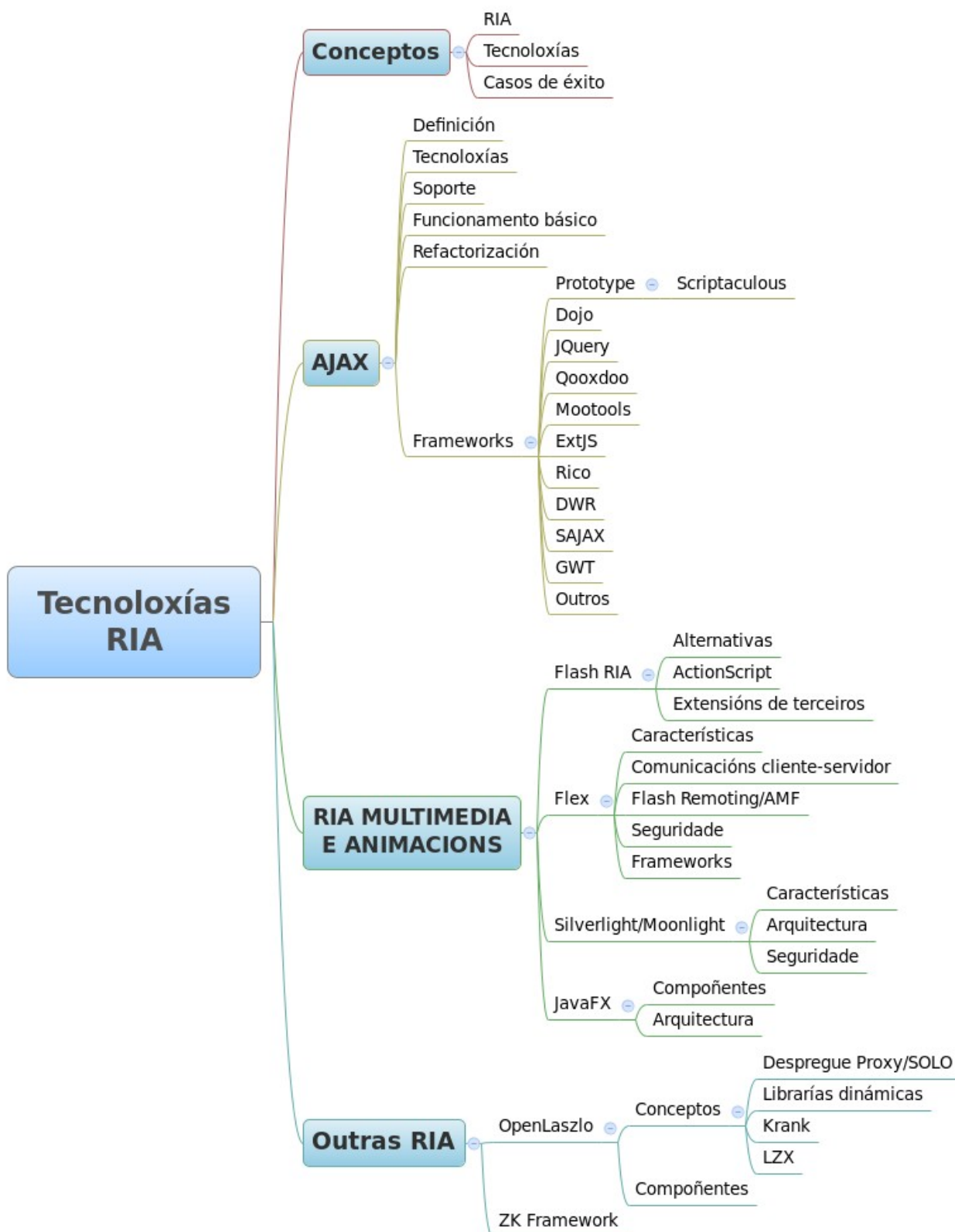
### 32.4.2 ZK FRAMEWORK

Trátase doutro *framework* orientado a eventos que en esencia poderíase incluír cos *frameworks* AJAX aínda que con algunhas diferenzas. En primeiro lugar emprega unha linguaxe de marcado propia para as interfaces de usuario denominada ZUML que pode mesturarse con outras linguaxes de marcado como XUL e XHTML, ademais de linguaxes de *script* e expresións EL para manipulación de compoñentes e datos. Deseñouse para integración con aplicacións JEE incorporando as capacidades de AJAX en desenvolvementos áxiles e reutilizables.

Prove dun *framework* cunha implementación de ZK Spring, adaptado do *framework* Spring, e librarías con compoñentes e etiquetas JSP con soporte para AJAX. No tocante á seguridade engade protección para ataques XSS, DoS e CSRF, ademais de reforzar a autenticación e os permisos coa incorporación de *frameworks* de terceiros como Spring Security.

### **31.5 ESQUEMA**





## **31.6 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 e O. U.**

**Colegiado del CPEIG**



**33. ENXEÑARÍA DO SOFTWARE.  
PROCESO SOFTWARE,  
MODELOS DE PROCESO  
SOFTWARE. CICLOS DE VIDA.  
MODELOS DE CICLO DE VIDA.  
FASES DO CICLO DE VIDA.  
MODELOS DE  
DESENVOLVEMENTO.**

## **Tema 33. Enxeñería do software. Proceso software, modelos de proceso software. Ciclo de vida. Modelos de ciclo de vida. Fases do ciclo de vida. Modelos de desenvolvemento.**

### **ÍNDICE**

33.1 ENXEÑERÍA DO SOFTWARE.....	2
33.1.1 <i>Inicios da enxeñería do software</i> .....	2
33.1.2 <i>Que é a enxeñería do software?</i> .....	3
33.2 PROCESO SOFTWARE. MODELOS DE PROCESO SOFTWARE.....	6
33.3 CICLO DE VIDA DO SOFTWARE.....	9
33.4 MODELOS DE CICLO DE VIDA DO SOFTWARE.....	12
33.4.1 <i>Modelo codificar e corrixir (Code and Fix)</i> .....	13
33.4.2 <i>Modelo por etapas</i> .....	13
33.4.3 <i>Modelo en fervenza</i> .....	14
33.4.4 <i>Modelos evolutivos</i> .....	17
33.4.4.1 <i>Modelo iterativo incremental</i> .....	18
33.4.4.2 <i>Modelo en espiral</i> .....	19
33.4.4.3 <i>Modelos baseados en prototipos</i> .....	23
33.4.4.3.1 <i>Prototipado rápido</i> .....	23
33.4.4.3.2 <i>Prototipado evolutivo</i> .....	24
33.4.5 <i>Modelos baseados en transformacións</i> .....	26
33.4.6 <i>Modelo baseado en compoñentes</i> .....	28
33.5 MODELOS DE DESENVOLVEMENTO.....	30
33.5.1 <i>Proceso Unificado de Desenvolvemento de Software (PUDS)</i> .....	30
33.5.2 <i>Programación extrema (eXtreme Programming)</i> .....	33

### **33.1 Enxeñería do software**

#### *33.1.1 Inicios da enxeñería do software.*

O auxe que se produciu no ámbito da informática nos anos sesenta, debido na súa maior parte á aparición da segunda xeración de ordenadores, tivo como consecuencia que se realizase unha masiva escritura incontrolada de liñas de código. Este proceso de creación de software levouse a cabo sen que se formulase ningún tipo de metodoloxía para o deseño e construción de software, nin ningún método para solucionar os problemas relacionados co mantemento, fiabilidade, etc.

Esta expansión sen control tivo como consecuencia a denominada **crise do software**, que é o nome xenérico que se acuñou para referirse a un conxunto de problemas que se han ir atopando no desenvolvemento do software. Esta problemática non só se limita ao software que non funciona adecuadamente, senón que abarca outros aspectos como a forma de desenvolver o software, o mantemento dun volume crecente de software existente e a forma de satisfacer a demanda crecente de software.

Os síntomas que fan palpable a aparición da crise do software son, entre outros, os seguintes:

- **Expectativas:** os sistemas non responden ás expectativas que deles teñen os usuarios.
- **Fiabilidade:** os programas fallan demasiado a miúdo.
- **Custo:** os custos do software son moi difíciles de prever e, frecuentemente, son moi superiores ao esperado.
- **Prazos:** o software adóitase entregar tarde e con menos prestacións das ofertadas.
- **Portabilidade:** é difícil cambiar un programa do seu contorno hardware, mesmo cando as tarefas que se realizan son as mesmas.
- **Mantemento:** a modificación do software é unha tarefa custosa, complexa e propensa a erros.

- **Eficiencia:** os esforzos que se fan para o desenvolvemento do software non fan un aproveitamento óptimo dos recursos dispoñibles (persoas, tempo, diñeiro, ferramentas, etc.).

A solución á crise do software céntrase, pois, en abordar e resolver os seguintes problemas principais:

- A planificación do proxecto software e a estimación dos custos de desenvolvemento, que son moi imprecisos.
- A produtividade das persoas, que non se corresponde coa demanda dos seus servizos.
- A calidade do produto software, que é, en moitos casos, inadecuada.

### 33.1.2 *Que é a enxeñería do software?*

Segundo Pressman, a enxeñería do software pódese definir como o *establecemento e uso de principios de enxeñería robustos, orientados a obter software económico que sexa fiable e funcione de maneira eficiente sobre máquinas reais.*

A enxeñería do software abarca tres elementos clave:

- **Métodos:** proporcionan a maneira de construír tecnicamente o software. Abarcan as tarefas de planificación e estimación de proxectos, análises dos requirimentos do sistema e do software, deseño das estruturas de datos, da arquitectura de programas e dos procedementos algorítmicos, e a codificación, probas e mantemento.
- **Ferramentas:** subministran o soporte automático ou semiautomático para os métodos; isto é, danlle soporte ao desenvolvemento do software.
- **Procedementos:** definen a secuencia en que se aplican os métodos, os controis que axudan a asegurar a calidade e a coordinar os cambios e as guías que facilitan aos xestores do software.

Pressman divide en tres fases o traballo asociado á enxeñería do software:

- **A fase de definición** (o *qué*). Quen desenvolve o software intenta identificar qué información debe ser procesada, qué función e rendemento se desexa, qué comportamento do sistema, qué interfaces van ser establecidas, qué restricións de deseño existen, e qué criterios de validación se necesitan para definir un sistema correcto. Xa que logo, han de identificarse os requisitos crave do sistema e do software. Aínda que os métodos aplicados durante a fase de definición variarán dependendo do paradigma de enxeñería do software (ou combinación de paradigmas) que se aplique, dalgún xeito terán lugar tres tarefas principais: enxeñería de sistemas ou de información, planificación do proxecto do software e análise dos requisitos.
- **A fase de desenvolvemento** (o *cómo*). É dicir, durante o desenvolvemento un enxeñeiro do software tenta definir como cómpre deseñar as estruturas de datos, como debe implementarse a función dentro dunha arquitectura de software, como deben implementarse os detalles procedementais, como deben caracterizarse interfaces, como debe traducirse o deseño nunha linguaxe de programación (ou linguaxe non procedemental) e como cómpre realizar a proba. Os métodos aplicados durante a fase de desenvolvemento variarán, aínda que sempre teremos: deseño do software, xeración de código e proba do software.
- **A fase de mantemento** (o *cambio*). O cambio vai asociado á corrección de erros, ás adaptacións requiridas a medida que evoluciona o contorno do software e a cambios debidos ás melloras producidas polos requisitos cambiantes do cliente. Durante a fase de mantemento atópanse catro tipos de cambios:
  - o **Corrección**. Mesmo levando a cabo as mellores actividades de garantía de calidade, é moi probable que o cliente descubra os



defectos no software. O *mantemento correctivo* cambia o software para corrixir os defectos.

- o **Adaptación.** Co paso do tempo, é probable que cambie o contorno orixinal para o que se desenvolveu o software. O *mantemento adaptativo* produce modificacións no software para acomodalo aos cambios do seu contorno externo (hardware, sistema operativo, regras de negocio...).
- o **Mellora.** Conforme se utilice o software, o cliente/usuario pode descubrir funcións adicionais que van producir beneficios. O *mantemento perfectivo* leva o software máis alá dos seus requisitos funcionais orixinais.
- o **Prevención.** O software de computadora deteriorase debido ao cambio. En esencia, o *mantemento preventivo* fai cambios en programas de computadora a fin de que se poidan corrixir, adaptar e mellorar máis facilmente.

Todas estas fases van acompañadas dun conxunto de actividades que se realizan ao longo de todo o proceso de creación de software. Estas actividades denomínanse actividades protectoras, sendo as máis importantes:

- Seguimento e control do proxecto
- Revisións técnicas formais
- Garantía de calidade do software
- Xestión de configuración do software
- Preparación e produción de documentos
- Xestión de reutilización
- Medicións



- Xestión de riscos

### **33.2 Proceso software. Modelos de proceso software**

Existen diversas definicións formais para determinar o concepto de *proceso de software*:

- *Un proceso do software é un conxunto de actividades que conducen á creación dun produto software.* Esta é unha definición proposta por Sommerville, onde estas actividades poden consistir no desenvolvemento de software desde cero, desenvolvemento de novo software ampliando e modificando sistemas existentes ou configurando e integrando software comercial ou compoñentes do sistema.
- Desde outro punto de vista, Fugetta determina un proceso software como *un conxunto coherente de políticas, estruturas organizacionais, tecnoloxías, procedementos e artefactos que son necesarios para concibir, desenvolver, instalar e manter un produto software.*

Os procesos do software son complexos e, como todos os procesos intelectuais e creativos, dependen das persoas que toman decisións e xuízos. Debido á necesidade de xulgar e crear, os intentos para automatizar estes procesos tiveron un éxito limitado.

As ferramentas de enxeñería do software asistida por computadora (CASE) poden axudar a algunhas actividades do proceso, pero teñen limitacións. Unha razón pola cal a eficacia das ferramentas CASE está limitada atópase na inmensa diversidade de procesos do software. Non existe un proceso ideal, e moitas organizacións desenvolveron o seu propio enfoque para o desenvolvemento do software. Os procesos evolucionaron para explotar as capacidades das persoas dunha organización, así como as características específicas dos sistemas que se están a desenvolver. Para algúns sistemas,

como os sistemas críticos, requírese un proceso de desenvolvemento moi estruturado. Para sistemas de negocio, con requirimentos rapidamente cambiantes, un proceso flexible e áxil probablemente sexa máis efectivo.

Aínda que existen moitos procesos diferentes de software, algunhas actividades fundamentais son comúns para todos eles:

1. **Especificación do software**, onde os clientes e enxeñeiros definen o software que se vai producir e as restricións sobre a súa operación.
2. **Desenvolvemento do software**, onde o software se diseña e programa.
3. **Validación do software**, onde o software se valida para asegurar qué é o que o cliente require.
4. **Evolución do software**, onde software debe evolucionar para cubrir as necesidades cambiantes do cliente.

Diferentes tipos de sistemas necesitan diferentes procesos de desenvolvemento. Polo tanto, estas actividades xenéricas poden organizarse de diferentes formas e describirse en diferentes niveis de detalle para diferentes tipos de software. O uso dun proceso inadecuado do software pode reducir a calidade ou a utilidade do produto de software que se vai desenvolver e/ou incrementar os custos de desenvolvemento.

Os procesos do software pódense mellorar coa estandarización. Isto mellora a comunicación e reduce o tempo de formación, e fai que a axuda ao proceso automatizado sexa máis económica. A estandarización tamén é un primeiro paso importante para introducir novos métodos, técnicas e boas prácticas de enxeñería do software.

De todos os xeitos, a existencia dun proceso de software non é garantía de que este vaia ser entregado a tempo, de que satisfará as necesidades do cliente, ou de que mostrará as características técnicas que conducirán a características de calidade a longo prazo. O proceso de software debe

**avaliarse** para asegurarse de que cumpra unha serie de criterios básicos que demostraron ser esenciais para unha enxeñería de software exitosa.

Un **modelo de procesos do software** é unha descrición abstracta e simplificada dun proceso do software que presenta unha visión dese proceso. Cada modelo de proceso representa un proceso desde unha perspectiva particular e así proporciona só información parcial sobre ese proceso. Son abstraccións dos procesos que se poden utilizar para explicar diferentes enfoques para o desenvolvemento de software. Pódese pensar neles como marcos de traballo do proceso que poden ser estendidos e adaptados para crear procesos máis específicos de enxeñería do software. Cada modelo describe unha sucesión de fases e un encadeamento entre elas. Segundo as fases e o modo en que se produza este encadeamento, temos diferentes modelos de proceso. Un modelo é máis adecuado ca outro para desenvolver un proxecto dependendo dun conxunto de características do proxecto. Os modelos poden incluír actividades que son parte dos procesos e produtos de software e o papel das persoas involucradas na enxeñería do software. Alternativamente, ás veces úsanse os termos **ciclo de vida, modelo de ciclo de vida e modelo de desenvolvemento**.

A maior parte dos modelos de procesos do software baséanse nun dos tres modelos xerais ou paradigmas de desenvolvemento de software:

1. **O enfoque en fervenza.** Considera as actividades anteriores e represéntaas como fases de procesos separados, tales como a especificación de requirimentos, o deseño do software, a implementación, as probas, etcétera. Despois de que cada etapa queda definida «asínase» e o desenvolvemento continúa coa seguinte etapa.
2. **Desenvolvemento iterativo.** Este enfoque entrelaza as actividades de especificación, desenvolvemento e validación. Un sistema inicial desenvólvese rapidamente a partir de especificacións moi abstractas.



Este refínase baseándose nas peticións do cliente para producir un sistema que satisfaga as súas necesidades. O sistema pode ser entregado daquela. De forma alternativa, pódese reimplementar utilizando un enfoque máis estruturado para producir un sistema máis sólido e fácil de manter.

3. **Enxeñería do software baseada en compoñentes (CBSE).** Esta técnica supón que as partes do sistema xa existen previamente. O proceso de desenvolvemento do sistema enfócase na integración destas partes máis que en desenvolveselas desde o principio.

Estes tres modelos de procesos xenéricos utilízanse exhaustivamente na práctica actual da enxeñería do software. Non se exclúen mutuamente, e a miúdo utilízanse xuntos, especialmente para o desenvolvemento de sistemas grandes. Os subsistemas dentro dun sistema máis grande poden ser desenvolvidos utilizando enfoques diferentes. Polo tanto, aínda que é conveniente estudar estes modelos separadamente, debe entenderse que, na práctica, a miúdo se combinan.

Pressman separa entre o **modelo persoal** (modelo utilizado por cada desenvolvedor) e **modelo en equipo** (cando o proxecto é dirixido por varios profesionais) para o proceso de software. inciden na medición, a planificación e a autodirección como ingredientes clave para un proceso de software exitoso.

### **33.3 Ciclo de vida do software**

O ciclo de vida dun sistema de información é *o marco de referencia que contén os procesos, as actividades e as tarefas implicadas no desenvolvemento, a explotación e o mantemento dun produto de software, abarcando a vida do sistema desde a definición dos requisitos ata a finalización do seu uso.*

Tamén se podería definir o ciclo de vida dun sistema de información como *o conxunto de etapas polas que atravesamos o sistema desde a súa concepción, ata a súa retirada de servizo, pasando polo seu desenvolvemento e explotación.*

Existen diversos modelos de ciclo de vida, os cales determinan unha serie de etapas, fases ou estados polos que debe pasar un produto software. Esta diversidade é debida en gran medida ao feito de que existen multitude de aplicacións diferentes e de distinta índole, o que provoca que existan modelos de ciclo de vida que se axusten mellor a uns desenvolvementos que a outros.

Con todo, malia esta variedade, todo modelo de ciclo de vida debe cubrir os seguintes obxectivos básicos:

- Definir as actividades que hai que realizar e en que orde, é dicir, determinar a orde das fases do proceso software.
- Establecer os criterios de transición para pasar dunha fase á seguinte.
- Proporcionar puntos de control para a xestión do proxecto, é dicir, calendario e organización.
- Asegurar a consistencia co resto dos sistemas de información da organización.

Cada proxecto debe seleccionar o modelo de ciclo de vida que sexa máis apropiado para o seu caso, o cal se elixe considerando unha serie de factores como: a cultura da organización, o desexo de asumir riscos, a área de aplicación, a volatilidade dos requisitos, a comprensión dos devanditos requisitos, etc. En calquera proxecto software, o modelo de ciclo de vida permite responder as preguntas de “que se vai facer a continuación?” e “por canto tempo se vai facer?” Dado que cada modelo de ciclo de vida ten as súas vantaxes e os seus inconvenientes, non se adoitan seguir na práctica os modelos na súa forma pura, senón que, de acordo coas

peculiaridades do sistema e a experiencia do persoal, poden adoptarse aspectos doutros modelos que sexan máis adecuados para o caso concreto.

É importante non confundir o concepto de ciclo de vida co de metodoloxía. Namentres que o ciclo de vida indica qué actividades hai que realizar e en que orde, a **metodoloxía** indica como avanzar na construción do sistema, isto é, con que técnicas, e entre as súas características está a de determinar os recursos que se van utilizar ou as persoas implicadas en cada actividade.

### **33.4 Modelos de ciclo de vida do software**

Os distintos modelos de ciclo de vida do software poden ser clasificados seguindo diversos criterios. Seguindo un criterio en función da súa utilización existen:

- **Modelos tradicionais:** Son os de máis ampla utilización.
  - o Modelo codificar e corrixir
  - o Modelo por etapas
  - o Modelo en fervenza
  - o Modelos evolutivos
    - Modelo iterativo incremental
    - Modelo en espiral
    - Modelos baseados en prototipos:
      - Modelo de construción de prototipos
      - Modelo de prototipado evolutivo
- **Modelos alternativos**
  - o Modelos baseados en transformacións: A filosofía xeral é chegar a xerar código a partir dunhas especificacións transformándoas por medio de ferramentas. Segundo usemos unhas ou outras ferramentas, habemos ter:
    - As que usan técnicas de cuarta xeración (Roger Pressman ): linguaxes non procedementais para consultas a BD; xeradores de código, de pantallas, de informes; ferramentas de manipulación de datos; facilidades gráficas de alto nivel.
    - Baseados en modelos de transformación (Carma McClure) => Baseados en ferramentas CASE que permiten, seguindo o MCV clásico, pasar dunha etapa a outra aplicando as transformacións que dan as ferramentas.
  - o Desenvolvemento de Software Baseado en Compoñentes (DSBC ou CBSB).

#### 33.4.1 *Modelo codificar e corrixir (Code and Fix)*

Este é un modelo simple, utilizado nos primeiros desenvolvementos de software, o cal se fundamenta na creación do código e na súa corrección e adaptación. Contén dous pasos:

- Escribir código.
- Corrixir problemas no código.

Trátase de primeiro implementar algo de código e logo pensar acerca de requisitos, deseño, validación, e mantemento. Este modelo ten tres problemas principais:

- Despois de correccións varias, o código pode ter unha moi mala estrutura e fai que os arranxos sexan moi custosos. Isto levou a ver a necesidade dunha fase previa de deseño antes da de codificación.
- Frecuentemente, incluso o software ben deseñado non se axusta ás necesidades do usuario, polo que é rexeitado ou a súa reconstrución é moi cara. Isto levou á necesidade de introducir unha fase de análise de requirimentos antes do deseño.
- O código é difícil de reparar pola súa pobre preparación para probar e modificar. Este problema levou a salientar a necesidade da planificación e preparación das distintas tarefas en cada fase.

#### 33.4.2 *Modelo por etapas*

O modelo por etapas nace como resposta aos problemas que xorden ao utilizar o modelo anterior. Como solución propónse un modelo para a creación de software que se basea nun conxunto de etapas ou fases sucesivas que van construíndo o sistema formulado. As etapas determinadas por este modelo (*Stage Wise*) son:

- Planificación
- Especificacións de operación



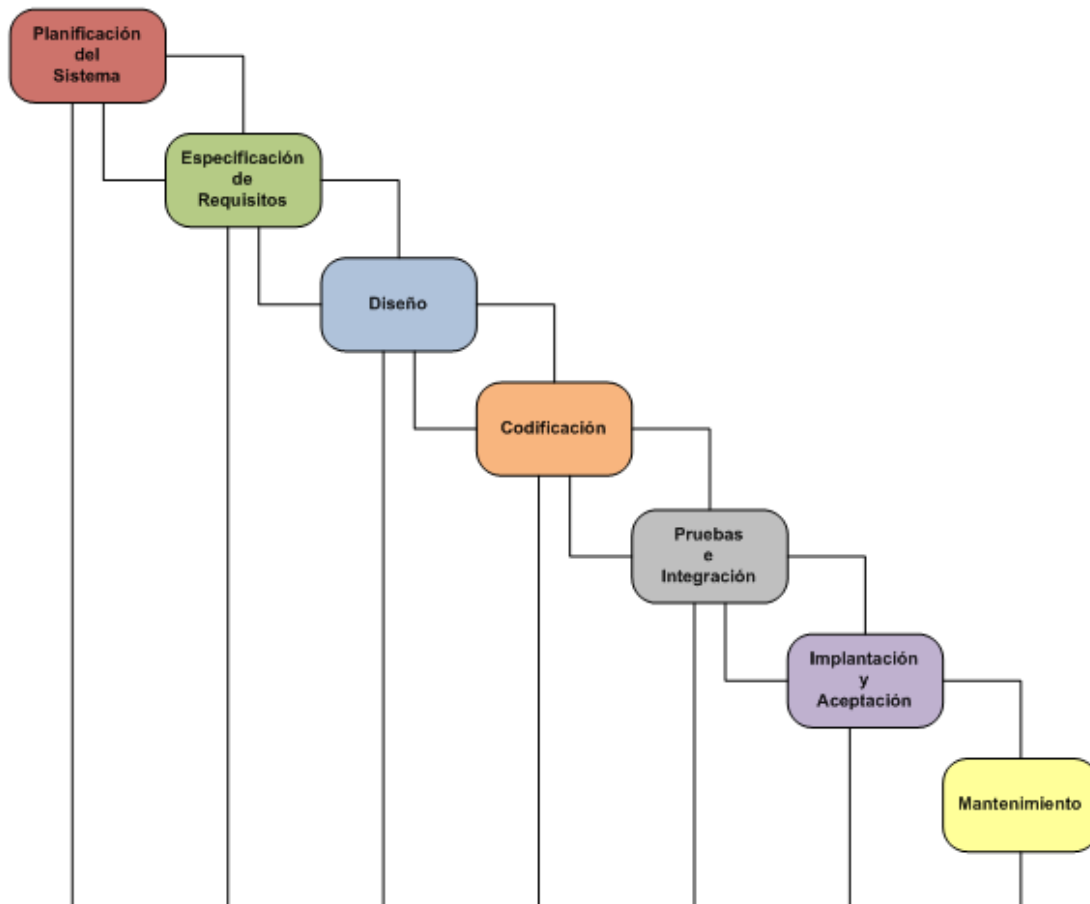
- Especificacións de codificación
- Codificación
- Proba de cada unidade
- Proba de integración
- Eliminación de problemas
- Avaliación do sistema

#### 33.4.3 *Modelo en fervenza*

Este modelo fundaméntase no modelo por etapas, ao que incorpora un conxunto de melloras tales como considerar a realización de bucles de realimentación entre etapas, permitindo que se poidan resolver os problemas detectados nunha etapa na etapa anterior, e permitir a incorporación inicial do prototipado a fin de captar as especificacións durante a análise, ou para probar distintas solucións durante o deseño.

O modelo en fervenza componse dunha serie de fases que se suceden secuencialmente, xerándose en cada unha delas uns resultados que serán necesarios para iniciar a fase seguinte. É dicir, a evolución do produto software prodúcese a través dunha secuencia ordenada de transicións dunha fase á seguinte, conforme unha orde lineal. O número de fases neste modelo é irrelevante, xa que o que o caracteriza é a *secuencialidade* daquelas e a *necesidade de completar* cada unha delas para pasar á seguinte. O modelo do ciclo de vida en fervenza está rexido pola documentación, é dicir, a decisión do paso dunha fase á seguinte tómase en función de se a documentación asociada á devandita fase está completa ou non. Non obstante, esta forma de proceder non é a máis axeitada para algúns tipos de software, como o que se usa nas aplicacións interactivas e de usuario final.

Desde a súa presentación, o modelo en fervenza tivo un papel fundamental no desenvolvemento de proxectos software. foi, e aínda segue a ser, o máis utilizado, tanto que este modelo se coñece co nome de ciclo de vida



clásico, aínda que incorporando infinidade de variacións que eliminan o carácter simplista do mesmo. Aínda así, existen unha serie de limitacións que xustifican a necesidade de definir outros modelos.

LENDAS: Planificación do sistema / Especificación de requisitos / Deseño / Codificación / Probas e integración / Implantación e aceptación / Mantemento.

Como se indicou anteriormente, as fases que comprende o ciclo de vida clásico son irrelevantes, tanto en número como en cáles sexan esas fases, sempre que se produzan secuencialmente. Posiblemente, o modelo clásico máis utilizado sexa o modelo de sete fases que son:



- **Planificación do sistema:** Nesta fase é necesario fixar o ámbito do traballo que se vai realizar, os recursos necesarios, as tarefas que se executarán, as referencias que hai que ter en conta, o custo estimado do proxecto, a composición do equipo de desenvolvemento e a orde das actividades.
- **Especificación de requisitos:** Nesta fase é preciso analizar, entender e documentar o problema que o usuario trata de resolver co sistema e débense especificar con detalle as funcións, obxectivos e restricións do mesmo, a fin de que usuarios e desenvolvedores poidan tomar estes como punto de partida para acometer o resto do sistema. É dicir, na fase de especificación de requisitos trátase de definir **qué** debe facer o sistema, e identificar a información que hai que procesar, as funcións que hai que realizar, o rendemento do sistema, as interfaces con outros sistemas e as ligaduras de deseño.
- **Deseño:** Arrinca das especificacións da fase anterior. Na fase de deseño, unha vez elixida a mellor alternativa, débese crear a solución ao problema descrito atendendo a aspectos de interfaces de usuario, estrutura do sistema e decisións sobre a implantación posterior. A fase de deseño trata de definir o **cómo**.
- **Codificación:** Esta fase consiste en traducir as especificacións e representacións do deseño a unha linguaxe de programación capaz de ser interpretada e executada polo ordenador.
- **Probas e integración:** Unha vez que se teñen os programas no formato adecuado ao ordenador, hai que levar a cabo as probas necesarias que aseguren a corrección da lóxica interna do programa e que este cobre as funcionalidades previstas. A integración das distintas partes que compoñen a aplicación ou o sistema debe garantir o bo funcionamento do conxunto.
- **Implantación e aceptación do sistema:** O obxectivo desta fase é conseguir a aceptación do sistema por parte dos seus usuarios, e levar a cabo as actividades necesarias para a súa posta en produción.

- **Mantemento do sistema:** A fase de mantemento comeza unha vez que o sistema lle foi entregado ao usuario e continúa mentres permanece activa a súa vida útil. Pódese deber a erros non detectados previamente (correctivo), a modificacións, melloras ou ampliacións solicitadas polos usuarios (perfectivo, ou aumentativo) ou a adaptacións requiridas pola evolución do contorno tecnolóxico ou cambios normativos (mantemento adaptativo).

As principais **críticas** ao modelo céntranse nas súas características básicas, é dicir, secuencialidade e utilización dos resultados dunha fase para acometer a seguinte, de maneira que o sistema só se pode validar cando está terminado. En canto ao fluxo secuencial, os proxectos reais raramente seguen o fluxo secuencial que propón o modelo. Sempre ocorren interaccións, e nas últimas fases sobre todo pódense realizar en paralelo algunhas áreas; por exemplo, codificación e probas. Unha aplicación do modelo en sentido estrito obrigaría á “conxelación” dos requisitos dos usuarios, suposto este completamente apartado da realidade. O modelo non contempla a posibilidade de realimentación entre fases. Doutra banda, o modelo non prevé revisións ou validacións intermedias por parte do usuario; así, os resultados dos traballos só se ven ao final dunha serie de tarefas e fases, de tal xeito que se se produciu un erro nas primeiras fases este só se detectará ao final, e a súa corrección terá un custo moi elevado, posto que será preciso refacer todo o traballo desde o principio.

#### *33.4.4 Modelos evolutivos*

O software evoluciona co tempo. Os requisitos do usuario e do produto adoitan cambiar conforme este se desenvolve. As datas de mercado e a competencia fan que non sexa posible agardar a poñer no mercado un produto absolutamente completo, polo que se debe introducir unha versión funcional limitada dalgunha forma para aliviar as presións competitivas.

Nestas ou noutras situacións semellantes os desenvolvedores necesitan modelos de progreso que estean deseñados para se acomodaren a unha evolución temporal ou progresiva, onde os requisitos centrais son coñecidos de antemán, aínda que non estean ben definidos a nivel detalle.

Os evolutivos son modelos iterativos, permiten desenvolver versións cada vez máis completas e complexas, ata chegar ao obxectivo final desexado; mesmo evolucionar máis alá, durante a fase de operación.

#### *33.4.4.1 Modelo iterativo incremental*

O incremental *é un modelo de tipo evolutivo que está baseado en varios ciclos ferverza realimentados aplicados repetidamente, cunha filosofía iterativa*, é dicir, consiste en desenvolver un sistema que logre cubrir unha parte dos requisitos especificados e logo ir xerando novas versións do sistema que incorporen o resto de funcionalidades e requisitos especificados, ata chegar a un produto final, que se asemelle ao sistema formulado.

Con este modelo, preténdese dispoñer pronto dun sistema que, aínda que sexa incompleto, sexa utilizable e satisfaga parte dos requisitos, evitando de paso o efecto *big-bang*, é dicir, que durante un período longo de tempo non se teña nada e de súpeto haxa unha situación completamente nova. Por outra banda, tamén se logra que o usuario se implique estreitamente na planificación dos pasos seguintes.

O modelo de desenvolvemento incremental tamén se utiliza para evitar a demanda de funcionalidades excesivas ao sistema por parte dos usuarios, xa que como a estes lles resulta difícil definir as súas necesidades reais tenden a pedir demasiado. Actuando con este modelo aténdese primeiro ás funcionalidades esenciais e as funcionalidades accesorias só se inclúen nas versións sucesivas cando realmente son necesarias.

#### 33.4.4.2 *Modelo en espiral*

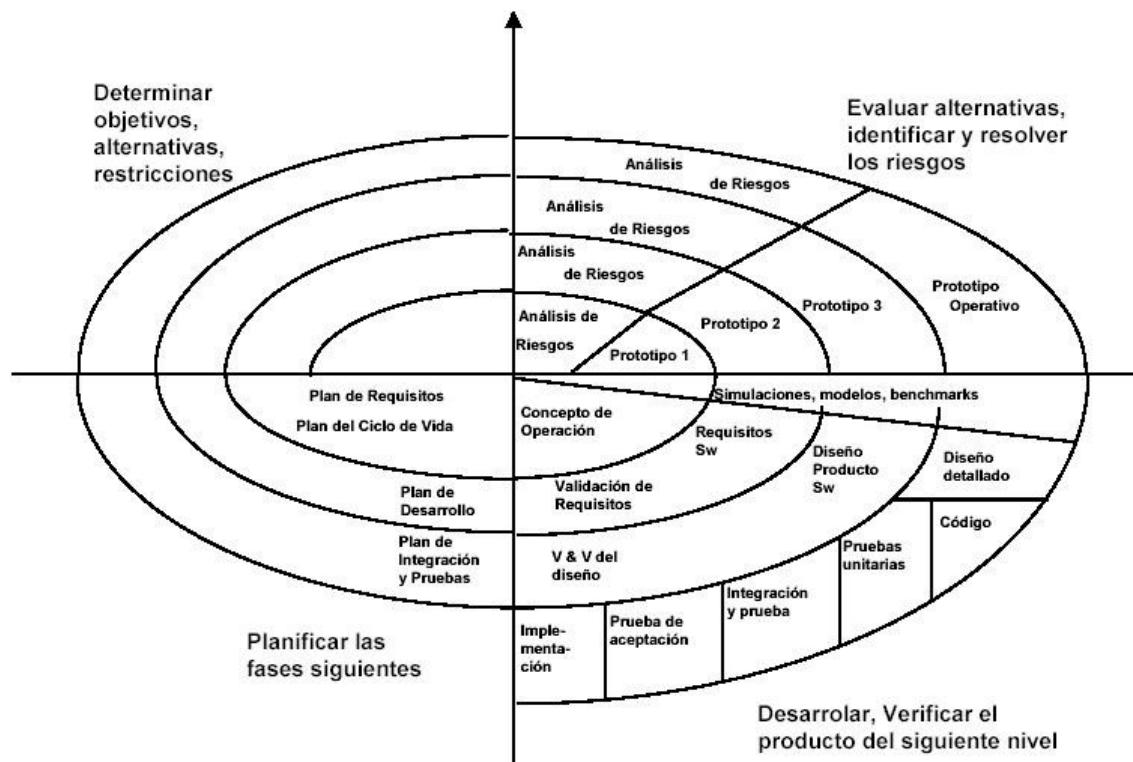
É un modelo de proceso de software evolutivo coas características propias dun desenvolvemento iterativo mediante o cal se xeran distintos prototipos, ás cales se lles suman os aspectos controlados e sistemáticos do modelo en fervenza.

Ofrece o potencial para o desenvolvemento rápido de versións incrementais do software. No modelo espiral, o software desenvólvese nunha serie de versións incrementais. Durante as primeiras iteracións, a versión incremental podería ser un modelo en papel ou un prototipo. Durante as últimas iteracións, prodúcese versións cada vez máis completas do sistema deseñado.

As súas diferenzas máis importantes cos modelos máis clásicos son:

- No modelo en espiral hai un recoñecemento explícito das diferentes **alternativas** para alcanzar os obxectivos do proxecto.
- O modelo en espiral céntrase na identificación dos **riscos** asociados a cada alternativa e na maneira de resolver os devanditos riscos.
- No modelo en espiral os proxectos divídense en ciclos (ciclos de espiral), avanzándose no desenvolvemento mediante consensos ao final de cada ciclo.
- O modelo en espiral adáptase a calquera tipo de actividade.

TEXTO LENDA: Determinar obxectivos, alternativas, restricións / Avaliar



alternativas, identificar e resolver os riscos / Planificar as fases seguintes / Desenvolver, verificar o produto do seguinte nivel / Plan de requisitos / Plan do ciclo de vida / Plan de desenvolvemento / Plan de integración e probas / Análise de riscos / Prototipo operativo / Prototipo / Simulacións, modelos, benchmarks / Concepto de operación / Requisitos Sw / Validación de requisitos / Deseño produto Sw / V & V do deseño / Deseño detallado / Implementación / Proba de aceptación / Integración e proba / Probas unitarias / Código.

O modelo en espiral reflicte a idea de que cada ciclo implica unha progresión no desenvolvemento do produto software que aplica a mesma secuencia de pasos para cada parte do produto e para cada un dos seus niveis de elaboración, desde a concepción global ata a codificación individual de cada programa.

Esta secuencia de pasos, iterativa en cada fase do desenvolvemento, componse das catro actividades seguintes:



- **Planificación:** Este primeiro paso co que comeza cada ciclo de espiral consiste na identificación dos obxectivos da parte do produto que está a ser elaborada (funcionalidade, rendemento, adaptación aos cambios, etc.), identificación das alternativas principais para realizar ou implementar esta parte do produto, e a identificación das restricións impostas (custo, prazo de realización, interfaces, etc.).
- **Análise de riscos:** Comeza coa avaliación de cada alternativa respecto dos obxectivos e ás restricións. Este proceso de avaliación identificará áreas de incerteza que son fontes significativas de risco no proxecto. Debe decidirse como resolver os riscos asociados á alternativa elixida.
- **Enxeñería.** Este paso consiste no desenvolvemento e verificación do produto obxecto da fase (ciclo de espiral) en que nos atopemos. Como esta implementación está dirixida polo risco, o desenvolvemento poderá seguir as pautas dun prototipado evolutivo, as do ciclo de vida clásico, as orientadas a transformacións automáticas, ou calquera outro enfoque do desenvolvemento. En definitiva, isto permítelle ao modelo en espiral acomodarse a calquera combinación de estratexias de desenvolvemento.
- **Avaliación do cliente.** Unha característica importante do modelo en espiral é que cada ciclo de espiral se completa cunha revisión na que participan aqueles que teñen relación co produto (desenvolvedores, usuarios, etc.). Esta revisión inclúe todos os produtos desenvolvidos durante o ciclo, os plans para o seguinte ciclo e os recursos necesarios para levalos a cabo.

Segundo isto, o modelo pódese representar mediante uns ciclos externos de espiral, que representan as fases en que se dividiu o desenvolvemento do proxecto software, normalmente as do modelo clásico, e uns ciclos internos, iterativos para cada fase, nos que se levan a cabo as catro actividades antes citadas. A dimensión radial indica os custos de



desenvolvemento acumulativos, en canto que a dimensión angular indica o progreso feito en cumprir cada fase.

A principal vantaxe do modelo en espiral é o amplo rango de opcións a que se pode axustar e que estas permiten utilizar os modelos de proceso de construción de software tradicionais; por outra banda, a súa orientación ao risco evita, se non elimina, moitas das posibles dificultades. Outras **vantaxes** son:

- Concentra a súa atención en opcións que permiten a reutilización de software xa existente.
- Céntrase na eliminación de erros e alternativas pouco atractivas.
- Non establece procedementos diferentes para o desenvolvemento do software e o seu mantemento.
- Proporciona un marco estable para desenvolvementos integrados hardware-software.
- Permite preparar a evolución do ciclo de vida do produto software, así como o seu crecemento e cambios.
- Permite incorporar obxectivos de calidade no desenvolvemento de produtos software.
- Adáptase moi ben ao deseño e programación orientada a obxectos. Posiblemente con este método é cando se obteñen mellores resultados.

En canto aos **inconvenientes** que presenta a utilización do modelo en espiral, cabe citar:

- Dificultade para adaptar a súa aplicabilidade ao software contratado, debido á pouca flexibilidade e liberdade deste.
- Dependencia excesiva da experiencia que se teña na identificación e avaliación de riscos.
- Necesidade dunha elaboración adicional dos pasos do modelo, o que depende tamén, en gran medida, da experiencia do persoal.

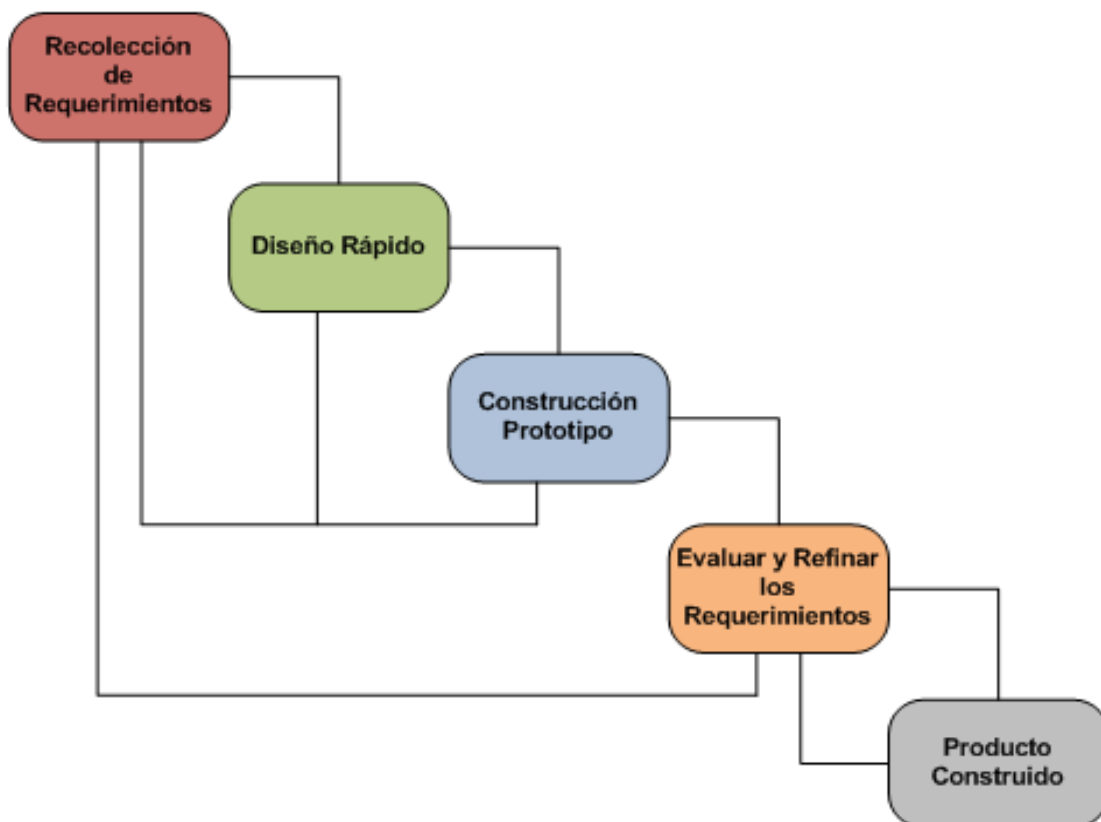
#### 33.4.4.3 *Modelos baseados en prototipos*

Os modelos baseados en prototipos céntranse na idea de ofrecer unha maior comprensión dos requisitos que o usuario formula, sobre todo se este non posúe unha idea clara e concreta das súas pretensións.

Ademais, este tipo de modelos pódese utilizar para intentar valorar dun xeito precoz a viabilidade da solución proposta, cando non se confía plenamente nela.

##### 33.4.4.3.1 Prototipado rápido

Este modelo fundaméntase na construción de prototipos dunha maneira fácil, barata e nun reducido período de tempo, permitindo así a súa avaliación temperá. Tamén se denominan de usar e tirar.



LENDAS: Recolección de requerimientos / Deseño rápido / Construción prototipo / Avaliar e refinar os requirimentos / Produto construído

O prototipo serve para crear e validar a especificación e para que o usuario teña unha idea de como será o software antes de que comece o desenvolvemento. É importante precisar que o prototipo se constrúe só para servir como mecanismo de definición dos requirimentos funcionais. Posteriormente hai que desbotalo e debe construírse o sistema cos criterios normais de calidade e mantemento, seguindo, por exemplo, o ciclo de vida clásico, xa que normalmente o prototipo se construíu tomando decisións de implementación contrarias ao bo criterio de desenvolvemento de software. Os obxectivos do prototipo son:

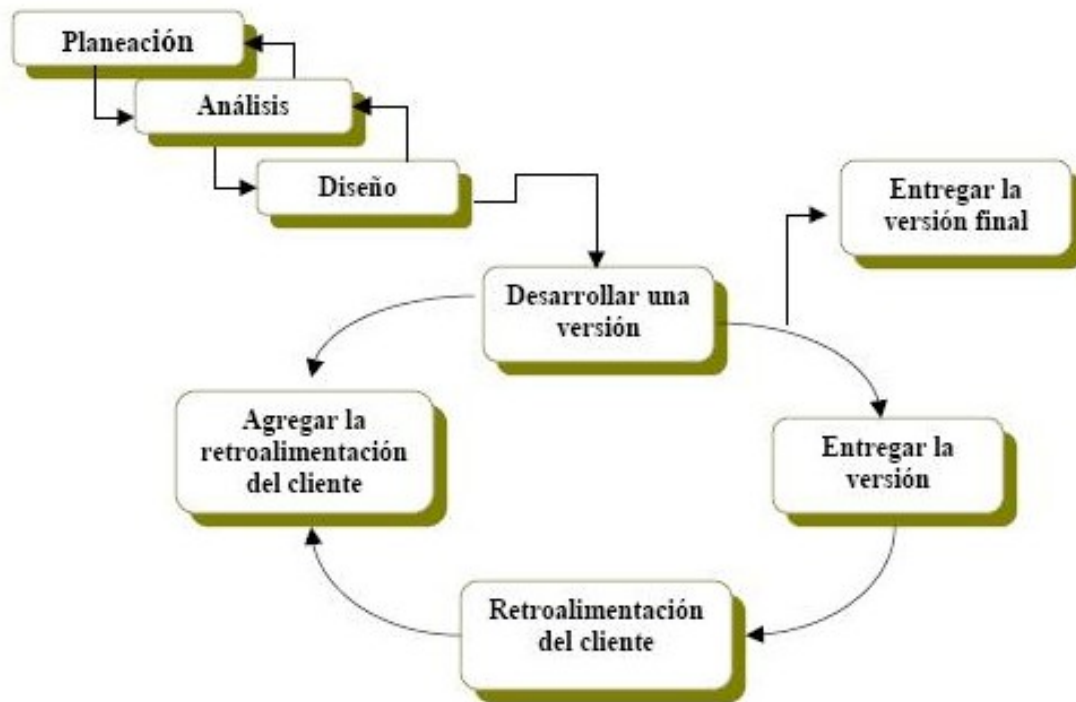
- Reducir o risco de construír un produto que se aparte das necesidades do usuario.
- Reducir o custo de desenvolvemento ao diminuír as correccións en etapas avanzadas do mesmo.
- Aumentar as posibilidades de éxito do produto.

O principal problema deste modelo é que o usuario ve no prototipo o que parece ser unha versión de traballo do software, sen saber que coa présa de facer que funcione non se tivo en conta a calidade do software global ou a facilidade de mantemento a longo prazo. Cando se informa de que o produto se debe construír outra vez para que se poidan manter os niveis altos de calidade, o cliente non o entende e pide que se apliquen uns pequenos axustes que poidan facer do prototipo un produto final.

#### 33.4.4.3.2 Prototipado evolutivo

Neste tipo de ciclo de vida constrúese unha implementación parcial do sistema que satisfai os requisitos coñecidos, a cal é utilizada polo usuario para chegar a comprender mellor a totalidade de requisitos que desexa.

LEND: Planificación / Análise / Deseño / Desenvolver unha versión /



Agregar a realimentación do cliente / Realimentación do cliente / Entregar a versión / Entregar a versión final.

Desde un punto de vista xenérico, pódese dicir que os modelos evolutivos se encamiñan a conseguir un sistema flexible que se poida expandir, de forma que se poida realizar rapidamente un novo sistema cando cambian os requisitos. Estes modelos consisten en implementar un produto software operativo e facelo evolucionar de acordo coa propia experiencia operacional. Están especialmente indicados en situacións en que se utilizan linguaxes de cuarta xeración (L4X) e para aqueloutras en que o usuario non pode dicir o que require, pero ha recoñecelo cando o vexa. Os modelos evolutivos danlle ao usuario unha rápida capacidade de operación inicial e unha boa base para determinar melloras do sistema. Están relacionados co concepto de RAD (*Rapid Application Development* – Desenvolvemento

Rápido de Aplicacións), que identifica os asistentes, cadros e contornos de fácil e rápida creación de software.

A *diferenza* fundamental entre o prototipado rápido e o evolutivo estriba en que namentres que no primeiro caso se asume que existen unha serie de requisitos reais —aínda que para definir o que o usuario quere realmente sexa preciso establecer unha serie de iteracións antes de que os requisitos se estabilicen ao final—, no caso evolutivo asúmese desde o principio que os requisitos cambian continuamente.

No prototipo rápido o lóxico é implementar só aqueles aspectos do sistema que se entenden mal, namentres que no prototipo evolutivo o lóxico é comezar polos aspectos que mellor se comprenden e seguir construíndo apoiados nos puntos fortes e non nos débiles. Como resultado desta forma de desenvolvemento, a solución software evoluciona, achegándose cada vez máis ás necesidades do usuario; agora ben, pasado un tempo o sistema software así construído deberá refacerse ou sufrir unha profunda reestruturación co fin de seguir evolucionando.

O modelo de prototipado evolutivo (*Evolutionary Development Model*) tamén ten as súas **dificultades**. Pódese considerar como unha nova versión —que utiliza linguaxes de programación de máis alto nivel— do vello modelo CODE-AND-FIX. Outro inconveniente que presenta é partir da suposición, moitas veces non realista, de que o sistema operacional do usuario final será o suficientemente flexible como para poder incorporar camiños de evolución futuros non planificados con anterioridade.

#### 33.4.5 *Modelos baseados en transformacións*

Xorden como solución ao problema que presentan os modelos de desenvolvemento que producen software con problemas estruturais. A súa principal virtude é que ofrecen a posibilidade de converter automaticamente unha especificación formal dun sistema nun software que cumpra o establecido nos requisitos.

Os pasos máis importantes que seguen este tipo de modelos son:

1. Especificación formal do produto tal como o permita a comprensión inicial do problema.
2. Transformación automática da especificación en código.
3. Realizar bucles iterativos para mellorar o rendemento do código resultante.
4. Probar o produto resultante.
5. Reaxustar as especificacións para deixalas en concordancia co resultado da experiencia operativa e volver xerar o código a partir das especificacións, volvendo optimizar e probar o produto.

O modelo de transformación, xa que logo, evita a dificultade de ter que modificar o código pouco estruturado (por pasar por sucesivas reoptimizacións), posto que aplica as modificacións sobre a especificación de partida. Isto tamén evita o tempo adicional que se empregaría nos pasos intermedios de deseño, codificación e probas.

A dificultade que presentan estes modelos é que as posibilidades de transformación automática normalmente só están dispoñibles para produtos relativamente pequenos e aplicados a unhas áreas moi limitadas. Tamén comparte algunhas das dificultades do modelo de desenvolvemento evolutivo tales como, por exemplo, a suposición de que o sistema operacional do usuario final se prestará a evolucións non planificadas con anterioridade.

Dentro deste tipo de modelos atópanse:

- Os que usan técnicas de cuarta xeración (Roger Pressman): adoitan estar baseados en ferramentas de cuarta xeración. Permiten a xeración de código rápido. Neles indícase qué se quere obter, non cómo.
- Baseados en modelos de transformación (Carma McClure) => Baseados en ferramentas CASE que permiten, seguindo o MCV

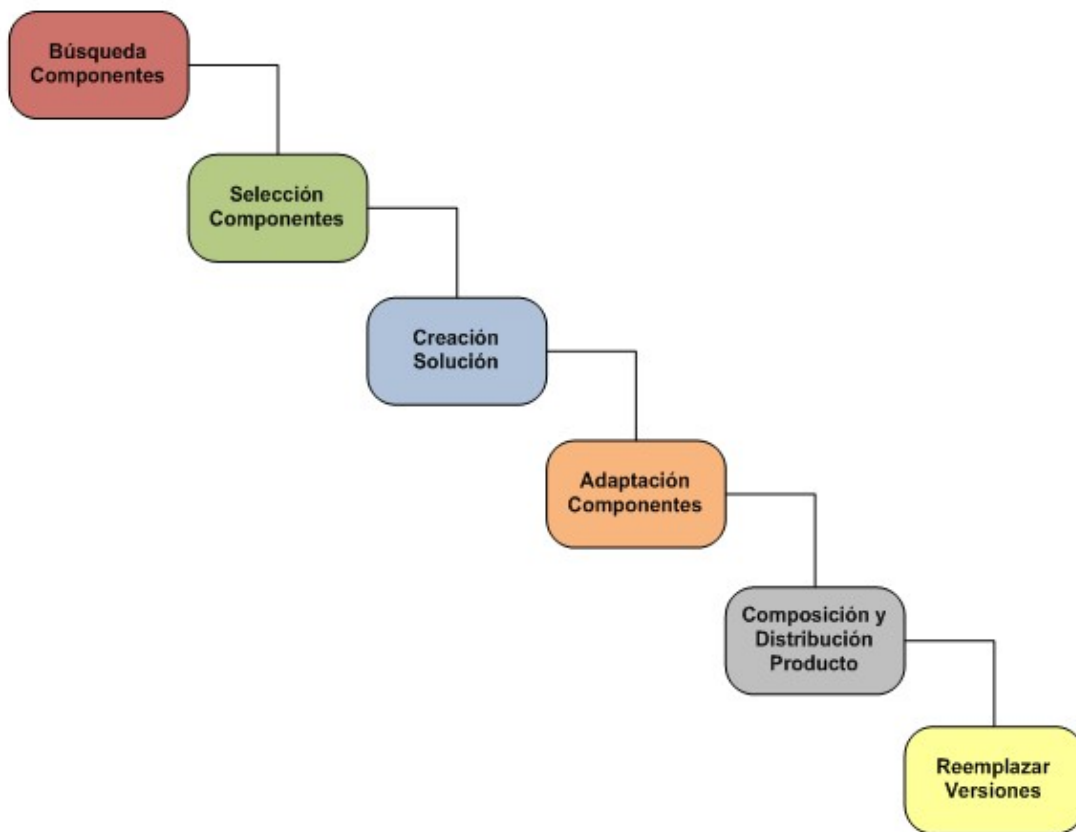
clásico, pasar dunha etapa a outra aplicando as transformacións que dan as ferramentas.

En ambos os casos, a filosofía xeral é chegar a xerar código a partir dunhas especificacións transformándoas por medio de ferramentas.

#### *33.4.6 Modelo baseado en compoñentes*

O modelo baseado en compoñentes xorde da necesidade de reutilización que os complexos sistemas actuais precisan para acelerar o seu desenvolvemento. Este modelo posibilita que certas pezas de código preelaboradas poidan ser reutilizadas noutras partes do sistema ou mesmo noutros sistemas para levar a cabo diversas tarefas, redundando en diversos beneficios como as melloras da calidade, a redución do ciclo de desenvolvemento e o maior retorno sobre o investimento.

Un compoñente é unha peza de código preelaborado que encapsula algunha funcionalidade exposta a través de interfaces estándar. Os compoñentes son os "ingredientes das aplicacións", que se xuntan e combinan para levar a cabo unha tarefa. O paradigma de ensamblar compoñentes e escribir código para facer que estes compoñentes funcionen coñécese como Desenvolvemento de Software Baseado en Compoñentes.



LENDAS: Busca compoñentes / Selección compoñentes / Creación solución / Adaptación compoñentes / Composición e distribución produto / Substituír versións.

Os pasos de que consta o ciclo de desenvolvemento para un sistema baseado en compoñentes son:

1. Buscar compoñentes, tanto COTS (*Comercial Off-The-Shelf*) como non COTS.
2. Seleccionar os compoñentes máis adecuados para o sistema.
3. Crear unha solución composta que integre a solución previa.
4. Adaptar os compoñentes seleccionados de forma que se axusten ao modelo de compoñentes ou aos requisitos da aplicación.
5. Compoñer e distribuír o produto.
6. Substituír versións anteriores ou manter as partes COTS e non COTS do sistema.

Ademais dos problemas inherentes á reutilización do software, os produtos COTS presentan problemas específicos como incompatibilidade,



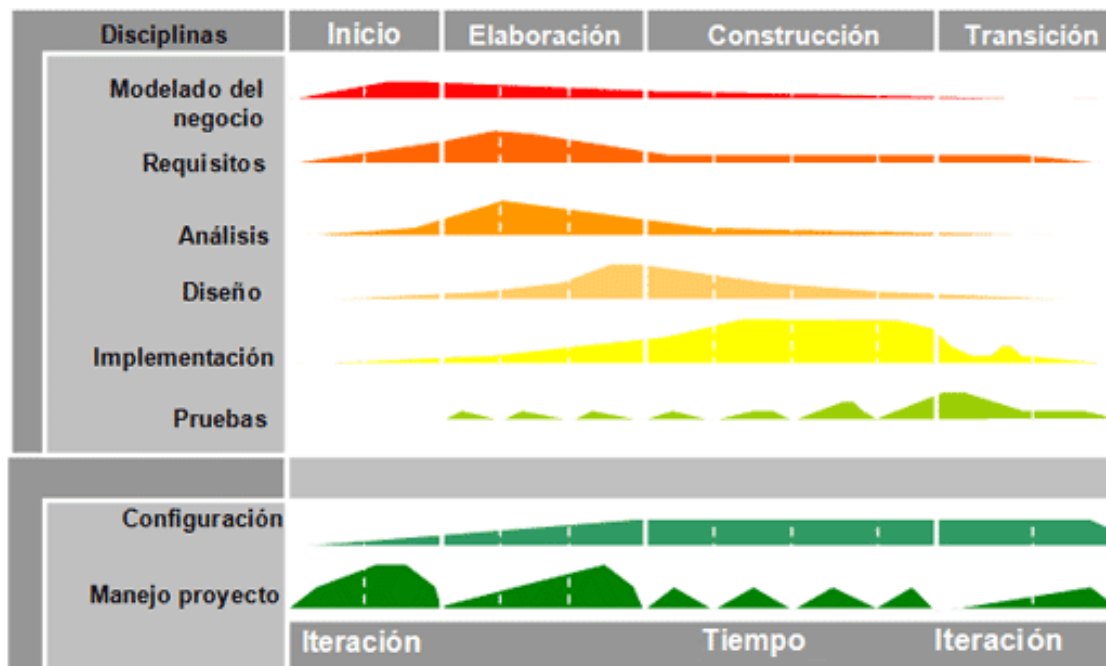
inflexibilidade (non existe código fonte), complexidade (esfuerzo de aprendizaxe) ou cambio de versións, polo que o establecemento de métodos sistemáticos e repetibles para avaliar e seleccionar os devanditos compoñentes é un aspecto importante para o desenvolvemento do software baseado en compoñentes e, en xeral, para a Enxeñería do Software Baseada en Compoñentes (ISBC).

Entre as vantaxes do desenvolvemento baseado en compoñentes temos que se reducen tempos e custos de desenvolvemento e se aumenta a fiabilidade. Entre os inconvenientes, están a dificultade para recoñecer os compoñentes potencialmente reutilizables, dificultade de catalogación e recuperación e os problemas de xestión de configuración.

### **33.5 Modelos de desenvolvemento**

#### *33.5.1 Proceso Unificado de Desenvolvemento de Software (PUDS)*

En realidade é unha metodoloxía que propón un modelo de ciclo de vida. Está desenvolvida por tres pais da IS moderna: Yourdon, Booch e Rumbaugh. Propón un modelo de ciclo de vida iterativo e incremental, centrado nunha arquitectura que guía o desenvolvemento do sistema, cuxas actividades están dirixidas por casos de uso e soporta as técnicas orientadas a obxectos. PUDS impulsa un control de calidade e unha xestión de riscos obxectivos e continuos.



LENDAS: Disciplinas / Inicio / Elaboración / Construcción / Transición / Modelaxe do negocio / Requisitos / Análise / Deseño / Implementación / Probas / Configuración / Manexo proxecto / Iteración / Tempo.

O PUDS componse de fases, iteracións e ciclos. Unha fase é o intervalo de tempo entre dous acontecementos importantes do proceso durante a cal se cumpre un conxunto ben definido de obxectivos, se completan entregables e se toman as decisións sobre se pasar ou non á seguinte fase. As **fases** son:

1. **Iniciación.** Nesta fase establécese a visión do negocio, que inclúe o contexto do negocio, os factores de éxito e a previsión económica. Para completar a visión do negocio xérase un plan do proxecto, unha descrición dos posibles riscos e do propio proxecto (requisitos principais do proxecto, restricións e características clave).
2. **Elaboración.** É onde o proxecto comeza a tomar forma. Nesta fase faise a análise do dominio do problema e obtense unha idea básica da arquitectura do sistema, ademais de revisárense os riscos. Nesta fase o proxecto aínda pode cancelarse ou redeseñarse.
3. **Construción.** Nesta fase o enfoque trasládase ao desenvolvemento de compoñentes e outras características do sistema que está a ser deseñado. Aquí realízase a maior parte das tarefas de codificación.



En proxectos grandes, pódese dividir a fase en varias iteracións para dividir os casos de uso en segmentos manexables que produzan prototipos funcionais.

4. **Transición.** O produto implántase na organización do usuario final. Aquí lévase a cabo a formación dos usuarios finais e as probas de aceptación do sistema para validalo contra as expectativas do usuario.

En cada fase hai unha ou varias iteracións. Unha **iteración** ofrece como resultado un incremento do produto desenvolvido que engade ou mellora as funcionalidades do sistema en desenvolvemento. Cada fase e iteración céntrase en diminuír algún risco e conclúe cun feito ben definido. O paso a través das 4 fases constitúe un **ciclo** de desenvolvemento e produce unha xeración de software. O primeiro ciclo é o inicial e despois serán ciclos de evolución do sistema.

Os fluxos de traballo do proceso son os seguintes:

- Modelaxe do negocio. O obxectivo é establecer unha mellor comprensión e unha mellor canle de comunicación entre os clientes e os expertos en sistemas.
- Requisitos. O obxectivo é describir o que o sistema debe facer.
- Análise e deseño. Aquí móstrase a forma que terá o sistema na fase de implementación.
- Implementación. Codificar e realizar probas unitarias.
- Probas. Realízanse probas de integración.
- Despregamento. Inclúe unha gran variedade de actividades, como a xeración de versións estables ou a distribución e instalación do software.
- Configuración e xestión de cambios.
- Xestión do proxecto. Realízase a 2 niveis: un nivel de gran groso, que trata a planificación das fases, e outro nivel de gran fino, que trata a planificación das iteracións.

- Contorno.

### 33.5.2 Programación extrema (eXtreme Programming)

Na programación extrema, todos os requirimentos se expresan como escenarios (chamados historias de usuario), os cales se implementan directamente como unha serie de tarefas. Os programadores traballan en parellas e desenvolven probas para cada tarefa antes de escribir o código. Todas as probas se deben executar satisfactoriamente cando o código novo se integre ao sistema. Existe un pequeno espazo de tempo entre as entregas do sistema. A programación extrema implica varias prácticas, que se axustan aos principios dos métodos áxiles:

1. O desenvolvemento incremental lévase a cabo a través de entregas do sistema pequenas e frecuentes e por medio dun enfoque para a descrición de requirimentos baseado nas historias de cliente ou escenarios que poden ser a base para o proceso de planificación.
2. A participación do cliente lévase a cabo a través do compromiso a tempo completo do cliente no equipo de desenvolvemento. Os representantes dos clientes participan no desenvolvemento e son os responsables de definir as probas de aceptación do sistema.
3. O interese nas persoas, en vez de nos procesos, lévase a cabo a través da programación en parellas, a propiedade colectiva do código do sistema, e un proceso de desenvolvemento sustentable que non implique excesivas xornadas de traballo.
4. O cambio lévase a cabo a través das entregas regulares do sistema, un desenvolvemento probado previamente e a integración continua.
5. O mantemento da simplicidade lévase a cabo a través da refactorización constante para mellorar a calidade do código e a utilización de deseños sinxelos que non prevén cambios futuros no sistema.

Os clientes do sistema son parte do equipo de desenvolvemento e discuten escenarios con outros membros do equipo. Desenvolven conxuntamente

unha «tarxeta de historias» (*story card*) que recolle as necesidades do cliente. O equipo de desenvolvemento intentará entón implementar ese escenario nunha entrega futura do software. Unha vez que se desenvolveron as tarxetas de historias, o equipo de desenvolvemento divídeas en tarefas e estima o esforzo e recursos requiridos para a súa implementación. O cliente establece entón a prioridade das historias que se van implementar.

O problema coa implementación de cambios imprevistos é que tenden a degradar a estrutura do software, polo que os cambios fanse cada vez máis difíciles de implementar. A programación extrema aborda este problema suxerindo que se debe refactorizar constantemente o software. Isto significa que o equipo de programación busca posibles melloras do software e as implementa inmediatamente. Polo tanto, o software sempre debe ser fácil de entender e cambiar cando se implementen novas historias.

Outra práctica innovadora que se introduciu é que os programadores traballan en parellas para desenvolver o software. As vantaxes disto son que apoia a idea da propiedade e responsabilidade comúns do sistema, actúa como un proceso de revisión informal do código e axuda na 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 da Escola Superior de Enxeñería Informática.**

**Universidade de Vigo.**



# **34. METODOLOXÍAS DE DESENVOLVEMENTO DE SISTEMAS DE INFORMACIÓN. MÉTRICA 3. RUP. METODOLOXÍAS ÁXILES.**

## **Tema 34. Metodoloxías de desenvolvemento de sistemas de información. Métrica 3. RUP. Metodoloxías áxiles.**

### **ÍNDICE**

#### **34.1 Metodoloxías de desenvolvemento de sistemas de información**

#### **34.2 Métrica versión 3**

##### **34.2.1 Procesos principais de métrica versión 3**

##### **34.2.2 Planificación de sistemas de información**

##### **34.2.3 Desenvolvemento de sistemas de información**

###### **34.2.3.1 Estudo de Viabilidade do Sistema (EVS)**

###### **34.2.3.2 Análise do Sistema de Información (ASI)**

###### **34.2.3.3 Deseño do Sistema de Información (DSI)**

###### **34.2.3.4 Construción do Sistema de Información (CSI)**

###### **34.2.3.5 Implantación e Aceptación do Sistema (IAS)**

##### **34.2.4 Mantemento de sistemas de información**

##### **34.2.5 Interfaces de métrica versión 3**

#### **34.3 RUP**

##### **34.3.1 Fases do ciclo de desenvolvemento**

##### **34.3.2 Fluxos de traballo**

#### **34.4 Metodoloxías áxiles**

##### **34.4.1 SCRUM**

##### **34.4.2 DSDM**

##### **34.4.3 Extreme Programming (XP)**

##### **34.4.4 FDD**

##### **34.4.5 Agile Modeling (AM)**

##### **34.4.6 Familia Crystal**



### 34.1 Metodoloxías de desenvolvemento de sistemas de información.

---

Desde que o desenvolvemento de software se comezou a considerar como un proceso de enxeñería, fóronse definindo diferentes marcos de traballo orientados a estruturar, planificar e controlar o proceso de desenvolvemento nos sistemas de información. O proceso detallado e completo de desenvolvemento de software adoita denominarse “metodoloxía”. As metodoloxías baséanse nunha combinación dos modelos de procesos xenéricos (fervenza, evolutivo, incremental, etc.).

As metodoloxías deben definir con precisión os produtos, roles e actividades involucrados, xunto con prácticas e técnicas recomendadas, guías de adaptación da metodoloxía ao proxecto, guías para uso de ferramentas de apoio, etc. As técnicas, notacións e guías asociadas que se aplican ás diferentes actividades do proceso de desenvolvemento son o que se coñece como "métodos".

A comparación e/ou clasificación de metodoloxías non é unha tarefa sinxela debido á diversidade de propostas e diferenzas no grao de detalle, información dispoñible e alcance de cada unha delas. A grandes trazos, se tomamos como criterio as notacións utilizadas para especificar produtos producidos en actividades de análise e deseño, podemos clasificar as metodoloxías en dous grupos: metodoloxías estruturadas e metodoloxías orientadas a obxectos. Por outra banda, considerando a súa filosofía de desenvolvemento, aquelas metodoloxías con maior énfase na planificación e control do proxecto, na especificación precisa de requisitos e modelado, reciben o apelativo de metodoloxías tradicionais (ou tamén denominadas pexorativamente metodoloxías pesadas, ou peso pesado). Outras metodoloxías, denominadas metodoloxías áxiles, están máis orientadas á xeración de código con ciclos moi curtos de desenvolvemento, diríxense a equipos de desenvolvemento pequenos, fan especial fincapé en aspectos humanos asociados ao traballo en equipo e implican activamente ao cliente

no proceso. Deseguido revísanse brevemente algunhas destas categorías de metodoloxías.

- **Metodoloxías estruturadas:** Os métodos estruturados comezaron a desenvolverse a finais dos setenta coa programación estruturada. A mediados dos setenta apareceron técnicas para o deseño (por exemplo, o diagrama de estrutura) primeiro e posteriormente para a análise (por exemplo, diagramas de fluxo de datos). Estas metodoloxías son particularmente apropiadas en proxectos que utilizan para a implementación linguaxes de 3.<sup>a</sup> e 4.<sup>a</sup> xeración. Exemplos de metodoloxías estruturadas de ámbito governamental: MERISE (Francia), MÉTRICA (España), SSADM (Reino Unido). Exemplos de propostas de métodos estruturados no ámbito académico: Gane & Sarson, Ward & Mellor, Yourdon & DeMarco e Information Engineering.
- **Metodoloxías orientadas a obxectos:** A súa historia vai unida á evolución das linguaxes de programación orientada a obxectos. A fins dos oitenta comezaron a consolidarse algúns métodos orientados a obxectos. En 1995 Booch e Rumbaugh propoñen o método unificado coa ambiciosa idea de conseguiren unha unificación dos seus métodos e notacións, que posteriormente se reorienta a un obxectivo máis modesto, para dar lugar ao Unified Modeling Language (UML), a notación OO máis popular na actualidade. Algúns métodos OO con notacións predecesoras de UML son: OOAD (Booch), OOSE (Jacobson), Coad & Yourdon, Shaler & Mellor e OMT (Rumbaugh). Algunhas metodoloxías orientadas a obxectos que utilizan a notación UML son: Rational Unified Process (RUP), OPEN, MÉTRICA (que tamén soporta a notación estruturada).
- **Metodoloxías tradicionais (non áxiles):** As metodoloxías non áxiles son aquelas que están guiadas por unha forte planificación durante todo o proceso de desenvolvemento; chamadas tamén metodoloxías tradicionais ou clásicas, onde se realiza unha intensa

etapa de análise e deseño antes da construción do sistema. Todas as propostas metodolóxicas antes indicadas poden considerarse como metodoloxías tradicionais.

- **Metodoloxías áxiles:** Un proceso é áxil cando o desenvolvemento de software é **incremental** (entregas pequenas de software, con ciclos rápidos), **cooperativo** (cliente e desenvolvedores traballan xuntos constantemente en estreita comunicación), **sinxelo** (o método en si mesmo é fácil de aprender e modificar, ben documentado), e **adaptable** (permite realizar cambios de último momento). Algunhas das metodoloxías áxiles identificadas son Extreme Programming, Scrum, familia de metodoloxías Crystal, Feature Driven Development, Proceso Unificado Rational, Dynamic Systems Development Method, Adaptive Software Development. Hase ver con máis detalle nun apartado posterior.
- **Proceso Unificado de Rational:** É un proceso de desenvolvemento de software e, xunto coa Linguaxe Unificada de Modelaxe UML, constitúe a metodoloxía estándar máis utilizada para a análise, implementación e documentación de sistemas orientados a obxectos. O RUP non é un sistema con pasos firmemente establecidos, senón un conxunto de metodoloxías adaptables ao contexto e necesidades de cada organización. Hase ver nun apartado posterior.
- **Métrica V3:** A metodoloxía MÉTRICA versión 3 ofrécelles ás organizacións un instrumento útil para a sistematización das actividades que dan soporte ao ciclo de vida do software. Hase ver nun apartado posterior.
- **Open Source Development Software:** Open Source é software desenvolvido con falta de coordinación, onde os programadores colaboran libremente, utilizando o código fonte distribuído e a infraestrutura de comunicacións de Internet. O código aberto baséase na filosofía do software libre, pero amplía esta ideoloxía lixeiramente

para presentar un enfoque máis comercial que inclúe tanto un modelo de negocio como unha metodoloxía de desenvolvemento.

### 34.2 Métrica versión 3.

---

Métrica versión 3 é unha evolución da metodoloxía métrica promovida polo Ministerio de Administracións Públicas do Goberno de España. Métrica consiste nunha metodoloxía para a planificación, desenvolvemento e mantemento dos sistemas de información, orientada á sistematización das actividades do ciclo de vida dos proxectos software no ámbito das administracións públicas. A metodoloxía MÉTRICA versión 3 ofrécelle ás organizacións un instrumento útil para a sistematización das actividades que dan soporte ao ciclo de vida do software dentro do marco que permite alcanzar os seguintes obxectivos:

- Proporcionar ou definir sistemas de información que axuden a conseguir os fins da organización mediante a definición dun marco estratéxico para o seu desenvolvemento.
- Dotar a organización de produtos software que satisfagan as necesidades dos usuarios dándolle unha maior importancia á análise de requisitos.
- Mellorar a produtividade dos departamentos de Sistemas e Tecnoloxías da Información e as Comunicacions, permitindo unha maior capacidade de adaptación aos cambios e tendo en conta a reutilización na medida do posible.
- Facilitar a comunicación e entendemento entre os distintos participantes na produción de software ao longo do ciclo de vida do proxecto, tendo en conta o seu papel e responsabilidade, así como as necesidades de todos e cada un deles.
- Facilitar a operación, mantemento e uso dos produtos software obtidos.

Na elaboración de MÉTRICA versión 3 cómpre ter en conta os métodos de desenvolvemento máis estendidos, así como os últimos estándares de enxeñería do software e calidade, ademais de referencias específicas en canto á seguridade e xestión de proxectos. Nunha única estrutura, a metodoloxía MÉTRICA versión 3 cobre distintos tipos de desenvolvemento, estruturado e orientado a obxectos, facilitando a través de interfaces a realización dos procesos de apoio ou organizativos: xestión de proxectos, xestión de configuración, aseguramento de calidade e seguridade.

No que se refire a estándares cómpre ter en conta como referencia o modelo de ciclo de vida de desenvolvemento proposto na norma ISO/IEC 12207 *Information technology - Software life cycle processes*. Seguindo este modelo elaborouse a estrutura de MÉTRICA versión 3, na que se distinguen procesos principais (planificación, desenvolvemento e mantemento) e interfaces (xestión de proxectos, aseguramento da calidade, seguridade e xestión de proxectos) que teñen como obxectivo darlle soporte ao proxecto nos aspectos organizativos. Ademais da norma ISO/IEC 12207, entre os estándares de referencia hai que destacar as normas ISO/IEC TR 15.504/SPICE *Software Process Improvement and Assurance Standards Capability Determination*, UNE-EN-ISO 9001:2000 *Sistemas de xestión da calidade. Requisitos*, UNE-EN-ISO 9000:2000 *Sistemas de xestión da calidade. Fundamentos e vocabulario* e o estándar IEEE 610.12-1.990 *Standard Glossary of Software Engineering Terminology*. Igualmente é preciso ter en conta outras metodoloxías como SSADM, Merise, Information Engineering, MAGERIT. *Metodoloxía de análise e xestión de riscos dos sistemas de información* promovida polo Consello Superior de Informática e EUROMÉTODO.

Diferenciouse entre a aplicación de técnicas, como conxunto de heurísticas e procedementos apoiados en estándares que utilizan notacións específicas en canto á sintaxe e semántica, e de prácticas, cuxa utilización

non implica regras preestablecidas coa mesma rixidez. As novas técnicas están amplamente soportadas por ferramentas comerciais.

### **34.2.1 Procesos principais de métrica versión 3**

MÉTRICA versión 3 ten un enfoque orientado ao ciclo de vida de software e por iso se enmarcou dentro da norma ISO/IEC 12207, que se centra na clasificación e definición dos procesos do ciclo de vida do software, cubrindo o proceso de desenvolvemento e o proceso de mantemento de sistemas de información.

MÉTRICA versión 3 foi concibida para abarcar o desenvolvemento completo de sistemas de información, sexa cal fose a súa complexidade e magnitude, polo cal a súa estrutura responde a desenvolvementos máximos e deberá adaptarse e dimensionarse en cada momento de acordo ás características particulares de cada proxecto. A metodoloxía descompón cada un dos procesos en actividades e estas, pola súa vez, en tarefas. Para cada tarefa descríbese o seu contido facendo referencia ás súas principais accións, produtos, técnicas, prácticas e participantes. A orde asignada ás actividades non se debe interpretar como secuencia na súa realización, xa que estas se poden realizar en orde diferente á súa numeración ou ben en paralelo. No entanto, non se dará por acabado un proceso ata non finalizar todas as actividades deste determinadas ao comezo do proxecto.

Así, os procesos da estrutura principal de MÉTRICA versión 3 son os seguintes:

- PLANIFICACIÓN DE SISTEMAS DE INFORMACIÓN.
- DESENVOLVEMENTO DE SISTEMAS DE INFORMACIÓN.
- MANTEMENTO DE SISTEMAS DE INFORMACIÓN.

### **34.2.2 Planificación de sistemas de información**

Os plans estratéxicos de sistemas de información pretenden abordar o estudo dos sistemas e recursos informáticos para conseguir uns obxectivos determinados dentro das organizacións. O obxectivo principal dun plan de sistemas de información é proporcionar un marco estratéxico de referencia para os sistemas de información dun determinado ámbito da organización. O resultado do plan de sistemas debe, xa que logo, orientar as actuacións en materia de desenvolvemento de sistemas de información co obxectivo básico de apoiar a estratexia corporativa, elaborando unha arquitectura de información e un plan de proxectos informáticos para darlles apoio aos obxectivos estratéxicos. Por este motivo é necesario un proceso como o de planificación de sistemas de información, no que participen, por unha banda, os responsables dos procesos da organización cunha visión estratéxica, e pola outra, os profesionais de SI capaces de enriquecer a devandita visión coa achega de vantaxes competitivas por medio dos sistemas e tecnoloxías da información e comunicacións.

Como produtos finais deste proceso obtéñense os seguintes:

- Catálogo de requisitos de PSI que xorde do estudo da situación actual —no caso de que sexa significativo o devandito estudo— do diagnóstico que se levou a cabo e das necesidades de información dos procesos da organización afectados polo plan de sistemas.
- Arquitectura de información que se compón dos seguintes produtos: modelo de información, modelo de sistemas de información, arquitectura tecnolóxica, plan de proxectos e plan de mantemento do PSI.

Este novo enfoque de aliñamento dos sistemas de información coa estratexia da organización, a implicación directa da alta dirección e a proposta de solución presenta como vantaxes:

- A implicación da alta dirección facilita que se poida desenvolver cos recursos necesarios e o calendario establecido.
- A perspectiva horizontal dos procesos dentro da organización facilita que se atenda a intereses globais e non particulares de unidades organizativas que poidan desvirtuar os obxectivos do plan.
- A prioridade do desenvolvemento dos sistemas de información da organización por obxectivos estratéxicos.
- A proposta de arquitectura de información que se fai no plan é máis estratéxica que tecnolóxica.

### **34.2.3 Desenvolvemento de sistemas de información**

O proceso de desenvolvemento de MÉTRICA versión 3 contén todas as actividades e tarefas que se deben levar a cabo para desenvolver un sistema, e abrangue desde a análise de requisitos ata a instalación do software. Ademais das tarefas relativas á análise, inclúe dúas partes no deseño de sistemas: arquitectónico e detallado. Tamén cobre as probas unitarias e de integración do sistema. Este proceso é, sen dúbida, o máis importante dos identificados no ciclo de vida dun sistema e relaciónase con todos os demais.

En MÉTRICA versión 3 abordáronse os dous tipos de desenvolvemento: estruturado e orientado a obxectos, polo que foi necesario establecer actividades que cómpre realizar en función do tipo de desenvolvemento elixido. Definíronse 5 subprocesos para este apartado:

- Estudo de Viabilidade do Sistema (EVS)
- Análise do Sistema de Información (ASI).
- Deseño do Sistema de Información (DSI).
- Construción do Sistema de Información (CSI).
- Implantación e Aceptación do Sistema (IAS).



#### **34.2.3.1 Estudo de Viabilidade do Sistema (EVS)**

Consiste en analizar un conxunto de necesidades concreto e definido, para elaborar unha solución inicial abarcable a curto prazo. Os criterios cos que se fai esta proposta non serán estratéxicos senón tácticos e relacionados con aspectos económicos, técnicos, legais e operativos. Os resultados do estudo de viabilidade do sistema constituirán a base para tomar a decisión de seguir adiante ou abandonar. Se se decide seguir adiante poden xurdir un ou varios proxectos que afecten a un ou varios sistemas de información. Consideraranse alternativas de solución baseadas en solucións "a medida", solucións fundamentadas na adquisición de produtos software do mercado ou solucións mixtas. Para valorar as alternativas propostas e determinar unha única solución, estudarase o impacto na organización de cada unha delas, o investimento e os riscos asociados. O resultado final deste proceso son os produtos relacionados coa solución que se propón para atender á necesidade concreta que apareceu no proceso, e que depende de se a solución implica desenvolvemento a medida ou non.

#### **34.2.3.2 Análise do Sistema de Información (ASI)**

Durante esta fase inicial do proceso, o obxectivo consiste en recompilar de forma detallada, concreta e específica todos os aspectos referentes ao sistema de información. O resultado obtido deberase presentar en forma de especificación dun catálogo de requisitos que satisfagan as necesidades de información dos usuarios finais cara a quen vai dirixido o sistema. Esta especificación representa a saída do proceso ASI e representa a entrada para o proceso de Deseño do Sistema de Información (DSI).

En primeiro lugar descríbese inicialmente o sistema de información a partir dos produtos xerados no proceso Estudo de Viabilidade do Sistema (EVS). Delimítase o seu alcance, xérase un catálogo de requisitos xerais e descríbese o sistema mediante uns modelos iniciais de alto nivel. Recóllense de forma detallada os requisitos funcionais que o sistema de información debe abarcar, catalogándoos, o que permite facer a traza ao longo dos procesos de desenvolvemento. Ademais, identifícanse os requisitos non funcionais do sistema, é dicir, as facilidades que debe proporcionar o sistema, e as restricións a que estará sometido en canto a rendemento, frecuencia de tratamento, seguridade, etc. Para facilitar a análise do sistema identifícanse os subsistemas de análise, e elabóranse os modelos de casos de uso e de clases, en desenvolvementos orientados a obxectos, e de datos e procesos en desenvolvementos estruturados. Especificáanse todas as interfaces entre o sistema e o usuario, como formatos de pantallas, diálogos, formatos de informes e formularios de entrada. Finalizados os modelos, realízase unha análise de consistencia. Unha vez realizada esta análise de consistencia, elabórase o produto ***Especificación de Requisitos Software***, que constitúe un punto de referencia no desenvolvemento do software e a liña base de referencia para as peticións de cambio sobre os requisitos inicialmente especificados. Neste proceso iníciase tamén a especificación do plan de probas, que se completará no proceso Deseño do Sistema de Información (DSI). Neste proceso é moi importante a participación dos usuarios a través de técnicas interactivas, como deseño de diálogos e prototipos, que lle permiten ao usuario familiarizarse co novo sistema e colaborar na súa construción e perfeccionamento.

#### **34.2.3.3 Deseño do Sistema de Información (DSI)**

O propósito do Deseño do Sistema de Información (DSI) é obter a definición da arquitectura do sistema e do contorno tecnolóxico que lle vai

dar soporte, xunto coa especificación detallada dos compoñentes do sistema de información. A partir desta información, xéranse todas as especificacións de construción relativas ao propio sistema, así como a especificación técnica do plan de probas, a definición dos requisitos de implantación e o deseño dos procedementos de migración e carga inicial; estes últimos cando proceda.

Este proceso consta dun primeiro bloque de actividades, que se realizan en paralelo e que teñen como obxectivo obter o deseño de detalle do sistema de información, que comprende a partición física do sistema de información, independente dun contorno tecnolóxico concreto, a organización en subsistemas de deseño, a especificación do contorno tecnolóxico sobre o que se despregan os devanditos subsistemas, e a definición dos requisitos de operación, administración do sistema, seguridade e control de acceso. No caso de deseño orientado a obxectos, convén sinalar que se preveu que o deseño da persistencia se levase a cabo sobre bases de datos relacionais.

Un segundo bloque de actividades completa o deseño do sistema de información, no que se xeran todas as especificacións necesarias para a construción do sistema de información.

#### **34.2.3.4 Construción do Sistema de Información (CSI)**

A Construción do Sistema de Información (CSI) ten como obxectivo final a construción e proba dos distintos compoñentes do sistema de información, a partir do seu conxunto de especificacións lóxicas e físicas, obtido no proceso de Deseño do Sistema de Información (DSI). Desenvólvense os procedementos de operación e seguridade e elabóranse os manuais de usuario final e de explotación; estes últimos cando proceda. Para conseguir este obxectivo, recóllese a información relativa ao produto do deseño Especificacións de construción do sistema de información,

prepárase o contorno de construción, xérase o código de cada un dos compoñentes do sistema de información e vanse realizando, a medida que se vaia finalizando a construción, as probas unitarias de cada un deles e as de integración entre subsistemas. Se fose necesario realizar unha migración de datos, é neste proceso onde se leva a cabo a construción dos compoñentes de migración e procedementos de migración e carga inicial de datos.

#### **34.2.3.5 Implantación e Aceptación do Sistema (IAS)**

Este proceso ten como obxectivo principal a entrega e aceptación do sistema na súa totalidade, que pode comprender varios sistemas de información desenvolvidos de maneira independente, segundo se estableceu no proceso de Estudo de Viabilidade do Sistema (EVS), e un segundo obxectivo, que é levar a cabo as actividades oportunas para o paso a produción do sistema. Establécese o plan de implantación, unha vez revisada a estratexia de implantación, e detállase o equipo que o realizará. Para o inicio deste proceso tómanse como punto de partida os compoñentes do sistema probados de forma unitaria e integrados no proceso Construción do Sistema de Información (CSI), así como a documentación asociada. O sistema someterase ás probas de implantación coa participación do usuario de operación, responsable, entre outros aspectos, de comprobar o comportamento do sistema baixo as condicións máis extremas. Tamén se someterá ás probas de aceptación; a execución destas é responsabilidade do usuario final. Neste proceso elabórase o plan de mantemento do sistema de forma que o responsable do mantemento coñeza o sistema antes de que este pase a produción. Tamén se establece o acordo de nivel de servizo requirido unha vez que se inicie a produción.

#### **34.2.4 Mantemento de Sistemas de Información (MSI)**

O obxectivo deste proceso é a obtención dunha nova versión dun sistema de información desenvolvido con MÉTRICA, a partir das peticións de mantemento que os usuarios realizan con motivo dun problema detectado no sistema ou pola necesidade dunha mellora deste. Só se considerarán en MÉTRICA versión 3 os tipos de mantemento **correctivo** e **evolutivo**. Ante unha petición de cambio dun sistema de información xa en produción, realízase un rexistro das peticións, diagnostícase o tipo de mantemento, decídese se se lle dá resposta ou non, en función do plan de mantemento asociado ao sistema afectado pola petición, e establécese con que prioridade. A definición da solución ao problema ou necesidade presentada polo usuario e que realiza o responsable de mantemento inclúe un estudo do impacto, a valoración do esforzo e custo, as actividades e tarefas do proceso de desenvolvemento que cómpre realizar e o plan de probas de regresión.

#### **34.2.5 Interfaces de métrica versión 3**

A estrutura de MÉTRICA versión 3 inclúe tamén un conxunto de interfaces que definen unha serie de actividades de tipo organizativo ou de soporte ao proceso de desenvolvemento e aos produtos, que, no caso de existiren na organización, deberán aplicarse para enriquecer ou influír na execución das actividades dos procesos principais da metodoloxía, e que se non existen haberá que realizar para complementar e garantir o éxito do proxecto desenvolvido con MÉTRICA versión 3. Son catro:

- **Xestión de proxectos:** Ten como finalidade principal a planificación, o seguimento e control das actividades e dos recursos humanos e materiais que interveñen no desenvolvemento dun sistema de información. Como consecuencia deste control é posible coñecer en

todo momento qué problemas se producen e resolvelos ou palialos o máis pronto posible, o cal evitará desviacións temporais e económicas.

As actividades da interface de xestión de proxectos son de tres tipos:

- o *Actividades de inicio do proxecto*, que permiten estimar o esforzo e establecer a planificación do proxecto.
  - o *Actividades de seguimento e control*, que supervisan a realización das tarefas por parte do equipo de proxecto e xestionan as incidencias e cambios nos requisitos que se poidan presentar e afectar á planificación do proxecto.
  - o *Actividades de finalización do proxecto*, peche e rexistro da documentación de xestión.
- **Seguridade:** A interface de seguridade fai posible incorporar durante a fase de desenvolvemento as funcións e mecanismos que reforzan a seguridade do novo sistema e do propio proceso de desenvolvemento, asegurando a súa consistencia e seguridade, completando o plan de seguridade vixente na organización ou desenvolvéndoo desde o principio, e utilizando MAGERIT como metodoloxía de análise e xestión de riscos no caso de que a organización non dispoña da súa propia metodoloxía. Prevé dous tipos de actividades diferenciadas: as relacionadas coa seguridade intrínseca do sistema de información, e as que velan pola seguridade do propio proceso de desenvolvemento do sistema de información. Ademais faise especial fincapé na formación en materia de seguridade. Ao seren finitos os recursos, non se poden asegurar todos os aspectos do desenvolvemento dos sistemas de información, polo que haberá que aceptar un determinado nivel de risco, concentrándose nos aspectos máis comprometidos ou ameazados.
- **Xestión da configuración:** A interface de xestión da configuración consiste na aplicación de procedementos administrativos e técnicos durante o desenvolvemento do sistema de información e o seu posterior mantemento. A súa finalidade é identificar, definir, proporcionar información e controlar os cambios na configuración do sistema, así como as súas modificacións e versións. Este proceso permitirá coñecer o

estado de cada un dos produtos que se definiron como elementos de configuración, garantindo que non se realizan cambios incontrolados e que todos os participantes no desenvolvemento do sistema dispoñen da versión adecuada dos produtos que manexan. A xestión de configuración facilita ademais o mantemento do sistema, proporcionando información precisa para valorar o impacto dos cambios solicitados e reducindo o tempo de implantación dun cambio, tanto evolutivo como correctivo.

- **Aseguramento da calidade:** O obxectivo da interface de aseguramento da calidade é proporcionar un marco común de referencia para a definición e posta en marcha de plans específicos de aseguramento de calidade aplicables a proxectos concretos. As actividades están orientadas a verificar a calidade dos produtos. Son actividades que avalían a calidade e que son realizadas por un grupo de asesoramento da calidade independente dos responsables da obtención dos produtos. As actividades consideradas permitirán reducir, eliminar e previr as deficiencias de calidade dos produtos que se van obter, así como alcanzar unha razoable confianza en que as prestacións e servizos esperados polo cliente ou o usuario queden satisfeitos.

### 34.3 RUP (Rational Unified Process)

---

É unha das metodoloxías máis estendidas e coñecidas pola súa gran difusión comercial; intenta integrar todos os aspectos que se deben ter en conta durante todo o ciclo de vida do software, co obxectivo de facer abarcables proxectos software tanto pequenos coma grandes. Foi definida polos creadores do UML unificando os métodos de Jacobson, Booch e Rumbaugh cando traballaban na empresa Rational. Ademais, Rational proporciona ferramentas para todos os pasos do desenvolvemento así como documentación en liña para os seus clientes. As **características principais** de RUP son:

- **Guiado/Manexado por casos de uso:** Un caso de uso é unha facilidade que o software debe prover aos seus usuarios. Os casos de uso substitúen a antiga especificación funcional tradicional e constitúen a guía fundamental establecida para as actividades que se van realizar durante todo o proceso de desenvolvemento, incluíndo o deseño, a implementación e as probas do sistema.
- **Centrado en arquitectura:** A arquitectura inclúe os elementos máis significativos do sistema e está influenciada, entre outros, por plataformas software, sistemas operativos, manexadores de bases de datos, protocolos, consideracións de desenvolvemento como sistemas herdados e requirimentos non funcionais. Os casos de uso guían o desenvolvemento da arquitectura e a arquitectura realiméntase nos casos de uso; os dous xuntos permiten conceptualizar, xestionar e desenvolver adecuadamente o software.
- **Iterativo e incremental:** Para facer máis manexable un proxecto recoméndase dividilo en ciclos. Para cada ciclo establécense fases de referencia, cada unha das cales debe ser considerada como un miniproxecto cun núcleo fundamental que está constituído por unha ou máis iteracións das actividades principais básicas de calquera proceso de desenvolvemento.
- **Desenvolvemento baseado en compoñentes:** A creación de sistemas intensivos en software require dividir o sistema en compoñentes con interfaces ben definidas, que posteriormente serán ensambladas para xerar o sistema. Esta característica nun proceso de desenvolvemento permite que o sistema se vaia creando a medida que se obteñen ou que se desenvolven e maduran os seus compoñentes.
- **Utilización dunha única linguaxe de modelaxe:** UML é adoptada como única linguaxe de modelaxe para o desenvolvemento de todos os modelos.
- **Proceso integrado:** Establécese unha estrutura que abranca os ciclos, fases, fluxos de traballo, mitigación de riscos, control de calidade,

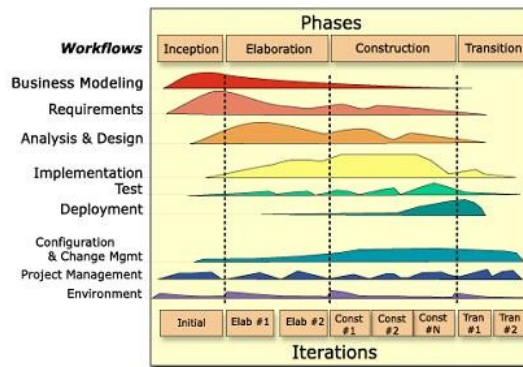


xestión do proxecto e control de configuración; o proceso unificado establece unha estrutura que integra todas estas facetas. Ademais esta estrutura inclúe os vendedores e desenvolvedores de ferramentas para soportar a automatización do proceso, soportar fluxos individuais de traballo, construír os diferentes modelos e integrar o traballo a través do ciclo de vida e a través de todos os modelos.

A **estrutura estática** do proceso unificado defínese en función de catro elementos:

- **Roles:** Un rol define o comportamento e responsabilidades dun individuo, ou dun grupo de individuos traballando xuntos como un equipo. Unha persoa pode desempeñar diversos roles, así como un mesmo rol pode ser representado por varias persoas. As responsabilidades dun rol son tanto o levar a cabo un conxunto de actividades como o ser o “dono” dun conxunto de produtos. Responde á pregunta **quen?**
- **Actividades:** Unha actividade dun traballador en concreto é unha unidade de traballo que se lle pode pedir que realice a unha persoa que desempeñe ese rol. As actividades teñen un obxectivo concreto, normalmente expresado como crear ou actualizar algún produto. Responden á pregunta **como?**
- **Produtos:** Un produto ou artefacto é un anaco de información que é producido, modificado ou usado por un proceso. Os produtos son os resultados tanxibles do proxecto, as cousas que vai creando e usando ata obter o produto final. Responden á pregunta **que?**
- **Fluxos de traballo:** A mera enumeración de roles, actividades e produtos non define un proceso; necesitamos definir a secuencia de actividades realizadas polos diferentes roles, así como a relación entre eles, que producen uns resultados observables. As distintas iteracións que se realicen consistirán na execución destes fluxos de traballo cunha maior ou menor intensidade, dependendo da fase e iteración na que nos atopemos. Responden á pregunta **cando?**

### 34.3.1 Fases do ciclo de desenvolvemento.



Este proceso de desenvolvemento considera que calquera desenvolvemento dun sistema software debe pasar por catro **fases**:

- **Fase 1: Inicio.** O seu obxectivo principal é establecer os obxectivos para o ciclo de vida do produto. Nesta fase establécese o caso do negocio co fin de delimitar o alcance do sistema, saber qué se cubrirá e delimitar o alcance do proxecto. Os produtos desta fase son:
  - Alcance do sistema
    - Lista de características
    - Modelo do dominio ou modelo do negocio (1.<sup>a</sup> versión)
    - Modelo de casos de uso, modelo de análise e modelo de deseño (1.<sup>a</sup> versión)
    - Requirimentos suplementarios (1.<sup>a</sup> versión)
  - Arquitectura inicial (proposta)
  - Lista inicial de riscos (riscos críticos máis importantes) e lista priorizada dos casos de uso
  - Prototipo para validación de conceptos (prototipo de descarte)
  - Contorna de desenvolvemento configurado (proceso e ferramentas) (configuración inicial)
  - Plan inicial do proxecto
  - Caso inicial do negocio (1.<sup>a</sup> versión) (contexto do negocio e criterios de éxito) (custo, tempos, calidade, utilidades)

- **Fase 2: Elaboración.** O seu obxectivo principal é formular a arquitectura para o ciclo de vida do produto. Nesta fase realízase captúraa da maior parte dos requirimentos funcionais, manexando os riscos que interfiran cos obxectivos do sistema, acumulando a información necesaria para o plan de construción e obtendo suficiente información para facer realizable o caso do negocio. Ao rematar, habemos ter os seguintes produtos:
  - o Contexto do sistema (modelo do dominio ou modelo do negocio preferiblemente completo)
  - o Captura do 80 % dos requirimentos funcionais
    - Modelo de casos de uso (aprox. o 80 %) e modelo de análise (realización dos casos de uso máis significativos)
    - Modelo de deseño, modelo de despregamento e modelo de implementación (menos do 10 %)
    - Niveis para os atributos de calidade e requirimentos suplementarios actualizados
    - Manual preliminar de usuario
  - o Arquitectura de referencia (liña de base) (descrición das vistas arquitecturais dos modelos do sistema)
  - o Lista actualizada de riscos (críticos e significativos) e riscos críticos mitigados
  - o Plan do proxecto para as fases de construción e transición
  - o Contorno de desenvolvemento adecuado (proceso e ferramentas)
  - o Caso do negocio completo (e “contrato” ou declaración do negocio)
- **Fase 3: Construción.** O seu obxectivo principal é alcanzar a capacidade operacional do produto. Nesta fase, a través de sucesivas iteracións e incrementos, desenvólvese un produto software, listo para operar; este é frecuentemente chamado versión beta. Os produtos obtidos serán:

- o Modelos completos (casos de uso, análise, deseño, despregamento e implementación)
  - o Arquitectura íntegra (mantida e minimamente actualizada)
  - o Riscos presentados mitigados
  - o Plan do proxecto para a fase de transición
  - o Manual Inicial de Usuario (con suficiente detalle)
  - o Prototipo operacional – beta
  - o Caso do negocio actualizado
- **Fase 4: Transición.** O seu obxectivo principal é realizar a entrega do produto operando, unha vez realizadas as probas de aceptación por un grupo especial de usuarios e efectuados os axustes e correccións que se requiran. Os produtos obtidos serán:
  - o Prototipo operacional
  - o Documentos legais
  - o Caso do negocio completo
  - o Liña de base do produto completa e corrixida que inclúe todos os modelos do sistema
  - o Descrición da arquitectura completa e corrixida
  - o Manuais para usuario final, operador e administrador do sistema, e materiais para adestramento

### **34.3.2 Fluxos de traballo.**

En RUP defínense nove **fluxos de traballo** distintos, separados en dous grupos: enxeñería (2, 3, 4, 5, 6, 9) e de apoio (1, 7, 8).

- 1- **Administración do proxecto.** O fluxo de traballo céntrase en tres aspectos: planificar un proxecto iterativo e cada iteración particular, administrar o risco e monitorar o progreso do proxecto a través de métricas. A planificación dun proxecto debe acometerse en dous niveis de abstracción: un plan de “gran groso” para as fases e un plan de “gran fino” para cada iteración. O plan de desenvolvemento

(ou plan de fases) debe conter as datas esperadas para os eventos principais. Tamén debería ter unha previsión das necesidades de persoal e medios.

- 2- **Modelado do negocio.** Con este fluxo de traballo pretendemos chegar a un mellor entendemento da organización onde imos implantar o noso produto. Este fluxo de traballo non será sempre necesario.
- 3- **Requisitos.** Establécese *QUÉ* é o que ten que facer exactamente o sistema que construíamos. Neste fluxo de traballo hai que analizar o problema, comprender as necesidades dos interesados e expresalas en forma de requisitos, construír diagramas de casos de uso para os requisitos funcionais, e os non funcionais describilos textualmente en especificacións suplementarias. Ademais, hai que xestionar os cambios nos requisitos ao longo de todo o proceso.
- 4- **Análise e deseño.** O obxectivo deste fluxo de traballo é traducir os requisitos a unha especificación que describe como implementar o sistema. A **análise** consiste en obter unha visión do sistema que se preocupa de ver *QUÉ* fai, de modo que só se interesa polos requisitos funcionais. Doutra banda, o deseño é un refinamento da análise que ten en conta os requisitos non funcionais; en definitiva, *CÓMO* cumpre o sistema os seus obxectivos. O resultado final máis importante deste fluxo de traballo será o modelo de deseño. Consiste en colaboracións de clases, que poden ser agregadas en paquetes e subsistemas.
- 5- **Implementación.** Neste fluxo de traballo impleméntanse as clases e obxectos en ficheiros fonte, binarios, executables e demais. Ademais, débense facer as probas unitarias: cada implementador é responsable de comprobar as unidades que produza. O resultado final deste fluxo de traballo é un sistema executable.
- 6- **Test.** Este fluxo de traballo é o encargado de avaliar a calidade do produto que estamos desenvolvendo. O papel desta comprobación non é asegurar a calidade, pero si avaliala, e proporcionar unha

realimentación a tempo, de forma que as cuestións de calidade se poidan resolver de modo efectivo en tempo e custo. Os principais aspectos que deben ser avaliados nun produto software son a *Fiabilidade* (resistente a fallos), a *Funcionalidade* (fai o que debe) e o *Rendemento* (leva a cabo o seu traballo de modo efectivo).

- 7- **Configuración e xestión de cambios.** A finalidade deste fluxo de traballo é manter a integridade de todos os produtos que se crean no proceso, así como a de proporcionar información do proceso evolutivo que seguiron. Inclúe tres funcións interdependentes, como son a **xestión da configuración**, a xestión **das peticións de cambio**, e a **realización de métricas**.
- 8- **Contorno.** A finalidade deste fluxo é darlle soporte ao proxecto coas adecuadas ferramentas, procesos e métodos. É dicir, ter a punto as ferramentas que se vaian necesitar en cada momento, así como definir a instancia concreta de proceso unificado que se vai seguir.
- 9- **Despregamento.** O obxectivo deste fluxo de traballo é producir con éxito distribucións do produto e distribuírllelo aos usuarios.

#### 34.4 Metodoloxías áxiles.

---

Nas **metodoloxías áxiles**, a creación de valor mediante a adaptación ás necesidades cambiantes aparece nun primeiro plano fronte á tradicional idea de deseñar un plan e cumprir uns calendarios/requirimentos estáticos. Os proxectos xestionados con metodoloxías áxiles iníciase sen un detalle pechado do que vai ser construído. Comercialmente, os proxectos poden ser vendidos como servizos e non como produtos. As características básicas dos proxectos xestionados con metodoloxías áxiles son as seguintes:

- **Incerteza:** a dirección indica a necesidade estratéxica que se desexa satisfacer (sen entrar en detalles), ofrecéndolle máxima liberdade ao equipo de traballo.

- **Equipos autoorganizados:** non existen roles especializados.
  - Autonomía: liberdade para a toma de decisións.
  - Autosuperación: de forma periódica avaláase o produto que se está a desenvolver.
  - Autoenriquecemento: transferencia do coñecemento.
- **Fases de desenvolvemento solapadas:** as fases non existen coma tal, senón que se desenvolven tarefas/actividades en función das necesidades cambiantes durante todo o proxecto. De feito, en moitas ocasións non é posible realizar un deseño técnico detallado antes de empezar a desenvolver e ver algúns resultados. Por outra banda, as fases tradicionais efectuadas por persoas diferentes non favorecen o traballo en equipo e poden chegar a xerar máis inconvenientes que vantaxes (por ex., un atraso nunha fase afecta a todo o proxecto).
- **Control sutil:** establecementos de puntos de control para realizar un seguimento adecuado sen limitar a liberdade e creatividade do equipo. Así mesmo, recoméndase:
  - Avaliar o ambiente laboral, sendo fundamental a elección de persoas que non xeren conflitos.
  - Recoñecer os méritos mediante un sistema de avaliación xusto e entender os erros como puntos de mellora e aprendizaxe.
  - Potenciar a interacción entre o equipo e o negocio, para que poidan coñecer as necesidades de primeira man.
- **Difusión e transferencia do coñecemento:** alta rotación dos membros dos equipos entre diferentes proxectos. Por outra banda, potenciar o acceso libre á información e documentación.

Algunhas das metodoloxías áxiles máis coñecidas habémolas ver nos apartados seguintes.

### 34.4.1 Scrum

*Scrum* é un proceso de desenvolvemento de software no que se aplican de maneira regular un conxunto de boas prácticas para traballar en colaboración, en equipo, e obter o mellor resultado posible dun proxecto. En *Scrum* realízanse entregas parciais e regulares do produto final, priorizadas polo beneficio que lle proporcionan ao receptor do proxecto. Por iso, *Scrum* está especialmente indicado para proxectos en contornos complexos, onde se necesita obter resultados pronto, onde os requisitos son cambiantes ou pouco definidos, onde a innovación, a competitividade, a flexibilidade e a produtividade son fundamentais.

*Scrum* representa un marco de traballo para a xestión e desenvolvemento de software baseado en procesos iterativo e incremental utilizado comunmente en contornos baseados na metodoloxía *Agile* de desenvolvemento de software. É un modelo de referencia que inclúe un conxunto de prácticas e roles predefinidos. Os roles principais en *Scrum* son o *ScrumMaster*, que mantén os procesos e traballa de forma similar ao director de proxecto, o *ProductOwner*, que representa os *stakeholders* (clientes externos ou internos), e o *Team*, que inclúe os desenvolvedores. Durante cada *sprint*, un período entre 15 e 30 días (a lonxitude é definida polo equipo), o equipo crea un incremento de software potencialmente entregable (utilizable). O conxunto de características que forma parte de cada *sprint* vén do **product backlog**, que é un conxunto de requisitos de alto nivel priorizados que dan forma ao traballo que se vai realizar. Os elementos do *backlog* que forman parte do *sprint* determínanse durante a reunión de **sprint planning**. Durante esta reunión, o *ProductOwner* informa o equipo sobre os elementos no *product backlog* que quere ver completados. O equipo determina entón a cantidade dese traballo que se pode comprometer a completar durante o seguinte *sprint*. Durante o *sprint*, ninguén pode cambiar o *sprint backlog*, o que significa que os requisitos están conxelados durante o *sprint*. Existen varias implementacións de sistemas para xestionar o proceso de *Scrum*, que van desde notas

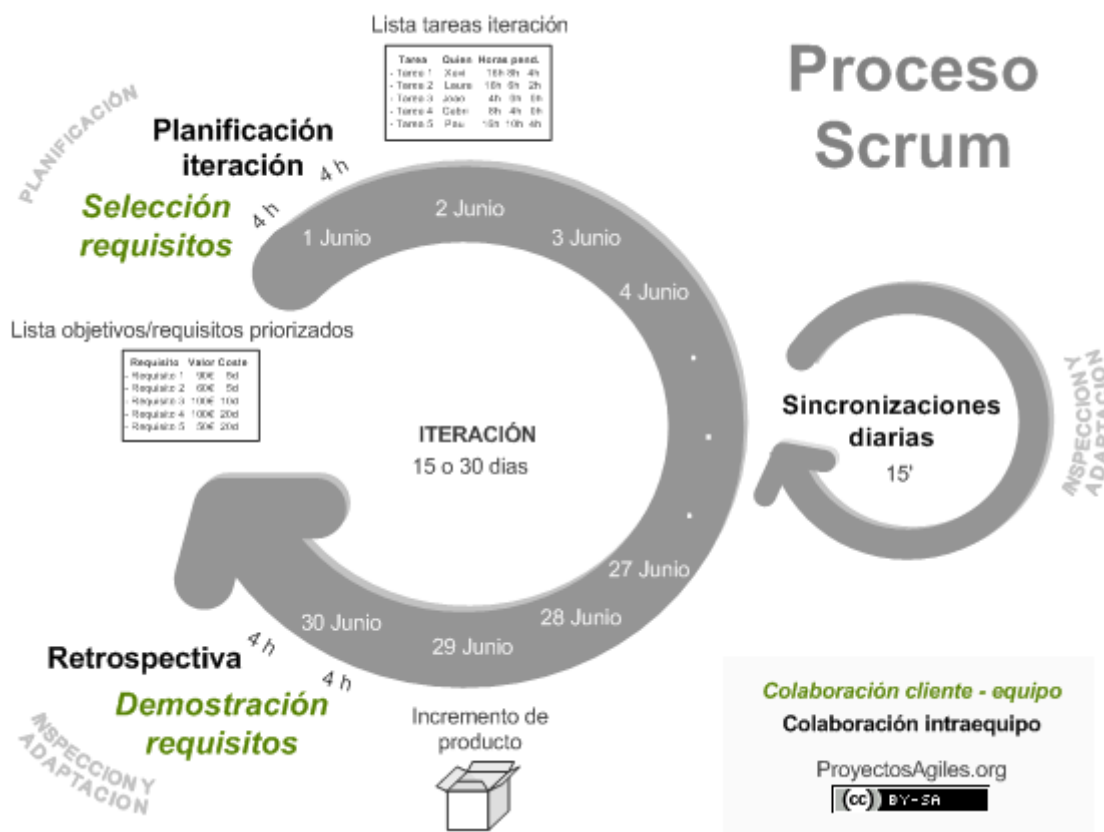


amarelas "*post-it*" e encerados ata paquetes de software. Unha das maiores vantaxes de *Scrum* é que é moi fácil de aprender e require moi pouco esforzo para comezarse a utilizar.



A modo de resumo, podemos establecer que a metodoloxía *Scrum* se basea en:

- Desenvolvemento incremental dos requisitos do proxecto en bloques temporais curtos e fixos.
- A priorización dos requisitos por valor para o cliente e custo de desenvolvemento en cada iteración.
- O control empírico do proxecto. Ao final de cada iteración demostráse ao cliente o resultado real obtido, de maneira que poida tomar as decisións necesarias en función do que observa e do contexto do proxecto nese momento. Doutra banda, o equipo sincronízase diariamente e realiza as adaptacións necesarias.
- A potenciación do equipo, que se compromete a entregar uns requisitos, e para iso outórgaselle a autoridade necesaria para organizar o seu traballo.
- A sistematización da colaboración e da comunicación tanto entre o equipo coma co cliente.
- O *timeboxing* das actividades do proxecto, para axudar á toma de decisións e conseguir resultados.



LENDAS: Lista tarefas iteración / Tarefa / NON SE ENTENDE / NON SE ENTENDE / PLANIFICACIÓN / Planificación iteración / Proceso Scrum / Selección requisitos / Listas obxectivos/requisitos priorizados / Requisitos / NON SE ENTENDE / NON SE ENTENDE / 1, 2, 3, 4, 27, 28, 29, 30 xuño / Sincronizacións diarias / INSPECCIÓN E ADAPTACIÓN / Retrospectiva / Demostración requisitos / INSPECCIÓN E ADAPTACIÓN / Incremento de produto / Colaboración cliente - equipo / Colaboración intraequipo.

#### **34.4.2 Dynamic Systems Development Method (DSDM)**

Proporciona un *framework* para o desenvolvemento áxil de software, apoiado pola continua implicación do usuario nun desenvolvemento iterativo e crecente. DSDM foi desenvolvido no Reino Unido nos anos noventa. Como extensión do Desenvolvemento Rápido de Aplicacións (RAD ), DSDM céntrase nos proxectos de sistemas de información que se

caracterizan por orzamentos e axendas apertadas. DSDM trata os problemas que ocorren con frecuencia no desenvolvemento dos sistemas de información polo que respecta a excederse no tempo e no orzamento e outras razóns comúns para a falta no proxecto, tal como a falta de implicación do usuario e da comisión superior da xerencia. DSDM consiste en 3 fases: fase do pre-proxecto, fase do ciclo de vida do proxecto, e fase do post-proxecto. A fase do ciclo de vida do proxecto subdivídese en 5 etapas: estudo de viabilidade, estudo da empresa, iteración do modelo funcional, deseño e iteración da estrutura, e implementación. Ten 9 principios fundamentais:

- **Involucrar o cliente** é a clave para conducir un proxecto eficiente e efectivo, onde ambos, cliente e desenvolvedores, comparten un contorno de traballo para que as decisións poidan ser tomadas con precisión.
- **O equipo do proxecto debe ter o poder** para tomar decisións que son importantes para o progreso do proxecto, sen esperar a aprobación de niveis superiores.
- DSDM céntrase na **entrega frecuente de produtos**, dando por suposto que entregar algo cedo é sempre mellor que entregar todo ao final. Ao entregar o produto frecuentemente desde unha etapa temperá do proxecto, o produto pode ser verificado e revisado alí onde se pode ter en conta a documentación de rexistro e revisión na seguinte fase ou iteración.
- O principal **criterio de aceptación** de entregables reside en entregar un sistema que satisfaga as necesidades actuais de negocio.
- O desenvolvemento é **iterativo e incremental**, guiado pola realimentación dos usuarios para converxer nunha solución de negocio precisa.
- Todos os **cambios** durante o desenvolvemento son reversibles.
- Requirimentos globais antes de comezar o proxecto.
- As probas son realizadas durante todo o ciclo vital do proxecto.
- A comunicación e cooperación entre todas as partes interesadas.

### **34.4.3 Extreme Programming (XP)**

A programación extrema, ou *Extreme Programming*, é unha das metodoloxías áxiles de desenvolvemento de software máis exitosas dos últimos tempos. A programación extrema diferénciase das metodoloxías tradicionais principalmente en que pon máis énfase na adaptabilidade que na previsibilidade. Os defensores de XP consideran que os cambios de requisitos sobre a marcha son un aspecto natural, inevitable, e mesmo desexable do desenvolvemento de proxectos. Coidan que ser capaz de adaptarse aos cambios de requisitos en calquera punto da vida do proxecto é unha aproximación mellor e máis realista que tentar definir todos os requisitos ao comezo do proxecto e investir esforzos despois en controlar os cambios nos requisitos. XP constrúe un proceso de deseño evolutivo que se basea en refactorizar un sistema simple en cada iteración. Todo o deseño se centra na iteración actual e non se fai nada anticipadamente para necesidades futuras. Os valores orixinais da programación extrema son: **simplicidade** (de deseño, código e documentación), **comunicación** (a comunicación co cliente é fluída, xa que o cliente forma parte do equipo de desenvolvemento; o cliente decide qué características teñen prioridade e sempre debe estar dispoñible para solucionar dúbidas), **retroalimentación** (*feedback*: ao estar o cliente integrado no proxecto, a súa opinión sobre o estado do proxecto coñécese en tempo real), e **coraxe** (cómpre coraxe para implementar as características que o cliente quere agora sen caer na tentación de optar por un enfoque máis flexible que permita futuras modificacións). Un quinto valor, o **respeto** (os membros do equipo respectan o traballo do resto sen facer de menos aos outros, senón orientándoos a realizalo mellor, obtendo como resultado unha mellor autoestima no equipo e elevando o ritmo de produción no equipo), foi engadido posteriormente.

As características fundamentais desta metodoloxía son:

- Desenvolvemento iterativo e incremental
- Probas unitarias continuas
- Programación en parellas
- Integración do equipo de programación con cliente
- Corrección de todos os erros
- Refactorización do código
- Propiedade do código compartida
- Simplicidade no código

#### **34.4.4 Feature Driven Development (FDD)**

Baséase nun proceso iterativo con iteracións curtas que producen un software funcional que o cliente e a dirección da empresa poden ver e monitorar. As iteracións decídense baseándose en funcionalidades, que son pequenas partes do software con significado para o cliente. Non cobre todo o ciclo de vida, senón só as fases de deseño e construción. Non require un modelo específico de proceso e complementase con outras metodoloxías. FDD consiste en cinco procesos secuenciais durante os cales se diseña e constrúe o sistema:

- **Desenvolvemento dun modelo xeral:** Cando comeza esta fase, os expertos do dominio xa teñen unha idea do contexto e dos requirimentos do sistema. O dominio global é dividido en diferentes áreas e realízase informe detallado para cada unha delas por parte dos expertos do dominio.
- **Construción da lista de funcionalidades:** Os ensaios, modelos de obxectos e documentación de requirimentos proporcionan a base para construír unha ampla lista de funcionalidades. Estas funcionalidades son pequenos ítems útiles aos ollos do cliente. A lista de funcionalidades é revisada polos usuarios e patrocinadores para

asegurar a súa validez. As funcionalidades que esixan de máis de dez días descompóñense noutras máis pequenas.

- **Planificación por funcionalidades:** Nesta etapa inclúese a creación dun plan de alto nivel, onde a lista de funcionalidades é ordenada en función da prioridade e da dependencia entre cada funcionalidade. Ademais, as clases identificadas na primeira etapa son asignadas a cada programador.
- **Deseño e construción por funcionalidades:** O deseño e construción da funcionalidade é un proceso iterativo durante o cal as funcionalidades seleccionadas son producidas. Unha iteración pode levar desde uns poucos días a un máximo de dúas semanas. Este proceso iterativo inclúe tarefas como inspección do deseño, codificación, probas unitarias, integración e inspección do código.

#### **34.4.5 Agile Modeling (AM)**

Pódese describir como unha metodoloxía baseada na práctica para a modelaxe efectiva de sistemas de software. Non define procedementos detallados de como crear un tipo de modelo dado. En lugar disto, suxire prácticas para que os modelos e a documentación sexan efectivos. O seu segredo non está nas técnicas de modelaxe que se usan, senón en como se aplican. Non é un desenvolvemento de software completo, xa que non abrangue actividades de programación, proba, xestión de proxectos, implementación, soporte ou outros elementos da realización de proxectos que non sexan a documentación e a modelaxe. É necesario, polo tanto, combinalo con outras metodoloxías como poden ser XP, DSDM, SCRUM ou RUP. Os valores desta metodoloxía son a **comunicación** (entre participantes do equipo de traballo, desenvolvedores e analistas, etc.), **simplicidade**, **coraxe** (para tomar decisións importantes e ser capaces de cambiar de dirección cando o camiño tomado non é o correcto) e

**humildade** (todos os interesados no proxecto poden contribuír en algo para unha mellor realización).

#### **34.4.6 Crystal**

*Crystal* é unha metodoloxía de desenvolvemento de software áxil. Máis ca unha metodoloxía, *Crystal* considérase unha familia de metodoloxías, dado que se subdivide en varios tipos de metodoloxías en función da cantidade de persoas que vaian participar no proxecto.

Alistair Cockburn é o impulsor desta serie de metodoloxías. O desenvolvemento desta familia de metodoloxías está fundamentado na análise de distintos proxectos de desenvolvemento de SW e a súa propia experiencia. Fálase de familia de metodoloxías porque, segundo o propio autor, os tipos diferentes de proxectos requiren tipos diferentes de metodoloxías. A óptica baixo a cal recolle esta perspectiva preséntase fundamentada en dous eixes: o número de persoas no proxecto, e as consecuencias dos erros. Dispón dun código de cor para marcar a complexidade de cada metodoloxía. Comparte coa XP unha orientación humana, pero esta centralización na xente faise dun xeito diferente. Alistair considera que ás persoas lles resulta difícil seguir un proceso disciplinado, así que, máis que seguir a alta disciplina da XP, Alistair explora unha metodoloxía menos disciplinada que aínda podería ter éxito, intercambiando conscientemente produtividade por facilidade de execución. El coida que, aínda que Crystal sexa menos produtivo que a XP, haberá máis persoas capaces de seguilo. Alistair tamén lles concede moita importancia ás revisións ao final da iteración, animando o proceso a ser “automellorable”. Defende que o desenvolvemento iterativo debe detectar os problemas cedo, permitindo daquela que se corrixan. Deste xeito ponse maior énfase na xente, supervisando o seu proceso e afinándoo conforme se desenvolve.

## BIBLIOGRAFÍA:

- [http://administracionelectronica.gob.es/archivos/pae\\_000001027.pdf](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 e 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](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 e 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. Scott 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](http://www.ort.edu.uy/fi/publicaciones/ingsoft/investigacion/ayudantias/metodologia_FDD.pdf). Metodología FDD. Cátedra de Enseñería 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 da Escola Superior de Enxeñería Informática.**



**Universidade de Vigo.**

# **35. ENXEÑARÍA DE REQUISITOS. VERIFICACIÓN. VALIDACIÓN. ESPECIFICACIÓN DE REQUISITOS. XESTIÓN DE REQUISITOS.**

## **Tema 35- Enxeñería de requisitos. Verificación. Validación. Especificación de requisitos. Xestión de requisitos.**

### **ÍNDICE**

- 35.1 Enxeñería de requisitos
  - 35.1.1 Tipos de requisitos
- 35.2 Identificación dos requisitos do software
  - 35.2.1 Entrevistas
  - 35.2.2 JAD (Joint Application Design)
  - 35.2.3 Prototipos
  - 35.2.4 Análise de factores críticos de éxito
  - 35.2.5 Brainstorming
  - 35.2.6 Escenarios e 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 Xestión de requisitos
  - 35.5.1 Planificación da xestión de requisitos.
  - 35.5.2 Xestión do cambio.

### **35.1 Enxeñería de requisitos**

A enxeñería de requisitos forma parte da enxeñería do software e comprende todas as tarefas relacionadas coa determinación das necesidades ou das condicións que hai que satisfacer para un software novo ou modificado, tomando en conta os diversos requisitos dos usuarios. Así, os requisitos xéranse a partir da interacción entre os usuarios e os

enxeñeiros do software, e representan as características do sistema que se vai construír, é dicir, as necesidades dos usuarios.

Hai múltiples definicións do termo 'requisito'; algunhas delas son:

- Segundo a asociación IEEE, un **requisito** é:
  - o Unha condición ou capacidade que necesita un usuario para resolver un problema ou acadar un obxectivo.
  - o Unha condición ou capacidade que debe cumprir ou posuír un sistema ou un compoñente deste para satisfacer un contrato, un estándar, unha especificación, ou outro documento imposto dunha maneira formal.
  - o Unha representación documentada dunha condición ou capacidade tal como as expresadas nos dous puntos anteriores.

En resumo, os requisitos son as características que debe cumprir o sistema para que satisfaga as necesidades dos usuarios. Moitas veces fálase de requirimentos no canto de requisitos. Isto débese a unha mala tradución do inglés. A palabra *requirement* debe ser traducida como 'requisito', namentres que 'requirimento' se traduce ao inglés como '*request*'.

Sommerville divide o proceso de enxeñería de requisitos en catro subprocesos que son: (1) a avaliación de se o sistema é útil para o negocio (**estudo de viabilidade**); (2) o **descubrimento de requisitos** (obtención e análise); (3) a transformación destes requisitos en formularios estándar (**especificación**); e (4) a verificación de que os requisitos realmente definen o sistema que quere o cliente (**validación**).

Para Thayer, *"a enxeñería de requisitos proporciona o mecanismo apropiado para entender o que o cliente quere, analizar as necesidades, avaliar a factibilidade, negociar unha solución razoable, especificar a solución sen ambigüidades, validar a especificación, e administrar os requisitos conforme se transforman nun sistema operacional"* e establece as seguintes fases para o proceso:



- **Inicio.** Establécese unha comprensión básica do problema por parte dos analistas.
- **Obtención.** Obtéñense os requisitos do software mediante a interacción entre os analistas e o cliente.
- **Elaboración.** Refínase a información obtida no paso anterior e enfócase á construción dun modelo de análise que represente o sistema que se vai construír.
- **Negociación.** Hai requisitos que non son implementables ou son difíciles de trasladar ao sistema. Por esta razón, os analistas negocian estes requisitos para chegar a un entendemento e lograr un sistema factible de desenvolverse nun prazo e cun custo determinados.
- **Especificación.** Confecciónase un conxunto de documentos (descricións en linguaxe natural, diagramas, etc.) que definan o que o sistema debe facer.
- **Validación.** Examínase a especificación para asegurarse de que todos os requisitos do software se estableceron dun modo preciso, que non hai inconsistencias, omisións nin erros, e que ademais se cumpren os estándares de calidade establecidos para o proxecto.
- **Xestión de requisitos.** Esta actividade permite tratar co inevitable problema dos cambios de especificacións, identificando, controlando e determinando o impacto do cambio de requisitos sobre o resto.

Outros autores modifican o número de etapas e divídenas en:

- **Dedución de requisitos:** nela os analistas obteñen as necesidades do cliente a partir de todas as fontes de información que teñen á súa disposición (documentación, entrevistas, estudo dos procesos da organización, etc.). Termos equivalentes usados polos enxeñeiros de software para esta actividade son: extracción de requisitos, identificación de requisitos, determinación de requisitos, etc. Vemos que estas se corresponderían coas dúas primeiras fases do modelo anterior.



- **Análise de requisitos:** procédese a traballar sobre os requisitos deducidos no paso anterior. Estúdanse estes requisitos en busca de conflitos e incoherencias, implicacións, información non obtida e aspectos non resoltos. Despois clasifícanse, avalíase a súa viabilidade e intégranse os novos requisitos cos xa existentes. O obxectivo final é lograr unha lista de requisitos que defina as necesidades do cliente. Corresponderíase coas fases de elaboración e negociación do modelo anterior.
- **Representación dos requisitos:** Actividade na que se representan os requisitos dunha ou máis formas, utilizando para iso diferentes técnicas; por exemplo, a linguaxe formal, a linguaxe natural, representacións gráficas, etc. Para a representación existen múltiples técnicas; as máis usadas son, entre outras, os diagramas de fluxo de datos, modelo entidade relación, casos de uso ou diagramas de clases. Unha vez que están os requisitos representados, é necesario que se reúnan os diversos participantes no desenvolvemento para revisalos e aprobalos. O produto final co que culmina esta fase é a especificación de requisitos do software, onde se describe con exactitude todo o que o sistema debe facer. Correspóndese coas fases de especificación e validación do modelo anterior.
- **Validación de requisitos:** Procédese a definir unha serie de criterios e técnicas que permitirán, cando o sistema estea construído, comprobar que este cumpre os requisitos.

Independentemente do modelo que usemos, o importante é termos claro que o obxectivo da enxeñería de requisitos é determinar con claridade e precisión qué é o que hai que facer, e para iso será necesario identificar os requisitos clave.

Os factores principais que conducen ao fracaso nos proxectos software e que teñen que ver cos requisitos son: a falta de comunicación cos usuarios, os requisitos incompletos e os cambios nos requisitos. A evidencia

demostra que os requisitos conteñen demasiados erros, que moitos destes erros non se detectan ao principio, pero poderían ser detectados, e que non detectar estes erros incrementa os custos do proxecto e a súa duración. A consecuencia é que o sistema non satisfará aos usuarios, produciranse desacordos entre usuarios e desenvolvedores e gastarase tempo e diñeiro en construír un sistema equivocado.

### *35.1 Tipos de requisitos*

A maioría dos autores distinguen entre:

- **Requisitos funcionais:** Son declaracións dos servizos que debe proporcionar o sistema, da maneira en que este debe reaccionar a entradas particulares e de como se debe comportar en situacións concretas. Nalgúns casos, os requisitos funcionais dos sistemas tamén poden declarar explicitamente o que o sistema non debe facer. Os requisitos funcionais dun sistema describen o que o sistema debe facer.
- **Requisitos non funcionais:** Son restricións dos servizos ou funcións ofrecidos polo sistema. Inclúen restricións de tempo sobre o proceso de desenvolvemento e estándares. Como o seu nome suxire, non se refiren directamente ás funcións específicas que proporciona o sistema, senón ás propiedades deste, coma a fiabilidade, o tempo de resposta e a capacidade de almacenamento. Poden vir das características requiridas do software (requisitos do produto), da organización que desenvolve o software (requisitos organizacionais) ou de fontes externas. Exemplos:
  - o **Requisitos do produto.** Estes requisitos especifican o comportamento do produto. Algúns exemplos son os requisitos de rendemento na rapidez de execución do sistema e canta memoria se require; os requisitos de fiabilidade que fixan a taxa de fallos para que o sistema sexa aceptable; os requisitos de portabilidade e os requisitos de usabilidade.
  - o **Requisitos organizacionais.** Estes requisitos derívanse de políticas e procedementos existentes na organización do cliente

e na do desenvolvedor. Algúns exemplos son os estándares nos procesos que deben utilizarse; os requisitos de implementación, como as linguaxes de programación ou o método de deseño que se utilice; e os requisitos de entrega, que especifican cando se entregará o produto e a súa documentación.

- o **Requisitos externos.** Este grande apartado inclúe todos os requisitos que derivan dos factores externos ao sistema e do seu proceso de desenvolvemento. Estes poden incluír os requisitos de interoperabilidade, que definen o modo en que o sistema interactúa con sistemas doutras organizacións; os requisitos legislativos que se deben seguir para garantir que o sistema funcione dentro da lei; e os requisitos éticos. Estes últimos son postos nun sistema para asegurar que será aceptado polos seus usuarios e polo público en xeral.

Sommerville distingue entre **requisitos do usuario**, que son declaracións, en linguaxe natural e en diagramas, dos servizos que se espera que o sistema proporcione e das restricións baixo as cales debe funcionar, e **requisitos do sistema**, que establecen con detalle as funcións, servizos e restricións operativas do sistema. Estes diferentes niveis de especificación serían de utilidade debido a que comunican a información do sistema a diferentes tipos de lectores.

## **35.2 Identificación dos requisitos do software**

A dedución, identificación ou determinación de requisitos é o paso durante o cal se obteñen os requisitos do software de fontes tales como: a xente implicada (usuarios, clientes, expertos na materia, etc.), as necesidades que debe satisfacer o sistema, o contorno físico que rodea o sistema, o contorno organizacional, etc.



Os problemas da obtención de requisitos pódense agrupar en tres categorías:

- 1- Problemas de alcance, xa que os requisitos poden implicar demasiada ou moi pouca información.
- 2- Problemas de comprensión, como consecuencia dunha pobre comunicación entre usuario e analista. Neste caso os requisitos obtidos son ambiguos, incompletos, inconsistentes e incorrectos, porque non responden ás verdadeiras necesidades dos usuarios.
- 3- Problemas de volatilidade, xa que os requisitos evolucionan co tempo. En efecto, a medida que avanza o desenvolvemento do sistema, as necesidades do usuario poden madurar a causa do coñecemento adicional froito do desenvolvemento ou de necesidades do contorno ou da organización non previstas.

A solución ao primeiro problema pasa por determinar claramente o contexto do sistema, é dicir, os seus límites e obxectivos. Se non se ten en conta o contexto onde vai funcionar o sistema, pódese chegar a requisitos incompletos, non verificables, innecesarios e non utilizables. A solución do segundo é que exista unha boa comunicación entre usuarios, desenvolvedores e clientes, a fin de que os requisitos se poidan escribir de maneira que permitan tanto que o desenvolvedor poida distinguir se os devanditos requisitos se poden implementar como que o persoal de control poida comprobar se a implementación cumpre cos requisitos. Para rematar, a solución ao terceiro problema é incorporar estes cambios aos requisitos orixinais, pois, se non se fai así, estes serán incompletos e inconsistentes coa nova situación.

Son numerosas as estratexias e técnicas que se desenvolveron para a obtención dos requisitos. As máis importantes ímolas ver deseguido.

### *35.2.1 Entrevista*

Enténdese por entrevista o encontro que se realiza “cara a cara” entre un usuario e a persoa responsable de obter a información (analista). Para realizar a entrevista só é necesario designar as persoas que deben participar nela e determinar o lugar onde poder levala a cabo. É importante identificar a que tipo de perfil vai dirixida a entrevista, a quen se vai entrevistar e cal é o momento máis oportuno, co fin de evitar situacións embarazosas e conseguir que a entrevista sexa eficaz e produtiva.

Como paso previo á realización da entrevista débense ter en conta unha serie de regras xerais ou directrices básicas:

- Desenvolver un plan global da entrevista.
- Asegurarse de que se conta coa aprobación para falar cos usuarios.
- Preparar a entrevista previamente.
- Realizar a entrevista.
- Consolidar o resultado da entrevista.

Ademais, é conveniente planificar as entrevistas estudando a secuencia en que se van levar a cabo, en función dos distintos perfís implicados e as relacións existentes entre os entrevistados. Segundo a información que se desexa obter e dependendo das distintas fontes que poden proporcionala, se cadra é necesario realizar unha entrevista conxunta con varias persoas. Durante a preparación da entrevista é imprescindible remitirlle ao usuario un guión previo sobre os puntos que se van tratar, para que poida estudalo con tempo e solicitar a información que estime conveniente para a entrevista. Débese pensar ben o tipo de guión, segundo o perfil e as responsabilidades do entrevistado, e a súa extensión, de forma que se poida conseguir a suficiente información sen provocar rexeitamento no entrevistado. Se se considera apropiado, pódense utilizar ferramentas automatizadas.

Unha vez que se dispón da aprobación para falar cos usuarios, faise a convocatoria da entrevista enviando a información oportuna e fixando os

obxectivos, o método de traballo que se vai seguir e o tempo do que se dispón.

Para realizar a entrevista, é importante facer un resumo xeral dos temas que se tratarán, utilizar un estilo apropiado e crear desde o seu inicio un clima de confianza entre os asistentes. É posible que o entrevistado se resista a dar información, sendo útil nestes casos utilizar técnicas específicas de comunicación.

Antes de finalizar a entrevista é importante que o entrevistador sintetice as conclusións e comprobe que todos os asistentes están de acordo, deixando sempre aberta a posibilidade de volver contactar para aclarar temas que xurdan ao estudar a información recompilada.

Finalmente, o responsable depura e consolida o resultado das entrevistas, elaborando un informe de conclusións. Nalgúns casos pode ser conveniente elaborar unha acta que reflicta estas conclusións e remitírllela aos entrevistados co obxectivo de asegurarse de que se comprenderon ben as especificacións dadas.

### *35.2.2 JAD (Joid Application Design)*

As características dunha sesión de traballo tipo JAD pódense resumir nos seguintes puntos:

- Establécese un equipo de traballo cuns compoñentes e responsabilidades perfectamente identificados, tendo en conta que o fin da sesión é conseguir o consenso entre as necesidades dos usuarios e os servizos do sistema en produción.
- Lévanse a cabo poucas reunións, de longa duración e moi ben preparadas.

- Durante a propia sesión elabóranse os modelos empregando diagramas fáciles de entender e manter, directamente sobre ferramentas CASE.
- Ao rematar a sesión obtéñense un conxunto de modelos que deberán ser aprobados polos participantes.

É importante definir claramente o perfil e as responsabilidades dos participantes dunha sesión JAD. Pódense distinguir os seguintes perfís:

- Moderador (líder) con amplos coñecementos da metodoloxía de traballo, dinámica de grupos e psicoloxía do comportamento, así como dos procesos da organización obxecto do estudo.
- Promotor, persoa que impulsou o desenvolvemento.
- Xefe de proxecto, responsable da implantación do proxecto.
- Especialista en modelización, responsable da elaboración dos modelos no transcurso da sesión.
- Desenvolvedores, que garanten que os modelos son correctos e responden aos requisitos especificados.
- Usuarios, responsables de definir os requisitos do sistema e validalos.

Para levar a cabo unha sesión JAD, é necesario realizar unha serie de actividades antes do seu inicio, durante o desenvolvemento e logo da súa finalización. Estas actividades detállanse a seguir:

- **Inicio:** defínese o ámbito e a estrutura do proxecto, os produtos que se van obter, prepárase o material necesario para a sesión, determínase o lugar onde se vai levar a cabo, selecciónanse os participantes e suxírese unha axenda de traballo.
- **Desenvolvemento:** identifícanse as saídas do proxecto e débese conseguir o consenso entre os participantes de modo que se materialice nos modelos.

- **Finalización:** válidase a información da sesión e xéranse os produtos da metodoloxía de traballo proposta. Se fose necesario, intégranse os produtos de saída.

### 35.2.3 Prototipado

Os prototipos son sistemas software que só implementan unha parte do sistema. Normalmente, os prototipos empréganse para obter requisitos do usuario cando estes non están completamente claros. É moito máis fácil que o usuario entenda e aprobe un sistema se ve unha versión reducida, inda que operativa, e pode interaccionar con el, a que revise unha longa lista de texto cos requisitos que describen o tal sistema. Ao cabo, como se adoita dicir, o prototipo permite salvar a situación seguinte: “Non sei o que quero, pero heino saber cando o vexa”. E, en efecto, será moito máis fácil para un usuario saber se o que quere é o que ten diante e co que pode interaccionar, que se é unha chea de follas con todos os requisitos escritos un a un.

A aplicación da técnica do prototipado consta dos seguintes pasos:

- 1- Estudo preliminar dos requisitos do usuario.
- 2- Proceso iterativo consistente en:
  - a. Construír un prototipo.
  - b. Avalialo cos usuarios.
  - c. Formular novos requisitos.
  - d. Desbotar o prototipo.

Os aspectos clave no deseño de prototipos son: a identificación dos usuarios aos que vai dirixido, tendo en conta que debe responder a diferentes individualidades, con distintos coñecementos e habilidades; qué funcións teñen asignadas; e qué tipo de información precisarán para levar a cabo as devanditas funcións.

#### 35.2.4 *Análise de factores críticos de éxito*

Esta técnica consiste en identificar e concentrarse nun pequeno conxunto de factores críticos dos que depende o éxito e efectividade do sistema. Aínda que a identificación dos factores críticos correctos é, ás veces, un labor complexo, esta técnica é bastante útil cando o sistema é tecnicamente complexo.

#### 35.2.5 *Brainstorming*

Esta técnica úsase principalmente para a xeración de ideas nos casos en que a xeración destas non é obvia. Trátase dunha técnica sinxela na que se reúnen un grupo de 4 a 10 persoas para xerar ideas, sen restricións, nun ambiente libre de críticas. Un dos principais puntos fortes da técnica é que ideas que nun principio poden ser desatinadas teñen cabida. Primeiro proporciónanse as ideas e nunha segunda volta refínanse. O *brainstorming* permite achegar á obtención de requisitos os seguintes aspectos:

- **Xera múltiples puntos de vista dun problema.** Cada un dá a súa visión do problema, que non ten por que ser a mesma. Unha vez vistos todos os puntos de vista, pódese atacar o problema dunha forma máis efectiva.
- **Formular un problema de distintas formas.** Cada participante pode ver o problema desde unha óptica distinta, polo que á hora de formulalo ha facelo dunha forma distinta. Estas diferenzas poden achegar un gran valor á hora do estudo do problema, identificando os puntos clave deste por parte de cada participante.

A técnica de *brainstorming*, para que sexa efectiva, debe prepararse previamente. As fases polas que pasa a execución da técnica son:



- 1- **Fase de preparación:** Identifícanse os participantes da sesión (clientes, usuarios, analistas, etc.), désígnase un líder que leva a sesión, planifícase esta sesión e búscase unha sala adecuada.
- 2- **Fase de xeración:** Comézase expoñendo as ideas de forma libre, por quendas ou espontaneamente. As ideas vanse apuntando nun encerado que todos poidan ver.
- 3- **Fase de consolidación:** Révísanse as ideas obtidas no paso anterior, acláranse se non están claras, reescríbense se é preciso, desbótanse as que non son utilizables, discútense as restantes e priorízanse.

#### 35.2.6 Escenarios e casos de uso

Normalmente, ás persoas resúltalles máis fácil dar exemplos da vida real que descricións abstractas. Os **escenarios** poden ser especialmente útiles para agregar detalle a un esbozo da descrición de requisitos. Son descricións de exemplos das sesións de interacción. Cada escenario abarca unha ou máis posibles interaccións. O escenario comeza cun esbozo da interacción e, durante a obtención, agréganse detalles para crear unha descrición completa desta interacción. De forma xeral, un escenario pode incluír:

- 1- Unha descrición do que esperan o sistema e os usuarios cando o escenario comeza.
- 2- Unha descrición do fluxo normal de eventos no escenario.
- 3- Unha descrición do que pode ir mal e como manexalo.
- 4- Información doutras actividades que se poderían levar a cabo ao mesmo tempo.
- 5- Unha descrición do estado do sistema cando o escenario remata.

Os escenarios pódense redactar como texto, complementados por diagramas, fotografías das pantallas, etcétera. De forma alternativa,

pódese adoptar un enfoque máis estruturado, como os escenarios de evento ou os casos de uso.

Os casos de uso son unha técnica que se basea en escenarios para a obtención de requisitos. Na súa forma máis simple, un caso de uso identifica o tipo de interacción e os actores implicados. Os actores no proceso represéntanse como figuras delineadas, e cada clase de interacción represéntase como unha elipse co seu nome. O conxunto de casos de uso representa todas as posibles interaccións que se representarán nos requisitos do sistema. Actualmente, convertéronse nunha característica fundamental da notación de UML, que se utiliza para describir modelos de sistemas orientados a obxectos.

Os escenarios e os casos de uso son técnicas eficaces para obter requisitos para os puntos de vista dos interactuadores, onde cada tipo de interacción se pode representar como un caso de uso. Non obstante, dado que se centran nas interaccións, non son tan eficaces para obter restricións e requisitos de negocio e non funcionais de alto nivel de puntos de vista indirectos ou para descubrir requisitos do dominio.

#### *35.2.7 Observación directa e investigación contextual (etnografía)*

A **etnografía** é unha técnica de observación que se pode utilizar para entender os requisitos sociais e organizacionais. Un analista introdúcese por si só no contorno laboral onde se utilizará o sistema. Observa o traballo diario e anota as tarefas reais nas que están implicados os participantes. O valor da etnografía é que axuda aos analistas a descubriren os requisitos implícitos que reflicten os procesos reais máis que os formais nos que a xente está implicada.

A etnografía é especialmente efectiva para descubrir dous tipos de requisitos:



- Os requisitos que derivan da forma en que a xente traballa realmente, máis que da forma en que as definicións dos procesos establecen que debería traballar.
- Os requisitos que derivan da cooperación e coñecemento das actividades dos demais.

Os estudos etnográficos poden revelar os detalles dos procesos críticos que outras técnicas de obtención de requisitos esquecen a miúdo. Así e todo, posto que se centran no usuario final, este enfoque non é axeitado para descubrir os requisitos organizacionais ou do dominio. Os estudos etnográficos non sempre poden identificar novas propiedades que se lle deban agregar ao sistema. Polo tanto, por si mesma a etnografía non é un enfoque completo para a obtención de requisitos, e debe utilizarse para complementar outros enfoques, coma a análise de casos de uso.

### **35.3 Verificación - Validación**

A **validación** de requisitos trata de mostrar que estes realmente definen o sistema que o cliente desexa. A validación de requisitos é importante debido a que os erros nos requisitos poden conducir a importantes custos ao ter que repetir o traballo cando son descubertos durante o desenvolvemento ou despois de que o sistema estea en uso. O custo de arranxar un problema nos requisitos facendo un cambio no sistema é moito maior que reparar os erros de deseño ou os de codificación.

A razón disto é que, normalmente, un cambio nos requisitos significa que o deseño e a implementación do sistema tamén deben cambiar e que este debe probarse novamente.

Durante o proceso de validación de requisitos, débense levar a cabo as seguintes **verificacións**:



- 1- **Verificacións de validez.** Un usuario pode pensar que se necesita un sistema para levar a cabo certas funcións. Con todo, o razoamento e a análise poden identificar que se requiren funcións adicionais ou diferentes. Tamén se deben ter en conta que nun mesmo sistema adoita haber diferentes usuarios, con diferentes puntos de vista, algunhas veces contrapostos, e que estes deben chegar a un compromiso á hora de definiren os requisitos do sistema.
- 2- **Verificacións de consistencia.** Os requisitos non se deben contradicir. Isto é, non debe haber restricións ou descricións contraditorias da mesma función do sistema.
- 3- **Verificacións de completitude.** Os requisitos deben definir todas as funcións e restricións propostas polo usuario do sistema.
- 4- **Verificacións de realismo.** Utilizando o coñecemento da tecnoloxía existente, os requisitos deben verificarse para garantir que se poden implementar. Estas verificacións tamén deben ter en conta o orzamento e a confección de axendas para o desenvolvemento do sistema.
- 5- **Verificabilidade.** Para reducir a posibilidade de discusións entre o cliente e o desenvolvedor, os requisitos do sistema sempre se deben redactar de tal forma que sexan verificables. Isto significa que se debe poder escribir un conxunto de probas que demostren que o sistema que se vai entregar cumpre cada un dos requisitos especificados.

Pódense utilizar, en conxunto ou de forma individual, varias técnicas de validación de requisitos:

- 1- **Revisións de requisitos.** Os requisitos son analizados manual e sistematicamente por un equipo de revisores formado por persoas tanto da organización do cliente coma da desenvolvedora. Verifícanse os requisitos en canto a anomalías e omisións. Poden ser informais ou formais. As informais simplemente significan que os



desenvolvedores deben tratar os requisitos con tantos usuarios do sistema como sexa posible. Na revisión formal de requisitos, o equipo de desenvolvemento debe «conducir» o cliente a través dos requisitos do sistema, explicándolle as implicacións de cada requisito. Os revisores deben comprobar:

- a. **Verificabilidade.** Pódese probar o requisito de modo realista?
- b. **Comprensibilidade.** As persoas que adquiren o sistema ou os usuarios finais comprenden correctamente o requisito?
- c. **Rastrexabilidade.** Está claramente establecida a orixe do requisito? Se cadra hai que volver á fonte do requisito para avaliar o impacto do cambio. A rastrexabilidade é importante, xa que permite avaliar o impacto do cambio no resto do sistema.
- d. **Adaptabilidade.** É adaptable o requisito? É dicir, pódese cambiar o requisito sen provocar efectos de grande escala nos outros requisitos do sistema?

Os conflitos, contradicións, erros e omisións nos requisitos deben ser sinalados polos revisores e rexistrarse formalmente no informe de revisión. Queda para os usuarios, a persoa que adquire o sistema e o desenvolvidor deste negociar unha solución para estes problemas identificados.

- 2- **Construción de prototipos.** Neste enfoque de validación móstraselles un modelo executable do sistema aos usuarios finais e aos clientes. Estes poden experimentar con este modelo para ver se responde ás súas necesidades reais.
- 3- **Xeración de casos de proba.** Os requisitos deben poder probarse. Se as probas para eles se conciben como parte do proceso de validación, a miúdo revelan os problemas nos requisitos. Se unha proba é difícil ou imposible de deseñar, normalmente significa que os

requisitos serán difíciles de implementar e deberían ser analizados de novo.

É difícil demostrar que un conxunto de requisitos responde ás necesidades do usuario. Como consecuencia, de cando en cando atópanse todos os problemas nos requisitos durante o seu proceso de validación. É inevitable que haxa cambios adicionais de requisitos para corrixir as omisións e as malas interpretacións despois de que o documento de requisitos é aprobado.

### **35.4 Especificación de requisitos**

O **documento de requisitos do software** (algunhas veces denominado *especificación de requisitos do software* ou **ERS**) é a declaración oficial de qué deben implementar os desenvolvedores do sistema. Ten un conxunto diverso de usuarios que vai desde os altos cargos da organización que pagan polo sistema ata os enxeñeiros responsables de desenvolver o software. Os obxectivos que pretende a ERS son os seguintes:

- Proporcionar os medios de comunicación entre todas as partes implicadas no sistema: clientes, usuarios, analistas e deseñadores.
- Servir como base para as actividades de proba e verificación.
- Axudar ao control da evolución do sistema software.

O documento ERS debe incluír unha descrición completa e concisa de toda a interface externa do sistema co seu contorno, incluído o resto do software, portos de comunicación, hardware e usuarios. É dicir, debe incluír tanto os requisitos de comportamento do sistema (funcionais), que son aqueles que definen o que fai este e a información que manexa, como os requisitos que non son de comportamento, isto é, aqueles que definen os atributos do sistema segundo realiza o seu traballo (eficiencia, fiabilidade, seguridade, etc.).

Por contra, un documento ERS non debe incluír os elementos de xestión do proxecto (planificacións, eventos, etc.), nin o deseño, nin os plans de control do produto (xestión de configuración, garantía de calidade, etc.). Un documento ERS debe reunir as seguintes características:

- **Correcto.** Cada requisito establecido debe representar algo requirido para o sistema.
- **Non ambiguo.** Cada requisito establecido ten unha soa interpretación.
- **Completo.** Debe incluír todo o que o software ten que facer.
- **Verificable.** Débese poder comprobar, mediante un proceso efectivo e de custo limitado, que o produto reúne cada requisito establecido.
- **Consistente.** Un requisito non pode estar en conflito con outros requisitos.
- **Modificable.** A estrutura e estilo do documento debe facer fáciles os cambios.
- **Conciso.** Comprensible polo usuario e organizado.
- **Referenciado.** Cada requisito debe estar cualificado e debidamente referenciado.

#### *35.4.1 IEEE/ANSI 830-1998*

Varias organizacións grandes, como o Departamento de Defensa dos Estados Unidos e o IEEE, definiron estándares para os documentos de requisitos. O estándar máis amplamente coñecido é o IEEE/ANSI 830-1998 (IEEE, 1998). Este estándar IEEE suxire a seguinte estrutura para os documentos de requisitos:

### **1. Introducción**

1.1 Propósito do documento de requisitos: propósito e a quen vai dirixido.

1.2 Alcance do produto.

1.3 Definicións, acrónimos e abreviaturas.

1.4 Referencias.

1.5 Descrición do resto do documento.

## **2. Descrición xeral**

2.1 Perspectiva do produto.

2.2 Funcións do produto.

2.3 Características do usuario.

2.4 Restricións xerais.

2.5 Suposicións e dependencias.

3. **Requisitos específicos.** Este será o groso do documento.

**3.1. Interfaces externas:** describiranse os requisitos que afecten á interface de usuario, interface con outros sistemas (hardware e software) e interfaces de comunicacións.

**3.2. Funcións:** esta subsección (se cadra a máis longa do documento) deberá especificar todas aquelas accións (funcións) que deberá levar a cabo o software. Se se considerase necesario, poderán utilizarse notacións gráficas e táboas, pero sempre supeditadas á linguaxe natural, e non ao revés. O estándar permite organizar esta subsección de múltiples formas e suxire, entre outras, as seguintes:

- **Por tipos de usuario:** Distintos usuarios posúen distintos requisitos. Para cada clase de usuario que exista na organización, especifícanse os requisitos funcionais que lle afecten ou teñan maior relación coas súas tarefas.
- **Por obxectos:** Os obxectos son entidades do mundo real que se reflectirán no sistema. Para cada obxecto, detállanse os seus atributos e as súas funcións. Os obxectos pódense agrupar en clases. Esta organización da ERS non quere dicir que o deseño do sistema siga o paradigma de orientación a obxectos.
- **Por obxectivos:** Un obxectivo é un servizo que se desexa que ofrezca o sistema e que require unha determinada entrada para



obter o seu resultado. Para cada obxectivo ou subobxectivo que se persiga co sistema, cómpre detallar as funcións que permitan levalo a cabo.

- **Por estímulos:** Especificáanse os posibles estímulos que recibe o sistema e as funcións relacionadas co devandito estímulo.
- **Por xerarquía funcional:** Se ningunha das anteriores alternativas resulta de axuda, a funcionalidade do sistema especificarase como unha xerarquía de funcións que comparten entradas, saídas ou datos internos. Detállanse as funcións (entrada, proceso, saída) e as subfuncións do sistema. Isto non significa que o deseño do sistema deba realizarse segundo o paradigma de deseño estruturado.

**3.3. Requisitos de rendemento:** Detallaríanse os requisitos relacionados coa carga que se espera que teña que soportar o sistema. Por exemplo, o número de terminais, o número esperado de usuarios simultaneamente conectados, o número de transaccións por segundo que deberá soportar o sistema, etc. Tamén, se é necesario, especificaríanse os requisitos de datos, é dicir, aqueles requisitos que afecten á información que se gardará na base de datos. Por exemplo, a frecuencia de uso, as capacidades de acceso e a cantidade de rexistros que se espera almacenar (decenas, centos, miles ou millóns).

**3.4. Restricións de deseño:** Todo aquilo que restrinja as decisións relativas ao deseño da aplicación: restricións doutros estándares, limitacións do hardware, etc.

**3.5. Atributos do sistema:** Detallaranse os atributos de calidade do sistema: fiabilidade, mantibilidade, portabilidade, e, moi importante, a seguridade. Deberíase especificar qué tipos de usuario están autorizados, ou non, a realizar certas tarefas, e como se implementarán os mecanismos de seguridade.

**3.6. Outros requisitos**

## 4. Apéndices

## **5. Índice**

O estándar IEEE é un marco xeral que se pode transformar e adaptar para definir un estándar axustado ás necesidades dunha organización en particular. A información que se inclúa nun documento de requisitos debe depender do tipo de software que se vai desenvolver e do enfoque de desenvolvemento que se utilice.

### **35.5 Xestión de requisitos**

Os requisitos para sistemas software grandes son sempre cambiantes. Como o problema non se pode definir completamente, é moi probable que os requisitos do software sexan incompletos. Durante o proceso do software, a comprensión do problema por parte dos clientes cambia, e daquela os requisitos deben evolucionar para reflectir isto. Ademais, unha vez que un sistema se instalou, inevitablemente xorden novos requisitos. Cando os usuarios finais traballan cun sistema, descubren novas necesidades e prioridades debidas a:

- Normalmente, os sistemas grandes teñen unha comunidade de usuarios diversa e estes teñen diferentes requisitos e prioridades. Os que se usaron para definir o sistema puideron non ser os mellores.
- As persoas que pagan polo sistema e os seus usuarios raramente son a mesma persoa. Os clientes do sistema impoñen requisitos debido ás restricións organizacionais e de orzamento. Estes poden estar en conflito cos requisitos dos usuarios finais e, despois da entrega, pódense ter que engadir novas características de apoio ao usuario se o sistema ten que cumprir os seus obxectivos.
- O contorno de negocios e técnico do sistema cambia despois da instalación, e estes cambios débense reflectir no sistema. Pódese introducir novo hardware, pode ser necesario que o sistema interactúe con outros sistemas, as prioridades de negocio poden



cambiar con modificacións consecuentes na axuda ao sistema, e pode haber unha nova lexislación e regulacións que deben ser implementadas polo sistema.

A **xestión de requisitos** é o proceso de comprender e controlar os cambios nos requisitos do sistema. É necesario poder avaliar o impacto dos cambios sobre os requisitos. Hai que establecer un proceso formal para implementar as propostas de cambios. O proceso de xestión de requisitos debería empezar en canto estivese dispoñible unha versión preliminar do documento de requisitos, pero debería empezar a planificar como xestionar os requisitos que cambian durante o proceso de obtención de requisitos.

Existen **requisitos duradeiros**, que son requisitos relativamente estables que derivan da actividade principal da organización e que están relacionados directamente co dominio do sistema. Estes requisitos pódense derivar dos modelos do dominio que mostran as entidades e relacións que caracterizan un dominio de aplicación. Doutra banda, existen **requisitos volátiles**, que son requisitos que probablemente cambian durante o proceso de desenvolvemento do sistema ou despois de que este se puxo en funcionamento debido a cambios no contorno, lexislación...

#### *35.5.1 Planificación da xestión de requisitos.*

Para cada proxecto, a etapa de planificación establece o nivel de detalle necesario na xestión de requisitos. Haberá que decidir sobre:

1. **A identificación de requisitos.** Cada requisito débese identificar de forma única de tal xeito que poidan ser remitidos por outros requisitos de modo que se poida utilizar nas avaliacións de rastrexo.
2. **Un proceso de xestión do cambio.** Este é o conxunto de actividades que avalían o impacto e custo dos cambios. Habémolo ver nun apartado posterior.

3. **Políticas de rastrexo ou trazabilidade.** Estas políticas definen as relacións entre os requisitos, e entre estes e o deseño do sistema que se debe rexistrar e a maneira en que estes rexistros se deben manter.
4. **Selección de ferramentas CASE.** A xestión de requisitos comprende o procesamento de grandes cantidades de información sobre os requisitos. As ferramentas que se poden utilizar van desde sistemas de xestión de requisitos especializados ata follas de cálculo e sistemas sinxelos de bases de datos.

O concepto de trazabilidade fai referencia á posibilidade de determinar como se chegou a un certo elemento do software a partir doutros. Para poder levar a cabo esta trazabilidade é especialmente importante poder relacionar uns requisitos con outros, e tamén relacionar requisitos con elementos do sistema aos que dá lugar. Fálase de trazabilidade *cara adiante* cando, partindo dun requisito, se chega a todos os elementos que materializan o devandito requisito, ou *cara atrás* cando, partindo dun elemento do sistema, se chega ao requisito que o xerou.

Un requisito débese poder relacionar con outros requisitos semellantes para así evitar repeticións nos mesmos. Ademais, cando se fai un cambio nun, é máis fácil localizar aqueles requisitos nos que hai relación, para ver o impacto do cambio. Doutra banda, é útil poder relacionar un requisito cos elementos do sistema aos que este dá lugar, por se hai que cambiar un elemento do sistema, ou simplemente para poder saber que requisitos deron lugar a un determinado compoñente do sistema. Esta relación non só debe ser entre requisitos, senón tamén entre calquera elemento que se derivase posteriormente, xa sexa da análise, do deseño, da construción, de probas, etc.

A xestión de requisitos necesita axuda automatizada. As ferramentas CASE para este fin débense escoller durante a fase de planificación. Precísanse ferramentas de axuda para:



1. **Almacenar requisitos.** Os requisitos deben gardarse nun almacén de datos seguro e administrado que sexa accesible a todos os que estean implicados no proceso de enxeñería de requisitos.
2. **Xestionar o cambio.**
3. **Xestionar o rastrexo.** As ferramentas de axuda para o rastrexo permiten que se descubran requisitos relacionados. Algunhas ferramentas utilizan técnicas de procesamento da linguaxe natural para axudar a descubrir posibles relacións entre os requisitos.

Para sistemas pequenos, é posible que non sexa necesario utilizar ferramentas de xestión de requisitos especializadas, pero si é moi conveniente para sistemas grandes.

#### 35.5.2 Xestión do cambio

A vantaxe de utilizar un proceso formal para xestionar o cambio é que todos os cambios propostos son tratados de forma consistente e que os cambios nos requisitos se fan de forma controlada. Existen varias etapas principais nun proceso de xestión de cambio:

- **Proposta de cambios.** O afectado por un requisito que non o satisfai debe cubrir un formulario de proposta de cambio indicando cal é o cambio que hai que realizar. Este cambio remíteselle ao equipo de xestión de requisitos para que o estude.
- **Análise de impactos.** A proposta de cambio avalíase para determinar o impacto do cambio no resto dos requisitos. Hai propostas cun impacto mínimo e outras cuxo impacto fai que se deba modificar unha parte substancial do sistema. Ademais do impacto, cómpre estudar a oportunidade ou necesidade do cambio. Ocorre moitas veces que a un usuario non lle parece ben un determinado aspecto do sistema pero a outros si os satisfai. Nestes casos débese chegar a un consenso entre todas as partes. Outras veces o cambio é



interesante pero considérase que non é oportuno facelo naquel momento, quizais porque se queira lanzar o sistema canto antes ou porque o cambio é considerable e sería mellor atacalo nunha fase posterior de desenvolvemento.

- **Toma de decisións.** Dependendo do impacto, da necesidade ou oportunidade do cambio e doutras cuestións específicas que poidan xurdir arredor do cambio, débese determinar se o cambio debe ser realizado ou non. Se se decide realizalo, cómpre facer as modificacións pertinentes no sistema para integrar o cambio co resto, empezando polos requisitos e finalizando polas partes máis avanzadas do sistema. Se, pola contra, se decide non facelo pódese optar por dúas solucións:
  - o Rexeitar o cambio, porque se considera que non ten sentido.
  - o Adiar a súa realización para un futuro; considérase o cambio necesario pero o momento non é oportuno. Posponse para cando se poida acometer.
- **Comunicación.** Tanto se se acepta coma se non, débenselles notificar os efectos da proposta de cambio a todos os afectados.
- **Incorporación.** Fanse as modificacións pertinentes que se identificaron na análise de impacto nos diferentes elementos afectados polo cambio.
- **Medición da estabilidade dos requisitos.** Avalíanse os parámetros que definen a estabilidade dos requisitos tras as modificacións que se realizaron.

## 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 segundo o 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 da Escola Superior de Enxeñaría Informática.**

**Universidade de Vigo.**

## **36. ANÁLISE ORIENTADA A OBXECTOS. LINGUAXE UNIFICADA DE MODELAXE (UML).**

## **Tema 36. Análise orientada a obxectos. Linguaxe Unificada de modelado (UML)**

### **ÍNDICE:**

#### **36.1 Análise orientada a obxectos**

##### **36.1.1 Introducción á orientación a obxectos**

##### **36.1.2 Elementos da orientación a obxectos**

##### **36.1.3 Propiedades da orientación a obxectos**

##### **36.1.4 Análise orientada a obxectos**

##### **36.1.5 Modelado de Clases-Responsabilidades-Colaboracións (CRC)**

#### **36.2 Linguaxe Unificada de modelado (UML)**

##### **36.2.1 Introducción**

##### **36.2.2 Elementos de construción**

##### **36.2.3 Relacións**

##### **36.2.4 Diagramas**

### **36.1 Análise orientada a obxectos**

#### *36.1.1 Introducción á orientación a obxectos*

O principal obxectivo da orientación a obxectos é reducir a complexidade do desenvolvemento e mantemento do software, e pódese describir como o conxunto de disciplinas que desenvolven e modelan software e que facilitan a construción de sistemas complexos a partir de compoñentes. Os conceptos de orientación a obxectos datan dos anos 60, pero dado que a tecnoloxía non estaba acorde coa súa implementación, mantívose só como concepto ata a súa grande expansión a mediados dos 80.

A Análise Orientada a Obxectos "é un método de análise que examina os requisitos desde a perspectiva das clases e obxectos atopados no

vocabulario do dominio do problema" (Booch 94). O modelo da Análise debe incluír información significativa desde a perspectiva do mundo real e debe presentar unha vista externa do sistema definindo os obxectos no dominio do problema. Debe ser comprendido polo cliente e servir de axuda para atopar os verdadeiros requisitos do sistema.

O ciclo de desenvolvemento do software orientado a obxectos comeza, en primeiro lugar, construíndo na **Análise** un modelo que abstrae os aspectos esenciais do dominio do problema, sen ter en conta nesta etapa a implementación concreta. Este modelo conceptual conterá obxectos atopados no dominio da aplicación e describirá as súas propiedades e comportamento. En segundo lugar, o Deseño engadirá detalles e tomará decisións que optimicen a implementación. No deseño, os obxectos descríbense en termos do dominio do ordenador. Finalmente, o modelo obtido no deseño **impleméntase** nunha linguaxe de programación, unha base de datos e un hardware concretos.

### *36.1.2 Elementos da orientación a obxectos*

- **Obxectos:** Os obxectos son módulos que conteñen os datos e as instrucións que manipulan eses datos; posúen unha funcionalidade porque poden reaccionar ante unha serie de mensaxes e procesar unha serie de peticións. Dito doutra forma, os obxectos son entidades que teñen atributos (datos) e formas de comportamento (procedementos) particulares. Dentro dun sistema orientado a obxectos represéntanse todos aqueles relevantes para o Universo de Discurso sobre o que trate o sistema.
- **Clases:** Unha clase describe un conxunto de obxectos diferentes con propiedades (atributos) semellantes e un comportamento común; podémola ver como un patrón que define as variables e métodos que son comúns para os obxectos de certo tipo. Cada un dos obxectos individuais pertencentes a unha clase denomínase instancia da



devandita clase. Unha clase que non teña instancias denomínase clase abstracta. Unha clase abstracta pode servir para declarar as propiedades ou o comportamento dun conxunto determinado de clases que derivarán dela. As clases son un concepto **estático** definido no programa fonte, son unha abstracción da esencia dun obxecto; namentres que os obxectos son entes **dinámicos**, que existen no tempo e no espazo e que ocupan memoria na execución dun programa.

- **Atributos:** representan os datos asociados aos obxectos instanciados por esa clase, é dicir, son as propiedades ou características dun obxecto.
- **Operacións** ou **métodos:** representan as funcións ou procesos propios dos obxectos dunha clase, caracterizando os devanditos obxectos. Os métodos dun obxecto invócanse exclusivamente coa mensaxe adecuada, e ao ser invocado un método dun obxecto só se referirá á estrutura de datos dese obxecto e non á doutros, aínda que sexan da mesma clase. A interface da clase estará definida polo conxunto de métodos que soporta e as mensaxes que é capaz de tratar.
- **Mensaxes.** Os obxectos teñen a posibilidade de actuar. A actuación prodúcese cando un obxecto recibe unha mensaxe, que non é máis que unha solicitude que lle pide que se comporte dalgunha forma determinada. A mensaxe contén o nome do obxecto ao que vai dirixida, o nome dunha operación e, en ocasións, un grupo de parámetros.

### *36.1.3 Propiedades da orientación a obxectos*

Os principios do modelo orientado a obxectos son:

- **Identidade:** Cada obxecto ten a súa propia identidade inherente; é dicir, dous obxectos son distintos aínda que teñan todas as súas propiedades iguais.
- **Clasificación.** Refírese a que os obxectos que teñen a mesma estrutura de datos (atributos) e o mesmo comportamento (operacións ) están agrupados nunha clase.
- **Herdanza.** A herdanza é o mecanismo mediante o cal unha clase (subclase) adquire as propiedades doutra clase xerarquicamente superior (superclase, clase base). A herdanza proporciona o mecanismo para compartir automaticamente métodos e datos entre clases, subclases e obxectos, e pode ser simple ou múltiple, dependendo de que unha subclase herde os datos e métodos dunha soa clase ou de máis dunha. Unha clase pódese definir de modo moi amplo e despois refinala en sucesivas subclases. Cada subclase incorpora ou “herda” todas as propiedades da súa superclase e engade as súas propiedades únicas, o que reduce en gran medida a repetición no deseño e a programación e é unha das principais vantaxes da Orientación a Obxectos. A herdanza proporciona relacións entre clases do tipo “es-un”. A herdanza permite que as clases derivadas proporcionen comportamentos específicos, mantendo unha clase base común.
- **Abstracción:** É unha descrición simplificada dun sistema que salienta algúns dos detalles ou propiedades do mesmo, en canto que suprime outros. Consiste na xeneralización conceptual do comportamento dun determinado grupo de obxectos e dos seus atributos. Trátase de abstraer os datos e métodos comúns a un conxunto de obxectos para almacenalos nunha clase. A orientación a obxectos fai que os programadores e usuarios pensen sobre as aplicacións de maneira abstracta, prestándolle atención ao que é un obxecto e o que fai antes de decidir como será implementado.

- **Encapsulación:** É o termo que se utiliza para expresar que os datos dun obxecto só poden ser manipulados mediante as mensaxes e métodos predefinidos. É dicir, os datos relativos a algún obxecto están almacenados xunto co proceso que crea e manipula eses datos. Desta forma, quedan escondidos os detalles de implementación dun obxecto que non contribúen a definir as súas características esenciais.

Os obxectos restrinxen a visibilidade dos seus recursos (atributos e métodos) para o resto de usuarios. Cada obxecto posúe unha interface que determina a maneira de interactuar con el. A implementación do obxecto (o seu interior) é encapsulada, o que quere dicir que desde fóra o obxecto é invisible; simplemente úsase.

- **Polimorfismo:** É a propiedade pola cal unha mesma mensaxe pode orixinar condutas diferentes ao ser recibida por obxectos diferentes. É dicir, a mesma operación pode comportarse de xeito diferente para clases diferentes. O polimorfismo é consecuencia da herdanza. As funcións dunha clase base poden ser substituídas nunha clase derivada mediante a redefinición da súa declaración na clase “filla”. Polo tanto, os obxectos das dúas clases poden reaccionar ambos ás mesmas mensaxes, pero han facelo de diferentes xeitos. Tamén falamos de polimorfismo cando temos distintos métodos que mostran un comportamento distinto en función do número ou tipo de parámetros que reciben. Neste caso falamos de **métodos polimórficos**.

O polimorfismo é posible grazas ás interfaces que permiten acceder a métodos co mesmo nome en diferentes clases. Dentro de cada clase particular pódese redefinir o método obtendo distintos métodos co mesmo nome. Xa que logo, un método non se define exactamente co seu nome, se non co seu nome e o nome da clase á que pertence.

- **Reusabilidade:** É a capacidade de producir compoñentes reutilizables para outros deseños ou aplicacións, é dicir, permite reutilizar parte do código para o desenvolvemento dunha aplicación similar. Na Orientación a obxectos conséguese dunha forma natural mediante o deseño de compoñentes.
- **Persistencia:** Un obxecto en software ocupa un determinado espazo de memoria e existe durante unha certa cantidade de tempo: é un concepto dinámico. A persistencia é a calidade que se refire á permanencia do obxecto, é dicir, ao tempo durante o cal se lle asigna espazo e permanece accesible na memoria do ordenador (principal ou secundaria).
- **Extensibilidade:** É a capacidade dun programa para ser facilmente alterado de forma que poida tratar con novas clases de entrada. Mediante esta propiedade, os obxectos poden ser usados para almacenar e procesar moitos tipos diferentes de datos, simplemente engadindo clases que traten os tipos de datos que sexan necesarios.

#### 36.1.4 Análise orientada a obxectos

A Análise Orientada a Obxectos enfatiza a construción de modelos baseados no mundo real, utilizando unha perspectiva deste baseada nas clases e obxectos atopados no dominio do problema. Firesmith describe a **análise do dominio** como *“a identificación, análise e especificación de requisitos comúns nun dominio de aplicación específico, normalmente para a súa reutilización en múltiples proxectos dentro do mesmo dominio de aplicación. A análise orientada a obxectos do dominio é a identificación, análise e especificación de capacidades comúns e reutilizables dentro dun dominio de aplicación específico, en termos de obxectos, clases, submontaxes e marcos de traballo comúns”*. Do mesmo xeito que nos métodos estruturados tradicionais, na etapa Análise hai que establecer que é o que se debe facer, deixando para etapas posteriores os detalles. O

resultado da análise debe ser unha completa comprensión do problema. As dúas grandes etapas de que consta a Análise son as seguintes:

1. A descrición ou especificación do problema. Esta descrición non debe considerarse inmutable, senón máis ben como a base para ir refinando as especificacións reais. A especificación do problema debe establecer o ámbito do problema, describir as necesidades e requisitos, o contexto da aplicación, os supostos de que se parte ou as necesidades de rendemento do sistema. Nestas especificacións, o usuario do sistema debe indicar cales son obrigadas e cales se pode considerar opcionais. Así mesmo, outros puntos que hai que tratar poden ser os estándares de Enxeñería do Software, deseño das probas que se efectuarán, previsión de futuras extensións, etc.
2. A modelización da Análise: As características esenciais deben abstraerse nun modelo. As especificacións expresadas en linguaxe natural tenden a ser ambiguas, incompletas e inconsistentes; no entanto, o Modelo de Análise é unha representación precisa e concisa do problema que permite construír unha solución. A etapa seguinte de deseño remitirase a este modelo, en lugar de ás vagas especificacións iniciais. O Modelo de Análise constrúese identificando as clases e obxectos do dominio do problema (estrutura estática), as interaccións entre os obxectos e o seu secuenciamento (estrutura dinámica) e as accións que debe realizar o sistema, que producen un resultado observable e valioso para os usuarios (estrutura funcional).

#### *36.1.5 Modelado de Clases-Responsabilidades-Colaboracións (CRC)*

O modelado de Clases-Responsabilidades-Colaboracións (CRC) achega un medio sinxelo de identificar e organizar as clases que resulten relevantes para o sistema ou requisitos do produto. Este modelo parte dos casos de uso (unha secuencia de accións realizadas polo sistema que producen un

resultado observable e valioso para un usuario en particular, é dicir, representa o comportamento do sistema co fin de lles dar respostas aos usuarios) que se utilizaron para modelar o sistema desde o punto de vista do usuario. Unha vez desenvolvidos os escenarios de uso básicos, identifícanse as clases candidatas, as súas responsabilidades e as súas colaboracións. “Un modelo CRC é unha colección de tarxetas que representan clases. As tarxetas están divididas en tres seccións. Ao longo da cabeceira da tarxeta vostede escribe o nome da clase. No corpo lístanse as responsabilidades da clase á esquerda e á dereita os colaboradores.”

Para identificar as **clases e obxectos**, pártese dunha análise léxico-gramatical o máis precisa posible da descrición do problema. Os **substantivos** convértense en clases/obxectos candidatos. Un obxecto/clase potencial debe satisfacer estas características para poder ser considerado como posible membro do modelo:

- Reter información: o obxecto potencial será útil durante a análise se a información sobre el debe gardarse para que o sistema funcione.
- Debe ter un conxunto de operacións que permitan cambiar os valores dos seus atributos.
- Atributos comúns: o conxunto de atributos definido para a clase debe ser aplicable a todas as ocorrencias do obxecto.
- Operacións comúns: a clase potencial debe definir un conxunto de operacións aplicables, igual ca antes, a todos os obxectos da clase.

As **responsabilidades** estarían formadas polos atributos e operacións das clases. Os **atributos** representan características ou propiedades dunha clase, é dicir, información sobre a clase. As **operacións** tamén se poden extraer da análise léxico-gramatical da descrición do problema. Os **verbos** transfórmanse en candidatos a operacións. Cada operación elixida para unha clase exhibe un comportamento da clase.

As clases cumpren coas súas responsabilidades de dúas formas: ou ben unha clase pode usar as súas propias operacións para manipular os seus propios atributos —cumprindo, xa que logo, cunha responsabilidade particular— ou ben pode colaborar con outras clases.

Dicimos que un obxecto **colabora** con outro se para executar unha responsabilidade necesita enviarlle algunha mensaxe ao outro obxecto. Unha colaboración simple flúe nunha dirección, representando unha solicitude do cliente ao servidor. Desde o punto de vista do cliente, cada unha das súas colaboracións está asociada cunha responsabilidade particular implementada polo servidor.

Cada tarxeta do modelo CRC contén unha clase cunha lista de responsabilidades. O seguinte paso é definir aquelas clases colaboradoras que axudan na realización de cada responsabilidade. Isto establece as **conexións ou relacións** entre clases. As **relacións** deben derivarse a partir do exame dos verbos na descrición do problema. Unha vez conectadas as clases cos seus colaboradores, etiquetamos cada unha destas conexións, engadímoslles unha dirección, en función de qué clase chama a qué outra e para rematar avalíase cada extremo da conexión para determinar a cardinalidade. Este modelo de clases conectadas dá lugar ao **modelo Obxecto-Relación**.

O modelo CRC e o modelo Obxecto-Relación representan elementos estáticos. Para ter un modelo dinámico, debemos introducir o comportamento do sistema como unha función de sucesos específicos e tempo. Identifícanse os sucesos que dirixen as secuencias de interacción entre obxectos, créase unha traza de sucesos para cada caso de uso e constrúese un diagrama de transición de estados para o sistema. Unha vez terminada esta tarefa teríamos o modelo **Obxecto-Comportamento**.

## **36.2 Linguaxe Unificada de Modelado (UML)**

### 36.2.1 Introducción

UML (*Unified Modeling Language*) é unha linguaxe que permite modelar, construír e documentar os elementos que forman un sistema software orientado a obxectos. Converteuse no estándar *de facto* da industria, debido a que foi impulsado polos autores dos tres métodos máis usados de orientación a obxectos: Grady Booch, Ivar Jacobson e Jim Rumbaugh. É o estándar actual do chamado *Object Management Group* (OMG). Un dos obxectivos principais da creación de UML era posibilitar o intercambio de modelos entre as distintas ferramentas CASE orientadas a obxectos do mercado. Para iso era necesario definir unha notación e semántica común.

Hai que ter en conta que o estándar UML non define un proceso de desenvolvemento específico; trátase tan só dunha notación. UML serve para *especificar*, modelos concretos, non ambiguos e completos. Un modelo de UML representa un sistema software desde unha perspectiva específica. Cada modelo permítenos fixarnos nun aspecto distinto do sistema. Debido á súa estandarización e á súa definición completa non ambigua —e aínda que non sexa unha linguaxe de programación— UML pódese conectar de xeito directo a linguaxes de programación como Java, C++ ou Visual Basic; esta correspondencia permite o que se denomina como enxeñería directa (obter o código fonte partindo dos modelos) pero ademais é posible reconstruír un modelo en UML partindo da implementación, ou sexa, a enxeñería inversa.

UML exprésase a través de **elementos de construción**, de **relacións** e de **diagramas** que conteñen elementos e relacións

### 36.2.2 Elementos de construción

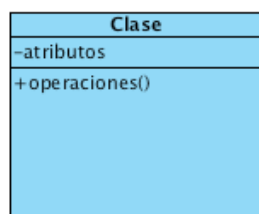
Chamámoslles “elementos” aos bloques básicos de construción. Son de catro tipos:

#### 36.2.2.1 Elementos estruturais



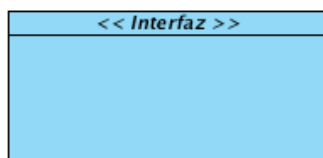
Na súa maioría son as partes estáticas do modelo. Son sete:

- **Clase:** Descrición dun conxunto de obxectos que comparten os mesmos atributos, operacións, relacións e semántica. Unha clase represéntase mediante unha caixa subdividida en tres partes: Na superior móstrase o nome da clase, na media os atributos e na inferior as operacións. Unha clase pódese representar de forma esquemática, cos detalles como atributos e operacións suprimidos, sendo daquela tan só un rectángulo co nome da clase.

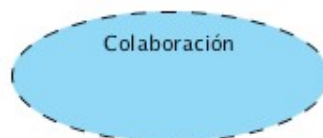


TEXTO CADRO: operacións

- **Interface:** colección de operacións que especifican un servizo dunha clase ou compoñente, mostrando o comportamento visible externamente dese elemento. Unha interface contén só as especificacións das operacións, é dicir a súa sinatura, pero non a implementación.



- **Colaboración:** define unha interacción e representa un conxunto de elementos do modelo que colaboran para proporcionar un comportamento cooperativo maior que a suma dos comportamentos dos seus elementos. Polo tanto, as colaboracións teñen tanto dimensión estrutural como de comportamento.



- **Caso de uso:** descrición dun conxunto de secuencias de accións que un sistema executa e que produce un resultado observable de interese para un usuario particular. Un caso de uso utilízase para estruturar os aspectos de comportamento nun modelo. Un caso de uso é realizado por unha colaboración.



- **Clase activa:** Clase cuxos obxectos teñen un ou máis procesos ou fíos de execución e, polo tanto, poden dar orixe a actividades de control.
- **Compoñente:** Parte física e substituíble dun sistema que representa tipicamente o empaquetamento físico de diferentes elementos lóxicos, como clases, interfaces e colaboracións.



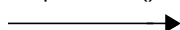
- **Nodo:** Elemento físico que existe en tempo de execución e representa un recurso computacional que normalmente dispón de memoria e capacidade de procesamento (Impresoras, PC...).

#### 36.2.2.2 Elementos de comportamento

Os elementos de comportamento son as partes dinámicas dos modelos. Representan comportamento no tempo e no espazo. Hai dous tipos de elementos de comportamento:

- **Interaccións:** unha interacción é un comportamento que comprende un conxunto de mensaxes intercambiadas entre un conxunto de obxectos dentro dun contexto particular para alcanzar un propósito

operación()



específico. O comportamento dunha sociedade de obxectos ou unha operación individual pódese especificar mediante unha interacción. Unha interacción comprende outros elementos, incluíndo mensaxes, secuencias de acción (o comportamento invocado por unha mensaxe) e enlaces (conexións entre obxectos).

- **Máquinas de estados:** unha máquina de estados especifica as secuencias de estados polas que pasa un obxecto ou unha interacción durante a súa vida en resposta a eventos. O comportamento dunha clase individual ou unha colaboración de clases pódese especificar cunha máquina de estados. Unha máquina de estados comprende outros elementos, incluíndo estados, transicións (o fluxo dun estado a outro), eventos (que disparan unha transición) e actividades (a resposta a unha transición).

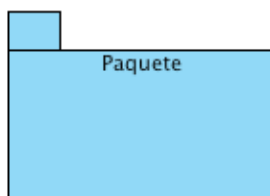


estado



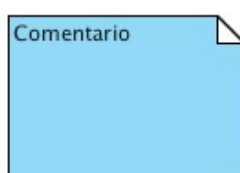
### 36.2.2.3 Elementos de agrupación

Os elementos de agrupación son as partes organizativas dos modelos de UML. Só hai un elemento de agrupación: o **paquete**, que é un mecanismo para organizar os elementos en grupos. Pode conter elementos estruturais, elementos de comportamento e mesmo outros paquetes.



### 36.2.2.4 Elementos de anotación

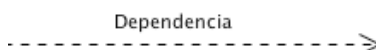
Os elementos de anotación son a parte explicativa dos modelos de UML. Son comentarios que se poden aplicar para describir, clarificar e facer observacións sobre calquera elemento dun modelo. O principal elemento de anotación é a nota, que é simplemente un símbolo para mostrar restricións e comentarios xunto a un elemento ou unha colección de elementos.



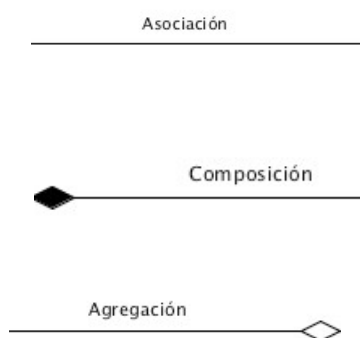
## 36.2.3 Relacións

Hai catro tipos de relacións en UML:

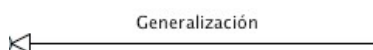
- **Dependencia:** é unha relación semántica entre dous elementos, na cal un cambio a un elemento (o elemento independente) pode afectar á semántica do outro elemento (o elemento dependente).



- **Asociación:** Unha **asociación** é unha relación estrutural que describe un conxunto de enlaces, que son conexións entre obxectos. A **agregación** é un tipo especial de asociación, que representa unha relación estrutural entre un todo e as súas partes. Graficamente, unha asociación represéntase como unha liña continua, posiblemente dirixida, que ás veces inclúe unha etiqueta e a miúdo inclúe outros adornos, como a multiplicidade e os nomes de rol. A agregación represéntase mediante un rombo situado na parte do todo. A **composición** é un tipo de agregación no que cada parte só pode pertencer a un todo e non pode existir a parte sen o todo. Represéntase igual que a agregación, só que o rombo está recheo.

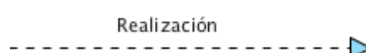


- **Xeneralización:** Unha xeneralización é unha relación de especialización /xeneralización na cal os obxectos do elemento especializado (o fillo) poden substituír os obxectos do elemento xeral (o pai). Desta forma, o fillo comparte a estrutura e o comportamento do pai.



LEENDA: Xeneralización

- **Realización:** Unha realización é unha relación semántica entre clasificadores, onde un clasificador especifica un contrato que outro clasificador garante que cumprirá. Pódense atopar relacións de realización en dous sitios: entre interfaces e as clases e compoñentes que as realizan, e entre os casos de uso e as colaboracións que os realizan.



### 36.2.4 Diagramas

Un diagrama é a representación gráfica dun conxunto de elementos, en xeral visualizado como un grafo conexo de nodos (elementos) e arcos (relacións). Os diagramas débúxanse para visualizar un sistema desde diferentes perspectivas. Pódense agrupar en dous bloques en función de se vemos o modelo de forma estática (estrutural) ou de forma dinámica (comportamento). A primeira inclúe os diagramas de despregamento, compoñentes, clases e obxectos, namentres que a segunda inclúe os diagramas de estados, actividades, secuencia, colaboración e casos de uso. Pasamos a ver cada un deles.

#### 36.2.4.1 Diagrama de casos de uso.

Un Diagrama de Casos de Uso mostra a relación entre os actores e os casos de uso do sistema e representa a funcionalidade que ofrece o sistema no que se refire á súa interacción externa. Un caso de uso é unha secuencia de accións realizadas polo sistema que producen un resultado observable e valioso para un usuario en particular, é dicir, representa o comportamento do sistema co fin de lles dar respostas aos usuarios e serve para describir ante os usuarios o devandito sistema.

A especificación dun caso de uso recolle, nun primeiro momento, unha descrición xeral. Esta descrición reflectirá posiblemente un ou varios

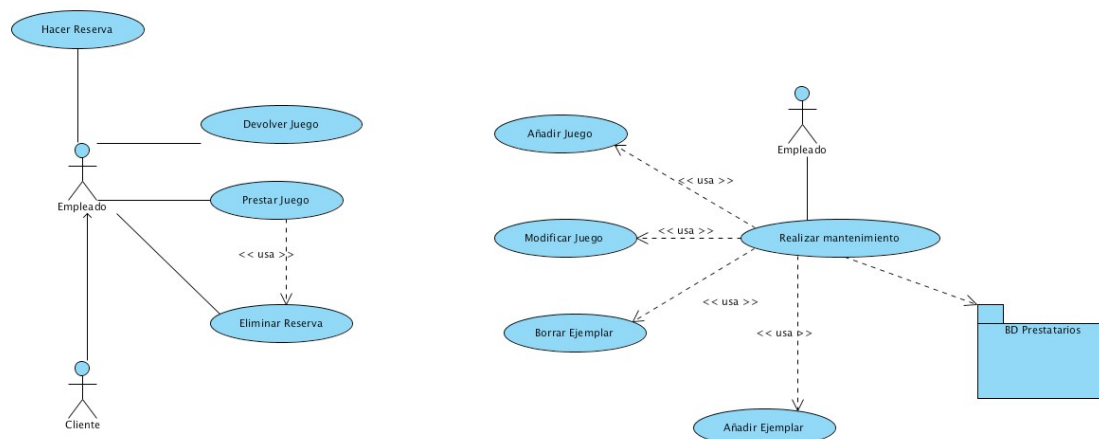
requisitos funcionais do sistema ou formará parte dalgún requisito. Pódese completar a descrición definindo cales son as precondicións e poscondicións. Tamén se poden enumerar os diferentes escenarios do caso de uso se os tivese e dar unha breve descrición deles. Os escenarios son os distintos camiños polos que pode evolucionar un caso de uso, dependendo das condicións que se van dando na súa realización.

Están formados por dous elementos: **actores**, que é algo ou alguén que se atopa fóra do sistema e que interactúa con el e pode referirse tanto a actores que sexan persoas como a outro tipo de actores (outros sistemas, sensores, etc), e **casos de uso**, que representan o comportamento que ofrece o sistema de información desde o punto de vista do usuario; ademais represéntanse as relacións entre os casos de uso. Opcionalmente tamén podería incluír paquetes que agruparían outras partes do sistema.

Entre os elementos dun diagrama de casos de uso pódense dar tres tipos de relacións:

- **Comunica:** É a relación entre un actor e un caso de uso, que denota a participación do actor no devandito caso de uso.
- **Usa:** Relación de dependencia entre dous casos de uso que denota a inclusión do comportamento dun escenario noutro. Úsase cando se quere reflectir un comportamento común en varios casos de uso.

**Estende:** Relación de dependencia entre dous casos de uso no que un é unha especialización do outro, existindo neste caso unha extensión da funcionalidade. Represéntanse como unha liña que une os dous casos de uso relacionados cunha frecha en forma de triángulo e cunha etiqueta <<estende>>, <<usa>> ou <<comunica>>, segundo sexa o tipo de relación.



Lenda: devolución do exemplar / prestar exemplar / engadir título / borrar ou actualizar título / mantemento / facer reserva

#### 36.2.4.2 Diagrama de clases

O obxectivo principal deste modelo é a representación dos aspectos estáticos do sistema utilizando diversos mecanismos de abstracción (clasificación, xeneralización, agregación). Recolle as clases de obxectos e as súas asociacións. Neste diagrama represéntase a estrutura e o comportamento de cada un dos obxectos do sistema e as súas relacións cos demais obxectos, pero non mostra información temporal. Sérvenos para visualizar as relacións entre as clases que involucran o sistema, as cales poden ser asociativas, de herdanza e de uso.

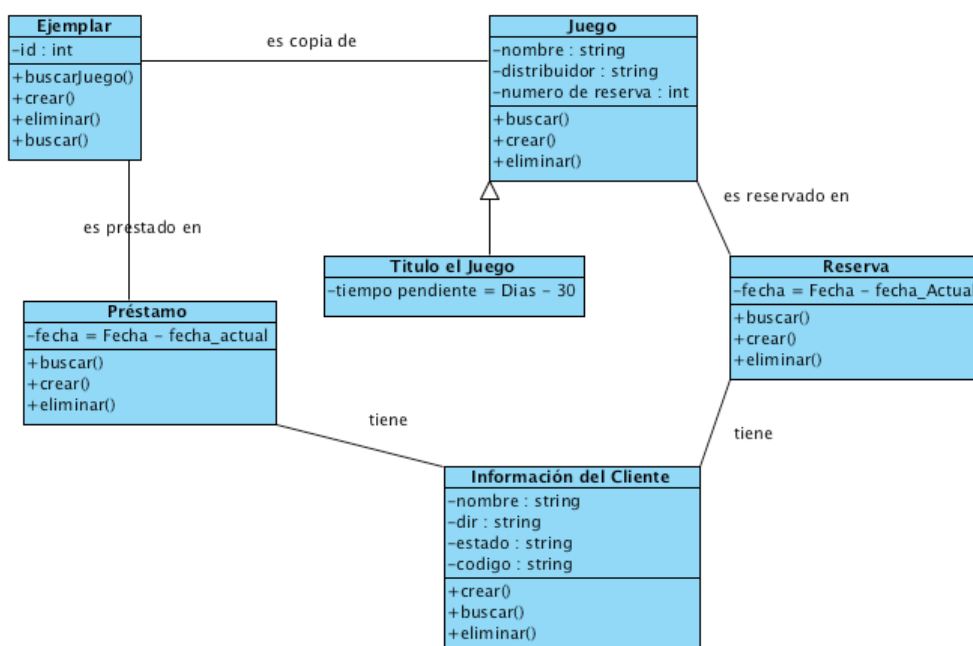
O modelo está formado por:

- **Clases:** Represéntase como unha caixa dividida en tres zonas. Na zona superior ponse o nome da clase. No centro colócanse os atributos (características) da clase co formato: *“visibilidade nome : tipo = valor-inicial { propiedades }”*. A visibilidade será en xeral



publica (+), privada (-) ou protexida. Na zona inferior inclúese unha lista coas operacións que proporciona a clase. Cada operación aparece nunha liña con formato: “*visibilidade nome (lista-de-parámetros): tipo-devolto { propiedade }*”

- **Relacións:** Asociacións, agregacións, composicións, dependencias ou herdanza. Pódense documentar cunha descrición do seu propósito, a súa multiplicidade, navegabilidade ou rol de cada unha das clases na relación.
- **Interfaces**
- **Paquetes**

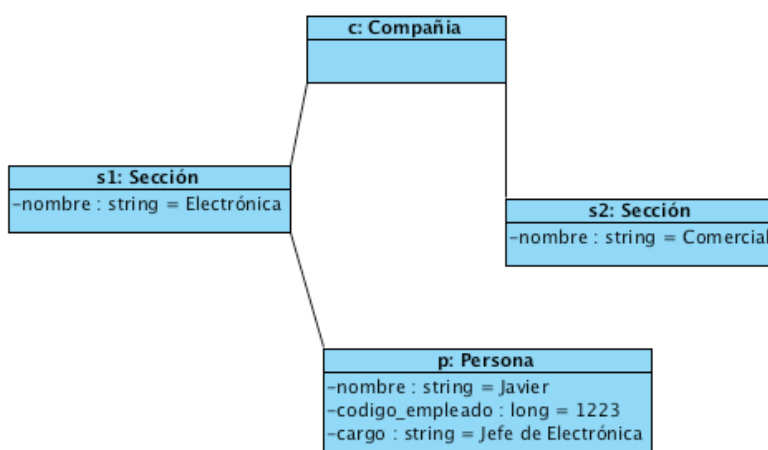


LEENDA: **Ejemplar**. buscarxogo/ é copia de / **Xogo**. nome: distribuidor / é prestado en / é reservado en / Título o Xogo / tempo pendiente = Días / data = Data - data\_Actual / ten / ten / Información do cliente / nome

### 36.2.4.3 Diagrama de obxectos

Modelan as instancias de elementos contidos nos diagramas de clases. Mostra un conxunto de obxectos e as súas relacións nun momento

concreto. Para mostrar o estado dun obxecto, indícase o valor dos seus atributos e os seus obxectos agregados. Os diagramas de obxectos non mostran multiplicidade nin roles, aínda que a súa notación é semellante á dos diagramas de clase.



Lenda: Compañía / nome / código empregado / Xefe de Electrónica

#### 36.2.4.4 Diagramas de Interacción

Os **diagramas de interacción** utilízanse para modelar os aspectos dinámicos do sistema e mostrar un patrón de interacción entre obxectos. Namentres que un diagrama de casos de uso presenta unha visión externa do sistema, a funcionalidade dos devanditos casos de uso recóllese como un fluxo de eventos. Por outra banda, os diagramas de clases e os de obxecto representan información estática, pero nun sistema funcional os obxectos interactúan entre si e os tales eventos ou interaccións suceden no tempo. Este fluxo de eventos pódese recoller nunha especificación texto acompañada de distintos escenarios especificados mediante diagramas de interacción onde cada diagrama será unha visión gráfica dun escenario. Existen dous tipos de diagramas de interacción: **secuencia** e **colaboración**. Ambos son equivalentes. A diferenza entre eles está nos aspectos que salientan. Os diagramas de secuencia destacan a orde

temporal das mensaxes, mentres que os diagramas de colaboración destacan a organización estrutural dos obxectos.

#### *36.2.4.4.1 Diagramas de secuencia*

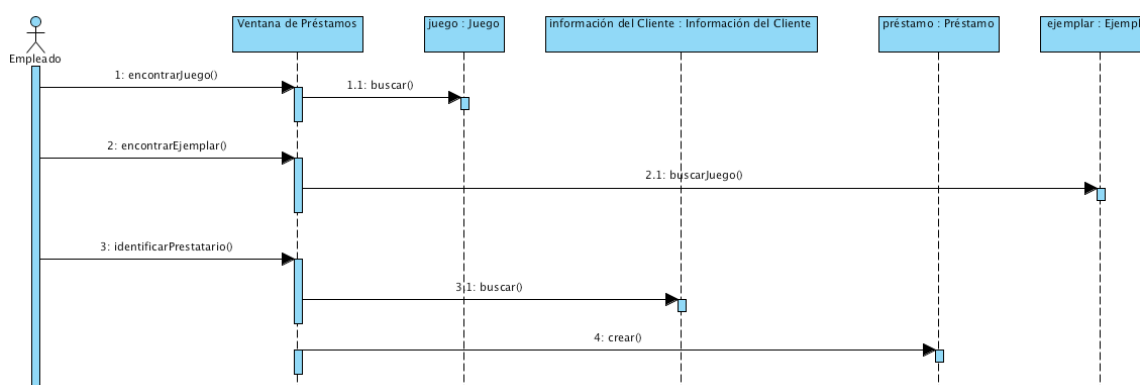
Mostran as interaccións entre obxectos ordenadas en **secuencia temporal**. Mostra os obxectos que se atopan no escenario e a secuencia de mensaxes intercambiadas entre os obxectos para levar a cabo a funcionalidade descrita polo escenario. Faise un diagrama de secuencia por cada caso de uso ou para unha parte deste.

O eixe vertical representa o tempo, e no eixe horizontal colócanse os obxectos e actores participantes na interacción, sen unha orde prefixada. Cada obxecto ou actor ten unha liña vertical e as mensaxes represéntanse mediante frechas entre os distintos obxectos. O tempo flúe de arriba abaixo. Pódense empregar etiquetas para especificar restricións de tempo, descricións de accións, etc; ben na marxe esquerda ou xunto á mensaxe ou activación á que se refira.

Os conceptos máis importantes relacionados cos diagramas de secuencia son:

- **Liña de vida** dun obxecto: representa a vida do obxecto durante a interacción. O obxecto represéntase como unha liña vertical punteada cun rectángulo de encabezado co nome do obxecto e da súa clase.
- **Activación:** Mostra o período de tempo durante o cal o obxecto se atopa desenvolvendo algunha operación. Denótase por un rectángulo sobre a liña de vida do obxecto.
- **Mensaxe:** Móstrase mediante unha liña sólida dirixida desde o obxecto que emite a mensaxe cara ao que a executa.

- **Camiños alternativos** de execución e concorrencia: Poden representar condicións na execución ou diferentes fíos de execución (*threads*).

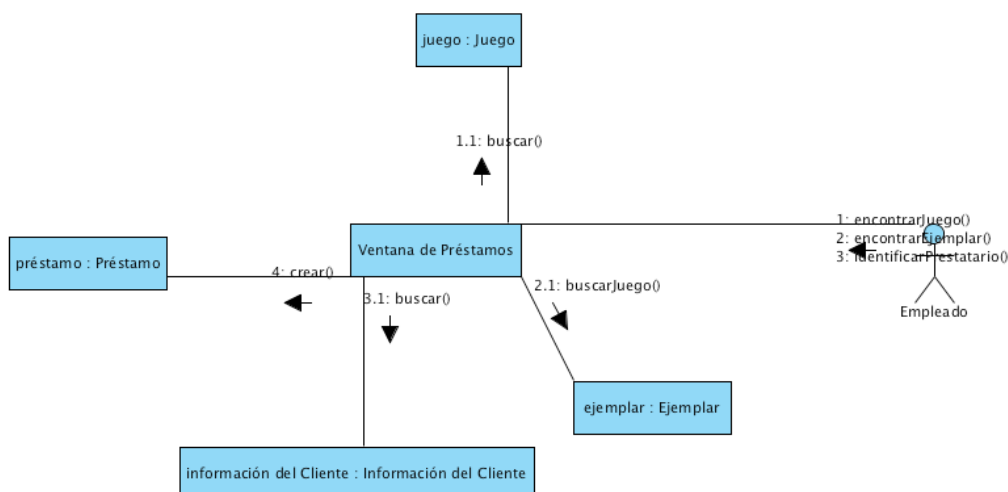


LEND: Ventá de Préstamos / xogo : Xogo / Información do Cliente /  
exemplar / Empregado / encontrarXogo / encontrar/exemplar / buscarXogo

#### 36.2.4.4.2 Diagramas de colaboración

Os diagramas de colaboración supoñen unha forma alternativa ao diagrama de secuencia para mostrar un escenario. Amosan a mesma información que un diagrama de secuencia pero de forma diferente. Nos diagramas de colaboración non existe unha secuencia temporal. Os elementos dun sistema traballan en conxunto para cumpriren cos obxectivos do sistema, e esta colaboración a que se reflicte. Nos diagramas de colaboración non existe unha secuencia temporal. Este diagrama resalta a **organización estrutural** dos obxectos que envían e reciben as mensaxes. Este tipo de diagrama mostra un conxunto de obxectos, enlaces entre eles e as mensaxes que intercambian.

A diferenza dos Diagramas de Secuencia, os Diagramas de Colaboración mostran as relacións entre os roles dos obxectos. A secuencia das mensaxes debe determinarse explicitamente mediante números de secuencia.



LEENDA: IGUAL ANTERIOR

#### 36.2.4.5 Diagramas de estados

Representan os estados que pode tomar un compoñente ou un sistema e mostran os eventos que implican o cambio dun estado a outro. Os diagramas de estado son útiles, entre outras cousas, para indicar os eventos do sistema nos casos de uso e para ilustrar qué eventos poden cambiar o estado dos obxectos dunha clase. Os dous elementos principais nestes diagramas son os estados e as posibles transicións entre eles.

- O estado dun compoñente ou sistema representa algún comportamento que é observable externamente e que perdura durante un período de tempo finito. Podémolo ver tamén como un período no que se satisfai unha condición. Vén dado polo valor dun ou varios atributos que o caracterizan nun momento dado.
- Unha **transición** é un cambio de estado producido por un evento e reflicte os posibles camiños para chegar a un estado final desde un estado inicial. Reflicte que un obxecto no primeiro estado pode entrar no segundo e executar certas operacións cando un evento ocorre e se certas condicións son satisfeitas.

Unha transición represéntase graficamente como unha liña continua dirixida desde a estado-orixe ata o estado-destino. Pode vir acompañada por un texto co seguinte formato:

nome-evento    '('lista-argumentos')'    '['guard-condition']    '/'  
expresión-acción '^' cláusula-envío.

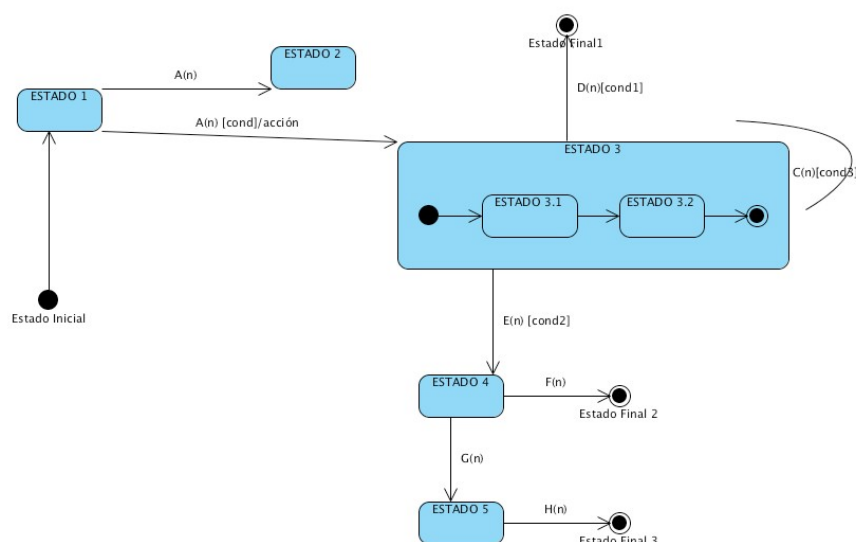
- *nome-evento* e *lista-argumentos* describen o evento que dá lugar á transición e forman o que se denomina *event-signature*.
- *guard-condition* é unha condición (expresión booleana) adicional ao evento e necesaria para que a transición se produza. Se a *guard-condition* se combina cunha *event-signature*, entón para que a transición se dispare teñen que suceder dúas cousas: debe ocorrer o evento e a condición booleana debe ser verdadeira.
- *expresión-acción* é unha expresión procedemental que se executa cando se dispara a transición. É posible ter unha ou varias expresión-acción nunha transición de estado, as cales se delimitan co carácter "/".
- *cláusula-envío* é unha acción adicional que se executa co cambio de estado; por exemplo, o envío de eventos a outros paquetes ou clases. Este tipo especial de acción ten unha sintaxe explícita para enviar unha mensaxe durante a transición entre dous estados. A sintaxe consiste nunha expresión de destino e nun nome de evento, separados por un punto.

Desde un estado poden xurdir varias transicións en función do evento que desencadea o cambio de estado, tendo en conta que as transicións que proveñen do mesmo estado non poden ter o mesmo evento, agás que exista algunha condición que se lle aplique ao evento. Un diagrama de estados pode representar ciclos continuos ou ben unha vida finita, na que

hai un estado inicial de creación e un estado final de destrución (do caso de uso ou do obxecto).

Un sistema só pode ter un **estado inicial**, que se representa mediante unha transición sen etiquetar ao primeiro estado normal do diagrama. En ningún caso pode haber unha transición dirixida ao estado inicial. O estado **final** representa que un compoñente deixou de ter calquera interacción ou actividade. Non se permiten transicións que partan do estado final. Pode haber varios estados finais nun diagrama.

Outros dous elementos que axudan a clarificar estes diagramas son as accións e as actividades. Unha acción é unha operación instantánea asociada a un evento, cunha duración que se considera non significativa e que se pode executar: dentro dun estado, ao entrar nun estado, ou ao saír del. Unha actividade é unha operación asociada a un estado que se executa durante un intervalo de tempo ata que se produce o cambio a outro estado.



#### 36.2.4.6 Diagrama de actividades

As actividades que ocorren dentro dun caso de uso ou dentro do comportamento dun obxecto danse, normalmente, en secuencia. Este tipo de diagrama pódese considerar un caso especial do diagrama de estados, no cal case todos os estados son estados-acción (identifican unha acción que se executa ao entrar nel) e case todas as transicións evolucionan ao termo da devandita acción. A interpretación dun diagrama de actividades depende da perspectiva considerada: nun diagrama conceptual, a actividade é algunha tarefa que debe ser realizada; nun diagrama de especificación ou de implementación, a actividade é un método dunha clase. Adóitanse utilizar para modelar os pasos dun algoritmo.

Os diagramas de actividade poden visualizar, especificar e documentar a dinámica dun conxunto de obxectos. Tamén se poden usar para modelar o fluxo de control dunha operación. Namentres que os diagramas de interacción enfatizan o fluxo de control dun obxecto a outro, os diagramas de actividade subliñan o fluxo de control dunha actividade a outra.

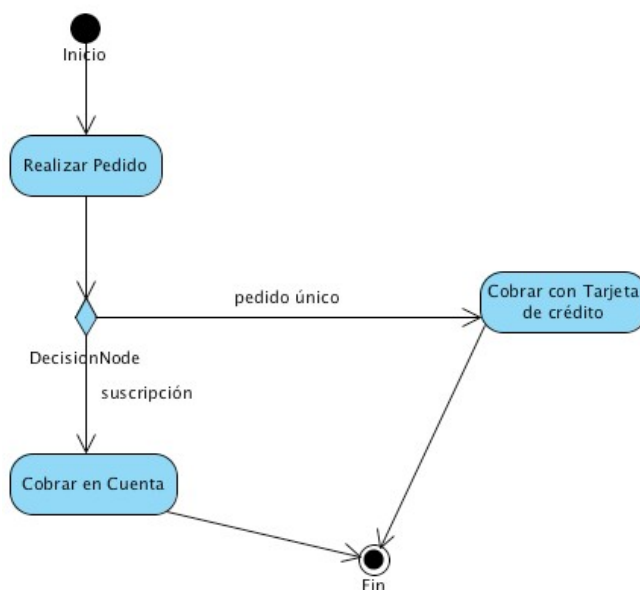
O principal inconveniente dos diagramas de actividade é que non indican explicitamente qué obxectos executan qué actividades nin tampouco a forma en que o servizo de mensaxería traballa entre eles. Para mostrar as tales interaccións de maneira clara son necesarios os diagramas de interacción, que son máis utilizados na práctica.

Nos diagramas de actividade, as decisións represéntanse mediante unha transición múltiple que sae dun estado onde cada camiño ten unha etiqueta distinta. Preséntase mediante un rombo ao cal chega a transición do estado-orixe e do cal saen as múltiples transicións dos estados-destino. Os diagramas de actividade son útiles cando queremos describir un comportamento paralelo, ou cando queremos mostrar qué comportamentos interactúan en varios casos de uso.



Un diagrama de actividades contén:

- *Estados de actividade e Estados de acción:* A representación de ambos é un rectángulo coas puntas redondeadas; no seu interior represéntase ben unha actividade ou ben unha acción.
  - Un estado que represente unha acción é atómico, o que implica que a execución pode considerarse instantánea e non se pode interromper.
    1. Un estado-actividade pode descompoñerse en máis sub-actividades representadas a través doutros diagramas de actividades. Ademais, estes estados poden interromperse e tardan certo tempo en completarse.
    2. Nos estados de actividade podemos atopar outros elementos adicionais, como son: accións de entrada e de saída do estado en cuestión.
- *Transicións:* Reflicten o paso dun estado a outro, ben sexa de actividade ou de acción. Esta transición prodúcese como resultado da finalización do estado do que parte o arco dirixido que marca a transición.



Lenda: suscripción / cobrar en conta / cargar con tarxeta de crédito

#### 36.2.4.7 Diagramas de implementación

Un diagrama de implementación mostra as dependencias entre as partes de código do sistema (**diagrama de compoñentes**) ou a estrutura do sistema en execución (**diagrama de despregamento**). Os diagramas de compoñentes utilízanse para modelar a vista de implementación estática dun sistema, en canto que os diagramas de despregamento se utilizan para modelar a vista de despregamento estática.

##### 36.2.4.7.1 Diagrama de compoñentes

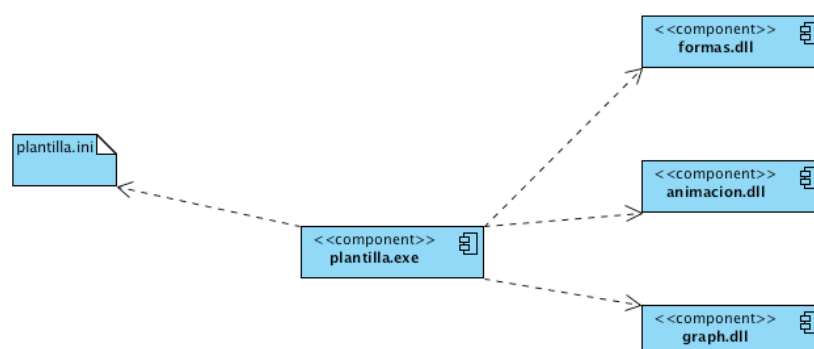
Mostra as organizacións e dependencias lóxicas entre compoñentes software, sexan estes compoñentes de código fonte, binarios, documentos, arquivos ou executables. Os diagramas de compoñentes representan calquera tipo de elemento software que participe no desenvolvemento dun sistema informático e poden ser simples arquivos, librerías, etc. Os

diagramas de compoñentes poden conter paquetes para organizar os elementos.

Dado que os diagramas de compoñentes mostran os compoñentes software que constitúen unha parte reusable, as súas interfaces e as súas interrelacións, en moitos aspectos pódense considerar como un diagrama de clases a grande escala. Cada compoñente do diagrama debe ser documentado cun diagrama de compoñentes máis detallado, un diagrama de clases, ou un diagrama de casos de uso.

Tipos de compoñentes:

- *Compoñentes de despregamento:* compoñentes necesarios e suficientes para formar un sistema executable, como poden ser as bibliotecas dinámicas e executables.
- *Compoñentes produto do traballo:* estes compoñentes son basicamente produtos que quedan ao final do proceso de desenvolvemento. Consisten en cousas como arquivos de código fonte e de datos a partir dos cales se crean os compoñentes de despregamento.
- *Compoñentes de execución:* son compoñentes que se crean como consecuencia dun sistema en execución.



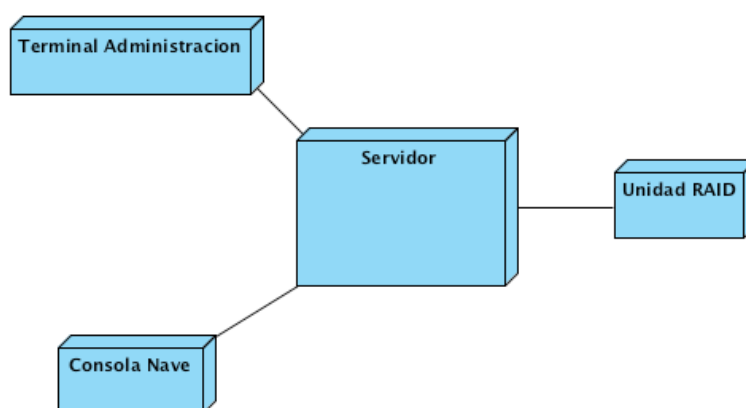
LENDIA: patrón / animación

#### 36.2.4.8 Diagrama de despregamento

Mostra as relacións físicas (arquitectura física) entre os compoñentes hardware e software no sistema final, é dicir, a configuración dos elementos de procesamento en tempo de execución e os compoñentes software (proceso e obxectos que se executan neles). Mostran a configuración en funcionamento do sistema, incluíndo hardware e software. Cobre principalmente a distribución, entrega e instalación das partes que configuran o sistema físico e adóitanse utilizar para modelar sistemas encaixados, sistemas cliente-servidor e sistemas distribuídos.

Nun diagrama de despregamento un nodo representa un elemento físico que existe en tempo de execución e que representa un recurso computacional. Os nodos conéctanse mediante asociacións de comunicación, tales como enlaces de rede, conexións TCP/IP, etc.

Os diagramas de despregamento son os complementos dos diagramas de compoñentes que, unidos, proporcionan a vista de implementación do sistema.



LEENDA: Unidade.

## **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](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 da Escola Superior de Enxeñería Informática.**

**Universidade de Vigo**

## **Tema 36. Análise orientada a obxectos. Linguaxe Unificada de modelado (UML)**

### **ÍNDICE:**

#### **36.1 Análise orientada a obxectos**

##### **36.1.1 Introducción á orientación a obxectos**

##### **36.1.2 Elementos da orientación a obxectos**

##### **36.1.3 Propiedades da orientación a obxectos**

##### **36.1.4 Análise orientada a obxectos**

##### **36.1.5 Modelado de Clases-Responsabilidades-Colaboracións (CRC)**

#### **36.2 Linguaxe Unificada de modelado (UML)**

##### **36.2.1 Introducción**

##### **36.2.2 Elementos de construción**

##### **36.2.3 Relacións**

##### **36.2.4 Diagramas**

### **36.1 Análise orientada a obxectos**

#### *36.1.1 Introducción á orientación a obxectos*

O principal obxectivo da orientación a obxectos é reducir a complexidade do desenvolvemento e mantemento do software, e pódese describir como o conxunto de disciplinas que desenvolven e modelan software e que facilitan a construción de sistemas complexos a partir de compoñentes. Os conceptos de orientación a obxectos datan dos anos 60, pero dado que a tecnoloxía non estaba acorde coa súa implementación, mantívose só como concepto ata a súa grande expansión a mediados dos 80.

A Análise Orientada a Obxectos "é un método de análise que examina os requisitos desde a perspectiva das clases e obxectos atopados no

vocabulario do dominio do problema" (Booch 94). O modelo da Análise debe incluír información significativa desde a perspectiva do mundo real e debe presentar unha vista externa do sistema definindo os obxectos no dominio do problema. Debe ser comprendido polo cliente e servir de axuda para atopar os verdadeiros requisitos do sistema.

O ciclo de desenvolvemento do software orientado a obxectos comeza, en primeiro lugar, construíndo na **Análise** un modelo que abstrae os aspectos esenciais do dominio do problema, sen ter en conta nesta etapa a implementación concreta. Este modelo conceptual conterá obxectos atopados no dominio da aplicación e describirá as súas propiedades e comportamento. En segundo lugar, o Deseño engadirá detalles e tomará decisións que optimicen a implementación. No deseño, os obxectos descríbense en termos do dominio do ordenador. Finalmente, o modelo obtido no deseño **impleméntase** nunha linguaxe de programación, unha base de datos e un hardware concretos.

### *36.1.2 Elementos da orientación a obxectos*

- **Obxectos:** Os obxectos son módulos que conteñen os datos e as instrucións que manipulan eses datos; posúen unha funcionalidade porque poden reaccionar ante unha serie de mensaxes e procesar unha serie de peticións. Dito doutra forma, os obxectos son entidades que teñen atributos (datos) e formas de comportamento (procedementos) particulares. Dentro dun sistema orientado a obxectos represéntanse todos aqueles relevantes para o Universo de Discurso sobre o que trate o sistema.
- **Clases:** Unha clase describe un conxunto de obxectos diferentes con propiedades (atributos) semellantes e un comportamento común; podémola ver como un patrón que define as variables e métodos que son comúns para os obxectos de certo tipo. Cada un dos obxectos individuais pertencentes a unha clase denomínase instancia da

devandita clase. Unha clase que non teña instancias denomínase clase abstracta. Unha clase abstracta pode servir para declarar as propiedades ou o comportamento dun conxunto determinado de clases que derivarán dela. As clases son un concepto **estático** definido no programa fonte, son unha abstracción da esencia dun obxecto; namentres que os obxectos son entes **dinámicos**, que existen no tempo e no espazo e que ocupan memoria na execución dun programa.

- **Atributos:** representan os datos asociados aos obxectos instanciados por esa clase, é dicir, son as propiedades ou características dun obxecto.
- **Operacións** ou **métodos:** representan as funcións ou procesos propios dos obxectos dunha clase, caracterizando os devanditos obxectos. Os métodos dun obxecto invócanse exclusivamente coa mensaxe adecuada, e ao ser invocado un método dun obxecto só se referirá á estrutura de datos dese obxecto e non á doutros, aínda que sexan da mesma clase. A interface da clase estará definida polo conxunto de métodos que soporta e as mensaxes que é capaz de tratar.
- **Mensaxes.** Os obxectos teñen a posibilidade de actuar. A actuación prodúcese cando un obxecto recibe unha mensaxe, que non é máis que unha solicitude que lle pide que se comporte dalgunha forma determinada. A mensaxe contén o nome do obxecto ao que vai dirixida, o nome dunha operación e, en ocasións, un grupo de parámetros.

### *36.1.3 Propiedades da orientación a obxectos*

Os principios do modelo orientado a obxectos son:



- **Identidade:** Cada obxecto ten a súa propia identidade inherente; é dicir, dous obxectos son distintos aínda que teñan todas as súas propiedades iguais.
- **Clasificación.** Refírese a que os obxectos que teñen a mesma estrutura de datos (atributos) e o mesmo comportamento (operacións ) están agrupados nunha clase.
- **Herdanza.** A herdanza é o mecanismo mediante o cal unha clase (subclase) adquire as propiedades doutra clase xerarquicamente superior (superclase, clase base). A herdanza proporciona o mecanismo para compartir automaticamente métodos e datos entre clases, subclases e obxectos, e pode ser simple ou múltiple, dependendo de que unha subclase herde os datos e métodos dunha soa clase ou de máis dunha. Unha clase pódese definir de modo moi amplo e despois refinala en sucesivas subclases. Cada subclase incorpora ou “herda” todas as propiedades da súa superclase e engade as súas propiedades únicas, o que reduce en gran medida a repetición no deseño e a programación e é unha das principais vantaxes da Orientación a Obxectos. A herdanza proporciona relacións entre clases do tipo “es-un”. A herdanza permite que as clases derivadas proporcionen comportamentos específicos, mantendo unha clase base común.
- **Abstracción:** É unha descrición simplificada dun sistema que salienta algúns dos detalles ou propiedades do mesmo, en canto que suprime outros. Consiste na xeneralización conceptual do comportamento dun determinado grupo de obxectos e dos seus atributos. Trátase de abstraer os datos e métodos comúns a un conxunto de obxectos para almacenalos nunha clase. A orientación a obxectos fai que os programadores e usuarios pensen sobre as aplicacións de maneira abstracta, prestándolle atención ao que é un obxecto e o que fai antes de decidir como será implementado.

- **Encapsulación:** É o termo que se utiliza para expresar que os datos dun obxecto só poden ser manipulados mediante as mensaxes e métodos predefinidos. É dicir, os datos relativos a algún obxecto están almacenados xunto co proceso que crea e manipula eses datos. Desta forma, quedan escondidos os detalles de implementación dun obxecto que non contribúen a definir as súas características esenciais.

Os obxectos restrinxen a visibilidade dos seus recursos (atributos e métodos) para o resto de usuarios. Cada obxecto posúe unha interface que determina a maneira de interactuar con el. A implementación do obxecto (o seu interior) é encapsulada, o que quere dicir que desde fóra o obxecto é invisible; simplemente úsase.

- **Polimorfismo:** É a propiedade pola cal unha mesma mensaxe pode orixinar condutas diferentes ao ser recibida por obxectos diferentes. É dicir, a mesma operación pode comportarse de xeito diferente para clases diferentes. O polimorfismo é consecuencia da herdanza. As funcións dunha clase base poden ser substituídas nunha clase derivada mediante a redefinición da súa declaración na clase “filla”. Polo tanto, os obxectos das dúas clases poden reaccionar ambos ás mesmas mensaxes, pero han facelo de diferentes xeitos. Tamén falamos de polimorfismo cando temos distintos métodos que mostran un comportamento distinto en función do número ou tipo de parámetros que reciben. Neste caso falamos de **métodos polimórficos**.

O polimorfismo é posible grazas ás interfaces que permiten acceder a métodos co mesmo nome en diferentes clases. Dentro de cada clase particular pódese redefinir o método obtendo distintos métodos co mesmo nome. Xa que logo, un método non se define exactamente co seu nome, se non co seu nome e o nome da clase á que pertence.

- **Reusabilidade:** É a capacidade de producir compoñentes reutilizables para outros deseños ou aplicacións, é dicir, permite reutilizar parte do código para o desenvolvemento dunha aplicación similar. Na Orientación a obxectos conséguese dunha forma natural mediante o deseño de compoñentes.
- **Persistencia:** Un obxecto en software ocupa un determinado espazo de memoria e existe durante unha certa cantidade de tempo: é un concepto dinámico. A persistencia é a calidade que se refire á permanencia do obxecto, é dicir, ao tempo durante o cal se lle asigna espazo e permanece accesible na memoria do ordenador (principal ou secundaria).
- **Extensibilidade:** É a capacidade dun programa para ser facilmente alterado de forma que poida tratar con novas clases de entrada. Mediante esta propiedade, os obxectos poden ser usados para almacenar e procesar moitos tipos diferentes de datos, simplemente engadindo clases que traten os tipos de datos que sexan necesarios.

#### 36.1.4 *Análise orientada a obxectos*

A Análise Orientada a Obxectos enfatiza a construción de modelos baseados no mundo real, utilizando unha perspectiva deste baseada nas clases e obxectos atopados no dominio do problema. Firesmith describe a **análise do dominio** como *“a identificación, análise e especificación de requisitos comúns nun dominio de aplicación específico, normalmente para a súa reutilización en múltiples proxectos dentro do mesmo dominio de aplicación. A análise orientada a obxectos do dominio é a identificación, análise e especificación de capacidades comúns e reutilizables dentro dun dominio de aplicación específico, en termos de obxectos, clases, submontaxes e marcos de traballo comúns”*. Do mesmo xeito que nos métodos estruturados tradicionais, na etapa Análise hai que establecer que é o que se debe facer, deixando para etapas posteriores os detalles. O

resultado da análise debe ser unha completa comprensión do problema. As dúas grandes etapas de que consta a Análise son as seguintes:

1. A descrición ou especificación do problema. Esta descrición non debe considerarse inmutable, senón máis ben como a base para ir refinando as especificacións reais. A especificación do problema debe establecer o ámbito do problema, describir as necesidades e requisitos, o contexto da aplicación, os supostos de que se parte ou as necesidades de rendemento do sistema. Nestas especificacións, o usuario do sistema debe indicar cales son obrigadas e cales se pode considerar opcionais. Así mesmo, outros puntos que hai que tratar poden ser os estándares de Enxeñería do Software, deseño das probas que se efectuarán, previsión de futuras extensións, etc.
2. A modelización da Análise: As características esenciais deben abstraerse nun modelo. As especificacións expresadas en linguaxe natural tenden a ser ambiguas, incompletas e inconsistentes; no entanto, o Modelo de Análise é unha representación precisa e concisa do problema que permite construír unha solución. A etapa seguinte de deseño remitirase a este modelo, en lugar de ás vagas especificacións iniciais. O Modelo de Análise constrúese identificando as clases e obxectos do dominio do problema (estrutura estática), as interaccións entre os obxectos e o seu secuenciamento (estrutura dinámica) e as accións que debe realizar o sistema, que producen un resultado observable e valioso para os usuarios (estrutura funcional).

#### *36.1.5 Modelado de Clases-Responsabilidades-Colaboracións (CRC)*

O modelado de Clases-Responsabilidades-Colaboracións (CRC) achega un medio sinxelo de identificar e organizar as clases que resulten relevantes para o sistema ou requisitos do produto. Este modelo parte dos casos de uso (unha secuencia de accións realizadas polo sistema que producen un

resultado observable e valioso para un usuario en particular, é dicir, representa o comportamento do sistema co fin de lles dar respostas aos usuarios) que se utilizaron para modelar o sistema desde o punto de vista do usuario. Unha vez desenvolvidos os escenarios de uso básicos, identifícanse as clases candidatas, as súas responsabilidades e as súas colaboracións. “Un modelo CRC é unha colección de tarxetas que representan clases. As tarxetas están divididas en tres seccións. Ao longo da cabeceira da tarxeta vostede escribe o nome da clase. No corpo lístanse as responsabilidades da clase á esquerda e á dereita os colaboradores.”

Para identificar as **clases e obxectos**, pártese dunha análise léxico-gramatical o máis precisa posible da descrición do problema. Os **substantivos** convértense en clases/obxectos candidatos. Un obxecto/clase potencial debe satisfacer estas características para poder ser considerado como posible membro do modelo:

- Reter información: o obxecto potencial será útil durante a análise se a información sobre el debe gardarse para que o sistema funcione.
- Debe ter un conxunto de operacións que permitan cambiar os valores dos seus atributos.
- Atributos comúns: o conxunto de atributos definido para a clase debe ser aplicable a todas as ocorrencias do obxecto.
- Operacións comúns: a clase potencial debe definir un conxunto de operacións aplicables, igual ca antes, a todos os obxectos da clase.

As **responsabilidades** estarían formadas polos atributos e operacións das clases. Os **atributos** representan características ou propiedades dunha clase, é dicir, información sobre a clase. As **operacións** tamén se poden extraer da análise léxico-gramatical da descrición do problema. Os **verbos** transfórmanse en candidatos a operacións. Cada operación elixida para unha clase exhibe un comportamento da clase.

As clases cumpren coas súas responsabilidades de dúas formas: ou ben unha clase pode usar as súas propias operacións para manipular os seus propios atributos —cumprindo, xa que logo, cunha responsabilidade particular— ou ben pode colaborar con outras clases.

Dicimos que un obxecto **colabora** con outro se para executar unha responsabilidade necesita enviarlle algunha mensaxe ao outro obxecto. Unha colaboración simple flúe nunha dirección, representando unha solicitude do cliente ao servidor. Desde o punto de vista do cliente, cada unha das súas colaboracións está asociada cunha responsabilidade particular implementada polo servidor.

Cada tarxeta do modelo CRC contén unha clase cunha lista de responsabilidades. O seguinte paso é definir aquelas clases colaboradoras que axudan na realización de cada responsabilidade. Isto establece as **conexións ou relacións** entre clases. As **relacións** deben derivarse a partir do exame dos verbos na descrición do problema. Unha vez conectadas as clases cos seus colaboradores, etiquetamos cada unha destas conexións, engadímoslles unha dirección, en función de qué clase chama a qué outra e para rematar avalíase cada extremo da conexión para determinar a cardinalidade. Este modelo de clases conectadas dá lugar ao **modelo Obxecto-Relación**.

O modelo CRC e o modelo Obxecto-Relación representan elementos estáticos. Para ter un modelo dinámico, debemos introducir o comportamento do sistema como unha función de sucesos específicos e tempo. Identifícanse os sucesos que dirixen as secuencias de interacción entre obxectos, créase unha traza de sucesos para cada caso de uso e constrúese un diagrama de transición de estados para o sistema. Unha vez terminada esta tarefa teríamos o modelo **Obxecto-Comportamento**.

## **36.2 Linguaxe Unificada de Modelado (UML)**

### 36.2.1 Introducción

UML (*Unified Modeling Language*) é unha linguaxe que permite modelar, construír e documentar os elementos que forman un sistema software orientado a obxectos. Converteuse no estándar *de facto* da industria, debido a que foi impulsado polos autores dos tres métodos máis usados de orientación a obxectos: Grady Booch, Ivar Jacobson e Jim Rumbaugh. É o estándar actual do chamado *Object Management Group* (OMG). Un dos obxectivos principais da creación de UML era posibilitar o intercambio de modelos entre as distintas ferramentas CASE orientadas a obxectos do mercado. Para iso era necesario definir unha notación e semántica común.

Hai que ter en conta que o estándar UML non define un proceso de desenvolvemento específico; trátase tan só dunha notación. UML serve para *especificar*, modelos concretos, non ambiguos e completos. Un modelo de UML representa un sistema software desde unha perspectiva específica. Cada modelo permítenos fixarnos nun aspecto distinto do sistema. Debido á súa estandarización e á súa definición completa non ambigua —e aínda que non sexa unha linguaxe de programación— UML pódese conectar de xeito directo a linguaxes de programación como Java, C++ ou Visual Basic; esta correspondencia permite o que se denomina como enxeñería directa (obter o código fonte partindo dos modelos) pero ademais é posible reconstruír un modelo en UML partindo da implementación, ou sexa, a enxeñería inversa.

UML exprésase a través de **elementos de construción**, de **relacións** e de **diagramas** que conteñen elementos e relacións

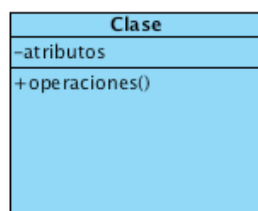
### 36.2.2 Elementos de construción

Chamámoslles “elementos” aos bloques básicos de construción. Son de catro tipos:

#### 36.2.2.1 Elementos estruturais

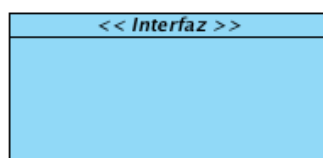
Na súa maioría son as partes estáticas do modelo. Son sete:

- **Clase:** Descrición dun conxunto de obxectos que comparten os mesmos atributos, operacións, relacións e semántica. Unha clase represéntase mediante unha caixa subdividida en tres partes: Na superior móstrase o nome da clase, na media os atributos e na inferior as operacións. Unha clase pódese representar de forma esquemática, cos detalles como atributos e operacións suprimidos, sendo daquela tan só un rectángulo co nome da clase.



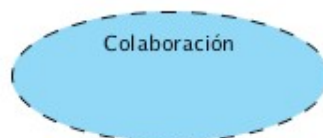
TEXTO CADRO: operacións

- **Interface:** colección de operacións que especifican un servizo dunha clase ou compoñente, mostrando o comportamento visible externamente dese elemento. Unha interface contén só as especificacións das operacións, é dicir a súa sinatura, pero non a implementación.



- **Colaboración:** define unha interacción e representa un conxunto de elementos do modelo que colaboran para proporcionar un comportamento cooperativo maior que a suma dos comportamentos dos seus elementos. Polo tanto, as colaboracións teñen tanto dimensión estrutural como de comportamento.





- **Caso de uso:** descrición dun conxunto de secuencias de accións que un sistema executa e que produce un resultado observable de interese para un usuario particular. Un caso de uso utilízase para estruturar os aspectos de comportamento nun modelo. Un caso de uso é realizado por unha colaboración.



- **Clase activa:** Clase cuxos obxectos teñen un ou máis procesos ou fíos de execución e, polo tanto, poden dar orixe a actividades de control.
- **Compoñente:** Parte física e substituíble dun sistema que representa tipicamente o empaquetamento físico de diferentes elementos lóxicos, como clases, interfaces e colaboracións.



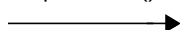
- **Nodo:** Elemento físico que existe en tempo de execución e representa un recurso computacional que normalmente dispón de memoria e capacidade de procesamento (Impresoras, PC...).

#### 36.2.2.2 Elementos de comportamento

Os elementos de comportamento son as partes dinámicas dos modelos. Representan comportamento no tempo e no espazo. Hai dous tipos de elementos de comportamento:

- **Interaccións:** unha interacción é un comportamento que comprende un conxunto de mensaxes intercambiadas entre un conxunto de obxectos dentro dun contexto particular para alcanzar un propósito

operación()



específico. O comportamento dunha sociedade de obxectos ou unha operación individual pódese especificar mediante unha interacción. Unha interacción comprende outros elementos, incluíndo mensaxes, secuencias de acción (o comportamento invocado por unha mensaxe) e enlaces (conexións entre obxectos).

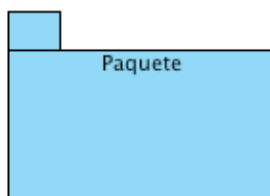
- **Máquinas de estados:** unha máquina de estados especifica as secuencias de estados polas que pasa un obxecto ou unha interacción durante a súa vida en resposta a eventos. O comportamento dunha clase individual ou unha colaboración de clases pódese especificar cunha máquina de estados. Unha máquina de estados comprende outros elementos, incluíndo estados, transicións (o fluxo dun estado a outro), eventos (que disparan unha transición) e actividades (a resposta a unha transición).

estado



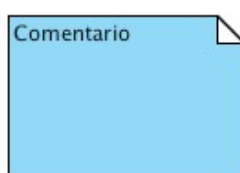
### 36.2.2.3 Elementos de agrupación

Os elementos de agrupación son as partes organizativas dos modelos de UML. Só hai un elemento de agrupación: o **paquete**, que é un mecanismo para organizar os elementos en grupos. Pode conter elementos estruturais, elementos de comportamento e mesmo outros paquetes.



### 36.2.2.4 Elementos de anotación

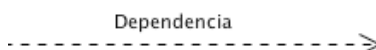
Os elementos de anotación son a parte explicativa dos modelos de UML. Son comentarios que se poden aplicar para describir, clarificar e facer observacións sobre calquera elemento dun modelo. O principal elemento de anotación é a nota, que é simplemente un símbolo para mostrar restricións e comentarios xunto a un elemento ou unha colección de elementos.



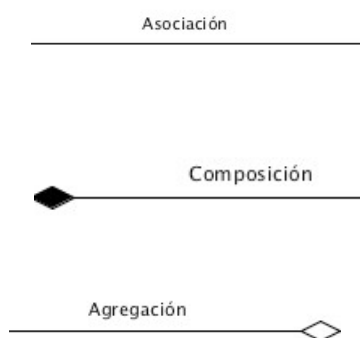
## 36.2.3 Relacións

Hai catro tipos de relacións en UML:

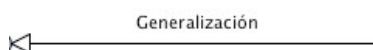
- **Dependencia:** é unha relación semántica entre dous elementos, na cal un cambio a un elemento (o elemento independente) pode afectar á semántica do outro elemento (o elemento dependente).



- **Asociación:** Unha **asociación** é unha relación estrutural que describe un conxunto de enlaces, que son conexións entre obxectos. A **agregación** é un tipo especial de asociación, que representa unha relación estrutural entre un todo e as súas partes. Graficamente, unha asociación represéntase como unha liña continua, posiblemente dirixida, que ás veces inclúe unha etiqueta e a miúdo inclúe outros adornos, como a multiplicidade e os nomes de rol. A agregación represéntase mediante un rombo situado na parte do todo. A **composición** é un tipo de agregación no que cada parte só pode pertencer a un todo e non pode existir a parte sen o todo. Represéntase igual que a agregación, só que o rombo está recheo.

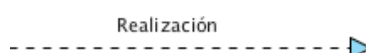


- **Xeneralización:** Unha xeneralización é unha relación de especialización /xeneralización na cal os obxectos do elemento especializado (o fillo) poden substituír os obxectos do elemento xeral (o pai). Desta forma, o fillo comparte a estrutura e o comportamento do pai.



LENDIA: Xeneralización

- **Realización:** Unha realización é unha relación semántica entre clasificadores, onde un clasificador especifica un contrato que outro clasificador garante que cumprirá. Pódense atopar relacións de realización en dous sitios: entre interfaces e as clases e compoñentes que as realizan, e entre os casos de uso e as colaboracións que os realizan.



### 36.2.4 Diagramas

Un diagrama é a representación gráfica dun conxunto de elementos, en xeral visualizado como un grafo conexo de nodos (elementos) e arcos (relacións). Os diagramas débúxanse para visualizar un sistema desde diferentes perspectivas. Pódense agrupar en dous bloques en función de se vemos o modelo de forma estática (estrutural) ou de forma dinámica (comportamento). A primeira inclúe os diagramas de despregamento, compoñentes, clases e obxectos, namentres que a segunda inclúe os diagramas de estados, actividades, secuencia, colaboración e casos de uso. Pasamos a ver cada un deles.

#### 36.2.4.1 Diagrama de casos de uso.

Un Diagrama de Casos de Uso mostra a relación entre os actores e os casos de uso do sistema e representa a funcionalidade que ofrece o sistema no que se refire á súa interacción externa. Un caso de uso é unha secuencia de accións realizadas polo sistema que producen un resultado observable e valioso para un usuario en particular, é dicir, representa o comportamento do sistema co fin de lles dar respostas aos usuarios e serve para describir ante os usuarios o devandito sistema.

A especificación dun caso de uso recolle, nun primeiro momento, unha descrición xeral. Esta descrición reflectirá posiblemente un ou varios

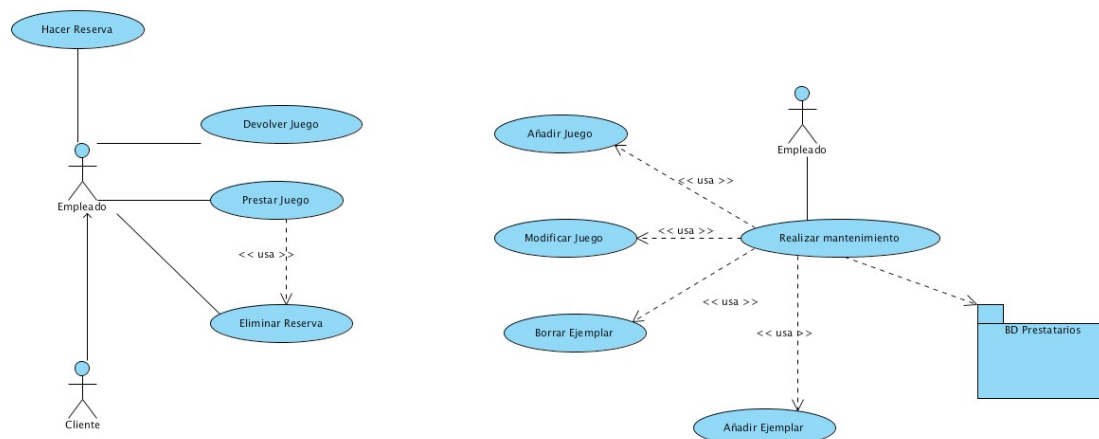
requisitos funcionais do sistema ou formará parte dalgún requisito. Pódese completar a descrición definindo cales son as precondicións e poscondicións. Tamén se poden enumerar os diferentes escenarios do caso de uso se os tivese e dar unha breve descrición deles. Os escenarios son os distintos camiños polos que pode evolucionar un caso de uso, dependendo das condicións que se van dando na súa realización.

Están formados por dous elementos: **actores**, que é algo ou alguén que se atopa fóra do sistema e que interactúa con el e pode referirse tanto a actores que sexan persoas como a outro tipo de actores (outros sistemas, sensores, etc), e **casos de uso**, que representan o comportamento que ofrece o sistema de información desde o punto de vista do usuario; ademais represéntanse as relacións entre os casos de uso. Opcionalmente tamén podería incluír paquetes que agruparían outras partes do sistema.

Entre os elementos dun diagrama de casos de uso pódense dar tres tipos de relacións:

- **Comunica:** É a relación entre un actor e un caso de uso, que denota a participación do actor no devandito caso de uso.
- **Usa:** Relación de dependencia entre dous casos de uso que denota a inclusión do comportamento dun escenario noutro. Úsase cando se quere reflectir un comportamento común en varios casos de uso.

**Estende:** Relación de dependencia entre dous casos de uso no que un é unha especialización do outro, existindo neste caso unha extensión da funcionalidade. Represéntanse como unha liña que une os dous casos de uso relacionados cunha frecha en forma de triángulo e cunha etiqueta <<estende>>, <<usa>> ou <<comunica>>, segundo sexa o tipo de relación.



Lenda: devolución do exemplar / prestar exemplar / engadir título / borrar ou actualizar título / mantemento / facer reserva

#### 36.2.4.2 Diagrama de clases

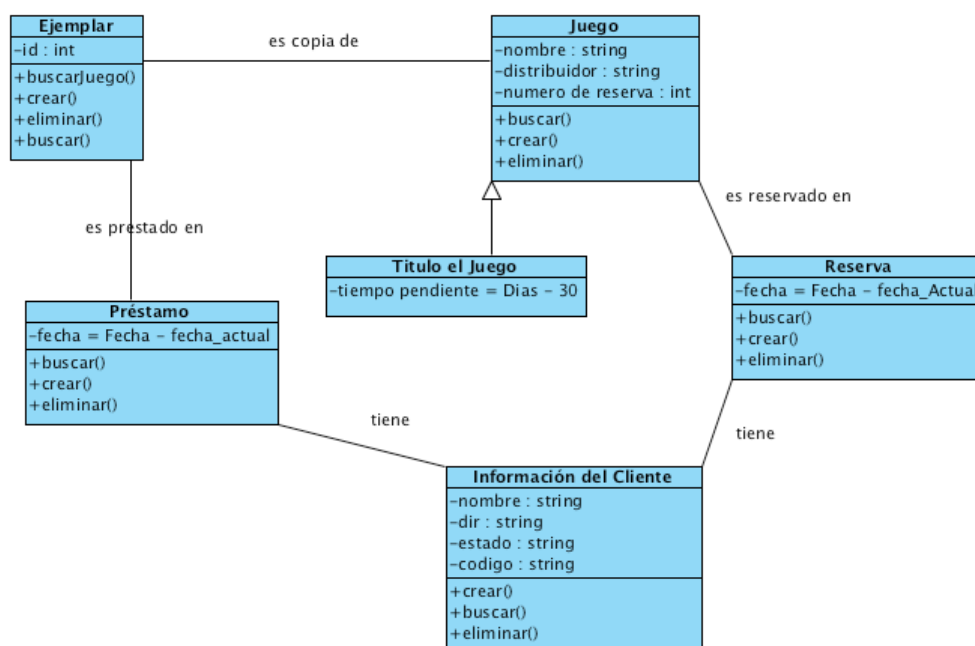
O obxectivo principal deste modelo é a representación dos aspectos estáticos do sistema utilizando diversos mecanismos de abstracción (clasificación, xeneralización, agregación). Recolle as clases de obxectos e as súas asociacións. Neste diagrama represéntase a estrutura e o comportamento de cada un dos obxectos do sistema e as súas relacións cos demais obxectos, pero non mostra información temporal. Sérvenos para visualizar as relacións entre as clases que involucran o sistema, as cales poden ser asociativas, de herdanza e de uso.

O modelo está formado por:

- **Clases:** Represéntase como unha caixa dividida en tres zonas. Na zona superior ponse o nome da clase. No centro colócanse os atributos (características) da clase co formato: *“visibilidade nome : tipo = valor-inicial { propiedades }”*. A visibilidade será en xeral

publica (+), privada (-) ou protexida. Na zona inferior inclúese unha lista coas operacións que proporciona a clase. Cada operación aparece nunha liña con formato: “*visibilidade nome (lista-de-parámetros): tipo-devolto { propiedade }*”

- **Relacións:** Asociacións, agregacións, composicións, dependencias ou herdanza. Pódense documentar cunha descrición do seu propósito, a súa multiplicidade, navegabilidade ou rol de cada unha das clases na relación.
- **Interfaces**
- **Paquetes**



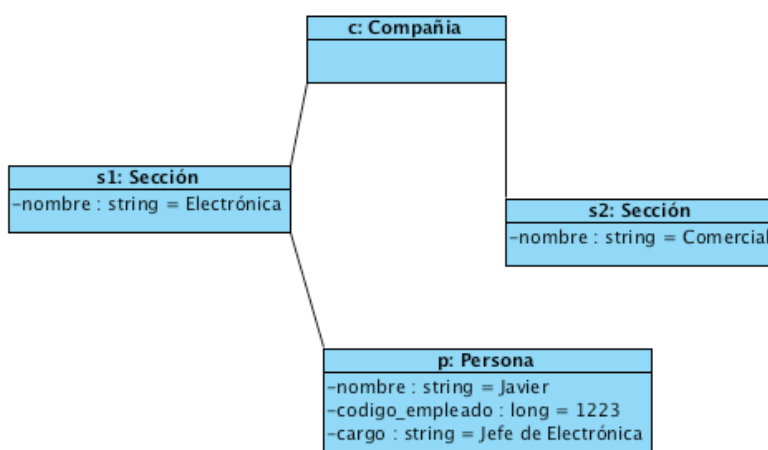
LEENDA: **Ejemplar**. buscarxogo/ é copia de / **Xogo**. nome: distribuidor / é prestado en / é reservado en / Título o Xogo / tempo pendiente = Días / data = Data - data\_Actual / ten / ten / Información do cliente / nome

### 36.2.4.3 Diagrama de obxectos

Modelan as instancias de elementos contidos nos diagramas de clases. Mostra un conxunto de obxectos e as súas relacións nun momento



concreto. Para mostrar o estado dun obxecto, indícase o valor dos seus atributos e os seus obxectos agregados. Os diagramas de obxectos non mostran multiplicidade nin roles, aínda que a súa notación é semellante á dos diagramas de clase.



Lenda: Compañía / nome / código empregado / Xefe de Electrónica

#### 36.2.4.4 Diagramas de Interacción

Os **diagramas de interacción** utilízanse para modelar os aspectos dinámicos do sistema e mostrar un patrón de interacción entre obxectos. Namentres que un diagrama de casos de uso presenta unha visión externa do sistema, a funcionalidade dos devanditos casos de uso recóllese como un fluxo de eventos. Por outra banda, os diagramas de clases e os de obxecto representan información estática, pero nun sistema funcional os obxectos interactúan entre si e os tales eventos ou interaccións suceden no tempo. Este fluxo de eventos pódese recoller nunha especificación texto acompañada de distintos escenarios especificados mediante diagramas de interacción onde cada diagrama será unha visión gráfica dun escenario. Existen dous tipos de diagramas de interacción: **secuencia** e **colaboración**. Ambos son equivalentes. A diferenza entre eles está nos aspectos que salientan. Os diagramas de secuencia destacan a orde

temporal das mensaxes, mentres que os diagramas de colaboración destacan a organización estrutural dos obxectos.

#### *36.2.4.4.1 Diagramas de secuencia*

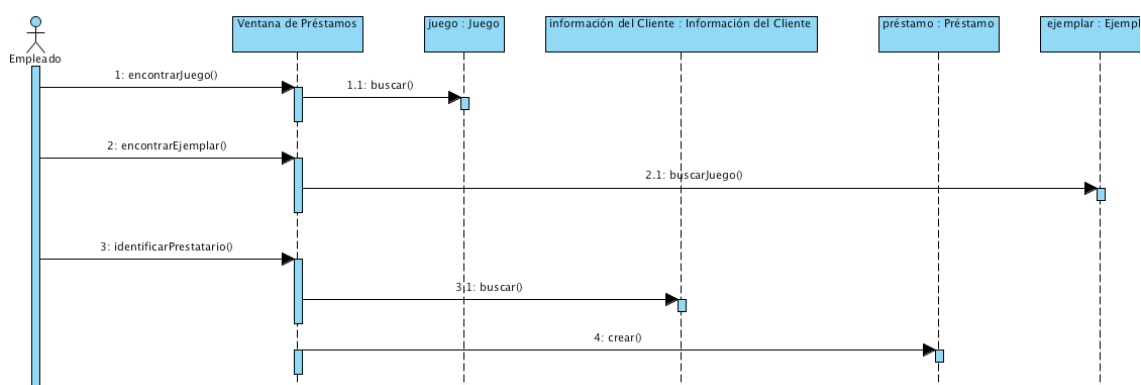
Mostran as interaccións entre obxectos ordenadas en **secuencia temporal**. Mostra os obxectos que se atopan no escenario e a secuencia de mensaxes intercambiadas entre os obxectos para levar a cabo a funcionalidade descrita polo escenario. Faise un diagrama de secuencia por cada caso de uso ou para unha parte deste.

O eixe vertical representa o tempo, e no eixe horizontal colócanse os obxectos e actores participantes na interacción, sen unha orde prefixada. Cada obxecto ou actor ten unha liña vertical e as mensaxes represéntanse mediante frechas entre os distintos obxectos. O tempo flúe de arriba abaixo. Pódense empregar etiquetas para especificar restricións de tempo, descricións de accións, etc; ben na marxe esquerda ou xunto á mensaxe ou activación á que se refira.

Os conceptos máis importantes relacionados cos diagramas de secuencia son:

- **Liña de vida** dun obxecto: representa a vida do obxecto durante a interacción. O obxecto represéntase como unha liña vertical punteada cun rectángulo de encabezado co nome do obxecto e da súa clase.
- **Activación:** Mostra o período de tempo durante o cal o obxecto se atopa desenvolvendo algunha operación. Denótase por un rectángulo sobre a liña de vida do obxecto.
- **Mensaxe:** Móstrase mediante unha liña sólida dirixida desde o obxecto que emite a mensaxe cara ao que a executa.

- **Camiños alternativos** de execución e concorrencia: Poden representar condicións na execución ou diferentes fíos de execución (*threads*).

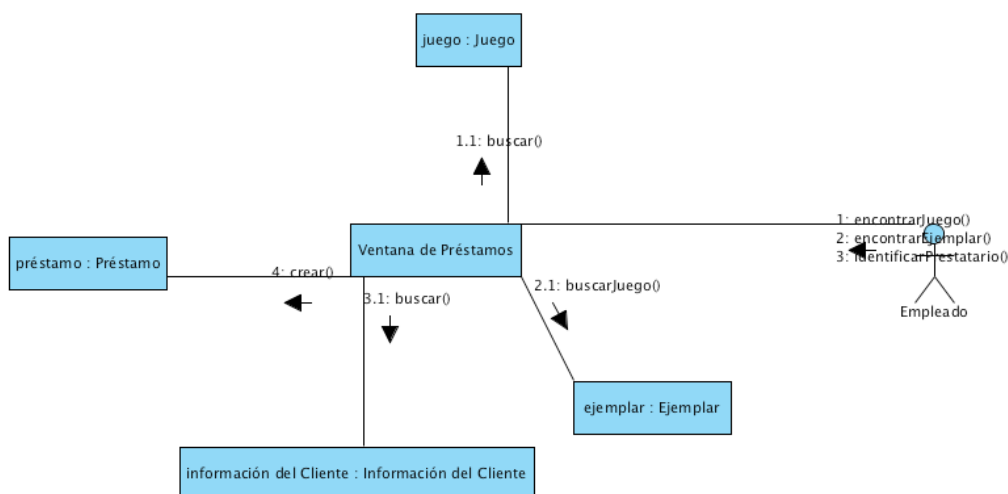


LEND: Ventá de Préstamos / xogo : Xogo / Información do Cliente /  
exemplar / Empregado / encontrarXogo / encontrar/exemplar / buscarXogo

#### 36.2.4.4.2 Diagramas de colaboración

Os diagramas de colaboración supoñen unha forma alternativa ao diagrama de secuencia para mostrar un escenario. Amosan a mesma información que un diagrama de secuencia pero de forma diferente. Nos diagramas de colaboración non existe unha secuencia temporal. Os elementos dun sistema traballan en conxunto para cumpriren cos obxectivos do sistema, e esta colaboración a que se reflicte. Nos diagramas de colaboración non existe unha secuencia temporal. Este diagrama resalta a **organización estrutural** dos obxectos que envían e reciben as mensaxes. Este tipo de diagrama mostra un conxunto de obxectos, enlaces entre eles e as mensaxes que intercambian.

A diferenza dos Diagramas de Secuencia, os Diagramas de Colaboración mostran as relacións entre os roles dos obxectos. A secuencia das mensaxes debe determinarse explicitamente mediante números de secuencia.



LEENDA: IGUAL ANTERIOR

#### 36.2.4.5 Diagramas de estados

Representan os estados que pode tomar un compoñente ou un sistema e mostran os eventos que implican o cambio dun estado a outro. Os diagramas de estado son útiles, entre outras cousas, para indicar os eventos do sistema nos casos de uso e para ilustrar qué eventos poden cambiar o estado dos obxectos dunha clase. Os dous elementos principais nestes diagramas son os estados e as posibles transicións entre eles.

- O estado dun compoñente ou sistema representa algún comportamento que é observable externamente e que perdura durante un período de tempo finito. Podémolo ver tamén como un período no que se satisfai unha condición. Vén dado polo valor dun ou varios atributos que o caracterizan nun momento dado.
- Unha **transición** é un cambio de estado producido por un evento e reflicte os posibles camiños para chegar a un estado final desde un estado inicial. Reflicte que un obxecto no primeiro estado pode entrar no segundo e executar certas operacións cando un evento ocorre e se certas condicións son satisfeitas.

Unha transición represéntase graficamente como unha liña continua dirixida desde a estado-orixe ata o estado-destino. Pode vir acompañada por un texto co seguinte formato:

nome-evento    '('lista-argumentos')'    '['guard-condition']    '/'  
expresión-acción '^' cláusula-envío.

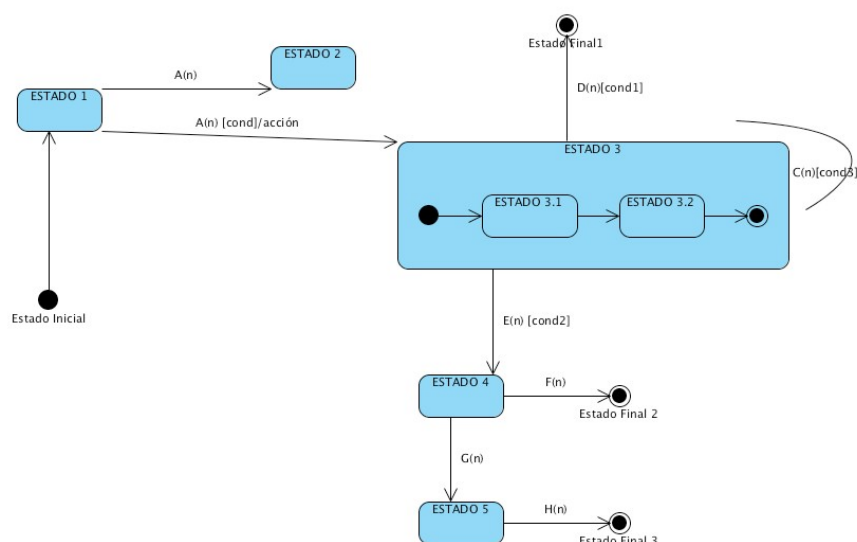
- *nome-evento* e *lista-argumentos* describen o evento que dá lugar á transición e forman o que se denomina *event-signature*.
- *guard-condition* é unha condición (expresión booleana) adicional ao evento e necesaria para que a transición se produza. Se a *guard-condition* se combina cunha *event-signature*, entón para que a transición se dispare teñen que suceder dúas cousas: debe ocorrer o evento e a condición booleana debe ser verdadeira.
- *expresión-acción* é unha expresión procedemental que se executa cando se dispara a transición. É posible ter unha ou varias expresión-acción nunha transición de estado, as cales se delimitan co carácter `"/"`.
- *cláusula-envío* é unha acción adicional que se executa co cambio de estado; por exemplo, o envío de eventos a outros paquetes ou clases. Este tipo especial de acción ten unha sintaxe explícita para enviar unha mensaxe durante a transición entre dous estados. A sintaxe consiste nunha expresión de destino e nun nome de evento, separados por un punto.

Desde un estado poden xurdir varias transicións en función do evento que desencadea o cambio de estado, tendo en conta que as transicións que proveñen do mesmo estado non poden ter o mesmo evento, agás que exista algunha condición que se lle aplique ao evento. Un diagrama de estados pode representar ciclos continuos ou ben unha vida finita, na que

hai un estado inicial de creación e un estado final de destrución (do caso de uso ou do obxecto).

Un sistema só pode ter un **estado inicial**, que se representa mediante unha transición sen etiquetar ao primeiro estado normal do diagrama. En ningún caso pode haber unha transición dirixida ao estado inicial. O estado **final** representa que un compoñente deixou de ter calquera interacción ou actividade. Non se permiten transicións que partan do estado final. Pode haber varios estados finais nun diagrama.

Outros dous elementos que axudan a clarificar estes diagramas son as accións e as actividades. Unha acción é unha operación instantánea asociada a un evento, cunha duración que se considera non significativa e que se pode executar: dentro dun estado, ao entrar nun estado, ou ao saír del. Unha actividade é unha operación asociada a un estado que se executa durante un intervalo de tempo ata que se produce o cambio a outro estado.



#### 36.2.4.6 Diagrama de actividades

As actividades que ocorren dentro dun caso de uso ou dentro do comportamento dun obxecto danse, normalmente, en secuencia. Este tipo de diagrama pódese considerar un caso especial do diagrama de estados, no cal case todos os estados son estados-acción (identifican unha acción que se executa ao entrar nel) e case todas as transicións evolucionan ao termo da devandita acción. A interpretación dun diagrama de actividades depende da perspectiva considerada: nun diagrama conceptual, a actividade é algunha tarefa que debe ser realizada; nun diagrama de especificación ou de implementación, a actividade é un método dunha clase. Adóitanse utilizar para modelar os pasos dun algoritmo.

Os diagramas de actividade poden visualizar, especificar e documentar a dinámica dun conxunto de obxectos. Tamén se poden usar para modelar o fluxo de control dunha operación. Namentres que os diagramas de interacción enfatizan o fluxo de control dun obxecto a outro, os diagramas de actividade subliñan o fluxo de control dunha actividade a outra.

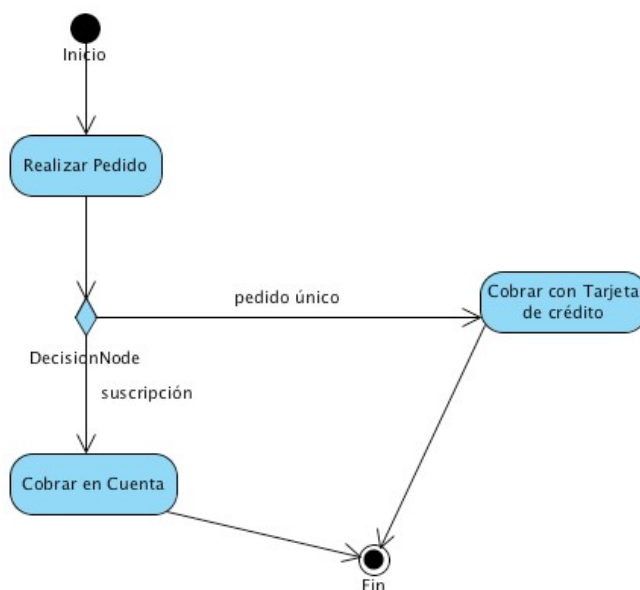
O principal inconveniente dos diagramas de actividade é que non indican explicitamente qué obxectos executan qué actividades nin tampouco a forma en que o servizo de mensaxería traballa entre eles. Para mostrar as tales interaccións de maneira clara son necesarios os diagramas de interacción, que son máis utilizados na práctica.

Nos diagramas de actividade, as decisións represéntanse mediante unha transición múltiple que sae dun estado onde cada camiño ten unha etiqueta distinta. Preséntase mediante un rombo ao cal chega a transición do estado-orixe e do cal saen as múltiples transicións dos estados-destino. Os diagramas de actividade son útiles cando queremos describir un comportamento paralelo, ou cando queremos mostrar qué comportamentos interactúan en varios casos de uso.

Un diagrama de actividades contén:

- *Estados de actividade e Estados de acción:* A representación de ambos é un rectángulo coas puntas redondeadas; no seu interior represéntase ben unha actividade ou ben unha acción.
  - Un estado que represente unha acción é atómico, o que implica que a execución pode considerarse instantánea e non se pode interromper.
    1. Un estado-actividade pode descompoñerse en máis sub-actividades representadas a través doutros diagramas de actividades. Ademais, estes estados poden interromperse e tardan certo tempo en completarse.
    2. Nos estados de actividade podemos atopar outros elementos adicionais, como son: accións de entrada e de saída do estado en cuestión.
- *Transicións:* Reflicten o paso dun estado a outro, ben sexa de actividade ou de acción. Esta transición prodúcese como resultado da finalización do estado do que parte o arco dirixido que marca a transición.





Lenda: suscripción / cobrar en conta / cargar con tarxeta de crédito

#### 36.2.4.7 Diagramas de implementación

Un diagrama de implementación mostra as dependencias entre as partes de código do sistema (**diagrama de compoñentes**) ou a estrutura do sistema en execución (**diagrama de despregamento**). Os diagramas de compoñentes utilízanse para modelar a vista de implementación estática dun sistema, en canto que os diagramas de despregamento se utilizan para modelar a vista de despregamento estática.

##### 36.2.4.7.1 Diagrama de compoñentes

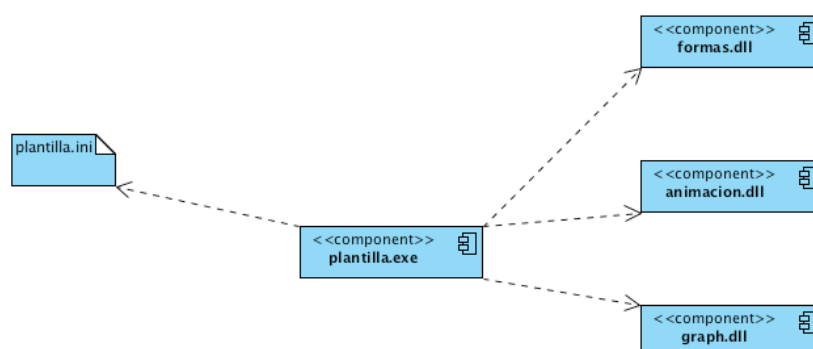
Mostra as organizacións e dependencias lóxicas entre compoñentes software, sexan estes compoñentes de código fonte, binarios, documentos, arquivos ou executables. Os diagramas de compoñentes representan calquera tipo de elemento software que participe no desenvolvemento dun sistema informático e poden ser simples arquivos, librerías, etc. Os

diagramas de compoñentes poden conter paquetes para organizar os elementos.

Dado que os diagramas de compoñentes mostran os compoñentes software que constitúen unha parte reusable, as súas interfaces e as súas interrelacións, en moitos aspectos pódense considerar como un diagrama de clases a grande escala. Cada compoñente do diagrama debe ser documentado cun diagrama de compoñentes máis detallado, un diagrama de clases, ou un diagrama de casos de uso.

Tipos de compoñentes:

- *Compoñentes de despregamento*: compoñentes necesarios e suficientes para formar un sistema executable, como poden ser as bibliotecas dinámicas e executables.
- *Compoñentes produto do traballo*: estes compoñentes son basicamente produtos que quedan ao final do proceso de desenvolvemento. Consisten en cousas como arquivos de código fonte e de datos a partir dos cales se crean os compoñentes de despregamento.
- *Compoñentes de execución*: son compoñentes que se crean como consecuencia dun sistema en execución.



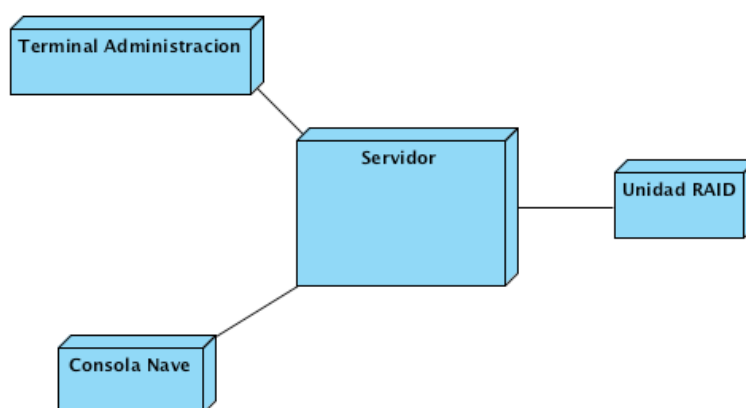
LEND: patrón / animación

#### 36.2.4.8 Diagrama de despregamento

Mostra as relacións físicas (arquitectura física) entre os compoñentes hardware e software no sistema final, é dicir, a configuración dos elementos de procesamento en tempo de execución e os compoñentes software (proceso e obxectos que se executan neles). Mostran a configuración en funcionamento do sistema, incluíndo hardware e software. Cobre principalmente a distribución, entrega e instalación das partes que configuran o sistema físico e adóitanse utilizar para modelar sistemas encaixados, sistemas cliente-servidor e sistemas distribuídos.

Nun diagrama de despregamento un nodo representa un elemento físico que existe en tempo de execución e que representa un recurso computacional. Os nodos conéctanse mediante asociacións de comunicación, tales como enlaces de rede, conexións TCP/IP, etc.

Os diagramas de despregamento son os complementos dos diagramas de compoñentes que, unidos, proporcionan a vista de implementación do sistema.



LEND: Unidade.

## **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](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 da Escola Superior de Enxeñería Informática.**

**Universidade de Vigo**



**37. TÉCNICAS DE  
PROGRAMACIÓN.  
PROGRAMACIÓN  
ESTRUTURADA.  
PROGRAMACIÓN ORIENTADA A  
OBJECTOS. ENXEÑARÍA  
INVERSA E REENXEÑARÍA.**

## **Tema 37. Técnicas de programación. Programación Estructurada. Programación orientada a obxectos. Enxeñería inversa e reenxeñería.**

### **ÍNDICE**

- 37.1 Técnicas de programación
  - 37.1.1 Clasificación e evolución das linguaxes de programación
- 37.2 Programación Estructurada
  - 37.2.1 Recursos abstractos
  - 37.2.2 Deseño descendente
  - 37.2.3 Estructuras básicas
- 37.3 Programación orientada a obxectos
- 37.4 Enxeñería inversa
  - 37.4.1 Modelo cíclico
  - 37.4.2 Modelo de ferradura
  - 37.4.3 Modelo do IEEE
  - 37.4.4 Método Análise de Opcións para Reenxeñería (OAR)

### **37.1 Técnicas de programación**

Unha **linguaxe de programación** é unha linguaxe artificial deseñada para representar expresións e instrucións de forma que as entenda un ordenador. Aínda que as linguaxes de programación son máis sinxelas que as linguaxes naturais, posúen tamén un alfabeto (símbolos básicos) cos que se constrúe o vocabulario (*tokens*, palabras reservadas), que se combinan segundo unhas regras sintácticas formando expresións e sentenzas, cuxo significado vén dado pola semántica da linguaxe. Chámasele **programa** ao conxunto de instrucións escritas nunha linguaxe de programación destinadas a realizar unha tarefa. De forma xeral, un programa tomará uns datos de entrada e devolverá uns datos de saída. Dise que o que fai o programa é producir un **algoritmo**, que é un conxunto finito de instrucións que se deben seguir para realizar unha determinada tarefa.

Entendemos a **programación** como *a planificación, proxección, desenvolvemento e implementación da resolución dun problema*, a que abarca obviamente a creación do algoritmo. Un profesional da

programación debe encarar a solución do problema de forma tal que o seu produto sexa útil agora e no futuro, estando ou non el no centro de desenvolvemento. Para logralo, débese ter moi presentes as posibles modificacións futuras do tal produto.

As características que debe ter un programa son:

- 1) **Claridade algorítmica:** Que sexa claro significa que a súa resolución algorítmica sexa sinxela, que estea correctamente estruturado e que resulte de fácil comprensión.
- 2) **Lexibilidade:** Que sexa lexible significa que cando se codificou se escolleron ben os nomes dos obxectos utilizados, que se agregaron comentarios para indicar o que se ía facendo e que se estruturou ben o código para resaltar o contido semántico sobre o sintáctico.
- 1) **Modificabilidade:** Que sexa facilmente modificable implica que calquera modificación do problema que xere unha agregación, supresión ou cambio dalgunha das súas partes, non debe obrigar a cambiar todo o programa, senón só esa parte.

Nos seus inicios, a programación non seguía ningunha metodoloxía e tiñamos centos ou milleiros de liñas de código feitas por un programador, que só el modificaba. Naquela época os profesionais programadores adoitaban estar vinculados á empresa e non era frecuente que a abandonasen. Os programas non tiñan estrutura definida. As modificacións no programa supoñían un custo importante, xa que cumpría revisar o código case liña a liña para buscar onde facer as modificacións. Ademais, estes cambios non deixaban de ser un risco importante debido aos posibles efectos colaterais. Isto derivou no que se denominou “crise do software”.

Para tratar de dar resposta á crise do software, nos anos 60 xurdiron técnicas de programación como a **programación modular** e a **programación estruturada**. Ambas as técnicas parten da idea do deseño descendente (tamén chamado refinamento sucesivo), que consiste en dividir un problema complexo en varios problemas máis pequenos e máis

sinxelos de resolver. Empézase expoñendo o problema e a súa solución a un nivel alto, e logo séguese descompoñendo o problema xeral noutros problemas máis doados de resolver. Este proceso continúa ata que chegamos a pequenos problemas, facilmente implementables en códigos chamados módulos. Un módulo é un conxunto de accións (un bloque do código do algoritmo total) xunto a un conxunto de especificacións de datos para realizar unha tarefa específica. Cando se utiliza esta técnica, a solución queda dividida en varias partes: un algoritmo principal e un ou varios subalgoritmos (os módulos). A execución iníciase no algoritmo principal e desde este invócase aos módulos. A programación estruturada fai uso da programación modular, ademais doutras características que se verán nun apartado posterior.

Tamén como resposta á crise do software xurdiron nos anos 60 os conceptos da orientación a obxectos, que tiñan como principal obxectivo reducir a complexidade do desenvolvemento e mantemento do software. Dado que a tecnoloxía non estaba acorde coa súa concreción, mantívose só como concepto ata a súa grande expansión a finais dos 80. A **programación orientada a obxectos** non supón unha ruptura radical fronte ao paradigma da programación estruturada / imperativa predominante ata a súa aparición, senón que supón unha evolución. Fronte á programación estruturada, cuns programas que separan datos e estruturas de datos de funcións e procedementos, a programación orientada a obxectos encapsula nunha mesma abstracción estes dous elementos clásicos dos sistemas de información: datos e procesos. Isto faino a través dunha nova abstracción: o obxecto. A orientación a obxectos consiste nunha visión dos obxectos como entidades activas que executan accións sobre os seus propios datos en resposta a peticións externas. Ademais, non considera uns e outros (datos e procesos) como realidades illadas susceptibles de analizarse e implantarse por separado. Os obxectos tratan de abstraer características comúns que se poderán compartir entre varias aplicacións e reutilizarse todo o posible. A creación dun novo sistema



consiste esencialmente nun labor de ensamblado de obxectos preexistentes, completado co desenvolvemento dunha porcentaxe reducida de novos obxectos que, pola súa vez, alimentarán as correspondentes librerías para poder ser utilizados nos próximos sistemas.

O paradigma de ensamblar compoñentes e escribir código para facer que estes compoñentes funcionen coñécese como **Desenvolvemento de Software Baseado en Compoñentes**. Un compoñente é unha peza de código preelaborado que encapsula algunha funcionalidade exposta a través de interfaces estándar. Cada compoñente é deseñado para se axustar perfectamente cos seus pares, as conexións son estándar e o protocolo de comunicación está xa preestablecido. Ao se uniren as partes, obtemos un sistema completo.

Para rematar, a **programación orientada a aspectos** xorde para resolver o problema da "dispersión de código" existente na programación orientada a obxectos para aqueles aspectos dun programa que non teñen que ver directamente co dominio de negocio do problema, como por exemplo, a xestión de conexións, logs, trazas de mensaxes, sincronización e concorrencia, manexo de erros e excepcións, etc. Este código está disperso ao longo de diferentes obxectos do programa (sendo, gran parte das veces, o mesmo código repetido), o que dificulta o seu mantemento. Esta é unha nova metodoloxía de programación que tenta separar os compoñentes e os aspectos os uns dos outros, proporcionando mecanismos que fagan posible abstraelos e compoñelos para formar todo o sistema. É un desenvolvemento que segue o paradigma da orientación a obxectos e, coma tal, soporta a descomposición orientada a obxectos, ademais da procedemental e da descomposición funcional. Pero, malia isto, non se pode considerar como unha extensión da programación orientada a obxectos (POO), posto que se pode utilizarse cos diferentes estilos de programación xa mencionados.

### 37.1.1 Clasificación e evolución das linguaxes de programación

Para explicar a evolución das linguaxes de programación falamos de xeracións:

- **Primeira xeración.** Linguaxe máquina. Empeza nos anos 1940-1950. Os programas están feitos de secuencias de uns e ceros que a computadora é capaz de interpretar. É o único que é directamente entendible polo ordenador, sen necesidade de tradución. Estes considéranse como de baixo nivel, porque non existe un programa de codificación menos complicado que o que utiliza os símbolos binarios 1 e 0.
- **Segunda xeración.** Ensamblador. Finais dos anos 50. Úsanse mnemotécnicos que substitúen os uns e ceros. Seguen a ser dependentes da máquina. O código fonte é traducido á linguaxe máquina mediante tradutores. Aínda se utilizan estas linguaxes cando interesa un nivel máximo de eficiencia na execución ou cando se requiren manipulacións intrincadas. Do mesmo xeito que as linguaxes máquina, as linguaxes ensambladoras son únicas para unha computadora particular. Esta dependencia da computadora fainas ser linguaxes de baixo nivel.
- **Terceira xeración.** Linguaxes de alto nivel. Anos 60. Linguaxes estruturadas con comandos similares á linguaxe natural. Foron creadas para facilitar o proceso de programación. Os comandos aseméllanse a palabras de uso común. As linguaxes desta xeración divídense en tres categorías, segundo se orienten a:
  - *procedementos*: Requiren que a codificación das instrucións se faga na secuencia en que se deben executar para solucionar o problema. Pola súa banda, clasifícanse en:
    - científicos (FORTRAN), empresariais (COBOL), e de uso xeral (BASIC).
    - Todas estas linguaxes permiten sinalar como se debe efectuar unha tarefa a un nivel maior que nas linguaxes ensambladoras.

Fan énfase nos procedementos ou as matemáticas implícitas, é dicir no que se fai (a acción).

- *problemas*: Están deseñados para resolver un conxunto particular de problemas e non requiren o detalle da programación que as linguaxes orientadas a procedementos. Fan fincapé na entrada e a saída desexadas.
- *obxectos*: A énfase faise no obxecto da acción. Os beneficios que proporcionan estas linguaxes inclúen unha maior produtividade do programador e claridade da lóxica, ademais de ofrecerem a flexibilidade necesaria para manexar problemas abstractos de programación.
- **Cuarta xeración**: Nacen as linguaxes 4G. Son linguaxes de propósito específico, orientadas a resolver problemas específicos, como xeración de informes, pantallas, consultas de bases de datos... Caracterízanse por ter unha maior facilidade de programación comparadas coas de terceira xeración, permitindo a creación de prototipos rapidamente, posto que xeran o código fonte automaticamente a través de asistentes, patróns, etc. A súa característica distintiva é a énfase en especificar que é o que se debe facer, en vez de como executar unha tarefa. As especificacións dos programas desenvólvense a un nivel máis alto que nas linguaxes da xeración anterior. A característica distintiva é allea aos procedementos, e o programador non ten que especificar cada paso para rematar unha tarefa ou procesamento. As características xerais das linguaxes de cuarta xeración son:
  - Uso de frases e oracións parecidas ao inglés para emitiren instrucións;
  - Non operan por procedementos, polo que lles permiten aos usuarios centrárense no que hai que facer, non en como facelo;

- Ao se faceren cargo de moitos dos detalles de como facer as cousas, incrementan a produtividade.

Hai dous tipos de linguaxes de cuarta xeración, segundo se orienten:

- Á produción: Deseñadas sobre todo para profesionais da computación.
- Ao usuario: Deseñadas sobre todo para os usuarios finais, que poden escribir programas para facer consultas nunha base de datos e para crear sistemas de información.
- **Quinta xeración:** Linguaxes Naturais. Son linguaxes orientadas á intelixencia artificial e aos sistemas expertos. En lugar de só executar ordes, o obxectivo dos sistemas é anticipar as necesidades dos usuarios. Están aínda en desenvolvemento.

As linguaxes de programación pódense clasificar segundo moitos criterios:

- Segundo o **nivel de abstracción**:
  - o **Linguaxes máquina e de baixo nivel**: a linguaxe ou código máquina está formada por cadeas binarias entendibles directamente pola máquina. Non necesitan tradución e son moi rápidas. A linguaxe ensambladora permite polo menos escribir as instrucións utilizando unha notación simbólica, utilizar enderezos de memoria relativos e non absolutos, inserir comentarios. Necesitan dun tradutor para converter a código máquina; tradución que resulta case trivial debido ao seu baixo nivel. Estas linguaxes son completamente dependentes da máquina. En xeral, emprégase este tipo de linguaxe para programar controladores (drivers).
    - Vantaxes:
      - Maior adaptación ao equipo.
      - Posibilidade de obter a máxima velocidade con mínimo uso de memoria.
    - Inconvenientes:



- Imposibilidade de escribir código independente da máquina.
  - Maior dificultade na programación e na comprensión dos programas.
  - o **Linguaxes de medio nivel:** aquí atoparíase a linguaxe C. A linguaxe C permite un manexo abstracto e independente da máquina (o que a achegaría ao alto nivel), pero sen perder a súa característica de potencia, eficiencia e proximidade á máquina (uso directo de punteiros, etc.)

Estas linguaxes son clasificadas moitas veces de alto nivel, pero permiten certos manexos de baixo nivel. Son precisas para certas aplicacións, como a creación de sistemas operativos, xa que permiten un manexo abstracto (independente da máquina, a diferenza da ensambladora), pero sen perder moito do poder e eficiencia que teñen as linguaxes de baixo nivel.
  - o **Linguaxes de alto nivel:** son independentes da arquitectura da máquina e aproxímanse á linguaxe natural; dispoñen de gran diversidade de instrucións potentes e usan unha sintaxe semellante á linguaxe natural, o que facilita a súa comprensión. Aquí estarían basicamente o resto das linguaxes coñecidas; de feito, pódese dicir que o principal problema que presentan as linguaxes de alto nivel é gran cantidade delas que existen actualmente en uso.
- Segundo a **forma de execución:**
    - o **Compiladas:** unha vez escrito o programa, este tradúcese a partir do seu código fonte por medio dun compilador nun arquivo executable para unha determinada plataforma; este arquivo chámase executable. O compilador le o código fonte e almacena o executable resultado da tradución para posibles execucións futuras. Un programa escrito nunha linguaxe

compilada posúe a vantaxe de non necesitar un programa anexo para ser executado unha vez que foi compilado. Ademais, como só é necesaria unha tradución, a execución vólvese máis rápida. Así e todo, non é tan flexible como un programa escrito en linguaxe interpretada, xa que cada modificación do arquivo fonte (o arquivo comprensible para os seres humanos: o arquivo a compilar) require da compilación do programa para aplicar os cambios. Exemplos: C, C++, Pascal, Kilix, Delphi...

- o **Interpretadas:** necesitan dun intérprete para executar o código escrito nos programas. As instrucións tradúcense ou interpretan unha a unha en tempo de execución a unha linguaxe intermedia ou linguaxe máquina. Na execución dunha linguaxe interpretada vanse lendo as liñas do código fonte e traducíndoas a medida que vai sendo necesario. Cada vez que se le unha instrución interprétase e execútase, xerando o seu código máquina “nun airiño”. Exemplos: Java, JavaScript, PHP, linguaxes de.NET...
- Segundo o **paradigma de programación:** Con isto referímonos ao enfoque á hora de afrontar o problema que tratamos de programar.
  - o **Imperativas:** fundaméntanse na utilización de variables para almacenar valores e na realización de instrucións para operar cos datos almacenados. Aparece o concepto de algoritmo, ou CÓMO conseguir o obxectivo. Dentro das linguaxes imperativas, podemos clasificalas en:
    - **Procedurais ou procedementais:** agrupan código en subprogramas que se poden chamar desde distintos puntos do programa. Ex.: C, Pascal, Fortran, Basic, etc.
    - **Orientadas a obxectos:** ven o programa como unha colección de obxectos que interactúan os uns cos outros a través de mensaxes. É a máis utilizada na actualidade.

Ex.: Smalltalk, C++, Java, C#, Visual Basic.NET, Eiffel, etc.

Na actualidade, case todas as novas versións das linguaxes incorporan características de orientación a obxectos. De feito, moitos autores propoñen o paradigma orientado a obxectos como paradigma propio, evolución do paradigma imperativo.

- o **Declarativas:** decláranse ou descríbense as propiedades ou características do problema, deixando que a solución a atope a máquina. Realmente, decláranse condicións, proposicións, feitos, regras, afirmacións, restricións, ecuacións, transformacións, etc. que deben cumprir o conxunto de valores que constitúen a solución. Dentro desta temos tres tipos:
  - **Funcional ou aplicativa:** Todas as construcións son funcións matemáticas. Non hai instrucións e tampouco hai instrución de asignación. O programa defínese por composición de funcións máis simples. Para executalo, chámase a unha función cos datos de entrada e obtense un resultado. Ex.: Haskell, LISP, CAML, etc.
  - **Lóxica:** Baséase na definición de regras lóxicas para logo interrogar o sistema e resolver problemas. A programación lóxica trata con relacións (predicados) entre obxectos (datos), en lugar de facelo con funcións. Ex.: Prolog.
  - **Alxébricas ou Relacionais:** Algúns autores falan deste outro paradigma para clasificar o SQL, que é a linguaxe utilizada para interrogar BBDD relacionais. Especificamos o resultado que queremos e a execución do SQL proporcionanolo.

Cómpre dicir que algunhas linguaxes son **multiparadigma**. Por exemplo, a C++ é unha linguaxe orientada a obxectos, pero tamén a podemos usar como linguaxe imperativa, sen facer uso da

orientación a obxectos; ou o Prolog, que é lóxica, pero tamén conta con estruturas repetitivas propias do paradigma imperativo.

## **37.2 Programación Estruturada**

A programación estruturada é un concepto que xorde como resposta á crise do software dos anos 60, cando o custo no desenvolvemento de programas era cada vez maior e seu o mantemento facíase cada vez menos manexable.

Foi desenvolvida nos seus principios por Edsger W. Dijkstra no seu libro *Notes on Structured Programming* e baséase no denominado “Teorema da Estrutura” ou “de Böhm-Jacopini” en honor de Corrado Böhm e Giuseppe Jacopini.

Edsger Dijkstra definiu a programación estruturada como “aquela que utiliza recursos abstractos, se basea no deseño descendente e respecta un conxunto de estruturas básicas chamadas Estruturas de Control: Estrutura secuencial, estruturas selectivas e estruturas repetitivas”.

### **37.2.1 Recursos abstractos**

Todas as linguaxes de programación posúen un conxunto de recursos que poderíamos denominar recursos concretos: instrucións, palabras reservadas, tipos de datos, funcións, regras, etc. No entanto, estes recursos non son abondos para escribir programas para distintas aplicacións, e xa que logo, o programador deberá valerse de artificios (recursos abstractos) para implementar os seus algoritmos utilizando só os recursos concretos.

Segundo Dijkstra, “escribir un programa en termos de recursos abstractos consiste en descompoñer as accións complexas en accións simples, capaces de ser executadas por unha máquina”. Isto significa que



é posible escribir programas complexos utilizando un conxunto limitado de instrucións moi simples.

### 37.2.2 *Deseño Descendente*

Existen dúas técnicas para escribir os algoritmos: o deseño ascendente e o deseño descendente.

Cando se utiliza deseño ascendente, pártese desde os detalles particulares de implementación da solución cara á solución xeral do problema. A solución do problema lógrase coa integración de todas as solucións particulares formuladas ao principio. Isto significa que primeiro se resolven partes particulares do problema e, por último, o problema en si. Esta técnica presenta dúas dificultades: lograr que as solucións particulares funcionen en conxunto e lograr que varios programadores traballen en coordinación.

O deseño descendente consiste en comprender o problema que hai que solucionar e logo descompoñelo nun conxunto de problemas menores. Cando se usa esta técnica, primeiro expónse a solución de forma xeral para logo pasar aos detalles particulares. Isto realízase en varios pasos chamados refinamentos. Poden existir varios niveis de refinamento ata chegar aos detalles de implementación da solución (subalgoritmos independentes chamados módulos). Unha vantaxe desta técnica é que permite a división de tarefas entre varios programadores, onde cada un poderá escribir un algoritmo que obteña unha parte da solución.

A programación estruturada fai, pois, uso da **programación modular**. Un módulo é un conxunto de accións que realiza unha tarefa específica. Pode realizar as mesmas accións que un programa: aceptar datos, realizar cálculos e devolver resultados. Non obstante, os módulos utilízanse para un fin específico. Cando se utiliza esta técnica, toda a solución (o algoritmo) queda dividida en varias partes: un algoritmo principal e un ou varios subalgoritmos (os módulos). A execución iníciase

no algoritmo principal e desde este invócase aos módulos. Os módulos tamén poden ser invocados desde outros módulos e o control da execución sempre se retorna ao punto desde onde se invocou por última vez.

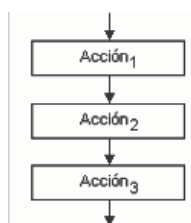
### 37.2.3 Estruturas básicas

Bohm e Jacopini demostraron que é posible resolver problemas escribindo programas denominados **propios**. Un programa defínese como propio se cumpre con:

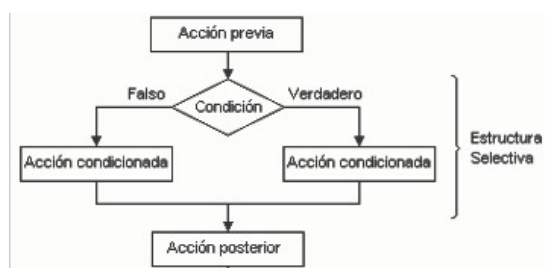
- ten un só punto de entrada e un só de saída (inicio e fin),
- todas as accións do algoritmo son accesibles, é dicir, que para cada acción existe un conxunto de datos que fará que esta sexa accesible desde o inicio e ademais se poderá chegar á fin.
- non posúe lazos ou bucles infinitivos.

Pois ben, o **teorema da estrutura** establece que “calquera programa propio pode ser escrito utilizando soamente as seguintes estruturas lóxicas de control: secuencia, selección e iteración”. Un algoritmo correctamente implementado posuirá un único punto de entrada, un único punto de saída, e permitirá a execución de todas as súas instrucións en función dos parámetros de entrada. A programación estruturada baséase no concepto de programa propio e utiliza soamente estas tres estruturas básicas:

- **Estrutura Secuencial:** Caracterízase porque unha acción se escribe e executa a continuación doutra. Está representada por unha sucesión de operacións que se executan secuencialmente.

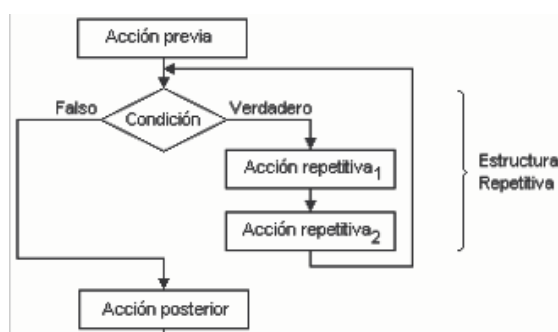


- **Estrutura selectiva:** Caracterízase porque existen dúas ou máis secuencias alternativas de accións no programa. A selección dunha ou outra realízase de acordo a unha *condición* que se debe cumprir para que o conxunto de accións sexa executado. Dise que as estruturas selectivas *bifurcan* a execución do programa. Unha instrución de bifurcación avalía unha *condición* e, en función do resultado desa avaliación, a execución bifúrcase a un determinado punto. Unha *condición* constrúese con expresións *lógicas*.



LENDAS: Verdadeiro / Estrutura Selectiva

- **Estrutura repetitiva ou bucle:** Caracterízase porque existe un conxunto de accións cuxa execución se debe repetir un determinado número de veces chamado bucle (ou lazo). A implementación do bucle debe ser tal que sexa posible acceder a el e tamén saír del. Non deben existir lazos de execución infinita. Para que un bucle cumpra coas condicións mencionadas (poder acceder e poder saír del) é preciso o uso dunha condición que o controle. En cada ciclo de execución do bucle deberá avaliarse a condición para decidir se se volve executar ou se se sae del; así, todo bucle deberá posuír un controlador (un contador ou unha sentinela), unha decisión (unha condición para decidir a repetición ou a saída do bucle) e un corpo (conxunto de accións que se repiten). Un contador é unha variable numérica enteira cuxo contido se incrementa ou se decrementa sucesivamente cun valor constante. Nun proceso de introdución de datos, a sentinela é o valor que indica a finalización do bucle.



Lenda: verdadeiro, estrutura repetitiva

Como exemplos de linguaxes de programación estruturadas temos FORTRAN, PASCAL, MODULA, ADA, C, etc.

### 37.3 Programación orientada a obxectos

A programación orientada a obxectos é o que se coñece como un paradigma ou modelo de programación. Isto significa que non é unha linguaxe específica ou unha tecnoloxía, senón unha forma de programar, un xeito de concibir a programación. O que caracteriza a programación orientada a obxectos é que tenta levar ao mundo do código o mesmo que atopamos no mundo real. Cando ollamos ao noso redor, que vemos? Pois, cousas, obxectos, e podemos recoñecer estes obxectos porque cada obxecto pertence a unha clase de obxecto. Iso permítenos distinguir, por exemplo, un can dun coche (porque son de clases diferentes) e tamén un televisor doutro (porque, aínda que sexan iguais, cada un é un obxecto distinto). Este é o modelo que a programación orientada a obxectos tenta seguir para estruturar un sistema.

A construción de software orientado a obxectos é o método de desenvolvemento de software que basea a arquitectura de calquera sistema software en módulos deducidos dos tipos de obxectos que

manipula (en lugar de basearse na función ou funcións que o sistema está destinado a asegurar). Os desenvolvedores analizarán os tipos dos obxectos do sistema e o deseño irá pasando polas sucesivas melloras da súa comprensión destas clases de obxectos. É un proceso ascendente, ao revés da programación estruturada que era descendente, de construción de solucións robustas e extensibles a certas partes do problema, e de combinación desas solucións en montaxes cada vez máis potentes, ata que a montaxe final dá unha solución do problema orixinal; ademais, os mesmos compoñentes ensamblados de xeito diferente, e combinados posiblemente con outros, deberán ser o suficientemente xerais para producir tamén outros subprodutos software, é dicir, deben ser reutilizables.

Así, un sistema concíbese como un conxunto de obxectos, pertencentes a algunha clase, que se comunican entre si mediante mensaxes. Os obxectos distínguense por:

- posuír un estado que pode cambiar,
- ter unha identidade única,
- soportar interrelacións con outros obxectos,
- posuír un comportamento,
- poder recibir e emitir mensaxes.

Un **obxecto** descríbese polas súas propiedades —tamén chamadas atributos (definen a estrutura do obxecto)— e polos servizos (métodos ou operacións) que pode proporcionar (comportamento do obxecto). O estado dun obxecto vén determinado polos valores que toman os seus atributos. O obxecto é a unidade fundamental de descomposición na programación orientada a obxectos.

Ademais, todo obxecto é unha instancia dalgunha **clase**. Todos os obxectos se crean de acordo a unha definición de clase de obxectos. Esta clase inclúe declaracións de todos os atributos e operacións que se

deberían asociar cun obxecto da tal clase. Unha clase é unha abstracción das propiedades comúns e comportamento dun conxunto de obxectos.

Xa que logo, un programa orientado a obxectos consta dunha ou máis clases interdependentes. As clases permiten describir as propiedades (atributos ou campos) e habilidades (métodos) dos obxectos cos que o programa ten que tratar. O conxunto de atributos e métodos dunha clase reciben tamén o nome de **membros** desa clase.

As definicións dos membros poden ir precedidas dun **modificador de acceso**, que é algo que indica desde qué puntos do código é accesible ese membro. Os tres principais modificadores de acceso son:

- **Public:** Pódese acceder desde calquera punto.
- **Protected:** É accesible desde os métodos da súa clase e das clases que dela se puidesen derivar.
- **Private:** Só se pode utilizar desde os métodos da propia clase.

•

Estes son os modificadores de acceso máis comúns aínda que, dependendo da linguaxe, poderíamos ter outros modificadores que varían os accesos en función de se as clases están no mesmo paquete, etc...

O comportamento dun obxecto vén determinado polo conxunto de métodos que este proporciona. Referirémonos indistintamente a eles como **métodos, servizos ou operacións**. Un método está formado por un conxunto de sentenzas (accións) que cómpre levar a cabo para facer efectivo un comportamento dun obxecto. Un obxecto proporciona un conxunto de métodos que se poden utilizar desde outros obxectos. O devandito conxunto de métodos constitúe o que se denomina **interface** do obxecto. Mediante a interface dun obxecto poderemos acceder aos valores dos seus atributos (estado) para a súa consulta e/ou modificación e activar un comportamento do mesmo. Cando se fai unha chamada a un método da interface dun obxecto dicimos que lle estamos enviando unha mensaxe ao

dito obxecto. Así, unha **mensaxe** pódese definir como unha petición a un obxecto para a obtención dalgún comportamento desexado deste. Unha chamada a un método pode conter **parámetros**, ou conxunto de datos de entrada do método. Os métodos poden devolver valores, obxectos ou nada (*void* nalgunhas linguaxes).

Dise que a información acerca dun obxecto está **encapsulada** polo seu comportamento. A un obxecto débenselle pedir os seus datos, ou pedir que os cambie cunha mensaxe. Ao encapsular ou ocultar información sepáranse os aspectos externos dun obxecto (os accesibles para todos) dos detalles de implementación (os accesibles para ninguén). Con isto trátase de lograr que ao haber algún cambio na implementación dun obxecto non se teñan que modificar os programas que utilizan tal obxecto.

Unha das propiedades máis característica da orientación a obxectos é a **herdanza**, que é a capacidade de crear novas clases (subclases) a partir doutra clase xa existente, especificando unicamente as diferenzas coa clase “pai”. Aínda que algunhas linguaxes permiten a herdanza múltiple (unha clase que deriva de máis dunha clase), en xeral, a maioría delas non o fan e só permiten que se herde dunha clase. Para simular a herdanza múltiple utilízanse as interfaces, que si son soportadas por todas as linguaxes orientadas a obxectos. As interfaces especifican (non implementan) conxuntos de métodos e atributos para que as clases as implementen. Unha clase que implementa unha interface está obrigada a ter unha implementación para cada método definido na interface.

Cando se diseña un modelo orientado a obxectos é útil introducir clases a certo nivel que poden non existir en realidade, pero que permiten actuar como un depósito de métodos e atributos compartidos para as subclases de nivel inferior. Estas clases denomínanse **clases abstractas** e non poden ter ningunha instancia. Non se poden crear obxectos da tal clase. Tamén temos **métodos abstractos**, que son aqueles nos que non se especifica ningunha implementación. Son as clases derivadas as que teñen

que facelo. Dise que unha **clase** é **selada** cando non pode ter clases derivadas. Igualmente, un **método selado** é aquel que non pode ser redefinido nas clases derivadas. Utilízanse para optimizar a súa execución a nivel de código, xa que o implementador sabe que non se pode utilizar como clase base doutras.

Os atributos de obxecto son aqueles que almacenan un valor para cada obxecto da clase. Os atributos de clase son aqueles que almacenan un valor accesible para todos os obxectos da clase. Os métodos de obxecto son aqueles que acceden ao estado dun obxecto concreto, namentres que os métodos de clases non necesitan acceder a ningún atributo de ningún obxecto. Os membros (atributos e métodos) de clase tamén son chamados estáticos ou compartidos.

Un **construtor** é un método especial que se executa automaticamente cando se crea o obxecto. O seu propósito é inicializar o obxecto con, polo menos, os datos mínimos que necesita. Igual que para o resto dos métodos, pode haber varios construtores sobrecargados. É dicir, podemos crear obxectos de distintas formas. Chámase construtor por defecto aquel que non ten argumentos. Un **destrutor** é un método especial que adoita liberar a memoria e outros recursos cando un obxecto deixa de ser usado. Pode ser chamado automaticamente, liberando así da responsabilidade ao programador.

Para rematar, falaremos doutra das características fundamentais da programación orientada a obxectos: o **polimorfismo**. O polimorfismo refírese a dous aspectos diferentes: por unha banda, a sobrecarga de métodos e operadores (métodos polimórficos) e doutra banda, a ligadura dinámica. O primeiro é a capacidade de ter distintos métodos na mesma clase co mesmo nome, aínda que con distinta sinatura (número de argumentos, tipos dos argumentos, orde). O que non poden é devolver un resultado de distinto tipo. O outro aspecto, a ligadura dinámica, refírese a que cando se lle envía unha mensaxe a un obxecto, o código que se chama



non se determina ata o momento da execución. O compilador asegura que a función existe, mais non coñece o código exacto que hai que executar. Para iso, o compilador insire un código especial en lugar dunha chamada absoluta. Este código calcula en tempo de execución o enderezo real do método que hai que executar utilizando a información almacenada no propio obxecto. Esta ligadura dinámica está relacionada coa herdanza. Dende un punto de vista práctico, o polimorfismo permite definir unha referencia a unha clase pai, que en tempo de execución apuntará a un obxecto concreto dalgunha clase filla (non coñecida en tempo de compilación). A chamada aos métodos virtuais (os métodos da clase pai que serán redefinidos na clase filla) a través da devandita referencia executarase correctamente, pois durante a execución verifícase o tipo do obxecto almacenado e chámase á versión correcta do método.

Exemplos de linguaxes de programación orientadas a obxectos 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 Enxeñería inversa e reenxeñería**

A Enxeñería Inversa ocúpase de estudar un sistema de información na orde inversa establecida no ciclo de vida habitual; isto é, partindo do código fonte hai que identificar os compoñentes do sistema e as relacións existentes entre eles. Ata a súa chegada, o ciclo de vida do software era, en teoría, nunha soa dirección; agora, pódese falar de dúas direccións: *forward* ou cara adiante, que é a tradicional, e *reverse* ou cara atrás, que é a da Enxeñería Inversa. A Enxeñería Inversa tamén é coñecida como “modernización de caixa branca” (*White-Box Modernization*).

Daremos un par de definicións de enxeñería inversa:

“A análise dun sistema para identificar os seus compoñentes actuais e as dependencias que existen entre eles, para extraer e crear abstraccións do devandito sistema e información sobre o seu deseño” [Chikofsky, 1990].

“O proceso de analizar o código, documentación e comportamento dun sistema para identificar os seus compoñentes actuais e as súas dependencias co fin de extraer e crear unha abstracción do sistema e información de deseño. O sistema en estudo non é alterado, senón que se obtén coñecemento adicional acerca do sistema” [SEI, 2004].

A partir destas definicións podemos declarar que a enxeñería inversa ten a misión de desentrañar os misterios e segredos dos sistemas en uso. Consiste principalmente en recuperar o deseño dunha aplicación a partir do código. Isto faise principalmente mediante ferramentas que extraen información dos datos, procedementos e arquitectura do sistema existente. O obxectivo primordial é proporcionar unha base para o mantemento e futuros desenvolvementos. Este obxectivo xeral pódese traducir nos seguintes obxectivos parciais:

- Reducir os erros e os custos do mantemento.
- Facer os sistemas máis fáciles de entender, cambiar e probar.
- Protexer e estender a vida do sistema.
- Facilitar a reutilización de compoñentes do sistema existentes.
- Proporcionar documentación que non existe, ou actualizar a existente.
- Migrar a outra plataforma hardware ou software, cando sexa necesario.
- Levar o sistema baixo o control dun contorno CASE.

Dados estes obxectivos, os sistemas candidatos a aplicarles a Enxeñería Inversa reúnen algunhas das seguintes características:

- As especificacións de deseño e a documentación non existen ou están incompletas.

- O código non é estruturado.
- Inexistencia de documentación interna nos programas, ou ben esta é incomprendible ou está desfasada.
- O sistema necesita un excesivo mantemento correctivo.
- Algúns módulos fixéronse excesivamente complexos debido aos sucesivos cambios realizados neles.
- Necesítase unha migración cara a unha nova plataforma de hardware ou de software.
- A aplicación está suxeita a cambios frecuentes, que poden afectar a parte do deseño.
- Prevese que a aplicación poida ter aínda longa vida.

Aplicar a Enxeñería Inversa supón un enorme esforzo e, xa que logo, faise necesario avaliar exhaustivamente, e sendo moi realistas, os casos nos que é rendible a súa aplicación. O seu resultado varía en gran medida en función dos seguintes elementos:

- **O nivel de abstracción** do proceso de Enxeñería Inversa e as ferramentas que se usen. Isto alude á sofisticación da información de deseño que se pode extraer do código fonte. O nivel de abstracción ideal deberá ser o máis alto posible. Isto é, o proceso de enxeñería inversa deberá ser capaz de derivar as súas representacións de deseño de procedementos (cun baixo nivel de abstracción); e a información das estruturas de datos e de programas (un nivel de abstracción lixeiramente máis elevado); modelos de fluxo de datos e de control (un nivel de abstracción relativamente alto); e modelos de entidades e de relacións (un elevado nivel de abstracción). A medida que crece o nivel de abstracción proporciónaselle ao enxeñeiro do software información que lle permitirá comprender máis facilmente estes programas.
- **A completitude** do proceso. A completitude dun proceso de enxeñería inversa alude ao nivel de detalle que se proporciona nun

determinado nivel de abstracción. Na maioría dos casos, a completitude decrece a medida que aumenta o nivel de abstracción. Por exemplo, dada unha listaxe do código fonte, é relativamente doado desenvolver unha representación de deseño de procedementos completa. Tamén se poden derivar representacións sinxelas do fluxo de datos, pero é moito máis difícil desenvolver un conxunto completo de diagramas de fluxo de datos ou un diagrama de transición de estados. A completitude mellora en proporción directa á cantidade de análise efectuada pola persoa que está a levar a cabo a enxeñería inversa.

- **A interactividade do proceso.** A interactividade alude ao grao en que o ser humano se “integra” coas ferramentas automatizadas para crear un proceso de enxeñería inversa efectivo. Na maioría dos casos, a medida que crece o nivel de abstracción, a interactividade deberá incrementarse, ou se non a completitude se verá reducida.
- **A direccionalidade do proceso.** Se a direccionalidade do proceso de enxeñería inversa é monodireccional, toda a información extraída do código fonte se lle proporcionará á enxeñería do software, que poderá daquela utilizala durante a actividade de mantemento. Se a direccionalidade é bidireccional, daquela a información se lle subministrará a unha ferramenta de reenxeñería que tentará reestruturar ou rexenerar o vello programa.

A Enxeñería inversa non supón a modificación do sistema nin a xeración de novos sistemas; así e todo, existen unha serie de técnicas intrinsecamente relacionadas con ela:

- **Redocumentación:** é a produción dunha representación semántica dun sistema a calquera nivel de abstracción que se requira. As ferramentas usadas parten do código fonte existente para producir diagramas de fluxo de datos, modelos de datos, etc. Se a redocumentación toma a forma de modificación de comentarios no

código fonte pode ser considerada unha forma suave de reestruturación. Se se pensa nela como unha transformación desde o código fonte a pseudocódigo e/ou prosa, esta última é considerada como de máis alto nivel de abstracción que a primeira.

- **Recuperación do deseño:** é un subconxunto da enxeñería inversa, no cal, á parte das observacións do sistema, se engaden coñecementos sobre o seu dominio de aplicación, información externa e procesos dedutivos, co obxecto de identificar abstraccións significativas a un maior nivel.
- **Reestruturación:** A transformación desde unha forma de representación a outra no mesmo nivel de abstracción, preservando as características externas do sistema (funcionalidade e semántica) [Chikofsky, 1990]. A reestruturación do software modifica o código fonte e/ou os datos nun intento de adecualos a futuros cambios. En xeral, a reestruturación non modifica a arquitectura global do programa. Tende a centrarse nos detalles de deseño de módulos individuais e en estruturas de datos locais definidas dentro dos módulos. Se o esforzo da reestruturación se estende máis alá dos límites dos módulos e abrangue a arquitectura do software, a reestruturación pasa a ser enxeñería directa (*forward engineering*). Arnold sinala que os beneficios que se poden lograr coa reestruturación do software consisten en obter programas de maior calidade, mellorar a produtividade dos enxeñeiros do software, reducir o esforzo requirido para levar a cabo actividades de mantemento e facer que o software sexa máis sinxelo de comprobar e de depurar.
- **Reenxeñería:** A reenxeñería parte dos resultados obtidos na enxeñería inversa para reconstruír o sistema mediante enxeñería cara adiante. A Reenxeñería non só recupera a información de deseño dun software existente, senón que a usa para alterar ou

reconstruír o sistema existente nun esforzo por mellorar a calidade xeral.

Chikofsky define a **reenxeñería** como o “exame e alteración dun sistema para reconstruílo dunha nova forma e a subseguinte implementación desta nova forma”. Arnold, pola súa banda, sinala que reenxeñería é “calquera actividade que mellore a nosa comprensión do software e prepare ou mellore o propio software, normalmente para a súa facilidade de mantemento, reutilización ou evolución.” A definición dada polo Reengineering Center do Software Engineering Institute é “a transformación sistemática dun sistema existente a unha nova forma co fin de realizar melloras da calidade en operación, capacidade do sistema, funcionalidade, rendemento ou capacidade de evolución a baixo custo, cun plan de desenvolvemento curto e con baixo risco para o cliente”.

A importancia das técnicas de reenxeñería do software estriban en que reducen os riscos evolutivos dunha organización, axudan ás organizacións a recuperar os seus investimentos en software, fan o software máis facilmente modificable, amplían a capacidade das ferramentas CASE e son un catalizador para a automatización do mantemento do software.

Para algúns autores, a reenxeñería de sistemas pode clasificarse segundo os niveis de coñecementos requiridos para levar a cabo o proxecto. A reenxeñería que require coñecementos a baixos niveis de abstracción (código fonte) chámase **Enxeñería Inversa ou Modernización de Caixa Branca** e aquela que só require o coñecemento das interfaces do sistema chámase **Reenxeñería** propiamente dita ou **Modernización de Caixa Negra**.

Para realizar a reenxeñería nos sistemas existentes (tamén chamados **legacy systems** ou **sistemas herdados**) empréganse técnicas métricas, de visualización de programas, de abstracción e reformulación do código. Tanto para reenxeñería como para enxeñería inversa, créanse patróns para

a resolución de problemas relacionados con estas técnicas. Tomando como base o coñecemento do sistema, os datos, as funcionalidades e as interfases, desenvólvense novas técnicas de reenxeñería non baseadas no coñecemento do código senón no exame do comportamento das entradas e saídas do sistema, desenvolvendo novos patróns de reenxeñería e sentando as bases da reenxeñería baseada en *wrapping*. En teoría, **wrapping** é unha reenxeñería na que só se analizan as interfases (as entradas e saídas) do sistema existente, ignorando os detalles internos. Esta solución non é aplicable sempre e ás veces require o concurso da enxeñería inversa para o coñecemento interno do sistema.

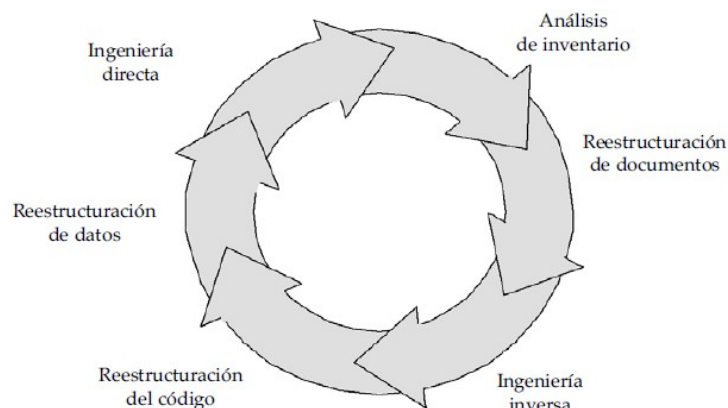
Veremos nos seguintes apartados distintos modelos de reenxeñería:

#### *37.4.1 Modelo Cíclico*

O modelo cíclico, debido a Pressman, concibe a reenxeñería como un proceso composto por seis actividades que se producen, normalmente, de forma secuencial e lineal. As actividades que se definen no modelo cíclico son:

- **Análise de inventario.** Todas as organizacións de software deberán dispoñer dun inventario de todas as súas aplicacións co fin de poder identificar os candidatos á reenxeñería.
- **Reestruturación de documentos.** Unha documentación escasa é a marca de moitos sistemas de información herdados. Ante iso será necesario ou ben crear a documentación ou ben actualizar a existente ou facela nova por completo.
- **Enxeñería Inversa.** A Enxeñería Inversa do software é o proceso de análise dun programa co fin de crear unha representación de programa cun nivel de abstracción máis elevado que o código fonte. A Enxeñería Inversa extráese do programa existente información do deseño arquitectónico e de proceso, e información dos datos.

- **Reestruturación do código.** O tipo máis común de reenxeñería é a reestruturación do código. Algúns sistemas herdados teñen unha arquitectura de programa relativamente sólida, pero os módulos individuais foron codificados dunha forma que fai difícil comprendelos, comprobalos e mantelos. Nestes casos, pódese reestruturar o código situado dentro dos módulos sospeitosos.
- **Reestruturación de datos.** Un programa que posúa unha estrutura de datos débil será difícil de adaptar e de mellorar. De feito, para moitas aplicacións, a arquitectura de datos ten máis que ver coa viabilidade a longo prazo do programa que o propio código fonte. Ao revés da reestruturación de código, que se produce nun nivel relativamente baixo de abstracción, a estruturación de datos é unha actividade de reenxeñería a grande escala.
- **Enxeñería directa (forward engineering).** A enxeñería directa non soamente recupera a información de deseño dun software xa existente, senón que, ademais, utiliza esta información nun esforzo por mellorar a súa calidade global. Na maioría dos casos, o software procedente dunha reenxeñería volve implementar a funcionalidade do sistema existente, e engade ademais novas funcións e/ou mellora o rendemento global.



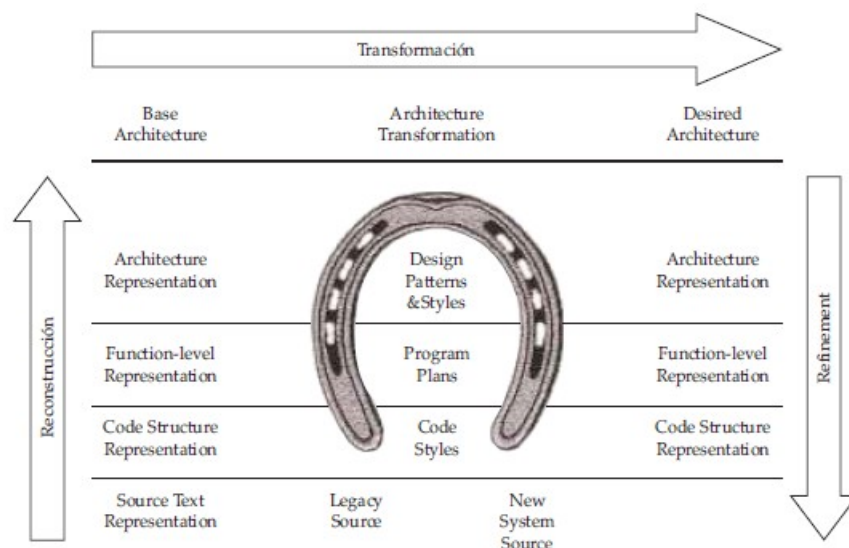
Lenda: enxeñería directa, análise de inventario, reestruturación do código, reestruturación de datos

#### 37.4.2 O modelo de ferradura



O modelo de ferradura fundaméntase en considerar tres niveis de abstracción en todo sistema e en que a reenxeñería está formada por tres procesos básicos:

- **Análise dun sistema existente:** sobe o extremo esquerdo da ferradura, e recupera a arquitectura por medio da extracción de artefactos desde o código fonte.
- **Transformación lóxica:** cruza a parte superior e é a transformación de arquitectura. A arquitectura antes construída é recuperada e reenxeñéizase para facer a nova arquitectura desexable.
- **Desenvolvemento dun novo sistema:** baixa polo extremo dereito da ferradura e constrúe a nova arquitectura desexable.



A riqueza do modelo de ferradura son os tres niveis de abstracción que poden ser adoptados para as descrições lóxicas, as cales poden ser artefactos tan concretos e simples como o código fonte do sistema ou tan complexos e abstractos como a arquitectura do sistema. Os tres niveis que adopta o modelo de ferradura son:

- **Representación da estrutura de código,** que inclúe código fonte e artefactos tales coma árbores de sintaxe abstractas e diagramas de fluxo.

- **Representación do nivel funcional**, que describe a relación entre as funcións do programa (chamadas), datos (funcións e relacións de datos) e arquivos (agrupamento de funcións e datos).
- **Nivel conceptual**, que representa grupo tanto de funcións e artefactos do nivel de código que son ensamblados dentro de subsistemas de compoñentes relacionados ou conceptos.

### 37.4.3 O modelo do IEEE

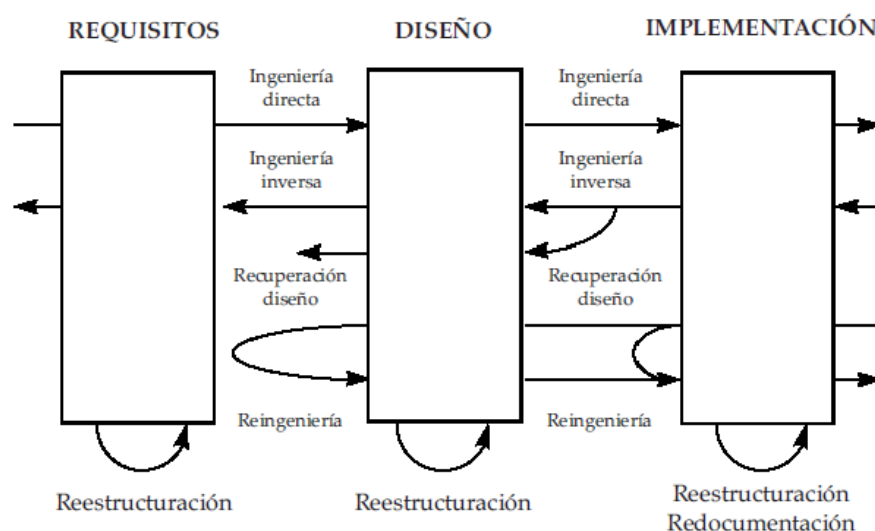
Este modelo baséase en considerar tres niveis de abstracción en todo sistema: o nivel requisitos, o nivel deseño e o nivel implementación, e en fixar unha terminoloxía. Os conceptos que define o IEEE, baseados nas definicións de Chikofsky e Cross, son os seguintes:

- **Enxeñería Inversa (Reverse Engineering)**: é o proceso de analizar un sistema para identificar os compoñentes e interrelacionalos entre eles, creando representacións do sistema noutra forma distinta á orixinal ou ben a un nivel superior de abstracción.
- **Reenxeñería (Reengineering)**: é o exame e modificación dun sistema para ser reconstruído dunha forma nova e ademais realizar a implantación derivada desa nova forma. Normalmente, a Reenxeñería inclúe algunha forma de Enxeñería Inversa e vai seguida dalgunha forma de Enxeñería “cara adiante” ou tamén dunha Reestruturación.
- **Reestruturación (Restructuring)**: é a transformación dunha forma de representación do sistema noutra distinta, pero do mesmo nivel de abstracción, sen modificar o comportamento externo do sistema.
- **Enxeñería Cara Adiante (Forward Engineering)**: é o proceso que vai desde un alto nivel de abstracción —que é independente da implementación concreta— ata a propia implementación física do

sistema. É dicir, é a Enxeñería do Software na súa vertente restrinxida ao novo desenvolvemento.

- **Reenxeñería de Empresas (Business Process Reengineering):** é a aplicación do concepto de Reenxeñería ao eido económico e desenvólvese arredor de tres actividades clave: redeseñar os procesos básicos de traballo para acadar os obxectivos do negocio; utilizar as novas tecnoloxías para concibir, deseñar e poñer en marcha novas actividades; e cambiar a forma en que traballan os empregados.

As relacións entre as definicións e os niveis de abstracción son as que se ven na figura.



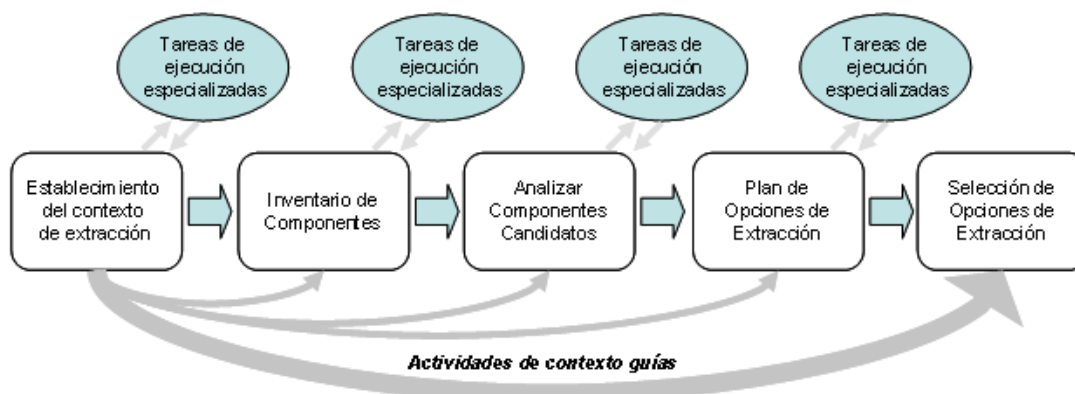
Lenda: deseño, enxeñería directa, enxeñería inversa, recuperación deseño, reenxeñería, reestructuración

#### 37.4.4 O método *Análise de Opcións para Reenxeñería* (Options Analysis for Reengineering [OAR])

É un método sistemático para a identificación e extracción de compoñentes dentro de grandes e complexos sistemas de software. OAR identifica compoñentes de arquitectura potencialmente relevantes e analiza os cambios esixidos para utilizalos nunha liña de produción de software ou novas arquitecturas de software. En esencia, OAR proporciona un conxunto

de opcións de extracción xunto coa estimación de custos, esforzo e riscos asociados con estas opcións. O método OAR consiste en cinco actividades principais:

- **Establecemento do contexto de extracción:** consiste en entrevistar os accionistas e estudar a liña de produción da organización ou novos requisitos de sistema, base herdada e expectativas para a extracción de compoñentes herdados. Estes esforzos establecen unha liña base dun conxunto de metas, expectativas e necesidades de compoñentes.
- **Inventario de Compoñentes:** o equipo OAR identifica os compoñentes do sistema herdado que, potencialmente, poden ser extraídos para utilizalos nunha liña de produción ou nunha nova arquitectura de software. Esta actividade deriva nun un inventario dos compoñentes herdados candidatos.
- **Análise de compoñentes candidatos:** O seguinte paso dos membros do equipo é analizar o conxunto de candidatos de compoñentes herdados para extraer os tipos de cambios que se requiren.
- **Plan de opcións de extracción:** Dado o conxunto de compoñentes candidatos analizados, o equipo desenvolverá alternativas para a extracción baseadas en consideracións de calendario, custo, esforzo, risco e recursos. O equipo OAR tamén filtra unha vez máis os compoñentes candidatos e analiza o impacto de agregación de diferentes compoñentes.
- **Selección de opcións de extracción:** Finalmente, os membros do equipo seleccionan a mellor opción de extracción ou combinación de opcións. Logo de avaliar cada opción de extracción, preparan un resumo no que presentan e xustifican as súas eleccións.



Lenda: tarefas de execución especializadas / establecemento do contexto de extracción, inventario de compoñentes, analizar compoñentes candidatos, plan de opcións de extracción, selección de opcións de extracción.

## 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 e 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 Jonathan.
- [http://www.cybertesis.edu.pe/sisbib/2007/acevedo\\_rj/pdf/acevedo\\_rj.pdf](http://www.cybertesis.edu.pe/sisbib/2007/acevedo_rj/pdf/acevedo_rj.pdf). *Ingeniería inversa aplicada a sistemas desarrollados con programación orientada a objetos para obtener la documentación.* Jessica Jahany Acevedo Ricse.

**Autor: Francisco Javier Rodríguez Martínez**

**Subdirector da Escola Superior de Enxeñería Informática**

**Universidade de Vigo**



# **38. MÉTODOS DE PROBA DO SOFTWARE. FUNDAMENTOS. CAIXA NEGRA E CAIXA BRANCA. ESTRATEXIAS DE PROBA DO SOFTWARE.**

## **Tema 38: Métodos de proba do software. Fundamentos. Caixa negra e caixa branca. Estratexias de proba do software.**

### **ÍNDICE**

#### **38.1 Métodos de proba do software. Fundamentos**

#### **38.2 Probas de Caixa negra e Caixa branca**

##### **38.2.1 Probas de Caixa branca**

###### **38.2.1.1 Proba do camiño básico**

###### **38.2.1.2 Proba da estrutura de control**

##### **38.2.2 Probas de Caixa Negra**

###### **38.2.2.1 Partición equivalente**

###### **38.2.2.2 Análise de valores límite**

###### **38.2.2.3 Valores típicos de erro e valores imposibles**

###### **38.2.2.4 Baseados en grafos**

###### **38.2.2.3 Táboa Ortogonal**

###### **38.2.2.4 Proba de comparación**

#### **38.3 Estratexias de proba do software.**

##### **38.3.1 Probas de Unidade**

##### **38.3.2 Probas de integración**

##### **38.2.3 Probas do sistema**

##### **38.2.4 Probas de implantación**

##### **38.2.5 Probas de aceptación**

### **38.1 Fundamentos das probas do software**

A proba do software é un elemento dun tema máis amplo que, a miúdo, é coñecido como **verificación** e **validación** (V&V). A **verificación** refírese ao conxunto de actividades que aseguran que o software implementa correctamente unha función específica. A **validación** refírese a un



conxunto diferente de actividades que aseguran que o software construído se axusta aos requisitos do cliente.

- **Verificación:** Estamos construíndo o produto correctamente?
- **Validación:** Estamos construíndo o produto correcto?

A proba presenta unha anomalía para o enxeñeiro do software, xa que, en canto que nas fases anteriores de definición e desenvolvemento, o enxeñeiro tenta construír, ao chegar as probas, o enxeñeiro diseña unha serie de casos de proba que pretenden “demoler” o construído. Por iso os autores din que a proba se pode ver como destrutiva, en lugar de construtiva.

O proceso de probas do software ten dous obxectivos distintos:

- Para demostrarlles ao desenvolvedor e ao cliente que o software satisfai os seus requisitos. Para o software a medida, isto significa que debería haber polo menos unha proba para cada requisito dos documentos de requisitos, do sistema e do usuario. Para produtos de software xenéricos, significa que debería haber probas para todas as características do sistema que se incorporarán na entrega do produto.
- Para descubrir erros no software en que o comportamento deste é incorrecto, non desexable ou non cumpre a súa especificación. A proba de erros está relacionada coa eliminación de todos os tipos de comportamentos do sistema non desexables, tales como caídas do sistema, interaccións non permitidas con outros sistemas, cálculos incorrectos e corrupción de datos.

Das moitas definicións válidas da “proba do software” podemos quedar con:

- A proba é o proceso de execución dun programa coa intención de descubrir erros (Glenford Myers).

- A proba é calquera actividade dirixida a avaliar a capacidade dun programa e a determinar que alcanza os resultados requiridos.

### *38.1.1 Principios das probas*

Coñecida a definición de proba, algúns dos principios que lles afectan son:

- A proba é o proceso de executar un programa coa intención de descubrir erros, polo que un bo caso de proba é aquel que ten unha alta probabilidade de descubrir un erro non atopado ata daquela.
- As probas deben planificarse antes de que se empece a codificar. Así, a planificación comeza co modelo de requisitos e mais a definición detallada dos casos de proba, unha vez que o deseño do sistema está consolidado.
- O 80% dos erros estarán localizados no 20% dos módulos.
- A proba completa é imposible.
- Para seren máis eficaces, as probas deberían ser feitas por un equipo independente.
- A probabilidade da existencia de máis erros nunha parte do software é proporcional ao número de erros xa atopados na devandita parte.

## **38.2 Probas de Caixa Negra e Caixa Branca**

Calquera produto de enxeñería pódese probar dunha destas dúas formas:

- Coñecendo a función específica para a que foi deseñado o produto, pódense levar a cabo probas que demostren que cada función é completamente operativa.
- Coñecendo o funcionamento do produto, pódense desenvolver probas que aseguren que “todas as pezas encaixan”, ou sexa, que a operación interna se axusta ás especificacións e que todos os compoñentes internos se comprobaron de forma adecuada.

O primeiro enfoque de proba denomínase proba de **caixa negra** e o segundo, proba de **caixa branca**.

A proba de **caixa negra** refírese ás probas que se levan a cabo sobre a interface do software. Ou sexa, os casos de proba pretenden demostrar que as funcións do software son operativas, que a entrada se acepta de forma adecuada e que se produce un resultado correcto, así como que a integridade da información externa (por exemplo, arquivos de datos) se mantén. Unha proba de caixa negra examina algúns aspectos do modelo fundamental do sistema sen ter en conta a estrutura lóxica interna do software.

A proba de **caixa branca** do software baséase no minucioso exame dos detalles procedementais. Compróbanse os camiños lóxicos do software propoñendo casos de proba que exerciten conxuntos específicos de condicións e/ou bucles. Pódese examinar o estado do programa en varios puntos para determinar se o estado real coincide co esperado ou mencionado.

### **38.2.1 Probas de caixa branca**

O enfoque da estratexia de probas coñecido polo nome de método de **caixa branca**, ou tamén **conducido pola lóxica** ou **logic driven**, céntrase en probar o comportamento interno e a estrutura do programa, examinando a súa lóxica interna e sen considerar os aspectos de rendemento. O obxectivo deste enfoque é executar, polo menos unha vez, todas as sentenzas e executar todas as condicións, tanto na súa vertente verdadeira coma falsa, tendo en conta que a única información de entrada con que se conta é o deseño do programa e o código fonte. As técnicas específicas máis usuais que seguen o método de caixa branca son:

- Proba do camiño básico
- Proba da estrutura de control
  - o Proba de condicións

- o Proba de fluxo de datos
- o Proba de bucles

#### *38.2.1.1. Proba do camiño básico*

A proba do camiño básico foi proposta inicialmente por Thomas J. McCabe. Tamén propuxo a expresión “complexidade ciclomática”, moi relacionada co camiño básico e que habemos ver máis adiante.

Esta proba do camiño básico permítelle ao deseñador de casos de proba obter unha medida da complexidade lóxica dun deseño procedemental e usar esa medida como guía para a definición dun conxunto básico de camiños de execución. Os casos de proba obtidos do conxunto básico garanten que durante a proba se execute polo menos unha vez cada sentenza do programa.

Da técnica do camiño básico dérivanse dúas probas complementarias e non excluíntes:

- *Proba de cobertura de sentenzas.* Consiste en xerar casos de proba que permitan probar todas e cada unha das sentenzas dun módulo unha vez. Esta proba é necesaria pero non é suficiente.
- *Proba de cobertura de condicións.* Consiste en deseñar xogos de proba que consideren todos os valores posibles de cada unha das condicións. Esta proba tamén é necesaria pero non é suficiente, xa que non garante que todos os camiños sexan cubertos polo que debe ser complementada coa anterior.

A técnica de proba do camiño básico utiliza unha convención de representación denominada “grafos de fluxo” para a determinación de camiños e para iso apóiase no concepto de “complexidade ciclomática”.

A notación de “**grafo de fluxo**” utilízase para simplificar o desenvolvemento do conxunto básico de camiños de execución. O seu

obxectivo é exemplificar o fluxo de control do módulo que se está a probar e para iso utiliza tres elementos:

- **Nodos** ou tarefas de procesamento (N). Representan cero, unha ou varias sentenzas procedementais. Cada nodo comprende como máximo unha sentenza de decisión (bifurcación). Cada nodo que contén unha condición denomínase **nodo predicado** e está caracterizado porque dúas ou máis arestas emerxen del.
- **Arestas**, fluxo de control ou conexións (A). Unen dous nodos, mesmo aínda que o nodo non represente ningunha sentenza procedemental.
- **Rexións** (R). Son as áreas delimitadas polas arestas e nodos. Cando se contabilizan as rexións debe incluírse a área externa como unha rexión máis.

A **complexidade ciclomática** é unha métrica do software baseada na teoría de grafos, que proporciona unha medición cuantitativa da complexidade lóxica dun programa. Cando se usa no contexto do método de proba do camiño básico, o valor calculado como complexidade ciclomática define o número de camiños independentes do conxunto básico dun programa e dáunos un límite superior para o número de probas que se deben realizar para asegurar que se executa cada sentenza polo menos unha vez. Un camiño independente é calquera camiño do programa que introduce, como mínimo, un novo conxunto de sentenzas de proceso ou unha nova condición. En termos do grafo de fluxo, un camiño independente está constituído polo menos por unha aresta que non fose percorrida anteriormente á definición do camiño. O valor da complexidade pódese obter de tres formas:

- 1- O número de rexións do grafo (R).
- 2- O número de arestas menos o número de nodos + 2. ( $A - N + 2$ ).
- 3- Número de nodos predicado + 1. ( $P + 1$ ).

A proba do camiño básico permítenos obter os casos de proba da seguinte forma:

- 1- Usando o deseño ou o código como base, debuxamos o correspondente grafo de fluxo.
- 2- Determinamos a complexidade ciclomática do grafo de fluxo resultante.
- 3- Determinamos un conxunto básico de camiños linealmente independentes.
- 4- Preparamos os casos de proba que forzarán a execución de cada camiño do conxunto básico.

#### *38.2.1.2 Probas da estrutura de control*

Dentro deste tipo de probas inclúese o método do camiño básico mencionado anteriormente, pero ademais complementáanse con outras probas asociadas que permiten ampliar a cobertura da proba e mellorar a súa calidade.

##### *38.2.1.2.1 Proba de condición*

É un método de deseño de casos de proba que exercita as condicións lóxicas contidas no módulo dun programa. Algúns conceptos empregados arredor desta proba son os seguintes:

- *Condición simple:* é unha variable lóxica ou unha expresión relacional ( $E_1 < \text{operador} - \text{relacional} > E_2$ ).
- *Condición composta:* está formada por dúas ou máis condicións simples, operadores lóxicos e parénteses.

En xeral, os tipos de erros que se buscan nunha proba de condición, son os seguintes:

- *Erro en operador lóxico* (existencia de operadores lóxicos incorrectos, desaparecidos, sobrantes).
- *Erro en variable lóxica.*
- *Erro en parénteses lóxica.*
- *Erro en operador relacional.*
- *Erro en expresión aritmética.*

#### *38.2.1.2.2 Proba do fluxo de datos.*

Selecciona camiños de proba dun programa de acordo coa localización das definicións e os usos das variables do programa.

#### *38.2.1.2.3. Proba de bucles*

A proba de bucles é unha técnica de proba de caixa branca que se centra exclusivamente na validez das construcións de bucles. Pódense definir catro clases diferentes de bucles:

- **Bucles simples.** Aos bucles simples débeseles aplicar o seguinte conxunto de probas, onde ***n*** é o número máximo de pasos permitidos polo bucle:
  1. pasar por alto totalmente o bucle
  2. pasar unha soa vez polo bucle
  3. pasar dúas veces polo bucle
  4. facer *m* pasos polo bucle con  $< m n$
  5. facer  $n - 1$ ,  $n$  e  $n+1$  pasos polo bucle
- **Bucles anidados.** Se estendésemos o enfoque de proba dos bucles simples aos bucles anidados, o número de probas posibles aumentaría xeometricamente a medida que aumenta o nivel de

aniñamento. Isto levaría A un número impracticable de probas. Suxírese un enfoque que axude a reducir o número de probas:

1. Comezar polo bucle máis interior. Establecer ou configurar os demais bucles cos seus valores mínimos.
  2. Levar a cabo as probas de bucles simples para o bucle máis interior, namentres se manteñen os parámetros de iteración (por exemplo, contador do bucle) dos bucles externos nos seus valores mínimos. Engadir outras probas para valores fóra de rango ou excluídos.
  3. Progresar cara a fóra, levando a cabo probas para o seguinte bucle, pero mantendo todos os bucles externos nos seus valores mínimos e os demais bucles aniñados nos seus valores “típicos”.
  4. Continuar ata que se probaron todos os bucles.
- **Bucles concatenados.** Os bucles concatenados pódense probar mediante o enfoque anteriormente definido para os bucles simples, mentres cada un dos bucles sexa independente do resto. Non obstante, se hai dous bucles concatenados e se usa o controlador do bucle 1 como valor inicial do bucle 2, daquela os bucles non son independentes. Cando os bucles non son independentes, recoméndase usar o enfoque aplicado para os bucles aniñados.
  - **Bucles non estruturados.** Neste caso, ante a complexidade que pode representar a comprensión do fluxo de control, é máis práctico redeseñar o módulo a probar, de forma que se codifique mediante bucles estruturados.

### 38.2.2 Probas de caixa negra

O enfoque da estratexia de probas coñecido polo nome de método de **caixa negra** ou, tamén, “**conducido polos datos**” (***data driven***) ou



**“conducido pola entrada/saída” (*input-output driven*)**, ou tamén **probas de comportamento**, non considera o detalle procedemental dos programas e céntrase en buscar situacións onde o programa non se axusta á súa especificación, utilizando esta como entrada para derivar os casos de proba.

Se polas especificacións funcionais se sabe o que ten que facer un módulo, é máis sinxelo comprobalo que esmiuzalo e examinalo internamente en todas as circunstancias posibles. Por iso, as probas de “caixa negra” son o enfoque máis simple de proba do software. Os casos de proba deséñanse a partir das especificacións funcionais.

Neste tipo de probas os casos de proba consisten en conxuntos de datos de entrada que deberán xerar unha saída acorde coa especificación. A atención céntrase, pois, nos datos de entrada e saída, ignorando intencionadamente o coñecemento do código do programa. Se con esta técnica se quixesen atopar todos os erros do programa, habería que recorrer a probar todas as posibles combinacións de casos de entrada, o que supoñería xerar todas as posibles combinacións de valores para todas as posibles variables de entrada, e iso, na realidade, é imposible. Desta imposibilidade pódese extraer a conclusión de que mediante o método da caixa negra non é posible asegurar que un programa estea libre de erros.

Dado que non se poden probar todos os casos posibles, o método de caixa negra aborda unha serie de técnicas encamiñadas a simplificar os casos de proba. Estas son:

- Partición equivalente.
- A análise de valores límite.
- Os valores típicos de erro e os valores imposibles.
- Métodos de proba baseados en grafos.
- Proba da táboa ortogonal.
- As probas de comparación.

### *38.2.2.1 Partición equivalente.*

A **partición equivalente** é un método de proba de caixa negra que divide o campo de entrada dun programa en clases de datos dos que se poden derivar casos de proba. Un caso de proba ideal descobre de forma inmediata unha clase de erros (por exemplo, proceso incorrecto de todos os datos de carácter) que, doutro xeito, habrían esixir a execución de moitos casos antes de detectar o erro xenérico. A partición equivalente diríxese á definición de casos de proba que descubran clases de erros, reducindo así o número total de casos de proba que hai que desenvolver.

O deseño de casos de proba para a partición equivalente baséase nunha avaliación das clases de equivalencia para unha condición de entrada. Unha **clase de equivalencia** representa un conxunto de estados válidos ou non válidos para condicións de entrada. Habitualmente, unha condición de entrada é un valor numérico específico, un rango de valores, un conxunto de valores relacionados ou unha condición lóxica. As clases de equivalencia pódense definir de acordo coas seguintes directrices:

- 1- Se unha condición de entrada especifica un rango, defínese unha clase de equivalencia válida e dúas non válidas.
- 2- Se unha condición de entrada require un valor específico, defínese unha clase de equivalencia válida e dúas non válidas.
- 3- Se unha condición de entrada especifica un membro dun conxunto, defínese unha clase de equivalencia válida e unha non válida.
- 4- Se unha condición de entrada é lóxica, defínese unha clase de equivalencia válida e unha non válida.

### *38.2.2.2 Análise de valores límite*

A **análise de valores límite** (AVL) é unha técnica de deseño de casos de proba que complementa a partición de equivalencia e xustifícase na constatación de que para unha condición de entrada que admite un rango de valores é máis fácil que existan erros nos límites ca no centro. Xa que logo, a diferenza entre esta técnica e a partición de equivalencia estriba en que na análise de valores límite non se selecciona un elemento representativo da clase de equivalencia, senón que se seleccionan un ou máis elementos de maneira que os límites de cada clase de equivalencia son obxecto de proba. Outra diferenza é que con esta técnica tamén se derivan casos de proba para as condicións de saída.

Do mesmo xeito que no caso anterior, a técnica de análise de valores límite non asegura a proba completa, xa que é imposible probar exhaustivamente todos os conxuntos de datos de entrada tanto na súa vertente válida como inválida. Con todo, a vantaxe que presenta esta técnica é que maximiza o número de erros atopados co menor número de casos de proba posibles, o que fai rendible o investimento efectuado na proba.

As directrices de AVL son semellantes en moitos aspectos ás que proporciona a partición equivalente:

- 1- Se unha condición de entrada especifica un rango delimitado polos valores a e b, débense deseñar casos de proba para os valores a e b, e para os valores xusto por baixo e xusto por riba de a e b, respectivamente.
- 2- Se unha condición de entrada especifica un número de valores, débense desenvolver casos de proba que exerciten os valores máximo e mínimo. Tamén se deben probar os valores xusto por riba e xusto por baixo do máximo e do mínimo.
- 3- Aplicar as directrices 1 e 2 ás condicións de saída.
- 4- Se as estruturas de datos internas teñen límites preestablecidos (por exemplo, unha matriz que teña un límite definido de 100 entradas),

hai que asegurarse de deseñar un caso de proba que exercite a estrutura de datos nos seus límites.

#### *38.2.2.3. Valores típicos de erro e valores imposibles*

Un bo complemento das dúas técnicas fundamentais de probas tipo “caixa negra” (particións de equivalencia e análise de valores límite) consiste en incluír nos casos de proba certos valores dos datos de entrada susceptibles de causar problemas, isto é, valores típicos de erro, e valores especificados como non posibles, é dicir, valores imposibles.

A determinación dos valores típicos de erro realízase en función da natureza e funcionalidade do programa que se vai probar, polo que depende en boa medida da experiencia do deseñador da proba.

Así mesmo, dentro das especificacións do sistema ou do programa que se proba pode haber valores de datos especificados como non posibles. O feito de probar estes valores imposibles débese a que os tales valores puideron ser xerados internamente polo sistema ou o programa, provocando un mal funcionamento deste. A proba de valores imposibles debe realizarse sempre que os devanditos valores poidan ser detectados e o programa poida manexalos adecuadamente sen provocar erros irreparables.

#### *38.2.2.4 Métodos de proba baseados en grafos*

Neste método débese entender os obxectos (obxectos de datos, obxectos de programa, tales coma módulos ou coleccións de sentenzas da linguaxe de programación) que se modelan no software e as relacións que conectan estes obxectos. Unha vez que se levou a cabo isto, o seguinte paso é

definir unha serie de probas que verifiquen que todos os obxectos teñen entre eles as relacións esperadas. Neste método:

1. Créase un grafo dos obxectos importantes e as súas relacións.
2. Deséñase unha serie de probas que cubran o grafo de maneira que se exerciten todos os obxectos e as súas relacións para descubrir erros.

Boris Beizer describe unha serie de modelados para probas de comportamento que poden facer uso dos grafos:

- *Modelado do fluxo de transacción.* Os nodos representan os pasos dalgunha transacción e os enlaces representan as conexións lóxicas entre eses pasos.
- *Modelado de estado finito.* Os nodos representan diferentes estados do software observables polo usuario e os enlaces representan as transicións que ocorren para moverse de estado a estado.
- *Modelado de fluxo de datos.* Os nodos obxectos de datos e os enlaces son as transformacións que ocorren para converter un obxecto de datos noutro.
- *Modelado de planificación.* Os nodos son obxectos de programa e os enlaces son as conexións secuenciais entre eses obxectos. Os pesos de enlace úsanse para especificar os tempos de execución requiridos ao se executar o programa.
- *Gráfica Causa-efecto.* Un gráfico de causa-efecto é unha linguaxe formal á que se traduce unha especificación permitindo seleccionar un gran conxunto de casos de proba. O gráfico é realmente un circuíto de lóxica dixital (unha rede combinatoria de lóxica), pero no canto da notación estándar da electrónica, utilízase unha notación algo máis simple. Non é preciso ter coñecementos de electrónica con excepción dunha comprensión da lóxica booleana (entendendo os

operadores da lóxica e, ou, e non). Ten un efecto secundario beneficioso, xa que permite precisar estados incompletos e ambigüidades na especificación.

- *38.2.2.5 Proba da táboa ortogonal*

Hai aplicacións onde o número de parámetros de entrada é pequeno e os valores de cada un dos parámetros están claramente delimitados. Cando estes números son moi pequenos (por exemplo, 3 parámetros de entrada tomando 3 valores diferentes), é posible considerar cada permutación de entrada e comprobar exhaustivamente o proceso do dominio de entrada. En calquera caso, cando o número de valores de entrada crece e o número de valores diferentes para cada elemento dos datos se incrementa, a proba exhaustiva faise impracticable.

A proba da **táboa ortogonal** pódese aplicar a problemas en que o dominio de entrada é relativamente pequeno pero demasiado grande para posibilitar probas exhaustivas. O método de proba da táboa ortogonal é particularmente útil ao encontrar erros asociados con fallos localizados — unha categoría de erro asociada con defectos da lóxica dentro dun compoñente software—. A proba de táboa ortogonal permite proporcionar unha boa cobertura de probas con bastantes menos casos de proba que na estratexia exhaustiva.

- *38.2.2.6 Proba de comparación*

Hai situacións nas que a fiabilidade do software é algo absolutamente vital. Nese tipo de aplicacións, a miúdo utilízase hardware e software redundante para minimizar a posibilidade de erro. Cando se desenvolve software redundante, varios equipos de enxeñería do software separados desenvolven versións independentes dunha aplicación, usando as mesmas especificacións. Nesas situacións, débense probar todas as versións cos mesmos datos de proba para garantir que todas proporcionen unha saída

idéntica. Logo, execútanse todas as versións en paralelo e faise unha comparación en tempo real dos resultados para garantir a consistencia.

Esas versións independentes son a base dunha técnica de proba de caixa negra denominada ***proba de comparación ou proba man a man***.

### **38.3 Estratexias de proba do software**

Unha estratexia de proba do software integra as técnicas de deseño de casos de proba nunha serie de pasos ben planificados que dan como resultado unha correcta construción do software. A estratexia proporciona un mapa que describe os pasos que cómpre levar a cabo como parte da proba, cando se deben planificar e realizar eses pasos, e canto esforzo, tempo e recursos se van requirir. Xa que logo, calquera estratexia de proba debe incorporar a planificación da proba, o deseño de casos de proba, a execución das probas e a agrupación e avaliación dos datos resultantes.

Unha estratexia de proba do software debe ser suficientemente flexible para promover a creatividade e a adaptabilidade necesarias para adecuar a proba a todos os grandes sistemas baseados en software. Ao mesmo tempo, a estratexia debe ser suficientemente ríxida para promover un seguimento razoable da planificación e a xestión a medida que progresa o proxecto.

Téñense proposto varias estratexias de proba do software con distintos autores. Todas estas estratexias lle proporcionan ao enxeñeiro do software un patrón para a proba e todas teñen as seguintes características xerais:

- As probas comezan a nivel de módulo e traballan “cara a fóra”, cara á integración de todo o sistema.
- Segundo o momento, son apropiadas diferentes técnicas de proba.
- A proba lévaa a cabo o responsable do desenvolvemento do software e (para grandes proxectos) un grupo independente de probas.

- A proba e a depuración son actividades diferentes, pero a depuración débese incluír en calquera estratexia de proba.

Unha estratexia de proba do software debe incluír probas de baixo nivel que verifiquen que todos os pequenos segmentos de código fonte se implementaron correctamente, así como probas de alto nivel que validen as principais funcións do sistema fronte aos requisitos do cliente. Unha estratexia débelle proporcionar unha guía ao profesional, así como un conxunto de fitos para o xefe de proxecto.

Débense abordar os seguintes puntos se se desexa implementar con éxito unha estratexia de proba do software:

- Especificar os requisitos do produto de maneira cuantificable moito antes de que comecen as probas.
- Establecer os obxectivos da proba de maneira explícita.
- Comprender qué usuarios van manexar o software e desenvolver un perfil para cada categoría de usuario.
- Desenvolver un plan de proba que faga fincapé na “proba de ciclo rápido”.
- Construír un software “robusto” deseñado para probarse a si mesmo.
- Usar revisións técnicas formais, efectivas como filtro antes da proba.
- Levar a cabo revisións técnicas formais para avaliar a estratexia de proba e os propios casos de proba.
- Desenvolver un enfoque de mellora continua ao proceso de proba.

Se consideramos o proceso desde o punto de vista dos procedementos e no contexto da enxeñería do software, a proba realmente é unha serie de cinco pasos que se levan a cabo secuencialmente. Nun principio, a proba céntrase en cada módulo individualmente, asegurando que estes funcionan adecuadamente como unha unidade. De aí o nome de *proba de unidade*. A proba de unidade fai un uso intensivo das técnicas de proba de caixa branca, exercitando camiños específicos da estrutura de control do módulo



para garantir un alcance completo e unha detección máxima de erros. Deseguido, débense ensamblar ou integrar os módulos para formar o paquete de software completo.

A *proba de integración* diríxese a todos os aspectos asociados co dobre problema de verificación e de construción do programa. Durante a integración, as técnicas que máis prevalecen son as de deseño de casos de proba de caixa negra, aínda que se poden levar a cabo algunhas probas de caixa branca para garantir que se abranguen os principais camiños de control. Unha vez que o software se integrou (construíu), diríxense un conxunto de *probos de alto nivel*. Débese comprobar que no software, ao combinalo con outros elementos do sistema (por exemplo, hardware, xente, bases de datos) cada elemento encaixa de forma adecuada e que se alcanza a funcionalidade e o rendemento esixido. Esta é a base da *proba de sistemas*.

Posteriormente, asegúrase mediante a *proba de implantación* o funcionamento correcto do sistema integrado de hardware e software no contorno de operación, e permíteselle ao usuario que, desde o punto de vista de operación, realice a aceptación do sistema unha vez instalado no seu contorno real e baseándose no cumprimento dos requisitos non funcionais especificados. A *proba de aceptación* proporciona unha seguridade final de que o software satisfai todos os requisitos funcionais, de comportamento e de rendemento. Durante as últimas tres probas (*sistemas, implantación e aceptación*) úsanse exclusivamente técnicas de proba de caixa negra.

### 38.3.1 Probas de Unidade

As probas de unidade teñen como obxectivo verificar a funcionalidade e estrutura de cada compoñente de maneira individual e unha vez que foi codificado.

A **proba de unidade** é un proceso para probar os subprogramas, as subrutinas, os procedementos individuais ou as clases nun programa. É dicir, é mellor probar primeiro os bloques desenvolvidos máis pequenos do programa, que probar primeiro o software na súa totalidade. As motivacións para facer isto son tres. (1) As probas de unidade son unha forma de manexar os elementos de proba combinados, posto que inicialmente se centra a atención en unidades máis pequenas do programa. (2) A proba dunha unidade facilita a tarefa de eliminar erros (o proceso de establecer claramente e de corrixir un erro descuberto), posto que, cando se atopa un erro, se sabe que existe nun módulo particular. Finalmente, (3) as probas de unidade introducen paralelismo no proceso de probas do software, presentándose a oportunidade de probar os múltiples módulos simultaneamente.

Cómpren dous tipos de información ao deseñar os casos de proba para unha proba de unidade: a especificación para o módulo e o código fonte do módulo. Habitualmente, a especificación define os parámetros de entrada e de saída do módulo e a súa función.

As probas de unidade están orientadas en gran parte á caixa branca. Unha razón é que, como en probas de entidades máis grandes tales coma programas enteiros (é o caso para os procesos de proba subsecuentes), a proba de caixa branca chega a ser menos factible. Unha segunda razón é que os procesos de proba subsecuentes están orientados a encontrar diversos tipos de erros. Polo tanto, o procedemento para o deseño de casos de proba para unha proba de unidade é a seguinte: analizar a lóxica do módulo usando un ou máis dos métodos de caixa branca e despois completar os casos de proba aplicándolle métodos de caixa negra á especificación do módulo.

### *38.3.2 Probas de integración*

O obxectivo das **probas de integración** é verificar a correcta ensamblaxe entre os distintos compoñentes, unha vez que foron probados unitariamente, co fin de comprobar que interactúan correctamente a través das súas interfaces, tanto internas coma externas, que satisfan a funcionalidade establecida e que se axustan aos requisitos non funcionais especificados nas verificacións correspondentes.

Nas probas de integración examínanse as interfaces entre grupos de compoñentes ou subsistemas para asegurar que son chamados cando é necesario e que os datos ou mensaxes que se transmiten son os requiridos. Debido a que nas probas de unidade é necesario crear módulos auxiliares que simulen as accións dos compoñentes invocados polo que se está probando, e debido a que se teñen que crear compoñentes "condutores" para establecer as precondicións necesarias, chamar o compoñente obxecto da proba e examinar os resultados da proba, a miúdo combínanse os tipos de proba unitarias e de integración.

Os tipos fundamentais de integración son os seguintes:

- *Integración incremental*: combínase o seguinte compoñente que se debe probar co conxunto de compoñentes que xa están probados e vaise incrementando progresivamente o número de compoñentes que proban. Co tipo de proba incremental, o máis probable é que os problemas que xurdan ao incorporar un novo compoñente ou un grupo de compoñentes previamente probado, sexan debidos a este último ou ás interfaces entre este e os outros compoñentes.
- *Integración non incremental*: próbase cada compoñente por separado e, posteriormente, intégranse todos dunha vez realizando as probas pertinentes. Este tipo de integración denomínase tamén **Big-Bang**.

Dentro da *integración incremental*, temos tres tipos de estratexias:

- *Estratexia Descendente (top-down)*: O primeiro compoñente que se proba é o primeiro da xerarquía. Os compoñentes de nivel máis baixo substitúense por compoñentes auxiliares chamados **resgardos** para simular os compoñentes invocados. Logo, vanse substituíndo os resgardos subordinados polos compoñentes reais. Vantaxes: As interfaces entre os distintos compoñentes próbanse nunha fase temperá e con frecuencia. Verifícanse os puntos de decisión ou de control principais ao principio do proceso de proba.
- *Estratexia Ascendente (bottom-up)*: Neste caso créanse primeiro os compoñentes de máis baixo nivel e créanse compoñentes **condutores ou controladores** para simular os compoñentes que os chaman. A continuación, substitúense os controladores polos módulos desenvolvidos de máis alto nivel e próbanse.
- *Estratexia combinada*: A miúdo é útil aplicar as estratexias anteriores conxuntamente. Deste xeito, próbanse as partes principais do sistema cun enfoque **top-down**, mentres que as partes de nivel máis baixo se proban seguindo un enfoque **bottom-up**.

Cada vez que se engade un novo módulo como parte dunha proba de integración, o software cambia. Establécense novos camiños de fluxo de datos, poden ocorrer novas E/S e invócase unha nova lóxica de control. Estes cambios poden causar problemas con funcións que antes traballaban perfectamente. Neste contexto, a **proba de regresión** é volver executar un subconxunto de probas que se levaron a cabo anteriormente para asegurarse de que os cambios non propagaron efectos colaterais non desexados.

### 38.3.3 Probas de sistema

As probas do sistema teñen como obxectivo validar o sistema, comprobando a integración do sistema de información globalmente, verificando o funcionamento correcto das interfaces entre os distintos subsistemas que o compoñen e co resto de sistemas de información cos que se comunica.

Unha vez que se probaron os compoñentes individuais e que se integraron, próbase o sistema de forma global. Nesta etapa pódense distinguir os seguintes tipos de probas, cada un cun obxectivo claramente diferenciado:

- **Probas funcionais.** Dirixidas a garantir que o sistema de información realiza correctamente todas as funcións que se detallaron nas especificacións dadas polo usuario do sistema.
- **Probas de comunicacións.** Determinan que as interfaces entre os compoñentes do sistema funcionan adecuadamente, tanto a través de dispositivos remotos coma locais. Así mesmo, débense probar as interfaces home/máquina.
- **Probas de rendemento.** Consisten en determinar que os tempos de resposta están dentro dos intervalos establecidos nas especificacións do sistema.
- **Probas de volume.** Consisten en examinar o funcionamento do sistema cando está traballando con grandes volumes de datos, simulando as cargas de traballo esperadas.
- **Probas de sobrecarga.** Consisten en comprobar o funcionamento do sistema no limiar límite dos recursos, someténdoo a cargas masivas. O obxectivo é establecer os puntos extremos nos cales o sistema empeza a operar por baixo dos requisitos establecidos.

- **Probas de dispoñibilidade de datos.** Consisten en demostrar que o sistema pode recuperarse ante fallos, tanto de equipo físico coma lóxico, sen poñer en perigo a integridade dos datos.
- **Probas de facilidade de uso.** Consisten en comprobar a adaptabilidade do sistema ás necesidades dos usuarios, tanto para garantir que se axeita á súa forma habitual de traballo, como para determinar as facilidades que proporciona ao introducir datos no sistema e obter os resultados.
- **Probas de operación.** Consisten en comprobar a correcta implementación dos procedementos de operación, incluíndo a planificación e control de traballos, arranque e rearranque do sistema, etc.
- **Probas de contorno.** Consisten en verificar as interaccións do sistema con outros sistemas dentro do mesmo contorno.
- **Probas de seguridade.** Consisten en verificar os mecanismos de control de acceso ao sistema para evitar alteracións indebidas nos datos.
- **Probas de configuración.** Programas tales coma sistemas operativos, sistemas de xestión de base de datos e programas de conmutación de mensaxes soportan diversas configuracións de hardware, incluíndo varios tipos e números de dispositivos de entrada-saída e liñas de comunicacións, ou diversos tamaños de memoria. A miúdo, o número de configuracións posibles é demasiado grande para probar cada un dos dispositivos, pero na medida do posible, débese probar o programa con cada tipo de dispositivo de hardware e coa configuración mínima e máxima. Se o programa por si mesmo se pode configurar para omitir compoñentes, ou se pode funcionar en diversas computadoras, cada configuración posible deste debe ser probada.

- **Probas de instalación.** Un funcionamento incorrecto do programa de instalación tería como resultado unha experiencia negativa do usuario, sendo unha das primeiras experiencias do usuario coa aplicación. Se esta fase se realiza mal, entón o usuario/o cliente pode buscar outro produto ou ter pouca confianza na validez da aplicación.
- **Probas de documentación.** A documentación do usuario debe ser inspeccionada, comprobándoa para saber se se presenta con exactitude e claridade. Calquera dos exemplos ilustrados na documentación débense probar, formar parte dos casos de uso, e débense introducir no programa.

#### *38.3.4 Proba de implantación*

O obxectivo das **probos de implantación** é comprobar o funcionamento correcto do sistema integrado de hardware e software no contorno de operación, e permitirlle ao usuario que, desde o punto de vista de operación, realice a aceptación do sistema unha vez instalado no seu contorno real e tomando como base o cumprimento dos requisitos non funcionais especificados.

Unha vez que sexan realizadas as probas do sistema no contorno de desenvolvemento, lévanse a cabo as verificacións necesarias para asegurar que o sistema funcionará correctamente no contorno de operación. Debe comprobarse que responde satisfactoriamente aos requisitos de rendemento, seguridade, operación e coexistencia co resto dos sistemas da instalación para conseguir a aceptación do usuario de operación.

As probas de seguridade van dirixidas a verificar que os mecanismos de protección incorporados ao sistema cumpren o seu obxectivo; as de rendemento a asegurar que o sistema responde satisfactoriamente nas marxes establecidas en canto tempos de resposta, de execución e de

utilización de recursos, así como os volumes de espazo en disco e capacidade; para rematar coas probas de operación compróbase que a planificación e control de traballos do sistema realízase de acordo aos procedementos establecidos, considerando a xestión e control das comunicacións e asegurando a dispoñibilidade dos distintos recursos.

Así mesmo, tamén son levadas a cabo as probas de xestión de copias de seguridade e recuperación, co obxectivo de verificar que o sistema non ve comprometido o seu funcionamento ao existir un control e seguimento dos procedementos de salvagarda e de recuperación da información, en caso de caídas nos servizos ou nalgúns dos seus compoñentes. Para comprobar estes últimos, provócase o fallo do sistema, verificando se a recuperación se leva a cabo de forma apropiada. No caso de realizarse de forma automática, avalía a inicialización, os mecanismos de recuperación do estado do sistema, os datos e todos aqueles recursos que se vexan implicados.

As verificacións das probas de implantación e as probas do sistema teñen moitos puntos en común ao compartir algunhas das fontes para o seu deseño, como poden ser os casos para probar o rendemento (probas de sobrecarga ou de stress).

O responsable de implantación xunto ao equipo de desenvolvemento determina as verificacións necesarias para realizar as probas así como os criterios de aceptación do sistema. Estas probas realízaas o equipo de operación, integrado polos técnicos de sistemas e de operación que recibiron previamente a formación necesaria para levalas a cabo.

#### *38.3.6 Probas de aceptación*

O obxectivo das **probas de aceptación** é validar que un sistema cumpre co funcionamento esperado e permitirlle ao usuario do devandito sistema que determine a súa aceptación desde o punto de vista da súa funcionalidade e rendemento.



As probas de aceptación son definidas polo usuario do sistema e preparadas polo equipo de desenvolvemento, aínda que a execución e aprobación final lle corresponden ao usuario. Estas probas van dirixidas a comprobar que o sistema cumpre os requisitos de funcionamento esperado —recollidos no catálogo de requisitos e nos criterios de aceptación do sistema de información— e conseguir así a aceptación definitiva do sistema por parte do usuario.

O responsable dos usuarios debe revisar os criterios de aceptación que se especificaron previamente no plan de probas do sistema e, posteriormente, dirixir as probas de aceptación final. A validación do sistema conséguese mediante a realización de probas de caixa negra, que demostran a conformidade cos requisitos e que se recollen no plan de probas; este define as verificacións que hai que realizar e os casos de proba asociados. O devandito plan está deseñado para asegurar que se satisfán todos os requisitos funcionais especificados polo usuario, tendo en conta tamén os requisitos non funcionais relacionados co rendemento, a seguridade de acceso ao sistema, aos datos e procesos, e aos distintos recursos do sistema.

A formalidade destas probas dependerá en maior ou menor medida de cada organización e virá dada pola criticidade do sistema, o número de usuarios implicados nelas e o tempo do que se dispoña para levalas cabo, entre outros.

Se o software se desenvolve como un produto que vai ser usado por moitos clientes, non é práctico realizar probas de aceptación formais para cada un deles. A maioría dos desenvolvedores de produtos de software levan a cabo un proceso denominado “proba alfa e beta para” descubrir erros que pareza que só o usuario final pode descubrir.

A **proba alfa** lévase a cabo por un cliente no lugar de desenvolvemento. Úsase o software de forma natural, co desenvolvedor como observador do

usuario, e rexistrando os erros e os problemas de uso. As probas alfa efectúanse nun contorno controlado.

A **proba beta** lévase a cabo polos usuarios finais do software nos lugares de traballo dos clientes. Ao contrario da proba alfa, normalmente o desenvolvedor non está presente. Así, a proba beta é unha aplicación “en vivo” do software nun contorno que non pode ser controlado polo desenvolvedor. O cliente rexistra todos os problemas (reais ou imaxinarios) que atopa durante a proba beta e informa a intervalos regulares ao desenvolvedor. Como resultado dos problemas comunicados durante a proba beta, o desenvolvedor do software leva a cabo modificacións e así prepara unha versión do produto de software para toda clase de clientes.

## Bibliografía

R. Pressman, *Software Engineering*, Editorial McGraw-Hill. 2009.

Ian Sommerville, *Ingeniería de Software*, 7.<sup>a</sup> Edición. Editorial Prentice Hall, 2005.

Carlo Ghezzi, Mehdi Jazayeri, Dino Mandrioli, *Fundamentals of Software Engineering*. Ed. Prentice-Hall. 200.

*Métrica 3 - Técnicas y Prácticas*. Ministerio de Administraciones Públicas.

**Autor: Francisco Javier Rodríguez Martínez**

**Subdirector da Escola Superior de Enxeñería Informática**

**Universidade de Vigo**



## **39. MODELOS DE CALIDADE. ENXEÑARÍA DE PROCESOS DE SOFTWARE: CMMI, ISO 15504, ISO 9000-3. MODELOS ÁXILES. SEGURANZA NOS SISTEMAS DE INFORMACIÓN.**

## **Tema 39: Modelos de calidade. Enxeñería de procesos de software: CMMI, ISO 15504, ISO 9000-3. Modelos áxiles.**

### ÍNDICE

#### 1- Introducción ao concepto de calidade

##### 1.1 Calidade do software

#### 2- Modelos de Calidade

##### 2.1 Modelo de calidade clásico de McCall

##### 2.2 CMM- CMMI

##### 2.3 Spice e a norma ISO 15504

##### 2.4 ISO 9000-3

##### 2.5 Modelos Áxiles.

## **1. Introducción ao concepto de calidade**

Ao longo do tema imos tratar a calidade coma un elemento básico que nos vai permitir valorar de xeito obxectivo determinados sistemas de información. Antes de entrarmos en detalle acerca de que representa a calidade no ámbito dos sistemas de información, e que mecanismos existen á nosa disposición para garantir un alcance mínimo desta medida cualitativa, precísase inicialmente acordar que entendemos por calidade.

A calidade, en xeral, podemos definila coma unha propiedade intrínseca de calquera cousa, que nos vai permitir poder comparala con outra entidade da mesma especie, co obxecto de determinar para certos aspectos cal presenta un mellor grao de satisfacción para un propósito determinado. O concepto actual de **calidade** procede do mundo empresarial e, máis concretamente, do dos procesos produtivos. No mundo empresarial é relativamente frecuente atopar o termo calidade asociado a outros conceptos tales como eficacia, eficiencia ou produtividade. Pódense atopar múltiples definicións do concepto de calidade, case tantas como autores falan sobre a materia:

- *“Propiedade ou conxunto de propiedades inherentes a algo, que permiten xulgar o seu valor”*. Real Academia da Lingua.
- *“O conxunto de todas aquelas propiedades e características dun produto ou servizo que se refiren á súa capacidade para satisfacer unhas necesidades implícitas ó explícitas”*. ISO. Aquí observamos que está orientada a satisfacer ao cliente, máis que a obter un produto ben feito.
- *“Un modelo sistemático e planificado de todas as accións necesarias para proporcionar a adecuada confianza que o proxecto precisa para os requirimentos establecidos”*. IEEE.



- “O conxunto de accións que permite asegurar que o produto responde ás necesidades expresadas polo usuario”. Marta D’Amore.
- “Consiste en deseñar, producir e servir un ben ou un servizo que sexa útil, o máis económico posible, e sempre satisfactorio para o usuario”. Ishikawa.

As definicións anteriores presentan a idea de satisfacción de necesidades. Fundaméntanse en que un compoñente básico da calidade é a percepción que teñen os clientes do produto en función do que esperan del. De forma sinxela, a satisfacción do cliente pódese definir como a diferenza entre as expectativas e a percepción do cliente respecto do produto ou servizo. A interpretación do termo calidade veu cambiando progresivamente, desde o concepto inicial de calidade aplicado ao produto ata chegar ao actual de calidade aplicado a toda a organización. Esta evolución foi pasando polas seguintes etapas:

- *Orientada ao produto:* **Inspección** despois da produción, auditoría sobre produtos acabados e actividades de resolución de problemas. É a fase inicial que algunhas empresas aínda hoxe non superaron.
- *Orientada ao proceso:* **Control da Calidade** durante a fabricación, incluíndo o Control Estatístico do Proceso.
- *Orientada ao sistema:* **Aseguramento da Calidade**, involucrando a todos os departamentos e, en certo modo, tamén aos provedores.
- Orientada cara á xestión: **Xestión da Calidade**, enfocada ao cliente, considerando a participación do persoal, baseada no desenvolvemento dos procesos e na mellora continua.
- *Orientada cara á excelencia* empresarial ou cara ás persoas: Corresponde á chamada **Calidade Total**, e apunta máis alá da calidade dos produtos e da eficiencia dos procesos para fixarse na organización na súa globalidade.



Estas etapas non están enfrontadas, senón que cada vez son máis extensas, de modo que cada etapa engloba a anterior.

A **Xestión da Calidade** representa a función dentro dunha organización que determina e aplica as políticas de calidade. En termos máis normalizados, a xestión da calidade aparece definida polas normas UNE-EN ISO 9000:2000 como as actividades coordinadas para dirixir e controlar unha organización no relativo á calidade. Inclúe actuacións como o establecemento da política da calidade e os obxectivos da calidade, a planificación da calidade, o control da calidade e a mellora da calidade.

A **calidade total** (Total Quality Management, TQM) representa o conxunto de principios e métodos nunha estratexia global para conseguir a dinamización da organización e a satisfacción do cliente. A calidade total xestiónase mediante un modelo de Xestión de Calidade Total (TQM) que representa a propia estratexia orientada a crear unha conciencia de calidade en todos os procesos da organización. A norma ISO 8402 defínea como *“Forma de xestión dunha organización centrada na calidade, baseada na participación de todos os seus membros e que pretende un éxito a longo prazo mediante a satisfacción do cliente e beneficios para todos os membros da organización e para a sociedade”*. Os aspectos máis salientables que a identifican son:

1. A participación de todos os profesionais no proceso de mellora continua. Todo o persoal da organización é axente e responsable da calidade.
2. Todas as actividades da organización están comprendidas na obtención da calidade.
3. A implicación da dirección na planificación, organización e asignación de recursos para a calidade, asumindo o papel de verdadeiros motores do cambio cultural da súa organización.
4. Unha cultura baseada en considerar o cliente como centro da nosa actividade. Unha forma de facer en positivo, exenta de



mecanismos de control punitivos, enfocada á superación de metas, tanto profesionais coma persoais.

5. O concepto cliente, desenvolvido na súa dobre versión de clientes internos e externos.
6. A prevención como un fin; o lema debe ser “facelo ben á primeira”. Empezando polo recoñecemento do erro, rompendo a permanente situación de negación das equivocacións e a detección de problemas como método de mellora.
7. O custo da non-calidade. A formulación de que a calidade vai ligada ao binomio custo-eficacia e de que os erros supoñen custos adicionais.

### *1.1 Calidade do software*

A calidade no software é unha preocupación actual á que se dedican cada vez máis esforzos. A dependencia tecnolóxica actual en todos os sectores fai necesario establecer sistemas operativos que proporcionen alto rendemento e fiabilidade para o control de tarefas que poden abranguer desde o máis sinxelo ata o máis crítico. Por iso o concepto de calidade ten un peso específico, debido a que está ligado a todo un conxunto de procedementos que permiten, ademais de ponderala, asegurar que se acadan uns mínimos razoables de calidade que permiten garantir que se cumpren determinadas expectativas para os usuarios. En calquera caso, cómpre poñer de manifesto que o software case nunca é perfecto; porén, todo proxecto de software debe formularse como obxectivo producir software da mellor calidade posible.

No caso do software, a calidade do produto software diferénciase da calidade doutros produtos de fabricación industrial debido ás características especiais que ten o propio software, tales como:



- É un produto abstracto, non restrinxido polas leis da física ou polos límites dos procesos de fabricación, e a súa calidade tamén o é.
- Desenvólvese, non se fabrica; polo tanto, o custo e os erros xéranse fundamentalmente na fase de deseño e non na de produción.
- Non se deteriora co tempo. Os problemas que xorden durante o mantemento estaban alí desde o principio, é dicir, non se xeran novos erros.
- O software con erros non se rexeita. Asímesse que é inevitable que o software presente erros.

Tamén é importante salientar que a calidade dun produto software debe considerarse en todos os seus estados de evolución (especificacións, deseño, código...) e non abonda con ter en conta só a calidade do produto unha vez finalizado. É dicir, como primeira aproximación ao concepto de calidade do software, é importante diferenciar entre a calidade do produto e a calidade do proceso de desenvolvemento. Non obstante, as metas que se fixen para a primeira van determinar as que se establezan para a segunda, xa que a calidade do produto vai estar en función da calidade do proceso de desenvolvemento.

Simplificando, poderíamos definir a **calidade do software** como a “creación de produtos software que, tanto eficaz como eficientemente, dean completa satisfacción ao usuario”. Esta definición merece algúns comentarios:

- 1– A calidade débese supeditar ao **grao** no cal un cliente ou usuario percibe que o software cumpre as súas expectativas. A palabra "grao" implica unha valoración cuantitativa. Neste sentido, as métricas constitúen unha ferramenta que axuda a cuantificar aspectos da calidade, de forma que esta sexa medible.



- 2- Na calidade interveñen os conceptos de **eficiencia** e de **eficacia**. Eficiencia é a capacidade para facer as cousas ben (“do things right”). Por exemplo, os desenvolvedores realizan as súas actividades correctamente, cometendo poucos erros. Eficacia, ou efectividade, é a capacidade para facer as cousas adecuadas (“do the right things”). Por exemplo, os desenvolvedores levan a cabo as tarefas adecuadas.
- 3- A calidade ten un enfoque dirixido ás **características do produto**. En consecuencia, en primeiro lugar hai que documentar, logo discutir, xa que pode haber distintos puntos de vista en canto ás percepcións e ás expectativas de cada usuario, e para rematar, consensuar. Estes pasos dan lugar a un proceso iterativo ata chegar ao consenso, que pasa por determinar os factores e criterios que interveñen na calidade do software, e por cuantificar eses factores e criterios.

Outros autores teñen dado definicións distintas para o concepto de calidade do software. Así, por exemplo, o IEEE define a calidade do software como o “graoo co cal un cliente ou usuario percibe que o software satisfai as súas expectativas”. JONES, sinala que a calidade do software é a “ausencia de defectos ou erros, sendo estes as desviacións respecto ao comportamento esperado”. Por último, PRESSMAN sinala que “calidade é a conformidade cos requisitos que se declararon explicitamente sobre funcionalidade e rendemento, cumprimento de estándares ou normas documentadas que se estableceron, e existencia doutras características implícitas que son de esperar nun produto desenvolvido nun contexto de práctica profesional”.

En calquera caso, os principais problemas aos que nos enfrontamos á hora de falar da calidade dun produto software son:

- **A definición mesma da calidade do software.** É realmente posible atopar un conxunto de propiedades nun produto



software que nos dean unha indicación da súa calidade? Para iso defínense os **factores** e os **criterios** de calidade.

- **A comprobación da calidade.** Como medir o grao de calidade dun produto software en función das súas propiedades? Para iso defínense as **métricas** de calidade.
- **A mellora da calidade do software.** Como utilizar a información dispoñible sobre a calidade do produto software para mellorar a súa calidade ao longo do ciclo de vida de desenvolvemento? Para iso defínense as actividades construtivas da garantía de calidade do software.

### 39.2 Modelos de calidade

A consecuente preocupación derivada da necesidade de elevar o control da calidade nas organizacións serviu para impulsar a aparición de varios modelos e sistemas de potenciación desta, modelos cos que se pretende estimar ou valorar en que grao a organización en cuestión alcanza o nivel de calidade acorde co modelo aplicado.

Xa que logo, podemos definir, de forma xeral, un **modelo de calidade** como o conxunto de ferramentas que conducen ás Organizacións á Mellora Continua e á Competitividade, dando as especificacións de que tipo de requisitos deben implantar para poder brindar produtos e servizos de alto nivel.

Como xa se comentou, existe unha gran cantidade de modelos de calidade que establecen mecanismos e procedementos de implantación e valoración de característica. Os máis coñecidos e aplicados internacionalmente son os correspondentes ás normas **ISO**. Porén, existen tamén outras alternativas como o Modelo Deming en Xapón, o Modelo Malcolm Baldrige en Estados Unidos, e o Modelo de Excelencia da EFQM, en Europa.



O modelo de Excelencia da EFQM (Fundación Europea para a Xestión da Calidade) introduciuse en 1991 como o marco de traballo para a autoavaliación das organizacións e como base para xulgar os concursantes polo Premio Europeo da Calidade. Este modelo é o máis amplamente empregado en Europa en materia de calidade, e está orientado a axudar a crear organizacións fortes que practiquen os principios da administración da calidade total (TQM) nos seus procesos de negocio e relacións con clientes, empregados, accionistas e comunidades nas que operan.



*Esquema de ponderación proposto polo Modelo de Excelencia da EFQM*

A xestión da calidade (*conxunto de actividades e medios necesarios para definir e implantar un sistema da calidade e responsabilizarse do seu control, aseguramento e mellora continua*) nas empresas ou organizacións de software seguiu dúas liñas que se poden complementar entre si perfectamente. Por unha banda, seguiu a liña marcada polas entidades internacionais de estandarización para todos os produtos e servizos a través das normas ISO 9000, e por outra, o mundo do software creou a súa propia liña de traballo na



xestión da calidade, centrándose nos procesos de produción de software como medio de asegurar a calidade do produto final.

Cando os estándares de calidade se orientaban sobre todo ao control, nas organizacións dedicadas ao software aparecen un grupo de modelos específicos con ese fin (modelos de calidade tradicionais), como: o Modelo FCM (*Factors/Criteria/Metrics*) de McCall (1977), o Modelo de Boehm (1978), o Marco ISO 9126 (ISO/IEC, 1991), o Paradigma GQM (*Goal-Question-Metric*) de Basili e Rombach (1988), o Modelo de Gilb (1988), etc.

Nos últimos anos en que os estándares de calidade internacionais evolucionaron cara ao aseguramento da calidade, primeiramente, e cara á calidade total, definitivamente, apareceron na industria do software dous importantes modelos de referencia que teñen en común a avaliación da capacidade dos procesos en niveis de desenvolvemento ou madurez: o Modelo CMM - CMMI (*Capability Maturity Model - Capability Maturity Model Integration*) (Paulk, 1993), e o Modelo SPICE (*Software Process Improvement and Capability determination*) (Rout, 1995), (SPICE, 1999), que veremos en apartados posteriores.

## **2.1 Modelo de calidade clásico de McCall**

O modelo de Jim McCall é un modelo de calidade clásico desenvolvido inicialmente para a forza aérea dos EEUU en 1977. É un dos modelos de calidade do software de xestión máis difundidos, e que serviu como base para outros modelos, como o de Boehm, ou o Software Quality Management -SQM- de Murine. Este modelo procura reducir a brecha entre usuarios e desenvolvedores centrándose nun número de factores de calidade que reflictan as prioridades de ambos os dous.



O modelo de calidade McCall está organizado sobre tres tipos de Características de Calidade:

- **Factores** (especificar): Describen a visión externa do software, como é visto polos usuarios.
- **Criterios** (construír): Describen a visión interna do software, como é visto polo desenvolvedor.
- **Métricas** (controlar): Defínense e úsanse para prover unha escala e método para a medida.

O modelo descríbennos 11 factores de calidade do software, para os cales establece 23 criterios e 41 métricas.

Os **factores de calidade** representan a calidade desde o punto de vista do usuario. Son, pois, elementos externos, e fan referencia, segundo o Modelo de McCall (ou **Modelo FCM**) ao comportamento actual do software (operación do produto), á facilidade de cambio do software (revisión do produto) e á facilidade de conversión do software (transición do produto). Os once factores son:

- 1– **Corrección:** Mide ata que punto un produto software cumpre as súas especificacións e satisfai os obxectivos requiridos polo usuario. Valórase segundo os seguintes aspectos:
  - ☐ Compleitude: Atributos do software que proporcionan a implementación completa de todas as funcións requiridas.
  - ☐ Consistencia: Atributos do software que proporcionan uniformidade nas técnicas e notacións de deseño e implementación.
  - ☐ Trazabilidade ou rastrexabilidade: Atributos do software que proporcionan unha traza desde os requisitos á implementación respecto dun contorno operativo concreto.
- 2– **Fiabilidade:** Mide ata que punto un produto software realiza as funcións previstas no seu deseño, coa precisión necesaria. É



dicir, ata que punto se pode confiar no funcionamento sen erros do software. Factores:

1. Precisión: Atributos do software que proporcionan o grao de precisión requirido nos cálculos e os resultados.
  2. Consistencia.
  3. Tolerancia a fallos: Atributos do software que posibilitan a continuidade do funcionamento baixo condicións non usuais.
  4. Modularidade: Atributos do software que proporcionan unha estrutura de módulos altamente independentes.
  5. Simplicidade: Atributos do software que posibilitan a implementación de funcións do xeito máis comprensible posible.
  6. Exactitude: A precisión dos cálculos e do control.
- 3– **Eficiencia:** Mide o grao de optimización co que o software utiliza os recursos informáticos para realizar a función que lle foi asignada (Consume os recursos Hw e Sw de forma óptima?).
- 4– **Integridade** (seguridade): Mide ata que punto se poden controlar os accesos ilegais (por persoas non autorizadas) aos programas e aos datos. Factores:
1. Control de accesos. Atributos do software que proporcionan control de acceso ao software e aos datos que manexa.
  2. Facilitade de auditoría: Atributos do software que facilitan a auditoría dos accesos ao software.
  3. [Seguridade: A dispoñibilidade de mecanismos que controlen ou protexan os programas ou os datos.](#)
- 5– **Usabilidade, facilidade de uso ou dispoñibilidade):** Mide o esforzo e custo necesarios para aprender, operar, preparar a entrada e interpretar a saída dun produto software. Isto é, para aprender a manexar o produto. (É cómodo e fácil de usar?).

- 6– **Mantibilidade** (facilidade de mantemento): Mide o esforzo e custo necesario para localizar e corrixir un erro nun produto software que estea operativo. (É susceptible de corrixirse?).
- 7– **Verificabilidade (facilidade de proba)**: Mide o esforzo e custo necesarios para verificar un produto software co fin de garantir que realiza a función prevista. Isto é, o esforzo e custo de probar un programa para comprobar que satisfai os seus requisitos. (Pódese probar?).
- 8– **Flexibilidade**: Mide o esforzo e custo necesarios para modificar un produto software operativo. (Pódese modificar?).
- 9– **Portabilidade**: Mide o esforzo e custo necesarios para transferir un produto software dunha configuración e/ou contorno de hardware a outro. (Pódese utilizar noutro equipo?).
- 10– **Reusabilidade (reutilizabilidade)**: Mide ata que punto se pode utilizar un produto software noutras aplicacións. É dicir, ata que punto se pode transferir un módulo ou programa a outra aplicación e con que esforzo. (Pode ser rendible total ou parcialmente noutras aplicacións?).
- 11– **Interoperabilidade**: Mide o esforzo e custo necesarios para axustar un sistema a outro; é dicir, para conectar dous produtos entre si. (Pode colaborar con outros produtos software?).

Estes factores pódense agrupar en tres grupos:

- Os factores de calidade que fan referencia ao comportamento actual do software (operación ou explotación do produto): Corrección, Fiabilidade, Eficiencia, Integridade e Usabilidade.
- Os que fan referencia á facilidade de cambio do produto (revisión): Mantibilidade, Verificabilidade e Flexibilidade.
- Os que se refiren á facilidade de conversión do software (transición do produto): Portabilidade, Reusabilidade e Interoperabilidade.





Cada un dos factores de calidade descomponse nun conxunto de **criterios** ou atributos internos de calidade que, cando están presentes, contribúen ao aspecto da calidade que o factor asociado representa. Trátase, pois, dunha visión da calidade desde o punto de vista do produto software. Xa que logo, os criterios de calidade son elementos internos ou dos realizadores do software e fan referencia á forma e estrutura dos programas, os datos e os documentos. A relación entre os factores de calidade e os criterios pódese ver na seguinte táboa:

<b>factores de calidade</b>	<b>criterios de calidade</b>
corrección	trazabilidade, completitude, coherencia
fiabilidade	coherencia, precisión, tolerancia a erros, simplicidade
eficiencia	eficiencia de memoria, eficiencia de execución
integridade	confidencialidade, control de accesos
usabilidade	operatividade, facilidade de aprendizaxe, comunicabilidade
mantibilidade	coherencia, simplicidade, modularidade, autodescrición, concisión
verificabilidade	simplicidade, modularidade, instrumentación, autodescrición
flexibilidade	modularidade, xeneralidade, expansibilidade, autodescrición
portabilidade	modularidade, autodescrición, independencia do contorno hardware, independencia do contorno software
reusabilidade	modularidade, xeneralidade, autodescrición, independencia do contorno hardware, independencia do contorno software

interoperabilidade	modularidade, estandarización de interfaces, estandarización de datos
--------------------	--

Por último, ao planificar a calidade dun produto hai que especificar para cada criterio o nivel de calidade que se considera aceptable; é dicir, o valor mínimo ou máximo aceptable. Xa que logo, para cada un dos criterios de calidade é necesario definir un conxunto de **métricas**, que son medidas cuantitativas de certas características do produto que, cando están presentes, dan unha indicación do grao en que o devandito produto posúe un determinado atributo de calidade.

As **métricas de calidade**, na súa maior parte medidas subxectivas, permiten a cuantificación dos factores e os criterios de calidade. Fundamentan a súa avaliación na medida dos factores de calidade do software a través dos criterios de calidade e baséanse no exame detallado dos produtos xa en proceso, aínda que tamén requiren unha análise estática das especificacións, deseño e programación das aplicacións.

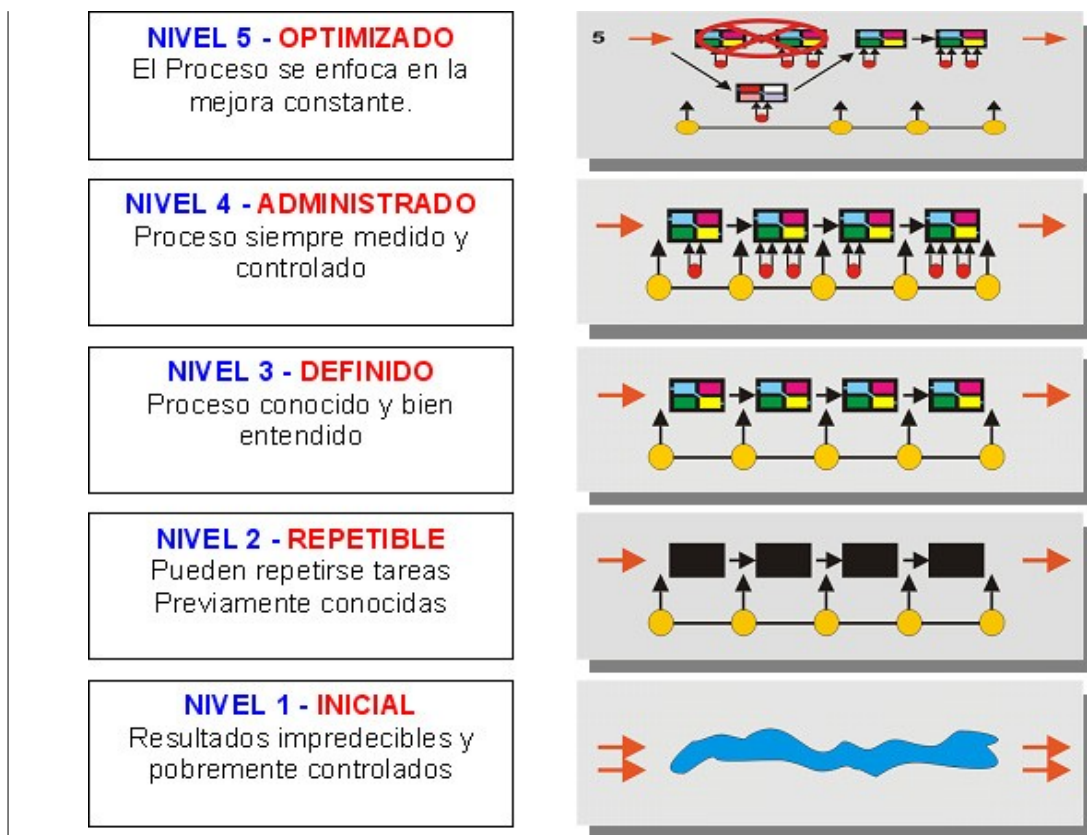
## 2.2 CMM-CMMI

O modelo CMM inicial representa un modelo para a avaliación dos procesos dunha organización, desenvolvido inicialmente para os procesos relativos ao desenvolvemento e implementación de software pola Universidade Carnegie-Mellon. O modelo CMM permite definir o grao de madurez das prácticas de xestión e reenxeñería de software das devanditas organizacións e determinar cales son as accións de mellora prioritarias para os seus procesos de software.

O modelo CMM componse de **cinco niveles de madurez**, de acordo coa capacidade do proceso de software, definidos polos obxectivos dos procesos que, cando son satisfeitos, permiten evolucionar ao



próximo nivel, dado que un ou máis compoñentes importantes do proceso de software foron estabilizados.



En cada nivel defínense un conxunto de **áreas clave do proceso** que describen as funcións de enxeñería do software que se deben levar a cabo para o desenvolvemento dunha boa práctica. Mediante un amplo conxunto de métricas determínase a calidade de cada unha das áreas clave, obténdose unha visión precisa do rigor, a eficacia e a eficiencia da metodoloxía de desenvolvemento dunha organización produtora de software.

Cada unha das áreas está organizada en cinco seccións, denominadas **características comúns**. Son as seguintes:

- **Compromiso.** É o conxunto de accións que a organización debe realizar para poder asegurar que o proceso é repetible e duradeiro. Normalmente está relacionado coas políticas da organización e o liderado da dirección.



- **Capacidade.** Describe as precondicións que se deben dar nun proxecto ou na organización para implantar de forma efectiva os procesos de software. Habitualmente afecta aos recursos, á estrutura e á formación.
- **Actividades.** Describen os roles e os procedementos necesarios para implantar unha área clave de proceso. Habitualmente inclúen procedementos relacionados coa planificación e o seguimento do traballo, así coma as accións correctivas necesarias.
- **Medidas e análises.** Describen a necesidade de realizar medicións dos procesos e analizan as tales medidas. Adoitan incluír exemplos das medidas tomadas para determinar o estado e a eficacia das actividades realizadas.
- **Verificación.** Describe os pasos que cómpre levar a cabo para asegurar que as actividades se realizan segundo os procesos establecidos. Habitualmente inclúe revisións e auditorías por parte da dirección e do grupo de aseguramento da calidade.

Pola súa banda, en cada característica común especifícanse unhas **prácticas clave**, que son normas, procedementos e actividades cuxa realización leva á consecución dos obxectivos da área. Nalgúns casos detállanse subprácticas máis específicas, guías e interpretacións da práctica e, cando procede, exemplos e referencias cruzadas a outras prácticas. Así mesmo, o modelo define **indicadores clave**, que son aquelas prácticas clave ou compoñentes de prácticas clave que ofrecen unha visión maior da consecución dos obxectivos dunha área clave de proceso.

Os cinco niveles de madurez, representados na imaxe anterior, que forman parte do modelo son:

- 1- **Inicial:** o proceso de software é un proceso improvisado e caótico. Non se definiron procesos metodolóxicos, ou definíronse pero non se seguen. O éxito que se poida obter



depende das habilidades, coñecementos e motivacións do persoal. Non existen calendarios nin estimacións de custos e as funcionalidades e calidade do produto son imprevisibles, nin tampouco un ambiente estable para o desenvolvemento e mantemento do software. O proceso do software é imprevisible polo cambio ou modificación continuos a medida que avanza o traballo.

- 2- **Repetible:** establécense políticas e procedementos de administración e implantación do proceso básico para determinar custos, calendarios e funcionalidades. A madurez metodolóxica da organización permite estimar de maneira fiable o tamaño funcional ou físico do sistema, así como recursos, esforzo, custos e calendario. Sentáronse as bases para repetir éxitos anteriores en proxectos con aplicacións similares. A organización amosa problemas de calidade e carece dunha estrutura adecuada para melloralas. Neste nivel, as áreas clave, cuxo estado se pode coñecer mediante diversas métricas, son as seguintes:

- Xestión de requisitos.
- Planificación do proxecto software.
- Seguimento e control do proxecto.
- Xestión da subcontratación do software.
- Aseguramento da calidade do software.
- Xestión da configuración do software.

- 3- **Definido:** o proceso de software para as actividades administrativas e técnicas está documentado, homoxeneizado e integrado nun proceso de software estándar dentro da organización que axudará a lograr un desempeño máis efectivo. O grupo que traballa no proceso centra e conduce os seus esforzos á mellora do seu desenvolvemento, facilita a introdución de técnicas e métodos e informa a administración



do estado do proceso. A capacidade do proceso está baseada nunha ampla comprensión común dentro da organización das actividades, roles e responsabilidades definidas no desenvolvemento de software. As áreas claves, definidas para este nivel, son as seguintes:

- Desenvolvemento e mellora dos procesos da organización.
- Definición dos procesos da organización.
- Programa de formación.
- Xestión integrada do software.
- Enxeñería de produto software.
- Coordinación intergrupos.
- Revisión conxunta.

4- **Xestionado:** recóllense medidas detalladas do proceso de software e da calidade do produto. Ambos son cuantitativamente entendidos e controlados. Este nivel de capacidade permítelle á organización predicir as tendencias na calidade do produto dentro dos límites establecidos e tomar as accións necesarias en caso de que se excedan. Pódese predicir que os produtos desta categoría son de alta calidade. As áreas clave definidas para este nivel son as seguintes:

- Xestión cuantitativa do proxecto.
- Xestión de calidade do software.

5- **Optimizado:** a mellora continua do proceso é garantida pola retroalimentación cuantitativa e a partir das probas de técnicas e ferramentas innovadoras. A organización dispón dos medios para identificar os puntos débiles e saber como fortalecelos. A súa actividade clave é a análise das causas dos defectos e a súa prevención. As áreas clave definidas para este nivel son:

- Prevención de defectos.
- Xestión de cambios tecnolóxicos



A estrutura do CMM brinda un camiño progresivo recomendado para as organizacións dedicadas ao desenvolvemento de software que queren mellorar a capacidade do seu proceso de software. De forma xeral identifícanse os seguintes **usos fundamentais**:

- Equipos de asesores, que empregan o modelo para identificar os puntos fortes e débiles na organización.
- Equipos de avaliación, que utilizan CMM para identificar o risco de seleccionar entre diferentes contratos de negocio e para monitoralos.
- Persoal técnico e de dirección, que usa CMM para entender aquelas actividades necesarias que axudan a planificar e implantar o programa de mellora do proceso de software da organización.
- Grupo de mellora do proceso, que o empregan como guía para axudar a definir e mellorar o proceso de software na organización.

Desde o ano 1991, o modelo CMM foise adaptando a múltiples disciplinas: Enxeñería de sistemas, Enxeñería do Software, compras, desenvolvemento de procesos e produtos integrados, etc., derivando modelos diferentes. A principal adaptación do modelo está orientada ao desenvolvemento software. O Modelo de Madurez da Capacidade do Software **SW-CMM** (*Software Capability Maturity Model*) foi definido por Paulk, Curtis, Chrisis e Weber en 1993 coma un modelo que establece os niveis polos que as organizacións de software fan evolucionar as súas definicións, implementacións, medicións, controles e melloras dos seus procesos de software. Ademais do Modelo de Madurez da Capacidade do Software existen o Modelo de Madurez da Capacidade na Adquisición de Software (SA-CMM), e o Modelo de Madurez da Capacidade das Persoas (P-CMM), etc. As organizacións que desexaban mellorar os seus procesos en todas estas disciplinas encontrábanse con que o modelo presentaba

grandes diferencias de arquitectura, enfoque, contido e aplicación.

Este feito provocaba un grande incremento no custo da implantación de CMM en canto a formación, avaliacións e actividades de mellora, xa que non existía unha integración de todos estes modelos. O proxecto de integración de CMM ou CMMI (Capability Maturity Mode of Software Integration) xurdiu como solución aos problemas de falta de integración e púxose en marcha para desenvolver un marco de traballo sinxelo de mellora de procesos destinado a organizacións que aspiran a mellorar en todos os ámbitos e niveis da empresa.

**CMMI** contén un conxunto de produtos que, ademais de numerosos modelos adaptables ás diferentes áreas de coñecemento, contén métodos de avaliación segundo cada modelo, así como material de formación. O obxectivo inicial de CMM — “obter produtos de calidade dentro das marxes temporais previstas co mínimo custo”— non mudou en CMMI. En cambio, CMMI basea a aplicación de todos os principios de CMM ao longo de todo o ciclo de vida de enxeñería, non unicamente durante o ciclo de vida do desenvolvemento do produto software. Ademais, o conxunto de produtos CMMI foi deseñado para manter compatibilidade e correspondencia co modelo **SPICE**. En resumo, CMMI pode ser considerado como unha extensión do CMM-SW. As diferenzas principais son:

- Engadíronse novas áreas de proceso.
- Engadíronse mellores e máis modernas prácticas clave.
- Engadiuse un obxectivo xenérico para cada área de proceso.

Se se analizan estas diferenzas en función do Nivel de madurez en que se atopan, pódense encontrar as seguintes áreas de proceso no modelo CMMI que non se atopan no modelo CMM:

- **Nivel 2.** Medición e análise. Foron illadas de CMM todas as prácticas relacionadas con este obxectivo e agrupáronse dentro desta nova área de proceso.





- **Nivel 3.** A área Enxeñería do produto software de CMM foi substituída en CMMI por múltiples e máis detalladas áreas de proceso:
  - o Desenvolvemento de requisitos.
  - o Solucións técnicas.
  - o Integración do produto.
  - o Verificación e Validación.

Na área de Xestión integrada do proxecto de CMM tíñase en conta a Xestión de riscos, pero agora considérase como unha área de proceso independente. Finalmente, a este Nivel engadíuselle unha nova área denominada Análise de decisións e resolución, que non se atopaba en CMM.

- **Nivel 4.** Este Nivel sufriu unha reestruturación e as áreas de Xestión cuantitativa de procesos e Xestión da calidade de software foron convertidas a Xestión cuantitativa do proxecto e Rendemento ou realización do proceso organizacional, respectivamente.
- **Nivel 5.** Tampouco houbo grandes cambios neste Nivel, simplemente unha fusión das áreas de Xestión dos cambios tecnolóxicos e Xestión do cambio nos procesos nunha única área de proceso: Innovación organizacional e despregamento. A área de Prevención de defectos foi reestruturada e rebautizada Análises causal e resolución.

CMMI v1.1 ten catro disciplinas dispoñibles:

- Enxeñería de Software: CMMI-SW (Software Engineering)
- Enxeñería de sistemas: CMMI-SE (Systems Engineering)
- Desenvolvemento integrado do produto e do proceso: CMMI-IPPD (Integrated Product and Process Development)
- Proveedores externos: CMMI-SS (Supplier Sourcing)



- **Continua:** capacidade de cada área de proceso. Nesta representación enfócase a capacidade de cada área de proceso de establecer unha liña a partir da cal pode medirse a mellora individual en cada área. Do mesmo xeito que o modelo por etapas, o modelo continuo ten áreas de proceso que conteñen prácticas, pero estas organízanse de maneira que soportan o crecemento e a mellora dunha área de proceso individual. Hai seis niveles de capacidade, do 0 ao 5. A representación continua céntrase en seleccionar unha certa área de procesos que mellorar e en fixar o nivel de capacidade desexado para esa área.
- **Por etapas:** madurez organizacional. Nesta representación dáse un mapa predefinido dividido en etapas (os niveis de madurez) para a mellora organizacional e que se basea en procesos probados, agrupados e ordenados e as súas relacións asociadas. Cada nivel de madurez ten un conxunto de áreas de proceso que indican onde unha organización debería enfocar a mellora do seu proceso. Cada área de proceso descríbese en relación a prácticas que contribúen a satisfacer os seus obxectivos. As prácticas describen as actividades que máis contribúen á implantación eficiente dunha área de proceso; auméntase o “nivel de madurez” cando se satisfán os obxectivos de todas as áreas de proceso dun determinado nivel de madurez.

Ambas as representacións inclúen Metas (Xenéricas e Específicas, definicións de resultados que hai que obter pola implantación efectiva dos grupos de prácticas) e Prácticas (Xenéricas e Específicas, accións que hai que realizar para cumprir obxectivos de área de proceso).



## 2.3 *Software Process Improvement Capability Determination* e a norma ISO 15504

En 1991, a ISO aprobou a realización dun estudo sobre a necesidade de crear un estándar internacional para a avaliación de procesos software, debido en gran parte ao gran número de métodos de avaliación de procesos dispoñibles, e ao uso crecente destas técnicas en áreas comerciais sensíbles. A raíz desta aprobación creouse o proxecto **SPICE (Software Process Improvement Capability Determination)** cuns obxectivos ben definidos:

- Desenvolver un borrador de traballo para un estándar de avaliación de procesos de software.
- Levar a cabo os ensaios da industria da norma emerxente.
- Promover a transferencia de tecnoloxía da avaliación de procesos de software á industria do software a nivel mundial.

O resultado deste proxecto recolleuse nun conxunto de normas que derivaron no que actualmente se coñece como familia de estándares **ISO/IEC 15504**.

O **ISO/IEC 15504** é un modelo para a mellora e a avaliación dos procesos de desenvolvemento e mantemento de sistemas de información e produtos de software. A súa filosofía é desenvolver un conxunto de medidas de capacidade estruturadas para todos os procesos do ciclo de vida e para todos os participantes.

SPICE inicialmente absorbe a escala de puntuación de capacidade de CMM; as actividades de proceso de enxeñería e ciclo de vida de ISO/IEC 12207, Trillium e CMM; a representación de capacidade baseada en perfís de atributos de BOOTSTRAP, e a experiencia do sistema de xestión da calidade xeral de ISO 9001.

O alcance de SPICE abrangue a planificación, xestión, execución, control e mellora da adquisición, provisión, desenvolvemento, operación, mantemento e soporte do software e da organización



responsable. Esta baseado nas “boas prácticas” da industria. Define os requisitos para a realización de avaliacións de procesos como punto de partida para a determinación da capacidade e mellora dos procesos. Ten unha arquitectura baseada en **dúas dimensións**: *de proceso e de capacidade de proceso*.

Hoxe en día estrutúrase en dez **partes**; as sete primeiras están xa rematadas, e da oito á dez en fase de desenvolvemento. As partes xa terminadas son:

- **Parte 1:** Conceptos e Vocabulario (publicada no 2004).
- **Parte 2:** Realización dunha Avaliación, Requisitos e Normativa (publicada no 2003).
- **Parte 3:** Guía para Realización de Avaliacións (publicada no 2004).
- **Parte 4:** Guía para o uso na mellora dos procesos e a determinación da capacidade (publicada no 2004).
- **Parte 5:** Exemplo dun Modelo de Avaliación de Procesos (publicada no 2006).
- **Parte 6:** Un exemplo de modelo de avaliación do ciclo de vida de sistema (publicada no 2008).
- **Parte 7:** Avaliación da madurez dunha organización (publicada no 2008).

Deseguido, mostramos os niveis de capacidade e os atributos dos procesos do modelo **ISO 15504**:

- 1- **Incompleto:** O proceso non está implantado ou falla á hora de alcanzar o seu propósito. Non é fácil identificar os produtos ou saídas dos procesos.
- 2- **Realizado:** O propósito do proceso lógrase normalmente, aínda que non sexa rigorosamente planificado nin levado a cabo. Hai produtos identificables que testifican o alcance do propósito.
  - o Realización do proceso.



- 3- **Xestionado:** O proceso é xestionado e os entregables, resultado de procedementos específicos, planificados e seguidos, con requisitos de calidade, tempo e recursos.
- o Xestión de realización.
  - o Xestión dos produtos do traballo.
- 4- **Establecido:** Un proceso realizado e xestionado usando un proceso definido, baseado nuns principios de boas prácticas de enxeñería do software.
- o Definición do proceso.
  - o Implantación do proceso.
- 5- **Previsible:** O proceso definido é posto consistentemente en práctica dentro de límites de control establecidos para acadar metas do proceso xa definidas. Entendemento cuantitativo da capacidade do proceso e habilidade mellorada de predicir e xestionar o rendemento.
- o Medida do proceso.
  - o Control do proceso.
- 6- **Optimizado:** Realización do proceso optimizada na procura das necesidades actuais e futuras do negocio. Obxectivos cuantitativos de eficiencia e efectividade que se establecen en función dos obxectivos da organización. A Optimización pode levar a estudar e adoptar ideas innovadoras ou produtos tecnolóxicos innovadores que inclúan e modifiquen o proceso definido.
- o Innovación do proceso.
  - o Optimización do proceso.

Para que unha organización poida alcanzar un nivel de madurez debe avaliarse fronte á norma ISO/IEC 15504. Existen 3 clases de avaliacións, clase 1, clase 2 e clase 3. As dúas últimas correspóndense con avaliacións internas e non ofrecen unha



certificación oficial, a diferenza da clase 1, que é unha avaliación máis exhaustiva e rigorosa que permite alcanzar unha puntuación oficial. En España **AENOR** ofrece este tipo de avaliacións e certificacións baixo esta norma.

Para rematar, dicir que existe equivalencia e compatibilidade con **CMMI**. ISO forma parte do panel elaborador do modelo CMMI e SEI, e viceversa, e mantense a compatibilidade e equivalencia desta última con 15504.

## **2.4 ISO 9000-3**

A Organización de Estandarización Internacional (ISO) definiu unha serie de estándares que, polo xeral, son aplicables a todos os procesos de produción.

A ISO 9000 proporciona un conxunto de estándares para a xestión da calidade en calquera actividade relacionada co proceso de produción. A ISO 9000 especializouse en todo o referente á solución do software na ISO 9000-3, posto que esta disciplina ten características propias diferentes como para distinguirse do proceso de produción en xeral.

As ideas básicas que se nos propoñen para o estándar ISO 9000-3 son as seguintes:

- O control de calidade débeseles aplicar a todas as fases da produción de software, incluído o mantemento e tarefas posteriores á súa implantación.
- Debe existir unha estrita colaboración entre a organización que adquire o software e o proveedor deste.
- O proveedor do software debe definir o seu sistema de calidade e asegurarse de que toda a organización poña en práctica este sistema.



É importante salientar que a ISO 9000-3 trata o concepto de ciclo de vida, pero en ningún momento desexa impoñer a utilización dun determinado ciclo, como pode ser o ciclo en espiral de Boeh. Pero á parte do ciclo de vida que elixamos, a ISO 9000-3 introduce outras actividades que teñen lugar de forma independente ás fases do ciclo e que son as actividades referentes á configuración, e distingue entre a verificación e validación.

Ademais, a ISO 9000-3 pode ser utilizada en relacións contractuais cando comprador e provedor establecen que algúns elementos de calidade deben formar parte do sistema de calidade que proporciona o provedor e que este se compromete a seguir os principios de calidade definidos no estándar.

A ISO 9000-3 é unha guía que está formada por unha serie de cláusulas que indican como aplicala. As cláusulas son as seguintes:

<b>NÚMER O CLÁUSULA</b>	
4.1	Administración da Responsabilidade
4.2	Sistema de Calidade
4.3	Auditorías Internas do Sistema de Calidade
4.4	Acción Correctora
5.1	Xeral
5.2	Revisión do Contrato
5.3	Especificación dos requirimentos da Organización
5.4	Planificación do desenvolvemento
5.5	Planificación da Calidade



- 5.6 Deseño e Implementación
- 5.7 Comprobación e Validación
- 5.8 Aceptación
- 5.9 Xeración, Entrega e Instalación
- 5.10 Mantemento
- 6.1 Administración da Configuración
- 6.2 Documentos de Control
- 6.3 Calidade dos Arquivos
- 6.4 Medidas
- 6.5 Regras e Convencións
- 6.6 Ferramentas e Técnicas
- 6.7 Compra
- 6.8 Produtos de software incluídos
- 6.9 Formación

A continuación, pasamos a comentar as cláusulas máis importantes:

- **Administración da Responsabilidade:** Esta cláusula permite organizar a estrutura do sistema de calidade abordando a estratexia e organización como requisitos para verificar e revisar a calidade.
- **Sistema de Calidade:** Require unha planificación e documentación do sistema de calidade, requisito coñecido como 'Plan de Garantía de Calidade do Software' ou SQAP, utilizado no estándar IEEE 730.
- **Acción correctora:** Non existe unha receita para o proceso de accións correctoras, pero o estándar IEEE 1044 pódenos ser útil para clasificar os tipos de anomalías que se poden atopar nun sistema semellante ao que estamos tratando.
- **Revisión do contrato:** Esta cláusula, aínda que aparentemente parece obvia, insiste na necesidade de que o





provedor examine os contratos referidos ao sistema de calidade.

- **Especificación dos requirimentos da Organización:** Establécese a premisa da mutua colaboración entre o provedor e a organización que adquire o produto software.
- **Planificación do desenvolvemento:** Esta cláusula sitúa os requirimentos nun plan de desenvolvemento. Particularmente a cláusula 5.4.2.1 esixe a definición dun proceso disciplinado ou metodoloxía que inclúe: fases de desenvolvemento, entradas, saídas e procesos de verificación. O estándar IEEE 1074, Procesos do Ciclo de Vida do Desenvolvemento de Software, podería resultarnos particularmente útil para satisfacer estes requirimentos.
- **Planificación da Calidade:** A metodoloxía de medidas de Calidade descrita no estándar IEEE 1061 pode sernos útil para establecer os obxectivos de calidade.
- **Deseño e Implementación / Comprobación e Validación:** Estas dúas cláusulas oríéntanse ás actividades centrais do proceso de desenvolvemento de software.
- **Aceptación:** Estas probas son máis ben xerais, dado que nos estándares do IEEE non hai definido un homólogo.
- **Xeración, Entrega e Instalación:** Os requirimentos de probas e medios de control existentes no IEEE 730 poden ser de utilidade, pero non son suficientes para abordar os contidos desta cláusula.
- **Mantemento:** Esta cláusula proporciona unha extensa lista de requirimentos de calidade para a fase de mantemento do ciclo de vida. O estándar IEEE 1219 subministra uns requirimentos detallados e importantes para levar a cabo un proceso de mantemento adecuado.



As cláusulas restantes proporcionan requisitos para as **actividades de soporte**; é dicir, aquelas que non son específicas de ningunha fase en concreto do ciclo de vida.

- **Administración da Configuración/ Documentos de Control:** As actividades que detallan estes requisitos atópanse nos chamados Plans de Xestión da Configuración do Software, os cales quedan descritos no estándar IEEE 828.
- **Medidas / Regras e Convencións / Ferramentas e Técnicas:** Estas cláusulas fálannos do uso de procedementos e ferramentas apropiados para implantar o sistema de calidade.
- **Compra / Produtos de software incluídos:** Os requisitos que rexen as compras do proveedor dos vendedores atópanse nestas dúas cláusulas.
- **Formación:** A única mención que se realiza nos estándares do IEEE atópase no estándar 730.

## 2.5 Modelos Áxiles

As metodoloxías áxiles son, sen dúbida, un dos temas recentes en enxeñería de software que están a acaparar grande interese. Os modelos áxiles son aqueles modelos con son unicamente o suficientemente bos, o que implica que exhiben as seguintes características:

1. Satisfán o seu propósito.
2. Son intelixibles.
3. Son suficientemente precisos.
4. Son suficientemente consistentes.
5. Son suficientemente detallados.
6. Achegan valor positivo.
7. Son o máis simples posible.

A orixe das metodoloxías áxiles xorde en marzo do 2001. O principal impulsor, Kent Beck, é o escritor dun libro, *Extreme Programming Explained*, no que se expoñía unha nova metodoloxía denominada Extreme Programming (Programación Extrema), fundamentada principalmente en poñer máis énfase na adaptabilidade que na previsibilidade. Beck, xunto cun grupo de críticos, analizou unha reformulación dos modelos de mellora do desenvolvemento de software baseados en procesos .

Na reunión acuñouse a expresión **Métodos Áxiles** para definir os métodos que estaban a xurdir como alternativa ás metodoloxías formais (*CMMI*, *SPICE*), que se consideraban excesivamente “pesadas” e ríxidas polo seu carácter normativo e a súa forte dependencia de planificación detallada previas ao desenvolvemento. Os integrantes da reunión resumiron os principios sobre os que se basean os métodos alternativos en catro postulados que quedaron acuñados como **Manifesto Áxil**.

Os **catro postulados** do Manifesto Áxil son:

- **Valorar máis os individuos e a súa interacción que os procesos e as ferramentas.** Este é posiblemente o postulado máis importante do manifesto. Por suposto que os procesos axudan ao traballo. Son unha guía de operación. As ferramentas melloran a eficiencia, pero sen persoas con coñecemento técnico e actitude adecuada non producen resultados. Os procesos deben ser unha axuda e un soporte para guiar o traballo. Débense adaptar á organización, aos equipos e ás persoas, e non ao revés. A defensa sen concesións dos procesos leva a postular que con eles se poden conseguir resultados extraordinarios con persoas mediocres, e o certo é que este principio é perigoso cando os traballos precisan creatividade e innovación.

- **Valorar máis o software que funciona que a documentación exhaustiva.** A posibilidade de poder ver anticipadamente como se comportan as funcionalidades esperadas sobre prototipos ou sobre as partes xa elaboradas do sistema final ofrece unha retroalimentación (*feedback*) moi estimulante e enriquecedora que xera ideas imposibles de concibir nun primeiro momento; e dificilmente ha poderse conseguir un documento que conteña requisitos detallados antes de comezar o proxecto. O manifesto non afirma que non fagan falta os documentos, pero salientase que son menos importantes que os produtos que funcionan. Os documentos non poden substituír nin poden ofrecer a riqueza e xeración de valor que se logra coa comunicación directa entre as persoas e a través da interacción cos prototipos.
- **Valorar máis a colaboración co cliente que a negociación contractual.** As prácticas áxiles están especialmente indicadas para produtos difíciles de definir con detalle ao principio, ou que, de ser definidos así, terían ao final menos valor que se se van enriquecendo con retroinformación continua durante o desenvolvemento. Tamén para os casos nos que os requisitos van ser moi inestables pola velocidade do contorno de negocio. Un contrato non lle achega valor ao produto. É unha formalidade que establece liñas divisorias entre responsabilidades, que fixa os referentes para posibles disputas contractuais entre cliente e provedor. No desenvolvemento áxil o cliente é un membro máis do equipo, que se integra e colabora no grupo de traballo.
- **Valorar máis a resposta ao cambio que o seguimento dun plan.** Para un modelo de desenvolvemento que xorde de contornos inestables, que teñen como factor inherente o cambio e a evolución rápida e continua, resulta moito máis valiosa a capacidade de resposta que a capacidade de



seguimento e aseguramento de plans preestablecidos. Os principais valores da xestión áxil son a anticipación e a adaptación.

Tras os catro postulados descritos, os asinantes redactaron os **12 principios** seguintes, derivados dos postulados:

1. A nosa maior prioridade é satisfacer o cliente mediante a entrega temperá e continua de software con valor.
2. Aceptamos que os requisitos cambien, mesmo en etapas tardías do desenvolvemento. Os procesos Áxiles aproveitan o cambio para proporcionarlle vantaxe competitiva ao cliente.
3. Entregamos software funcional frecuentemente, entre dúas semanas e dous meses, con preferencia ao período de tempo máis curto posible.
4. Os responsables de negocio e os desenvolvedores traballamos xuntos de forma cotiá durante todo o proxecto.
5. Os proxectos desenvólvense arredor de individuos motivados. Cómpre darlles o contorno e o apoio que precisan, e confiarlles a execución do traballo.
6. O método máis eficiente e efectivo de comunicarlle información ao equipo de desenvolvemento e entre os seus membros é a conversa cara a cara.
7. O software funcionando é a medida principal de progreso.
8. Os procesos Áxiles promoven o desenvolvemento sustentable. Os promotores, desenvolvedores e usuarios debemos ser capaces de manter un ritmo constante de forma indefinida.
9. A atención continua á excelencia técnica e ao bo deseño mellora a Axilidade.
10. A simplicidade, ou a arte de maximizar a cantidade de traballo non realizado, é esencial.
11. As mellores arquitecturas, requisitos e deseños emerxen de equipos autoorganizados.



12. A intervalos regulares o equipo reflexiona sobre como ser máis efectivo para, deseguido, axustar e perfeccionar en consecuencia o seu comportamento.

Podemos dicir, xa que logo, que as metodoloxías áxiles serían mellores que as formais cando os requirimentos son pouco claros, cando se desexa fomentar a mellora continua do proceso, ou o cliente entende o proceso e está disposto a implicarse para que saia adiante.

## **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](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 e Tecnoloxía da Información.
- "ISO 9000-3". Laboratorio de Sistemas de Información. Facultade de Informática - Universidade Politécnica de Valencia.
- <http://agilemanifesto.org/iso/es/>
- [http://es.wikipedia.org/wiki/Manifiesto\\_ágil](http://es.wikipedia.org/wiki/Manifiesto_ágil)

**Autor: Francisco Javier Rodríguez Martínez**

**Subdirector da Escola Superior de Enxeñería Informática.**

**Universidade de Vigo**

# **40. SEGURANZA INFORMÁTICA: AUTENTICACIÓN, INTEGRIDADE, CONFIDENCIALIDADE, DISPOÑIBILIDADE, RASTREXABILIDADE. ANÁLISE E XESTIÓN DE RISCOS. METODOLOXÍA MAGERIT.**



## **Tema 40. Seguridade Informática: Autenticación, Integridade, Confidencialidade, Disponibilidade, Trazabilidade. Análise e xestión de riscos. Metodoloxía MAGERIT.**

### ÍNDICE

<b>1. SEGURIDADE INFORMÁTICA: AUTENTICIDADE, INTEGRIDADE, CONFIDENCIALIDADE, DISPOÑIBILIDADE, TRAZABILIDADE.....</b>	<b>2</b>
1.1. Introducción.....	2
1.2. Plan de seguridade e plan de continxencias.....	3
1.2.1. O plan de seguridade.....	3
1.2.2. O plan de continxencias.....	4
1.2. As dimensións da seguridade.....	5
1.3. Ameazas á seguridade.....	8
1.3.1. Persoas.....	8
1.3.2. Ameazas lóxicas.....	8
1.3.3. Catástrofes.....	10
1.4. Seguridade Física.....	11
1.5. Seguridade Lóxica.....	13
1.5.1. Ataques contra a seguridade lóxica .....	14
1.5.2. A protección da seguridade lóxica.....	20
<b>2. ANÁLISE E XESTIÓN DE RISCOS.....</b>	<b>24</b>
2.1. Introducción.....	24
2.2. Análise de riscos.....	25
2.3. Xestión de riscos.....	26
2.1. A metodoloxía MAGERIT.....	28
2.1.1. Elementos da metodoloxía.....	29
2.1.2. Estrutura da metodoloxía:.....	30
2.1.3. Procesos da metodoloxía:.....	31
<b>3. REFERENCIAS.....</b>	<b>34</b>

## **1. SEGURIDADE INFORMÁTICA: AUTENTICIDADE, INTEGRIDADE, CONFIDENCIALIDADE, DISPOÑIBILIDADE, TRAZABILIDADE.**

### **1.1. Introducción**

Definimos un sistema informático como o conxunto formado por recursos físicos denominados *hardware*, recursos lóxicos denominados *software* e recursos humanos, que interactúan entre si co obxectivo de obter, almacenar e procesar a información.

Neste contexto, a seguridade informática será unha característica dos sistemas informáticos que indicará se o sistema está libre de perigo, dano ou risco. Con frecuencia, a seguridade absoluta é difícil, ou mesmo imposible, de acadar e os sistemas informáticos non son unha excepción.

Nun sistema informático os esforzos centraranse en protexer o software, o hardware e os datos. Estes adoitan ser o elemento máis valioso polo que requiren dun maior investimento en seguridade ao tratarse do recurso máis ameazado e o máis difícil de recuperar.

Non obstante, tendo en conta que a seguridade absoluta dos sistemas de información é inalcanzable, cómpre buscar sempre un compromiso entre o nivel de risco asumido e o custo das medidas de seguridade, de tal xeito que o devandito custo non supere nunca o valor do que se pretende protexer.

A seguridade nos sistemas de información afecta a todos os membros da organización. A súa natureza dinámica fai que deba ser planificada, deseñada, executada e mellorada de forma continua, xa que todos os días xorden novas ameazas. Para protexernos contra elas non é abondo con implantar medidas técnicas, senón que teremos que preparar unha política

de seguridade da organización, plans de actuación, medidas de seguridade física, formación, concienciación, etc.

## **1.2. Plan de seguridade e plan de continxencias**

A seguridade informática non é unha tarefa exclusiva dos departamentos de tecnoloxías da información ou unha cuestión meramente técnica. Debe ser unha cuestión que abranca todos os ámbitos da organización, cun gran compoñente técnico baseado en tecnoloxías da información, pero tamén político, de concienciación e formación de todo o persoal.

### **1.2.1. O plan de seguridade**

O Plan de Seguridade Informática establece os principios organizativos e funcionais da actividade de seguridade informática nunha organización. Recolle claramente as políticas de seguridade e as responsabilidades de cada un dos participantes no proceso informático, así como as medidas e procedementos que permitan previr, detectar e responder ás ameazas que gravitan sobre o mesmo.

Logo de aprobarse a política de seguridade, debe poñerse á disposición de todos os membros da organización xa que serán eles os responsables finais do seu éxito. As políticas deben ser revisadas e actualizadas anualmente (ou se é posible cada seis meses) para reflectir os cambios na organización.

Non debería haber dúas políticas de seguridade iguais, xa que cada empresa é diferente e os detalles da política dependen das necesidades exclusivas de cada unha. Sen embargo, pódese comezar cun conxunto xeral de políticas de seguridade e despois personalizalo de acordo cos requisitos específicos, limitacións de financiamento e infraestrutura existente.

Un plan de seguridade informática completo é un recurso valioso que xustifica a dedicación de tempo e esforzo á súa elaboración.

### **1.2.2. O plan de continxencias**

Un plan de continxencias é un conxunto de procedementos alternativos á orde normal da organización, cuxo fin é permitir o normal funcionamento desta, mesmo cando algunha das súas funcións for danada por un fallo de seguridade.

Que unha organización prepare os seus plans de continxencias non significa que recoñeza a ineficacia do seu plan de seguridade, senón que supón un avance para superar calquera eventualidade que poida carrexar perdas importantes.

Os plans de continxencias débense facer de cara a futuros acontecementos para os que cómpre estar preparado.

A función principal dun plan de continxencias é a continuidade das operacións da empresa. Dividimos a súa elaboración en catro etapas:

1. Avaliación.
2. Planificación.
3. Probas de viabilidade.
4. Execución.

As tres primeiras fan referencia ao compoñente preventivo e a última á execución do plan logo de acontecido o sinistro.

Cómpre crear plans de continxencias para todos os riscos de seguridade coñecidos para previr a aparición de novas ameazas ou vulnerabilidades descoñecidas que danen os nosos sistemas.

Os plans de continxencias de seguridade deben especificar claramente as accións que se realizarán de producirse un incidente para minimizar as consecuencias e a repercusión nos activos da organización. O ideal é contar con plans de resposta a incidentes e plans de continuación de negocio para garantir unha reacción eficaz durante e despois dun ataque.

## **1.2. As dimensións da seguridade**

As dimensións da seguridade, tamén denominadas servizos ou factores de seguridade, fan referencia ás propiedades que a información debe posuír para considerar un sistema como seguro. Un sistema informático atópase en óptimas condicións de seguridade para operar cando é capaz de garantir a seguridade de todos os seus compoñentes en cinco dimensións:

- **Confidencialidade:** é a propiedade da información pola que se garante que unicamente está accesible para os usuarios e procesos.

Se a información se atopa almacenada nun sistema propio, a confidencialidade baséase en primeiro lugar en garantir a autenticidade de calquera usuario que intente acceder a ela. Unha vez autenticado, debe controlarse que o usuario está autorizado, é dicir, que conta cos permisos para acceder a esa información en concreto.

Porén, cando a información se transmite entre un emisor e un receptor a través dun medio externo e por tanto inseguro, a confidencialidade debe garantirse mediante o uso de técnicas de cifrado, co fin de evitar que un terceiro que poida interceptar a

mensaxe sexa quen de extraer dela calquera información intelixible.

- **Integridade:** é a propiedade da información pola que se garante que esta non foi manipulada intencionada ou accidentalmente por usuarios non autorizados.

A integridade pode protexerse mediante técnicas de validación de datos que permitan detectar calquera alteración deles como sumas de validación (*checksum*), uso de bits de paridade, chequeos de redundancia cíclica (CRC), algoritmos de resumo (SHA1, MD5, etc.) e calquera outro algoritmo destinado a detectar calquera cambio non autorizado na información.

- **Dispoñibilidade:** é a propiedade da información pola que se garante que esta se atopará a disposición das persoas, procesos ou aplicacións que deban acceder a ela e dispoñan de autorización para iso.

A dispoñibilidade implica que o sistema, tanto o hardware coma o software, debe manterse funcionando eficientemente e que é capaz de se recuperar rapidamente en caso de fallo. Isto conséguese deseñando os sistemas de xeito apropiado en termos de capacidade e escalabilidade para poder crecer de forma ordenada en caso de ser necesario. Ademais disto, existen técnicas destinadas a evitar problemas de dispoñibilidade como o balanceo de carga entre servidores, a virtualización de servidores, a redundancia de sistemas de comunicacións, a alimentación eléctrica e de almacenamento (RAID) ou os sistemas de recuperación.

- **Autenticidade:** é a propiedade da información pola que se garante a súa xenuinidade e que permite identificar o seu autor ou xerador.

Existe unha propiedade relacionada coa autenticidade coñecida como imposibilidade de rexeitamento ou 'non repudio'. Esta propiedade permite demostrar ante terceiros que unha información foi enviada ou consignada por unha entidade sen que esta poida negalo.

A autenticidade implica a necesidade de dar probas de identidade dos participantes nunha comunicación. O modo en que un usuario pode demostrar a súa identidade recae nun ou máis dos seguintes factores: algo que o usuario sabe (por exemplo, unha clave de acceso), algo que ten (por exemplo, unha tarxeta de acceso) ou algo que é parte do propio usuario (por exemplo, medidas biométricas como as impresións dixitais). Considérase que para que unha autenticación sexa realmente segura debe incluír polo menos elementos de dous dos tres (se non dos tres) factores.

Por exemplo, a arquitectura de sinatura electrónica con certificados emitidos por entidades fiables (Autoridades de Certificación) é un sistema de autenticación multifactor, xa que primeiro debemos posuír un documento que nos identifique para poder obter un certificado avalado por un terceiro e coñecer un código persoal para realizar as sinaturas.

- **Trazabilidade:** a trazabilidade nun sistema de información fai referencia á súa capacidade para seguir e conservar a secuencia de todas as accións (ou polo menos daquelas que poidan afectar á seguridade do sistema) que ocorran no sistema para determinar a súa orixe. Un sistema con procesos trazables facilitará a resposta a incidencias na seguridade. Tamén será de grande axuda á hora

de realizar auditorías de seguridade e de deseñar sistemas de reposta baseados no estudo de patróns de situacións, como os sistemas de detección de intrusos (IDS).

### **1.3. Ameazas á seguridade**

Os sistemas informáticos atópanse expostos a diversos axentes externos ou internos capaces de causarlles dano. Dependendo da súa orixe, distinguiremos tres tipos de ameazas: persoas, ameazas lóxicas e catástrofes.

#### **1.3.1. Persoas**

Tanto o propio cadro de persoal da organización coma curiosos ou intrusos supoñen unha ameaza para a seguridade da información. Os primeiros, malia que normalmente o farán de forma non intencionada, poden causar danos ao sistema durante o exercicio da súa actividade diaria. Estes danos serán proporcionais ao nivel de exposición da información, xa que non todos os usuarios terán o mesmo nivel de acceso á información. Pola súa banda, os intrusos supoñen a miúdo unha ameaza maior, xa que atacan de forma consciente coa intención de facer o maior dano posible. Dentro deste grupo podemos incluír exempregados, *crackers*, terroristas, intrusos remunerados, etc.

#### **1.3.2. Ameazas lóxicas**

Nesta categoría inclúense todo tipo de programas que, dun xeito ou doutro, poden danar o noso sistema, xa sexa intencionadamente ou por erro. Podemos enumerar nesta categoría as seguintes ameazas:



- **Software incorrecto:** programas que, debido a defectos no seu código, poden causar danos no sistema ou facilitar ataques desde o exterior.
- **Ferramentas de seguridade:** poden ser unha excelente ferramenta de axuda para xestionar a seguridade e configurar os nosos sistemas correctamente; pero constitúen unha arma de dobre fío, xa que tamén son útiles para descubrir vulnerabilidades no noso sistema. Exemplos deste tipo de ferramentas son os *sniffers*<sup>1</sup> (como por exemplo, *Wireshark*) ou as ferramentas de escaneo de portos (como por exemplo, *nmap*)
- **Bombas lóxicas:** son partes do código de certos programas que permanecen inactivas ata que se cumpre certa condición (ausencia ou presenza de certos ficheiros, datas, etc.). Cando esta condición se activa, execútase o código malicioso que ataca ao sistema.
- **Canles de comunicación ocultas:** permiten que un proceso transfira información, violando a política de seguridade.
- **Portas traseiras:** son ‘atallos’ deixados polos programadores para acelerar os procesos de probas do software, pero que se non son corrixidos antes do paso a produción se poden converter en perigosos buracos na seguridade.
- **Virus:** son secuencias de código que se insiren nalgún lugar do sistema (habitualmente en arquivos executables, aínda que poden residir noutros lugares) para realizar a súa tarefa maliciosa e tentar estenderse a outras partes do mesmo sistema ou incluso a outros sistemas.

---

<sup>1</sup> Programas que permiten rexistrar e analizar toda a información transmitida a través dunha rede.

- **Vermes:** programas capaces de executarse e propagarse por si mesmos a través de redes.
- **Troianos:** son instrucións de código escondidas en programas que se aloxan no sistema e que realizan funcións ocultas, normalmente destinadas a tomar o control dun sistema (Por exemplo, os rootkit).
- **Programas coello** (tamén coñecidos como programas bacteria): programas que non fan nada fóra de reproducirse ata esgotar os recursos do sistema e conseguir bloquealo.
- **Técnicas Salami:** roubo automatizado e sistemático de pequenas cantidades de bens dunha gran cantidade orixinal

### **1.3.3. Catástrofes**

As catástrofes, sexan naturais ou artificiais, constitúen a ameaza menos probable pero tamén a máis desastrosa para os sistemas de información. A defensa contra elas baséase en recursos físicos e nun deseño adecuado da sede física dos nosos sistemas

- **Incendios:** O centro de proceso de datos debe contar cun sistema de extinción de incendios axeitado que permita sufocar calquera conato sen que a propia extinción lles cause danos aos sistemas.
- **Inundacións:** Ademais de buscar un emprazamento co mínimo risco de inundación, é recomendable instalar sensores que detecten posibles fugas de auga e alerten sobre elas antes de que poidan causar dano.
- **Terremotos:** Nas zonas con actividade sísmica é un risco que cómpre ter en conta.

- Tormentas eléctricas: A instalación eléctrica debe contar con todas as garantías proporcionando alimentación ininterrompida e neutralizando os picos de tensión que se puidesen producir.
- Temperaturas extremas: Os equipos informáticos, como aparatos electrónicos que son, necesitan unhas condicións de temperatura e humidade axeitadas para un funcionamento óptimo. Estas condicións adoitan conseguirse mediante a instalación de equipos de climatización.

#### **1.4. Seguridade Física**

A seguridade física encárgase da protección contra ameazas ás instalacións, equipamentos, sistemas de comunicacións e persoal que forman parte dun sistema de información. Consiste na aplicación de barreiras físicas e procedementos de control ante ameazas aos recursos do sistema.

Resulta habitual que as organizacións se centren na seguridade lóxica, descoidando ás veces, a seguridade física, o que pode ser fonte de problemas, xa que a seguridade física afecta aos tres tipos de recursos — hardware, software e datos— e os ataques con acceso físico exitosos poden facer moito mal. Por exemplo, un acceso non autorizado que ten como resultado a desaparición dun equipo con datos sensibles da organización.

As ameazas á seguridade física poden clasificarse atendendo a diversos aspectos. Establecemos aquí tres tipos:

- Ameazas ocasionadas involuntariamente por persoas: trátase de accidentes causados por persoas de forma fortuíta por accidente ou neglixencia no uso do sistema. Estas persoas non teñen por que ser exclusivamente traballadores técnicos. Inclúe tamén persoal de limpeza e mantemento, visitantes, etc. Na práctica

tradúcese en derrames de líquidos, desconexións bruscas da rede, caídas e roturas de material, etc.

- Accións hostís deliberadas: trátase de ameazas que poden ser realmente perigosas en función da capacidade e intencións do atacante. Son accións deliberadas e usualmente planificadas contra o noso sistema ou as persoas que traballan nel. Inclúe accesos non autorizados ás instalacións, roubo, secuestros, fraudes, sabotaxes, etc.
- Desastres naturais, incendios, humidade e inundacións: son axentes externos que, de afectaren aos nosos sistemas, adoitan causar graves danos. Aínda que son infrecuentes, é necesario prevelos e telos en conta ao longo de todo o deseño e a vida útil do noso sistema.

As medidas de seguridade física permiten limitar o alcance das ameazas citadas mediante o uso de controis e procedementos de seguridade. O estándar TIA-942, aprobado pola *Telecommunications Industry Association* e por ANSI<sup>2</sup>, proporciona unha guía de recomendacións e normas para o deseño e instalación de infraestruturas de centros de procesamento de datos (CPD) que contribúen a un considerable aumento da seguridade física do sistema de información. Establece catro niveis (*tiers*) de dispoñibilidade implantados mediante medidas de carácter arquitectónico, de telecomunicacións, eléctricas e mecánicas.<sup>3</sup>

---

<sup>2</sup> Siglas en inglés de American National Standards Institute.

<sup>3</sup> Deixamos para o tema 56, dedicado ao deseño de centros de procesamento de datos, o desenvolvemento das medidas de seguridade física.

### **1.5. Seguridade Lóxica**

A seguridade lóxica fai referencia ao conxunto de operacións e técnicas destinadas á protección da información, procesos e programas contra a destrución, a modificación, a divulgación indebida ou o atraso na súa xestión..

É pouco frecuente que un ataque lóxico afecte ao hardware, aínda que existe a posibilidade de que algún ataque deste tipo poida chegar a danar algún compoñente.

Nun sistema de información, os datos constitúen un dos recursos máis importantes e valiosos. A gran variedade dos ataques, a súa posible orixe remota e as repercusións que poden ter obríganos a establecer medidas de protección semellantes ou superiores ás asumidas na seguridade física.

A seguridade lóxica suscita unha serie de requisitos intimamente relacionados coas precitadas dimensións da seguridade, entre os que podemos mencionar os seguintes:

- Asegurar que os operadores poidan traballar sen necesidade dunha supervisión minuciosa e que non poidan modificar os programas nin os arquivos que non lles correspondan.
- Asegurar que se estean utilizando os datos e os programas correctos polo procedemento correcto.
- Restrinxir o acceso ao software e aos datos.
- Que a información transmitida sexa recibida polo destinatario ao que lle foi enviada e non por outro.
- Prover técnicas que permitan garantir que a información non resulta alterada durante un proceso de transmisión.

- Procurar que os sistemas de comunicación entre os distintos compoñentes do sistema de información estean redundados.
- Manter un rexistro das operacións levadas a cabo no sistema xunto co usuario que as realiza para poder realizar o seu seguimento en caso de ser necesario.

### **1.5.1. Ataques contra a seguridade lóxica**

A seguridade lóxica pode ser vulnerada por medio de ataques moi heteroxéneos e que, ademais, evolucionan constantemente. Dada a gran diversidade de sistemas operativos, aplicacións e protocolos, é imposible determinar o seu número, que segue a aumentar día a día.

Por outra banda, a transmisión de información a través de sistemas de alleos á organización, como internet, resulta cada vez máis frecuente e o volume de información transmitido aumenta tamén dun xeito notable. Estas operacións de transmisión de información a través dunha canle non controlada pola organización e compartida con terceiros son especialmente vulnerables aos ataques destes.

Podemos clasificar estes ataques atendendo ao seu obxectivo da seguinte maneira:

1. **Ataques Pasivos:** a información non resulta alterada, senón que o atacante unicamente a captura ou monitorea para obter os datos que están a ser transmitidos.

Os obxectivos destes ataques son a interceptación de datos e a análise de tráfico coas seguintes finalidades:

- o Recompilación de datos sobre contas de usuarios e claves de acceso para utilizar máis tarde en ataques activos.

- o Obtención da orixe e destinatario da comunicación a través da lectura das cabeceiras dos paquetes monitorados.
  - o Monitorización do volume de tráfico intercambiado entre as entidades obxecto do ataque, conseguindo así información acerca de actividade ou inactividades inusuais.
  - o Monitorización das horas habituais de intercambio de datos entre as entidades da comunicación para extraer información acerca dos períodos de actividade.
2. **Ataques activos:** ataques implican algún tipo de modificación dos datos ou a creación de datos falsos. Adoitan ser intencionados e realizados por persoas con coñecementos e consciencia do que están facendo.

Pódense subdividir en varias categorías atendendo ás accións que se realizan durante o ataque:

- o **Interceptación:** un elemento non autorizado consegue un acceso a un determinado obxecto do sistema, pero este non é modificado en ningún modo. Se se trata dunha comunicación, esta chegará ao seu destino sen constancia da interceptación.
- o **Destrucción:** algúns autores consideran un caso especial da modificación a destrución, entendéndoa como unha modificación que inutiliza o obxecto afectado.
- o **Modificación:** Se ademais de lograr unha interceptación, o ataque consegue modificar o obxecto de datos.
- o **Interrupción:** un ataque clasifícase como interrupción se fai que un obxecto do sistema se perda, quede inutilizable ou non dispoñible.

- o **Fabricación:** modificación destinada a suplantar o obxecto real.

Como dicíamos, existe un elevado número de tipos de ataques contra a seguridade lóxica. Citamos deseguido algúns deles:<sup>4</sup>

- **Enxeñería Social:** consiste en manipular as persoas do contorno para obter acceso aos sistemas ou a información confidencial que facilite outros ataques técnicos.
- **Enxeñería Social Inversa:** o intruso dá a coñecer dalgún xeito que é capaz de brindarlles axuda aos usuarios, e estes chámanos ante algún imprevisto. O intruso aproveitará a oportunidade para pedir información necesaria para solucionar o problema, conseguindo de paso información útil para realizar ataques.
- **Shoulder-surfing**<sup>5</sup>: consiste en espiar fisicamente aos usuarios namentres introducen o seu nome de usuario e clave de acceso correspondente, ou cando están accedendo a información restrinxida.
- **Piggybacking:** relacionado co anterior. Hoxe en día fai referencia ao uso de redes *wireless* alleas, pero o seu significado orixinal era o de “coarse” nun lugar detrás doutra persoa.
- **Masquerading/spoofing** (Suplantación): suplantación electrónica ou física de persoas autorizadas para acceder ao sistema ou obter información relevante sobre el. Dependendo do obxecto da suplantación, poderíamos falar de *IP spoofing*, *DNS spoofing*, *web spoofing*, etc.

---

<sup>4</sup> O RFC 4949 (*Internet Security Glossary, Version 2*) proporciona unha listaxe máis extensa e descritiva.

<sup>5</sup> Expresión en inglés que se refire a mirar por enriba do ombro.





- **Scavenging:** paradoxalmente, un dos ataques máis efectivos. Consiste en inspeccionar os refugallos en papeleiras, colectores, etc., en busca de información sensible.
- **Exploits:** aproveitamento de erros coñecidos (*bugs*) en determinadas versións do software instalado no sistema de información que poden ser usados como porta de entrada de ataques.
- **Escaneo de portos:** técnicas de ataque pasivas que analizan as máquinas dun sistema para determinar cal é o estado dos portos (aberto/pechado). Nalgúns casos permiten coñecer mesmo cal é o sistema operativo da máquina e incluso que software e que versión do mesmo se encontra escoitando en cada porto.
- **Wiretapping:** un tipo de ataque que intercepta e accede á información que se transmite por unha canle de comunicacións. O nome do termo (que poderíamos traducir como “intervir cables”) ten como orixe a intervención de teléfonos que se facía de forma mecánica. Hoxe en día fai referencia á captura de datos mediante calquera técnica, con ou sen cables polo medio.
- **Eavesdropping-packet sniffing:** un tipo de ataque *wiretapping* pasivo. É a interceptación pasiva do tráfico de rede. Realízase con aplicacións chamadas *sniffers*, que son programas que capturan paquetes de datos que circulan pola rede. Pódese facer colocando o *sniffer* nun dos equipos pertencentes á rede ou conseguindo conectar un equipo externo á ela. Este último caso é a forma máis habitual en redes *wireless*.
- **Man-in-the-middle:** un tipo de ataque *wiretapping* activo. O atacante intercepta e modifica selectivamente os paquetes de

datos capturados para simular ser un dos participantes nunha comunicación allea.

- **Denegación de servizo:** coñecido habitualmente polas súas siglas en inglés, DoS (*Denial of Service*); este tipo de ataques consiste en conseguir que o obxectivo do ataque deixe de realizar a súa función de modo temporal ou definitivo. O obxectivo do ataque pode ser unha máquina, unha rede de comunicacións, un servizo concreto, etc. É dun dos tipos de ataques máis comúns e efectivos. Na práctica existen múltiples variedades deste ataque, das que podemos citar: *Flooding*, *ICMP flood*, *Syn flood*, *ping of death*, *land*, *smurf*, *teardrop*, etc.
- **Denegación de Servizo Distribuída:** un caso especial do anterior, tamén coñecido polas súas siglas en inglés, DDoS (*Distributed Denial of Service*). Neste caso o ataque de DoS non provén dun único atacante, senón que provén de moitos á vez de forma coordinada. O conxunto de atacantes pode non ser realmente un conxunto de persoas, xa que é habitual o uso de máquinas secuestradas (“máquinas zombis”) que participan no ataque, moitas veces sen que o seu lexítimo dono teña coñecemento.
- **Ataques de secuestro (*Hijack*):** céntranse no secuestro dalgún elemento nunha comunicación previamente establecida pola vítima ou dun recurso vital dunha máquina. Os obxectivos do secuestro poden ser a sesión dun usuario xa autenticado nun sistema, o propio navegador da vítima ou ata unha páxina ofrecida por un servidor para modificala e facer que os datos inseridos nela lle sexan enviados a unha máquina baixo o control do atacante, por exemplo.



- **Tamper:** ataque consistente en realizar modificacións na configuración dunha máquina ou sistema obxectivo que degraden o nivel de seguridade destes.
- **Phishing:** é, en realidade, un tipo de ataque de tipo *masquerading* que creceu en frecuencia nos últimos anos. É un ataque que tenta adquirir información sensible do obxectivo (número de contas bancarias, nomes de usuario e claves de acceso, etc.) mediante unha solicitude fraudulenta nun correo electrónico ou páxina web que o atacante construíu para simular ser unha entidade ou persoa de confianza do obxectivo.
- **SQL injection:** é un tipo de ataque por inserción de código dirixido á base de datos en linguaxe SQL. A técnica consiste en inserir secuencias concretas que son sintacticamente correctas en SQL en campos de texto de aplicacións (usualmente web) para executar consultas fraudulentas. Aínda que é un ataque perigoso, é facilmente contrarrestable filtrando adecuadamente as entradas.
- **Cross-site request forgery:** abreviado habitualmente como CSRF ou XSRF, é tamén coñecido como “ataque dun click”. Baséase en tirar partido da confianza que un sitio web ten no navegador web dun usuario. A vítima é enganada para usar un hiperenlace manipulado polo atacante. A manipulación consiste na construción dun obxecto de petición (*request*) que realiza directamente unha acción fraudulenta e involuntaria para o usuario que a executa. A clave reside en que o sitio web debe confiar no usuario (porque xa se autenticou previamente, por exemplo) e executar a petición directamente; de aí o nome de “ataque nun click”.

- **Cross site scripting:** abreviado habitualmente como XSS. Trátase de calquera ataque que permita executar código de *scripting* (*VBScript, Javascript, etc.*) inserido polo atacante no contexto dun sitio web.

### 1.5.2. A protección da seguridade lóxica

Existen medidas de protección que poden e deben ser utilizadas para aumentar a seguridade dos nosos sistemas de información.

Máis adiante veremos que os niveis de seguridade poden ser controlados e xestionados mediante a análise de riscos, polo que neste apartado nos limitaremos a enunciar as medidas organizativas e técnicas que podemos aplicar para aumentar a nosa seguridade.

Os ataques á seguridade lóxica adoitan basearse en realidade en fallos de deseño inherentes a internet (ou aos seus protocolos), ou aos sistemas operativos utilizados. A continua aparición de novas tecnoloxías fai que o número de tipos de ataques tamén aumente.

Polo tanto, os responsables de seguridade e administradores dos sistemas deben manterse actualizados respecto dos novos ataques e de como protexerse contra eles. E, por suposto, é de vital importancia que manteñan actualizado o sistema operativo e todo o software utilizado nas máquinas do sistema.

Unha máquina que conteña información que non sexa considerada valiosa, debe terse en conta igualmente á hora de definir as políticas de seguridade xa que pode resultar útil para un atacante á hora de empregala nun ataque de denegación de servizo distribuído (DDoS) ou de utilizala como paso intermedio para ocultar o verdadeiro enderezo do atacante

Cómpre realizar auditorías de seguridade de forma periódica e valorar a posibilidade de implantar sistemas de xestión da seguridade da

información (SXI) que garantan a calidade dos nosos sistemas e medidas de seguridade.

Un dos ataques con maior taxa de éxito de todos os citados é o da enxeñería social. De nada serve que teñamos o noso sistema perfectamente actualizado e que contemos coas medidas de seguridade físicas e lóxicas máis avanzadas se mediante unha chamada telefónica un atacante pode conseguir que un usuario lle transmita o seu usuario e clave de acceso.

A defensa contra ataques de enxeñería social pasa por manter aos usuarios do sistema informados e formados en materia de seguridade. Cómpre mantelos alerta e inculcar neles un espírito de desconfianza que permita evitar ataques baseados na enxeñería social ou o *phishing*

Algunhas ferramentas e técnicas de protección da seguridade que podemos aplicar nos nosos sistemas de información son:

- **Análise de riscos:** a análise de riscos debe realizarse sempre como paso inicial no deseño da seguridade dos nosos sistemas de información. Supón identificar os activos que hai que protexer e o dano que sufriría a organización en caso de que estes fosen afectados por un ataque. Veremos este punto en profundidade no próximo capítulo.
- **Identificación de ameazas:** consiste en identificar cada unha das ameazas e vulnerabilidades que poden afectar aos recursos do sistema.
- **Políticas de seguridade:** é fundamental contar cunha política de seguridade, deseñada a medida para a organización e coñecida por todos os empregados e/ou usuarios. Neste sentido, o RFC 2196 *Site Security Handbook* é unha guía para o desenvolvemento de políticas e procedementos de seguridade

aplicables a sistemas de información. Está destinado principalmente a sistemas que traballan no ámbito de internet, pero tamén a aqueles sistemas que simplemente se comunican con outros. E de xeito xeral tamén pode ser utilizado en sistemas illados. O contido inclúe políticas, conceptos de seguridade en redes e sistemas, e respostas aos incidentes de seguridade.

- **Estratexia de seguridade:** unha estratexia adecuada debe ser concibida de modo que abarque varios niveis de seguridade: seguridade física, seguridade lóxica, o persoal da organización e a interacción que existe entre estes factores. O plan de seguridade é un documento fundamental na organización que debe incluír unha estratexia de previsión de ataques para minimizar os puntos vulnerables existentes na directiva de seguridade. Debe desenvolver así mesmo plans de continxencias. Estes servirán como unha estratexia reactiva de resposta ao ataque que axude ao persoal de seguridade a avaliar o dano causado e a recuperar os niveis de servizo necesarios.
- **Uso de sistemas operativos seguros:** o mercado ofrece diferentes sistemas operativos que poden ser usados nos nosos sistemas. Como é de supoñer, non todos eles ofrecen o mesmo nivel de seguridade. É conveniente usar sistemas operativos con niveis de seguridade acordes ás necesidades da nosa estratexia de seguridade. Existe unha catalogación dos niveis de seguridade que ofrece un sistema operativo determinada polo estándar unificado *Common Criteria for Information Technology Security Evaluation* (simplificado habitualmente como *Common Criteria*).
- **Equipos de resposta a incidencias:** é aconsellable formar un equipo de respostas a incidencias que lle dea apoio ao responsable de seguridade e que actúe seguindo os plans de continxencia en caso de ser necesario.

- **Copias de seguridade** (*backups*): o *backup* de datos permite ter dispoñible unha copia íntegra dos datos en caso de perda ou corrupción destes tras un ataque ou un accidente. É conveniente deseñar coidadosamente a política e o procedemento de creación, transporte e almacenamento das copias de seguridade dos datos e tamén dos programas usados na organización.
- **Devasas** (*firewalls*): son sistemas, hardware ou software, destinados a filtrar o tráfico que circula polos sistemas de comunicacións. É habitual utilízalos para controlar o tráfico que entra e sae da nosa organización para evitar así algúns tipos de ataques baseados en manipulación de paquetes. Ademais, permiten tamén controlar as aplicacións e protocolos que son utilizados polos empregados.
- **Sistemas de Detección de Intrusos**: coñecidos polas súas siglas en inglés, IDS. Un IDS é capaz de recoller e utilizar información dos eventos ocorridos no sistema para detectar patróns de ataques e alertar ao administrador de posibles ataques. Algúns tipos de IDS son mesmo capaces de levar a cabo accións reactivas destinadas a abortar os ataques detectados.
- **Programas antivirus**: son programas destinados á detección e eliminación de virus informáticos. Convén contar con antivirus en todos os equipos do sistema de información. Para que os antivirus sexan efectivos é vital que estean actualizados.
- **Ferramentas de seguridade**: como xa se comentou, poden ser de grande utilidade para xestionar a seguridade e configurar os nosos sistemas correctamente, aumentando así a súa protección.
- **Encriptación da información**: dado que por moitas medidas de seguridade que tomemos seguiremos correndo o risco de sufrir

accesos non autorizados á nosa información, é unha boa práctica usar a encriptación para aumentar a protección da información sensible. A encriptación débesele aplicar tanto á información que se transmite a través de sistemas de comunicación como á aquela de especial importancia, aínda que esta non saia do noso sistema.

## **2. ANÁLISE E XESTIÓN DE RISCOS**

### **2.1. Introducción**

En toda organización existen unha serie de activos sensibles desde o punto de vista da seguridade. Estes activos están suxeitos a riscos que, en caso de se materializaren, han danalos causándolle un prexuízo á organización. Unha das tarefas na xestión da seguridade pasa por analizar e xestionar eses riscos para mantelos baixo control ou para estar preparados para reaccionar no caso de que danen ou destrúan os nosos activos.

A análise de riscos consiste en identificar as ameazas aos nosos activos e estimar a súa magnitude. Debe realizarse para todos aqueles activos de importancia estratéxica na continuidade do negocio, aqueles de carácter único ou aqueles necesarios para cumprir coa lexislación vixente.

A xestión dos riscos defínese como a selección e implantación de medidas de seguridade para coñecer, previr, reducir ou controlar os riscos identificados. A xestión dos riscos debe ter como obxectivo manter o nivel de risco por debaixo dun limiar determinado pola organización.

O proceso de análise e xestión de riscos pódese completar mediante auditorías internas e externas que garantan a revisión obxectiva das decisións tomadas. Mesmo é posible chegar a obter certificacións do noso sistema de xestión da seguridade da información (SXSI) coma a ISO/IEC 27001.



Por último, cómpre ter en conta que unha organización e os seus activos son elementos dinámicos que mudan co tempo e que, polo tanto, os riscos que lles afectan tamén o fan. Na práctica isto ten como consecuencia a necesidade da revisión periódica das análises de riscos e das medidas de xestión de riscos implementadas.

## 2.2. **Análise de riscos**

O proceso da análise de riscos inclúe as seguintes tarefas:

- **Identificar e valorar os activos:** todos os activos da organización deben ser identificados e valorados economicamente desde o prisma do sistema da información. Ademais, cómpre identificar as relacións de dependencia que existen entre eles.
- **Identificar vulnerabilidades:** todas aquelas debilidades ou posibles buracos de seguridade que poderían ser aproveitados para realizar ataques contra os activos.
- **Identificar ameazas:** serán todas aquelas situacións que poderían xerar unha situación de perigo ou dano para os activos.
- **Clasificar os riscos:** debe obterse unha clasificación de todos os riscos que afectan á seguridade da organización, ordenados segundo o nivel de risco que soporte. O nivel de risco será unha medida combinada do valor do activo afectado, a valoración do impacto e a probabilidade de que este ocorra.
- **Avaliar o impacto:** estimaremos tamén que probabilidade existe de que unha das ameazas se materialice sobre un activo, e que custo tería iso para a organización se o activo quedase danado ou inutilizado.

- **Determinar o grao de aseguramento:** para rematar, debe determinarse o nivel de risco que a organización está disposta a asumir. Servirá como medida na fase de xestión de riscos para decidir que controis debemos aplicar en cada caso para obter un risco aceptable e conforme co grao de aseguramento que a organización precisa.

A análise de riscos ten un carácter altamente subxectivo, xa que calquera valoración se fai sempre partindo das necesidades e obxectivos da organización sobre a que se realiza a análise.

Aínda así, existen técnicas destinadas a realizar as avaliacións de modo cualitativo (sesións de *brainstorming*, entrevistas e cuestionarios estruturados, técnicas Delphi, gráficos DAFO, etc.) e mesmo cuantitativo (método Montecarlo, análise algorítmica-cuantitativa, etc.).

### 2.3. Xestión de riscos

Como xa apuntamos, a fase de xestión de riscos implica deseñar e aplicar as accións ou políticas necesarias para que os riscos identificados se manteñan por baixo do nivel de risco que a organización pode aceptar.

Basicamente, existen catro accións que podemos realizar para reducir o risco na organización:

- **Aceptar:** a priori é a menos custosa, xa que simplemente se coñecen os riscos e a probabilidade de que ocorran, pero acéptanse sen realizar ningunha acción de protección.

Evidentemente, esta opción é válida só para riscos sobre activos realmente pouco importantes ou con probabilidades de materialización ínfimas. Algúns riscos de seguridade, especialmente as ameazas relacionadas con desastres naturais,

son de tal envergadura que, en realidade, non é posible intervir con medidas preventivas nin reactivas dunha forma eficaz.

Polo tanto, o equipo de seguridade pode decidir simplemente aceptar o problema de seguridade. Aínda así, e malia aceptar o risco, deberían desenvolverse plans de continxencias para o caso en que un desastre chegase a suceder.

- **Anular:** nalgúns casos pode ser beneficioso para a organización a anulación total dos riscos dun activo simplemente prescindindo do tal activo.

Isto pode implicar, por exemplo, a eliminación dalgún servizo non esencial, ou deixar de usar algún software ou cortar o tráfico de certos protocolos de rede no noso sistema.

- **Transferir:** ás veces é posible cederlle a responsabilidade sobre o activo a un terceiro. Esta opción pasa por contratar seguros sobre os nosos activos ou utilizar directamente os activos doutra entidade provedora.

A transferencia dun risco de seguridade non significa que un risco se elimínase. En xeral, unha estratexia de transferencia xerará novos riscos de seguridade relacionados cos provedores ou aseguradoras que requirirán administración preventiva. Así e todo, a transferencia do risco reducirá a ameaza a un nivel máis aceptable.

- **Mitigar:** consiste en implementar medidas de seguridade efectivas que nos permitan reducir os riscos identificados. A mitigación supón tomar accións preventivas para evitar que un risco se materialice ou para reducir as súas consecuencias a un nivel aceptable.

O obxectivo é a prevención e a minimización das ameazas ata niveis aceptables pola organización. Por exemplo, o uso dunha directiva de contrasinal seguro reducirá a probabilidade de que un usuario externo descubra un contrasinal para ter acceso a un sistema de nóminas.

Os controis de seguridade que se aplicarán e as medidas que permitan determinar a súa eficacia deben ser seleccionados, deseñados e, logo de implantados, revisados periodicamente co fin de descubrir necesidades de novos controis ou a súa adaptación.

## **2.1. A metodoloxía MAGERIT**

MAGERIT é unha metodoloxía para a análise e xestión de riscos dos sistemas de información elaborada orixinalmente polo Consello Superior de Administración Electrónica do Goberno de España (aínda que actualmente depende do Ministerio de Política Territorial e Administración Pública e é administrada pola Dirección Xeral para o Impulso da Administración Electrónica).

O seu obxectivo final é a minimización dos riscos da implantación e uso das tecnoloxías da información nas administracións públicas. Actualmente atópase na súa versión 2.

A utilización da metodoloxía MAGERIT en si non require de ningún tipo de autorización previa e a documentación que a describe é de dominio público, e incluso o Centro Criptolóxico Nacional (CCN) ofrece de forma gratuíta unha aplicación (chamada PILAR<sup>6</sup>) que constitúe un Contorno de Análise de Riscos (CAR) para a análise e xestión de riscos dun Sistema de Información usando a metodoloxía MAGERIT. Este aperturismo débese á convicción de que la xeneralización do uso das tecnoloxías da información

---

<sup>6</sup> Pódese atopar na páxina do CCN (<https://www.ccn-cert.cni.es/>) dentro do apartado ferramentas.

e das comunicacións é potencialmente beneficiosa para os cidadáns, as empresas e a propia Administración Pública, pero que tamén dá lugar a certos riscos que se deben minimizar con medidas de seguridade que xeren confianza na súa utilización.

En definitiva, MAGERIT persegue os seguintes obxectivos:

- Concienciar os responsables dos sistemas de información da existencia de riscos e da necesidade de atallalos a tempo.
- Ofrecer un método sistemático para analizar os tales riscos.
- Axudar a descubrir e planificar as medidas oportunas para manter os riscos baixo control.
- Preparar a Organización para procesos de avaliación, auditoría, certificación ou acreditación, segundo corresponda en cada caso.

### **2.1.1. Elementos da metodoloxía**

Deseguido, e aínda que algún deles xa foi citado no contexto dos riscos de seguridade, definimos brevemente os elementos considerados significativos por MAGERIT para o estudo da Seguridade en Sistemas de Información.

- **Activos:** recursos do sistema de información ou relacionados con este, necesarios para que a organización funcione correctamente e alcance os obxectivos propostos pola dirección.
- **Ameazas:** eventos que poden desencadear un incidente na organización, producindo danos materiais ou perdas inmateriais nos seus activos.

- **Vulnerabilidade dun activo:** potencialidade ou posibilidade de ocorrencia da materialización dunha ameaza sobre o devandito activo.
- **Impacto nun activo:** consecuencia sobre este da materialización dunha ameaza.
- **Risco:** posibilidade de que se produza un impacto determinado nun activo, nun dominio ou en toda a organización
- **Servizo de salvagarda:** acción que reduce o risco.
- **Mecanismo de salvagarda:** procedemento, dispositivo, físico ou lóxico, que reduce o risco.

Os activos están expostos a ameazas que, cando se materializan, degradan o activo, producindo un impacto. Se estimamos a frecuencia con que se materializan as ameazas, podemos deducir o risco ao que está exposto o sistema. Degradación e frecuencia cualifican a vulnerabilidade do sistema. O administrador do sistema de información dispón de salvagardas que, ou ben reducen a frecuencia de ocorrencia, ou ben reducen ou limitan o impacto.

#### **2.1.2. Estrutura da metodoloxía:**

O desenvolvemento da metodoloxía MAGERIT versión 2 estrutúrase en tres guías:

- **Método:** describe os procesos, actividades e tarefas para realizar un proxecto de análise e xestión de riscos e proporciona unha serie de consellos e casos prácticos de exemplo. Inclúe ademais un anexo no que se establecen correspondencias coa versión 1 de MAGERIT.

- **Catálogo de Elementos:** ofrece unha serie de pautas en canto a tipos de activos, dimensións de valoración dos activos, criterios de valoración dos activos, ameazas típicas sobre os sistemas de información e salvagardas que convén ter en conta para protexer os sistemas de información.
- **Guías de Técnicas:** trátase dunha guía de consulta que proporciona algunhas técnicas que se empregan habitualmente para levar a cabo proxectos de análises e xestión de riscos: técnicas específicas para a análise de riscos, análises mediante táboas, análise algorítmica, árbores de ataque, técnicas xerais, análises custo-beneficio, diagramas de fluxo de datos, diagramas de procesos, técnicas gráficas, planificación de proxectos, sesións de traballo (entrevistas, reunións e presentacións) e valoración Delphi.

### 2.1.3. Procesos da metodoloxía:

A guía do Método Magerit Versión 2 especifica que un proxecto de análise e xestión de riscos consta de tres procesos que, pola súa banda, se dividirán en actividades e tarefas que se detallan na guía do Método:

- Proceso P1: Planificación:
- Establécense as consideracións necesarias para arrincar o proxecto de análise e xestión de riscos.
- Investígase a oportunidade de realizalo.
- Defínense os obxectivos que debe cumprir e o dominio (ámbito) que abarcará.



- Planifícanse os medios materiais e humanos para a súa realización.
- Procédese ao lanzamento do proxecto.
- Xéranse os seguintes documentos: Tipoloxía de Activos, Dimensións de Seguridade Relevantes, Criterios de Avaliación.
- 
- Proceso P2: Análise de riscos:
  - Identifícanse os activos que se van tratar, as relacións entre eles e a valoración que merecen.
  - Identifícanse as ameazas significativas sobre os tales activos e valóranse en canto á frecuencia de ocorrencia e a degradación que causan sobre o valor do activo afectado.
  - Identifícanse as salvagardas existentes e valórase a eficacia da súa implantación.
  - Estímase o impacto e o risco ao que están expostos os activos do sistema.
  - Interpretase o significado do impacto e o risco.
- Xéranse os seguintes documentos: Modelo de Valor, Mapa de Riscos, Avaliación de Salvagardas, Estado de Risco, Informe de Insuficiencias.
- 
- Proceso P3: Xestión de riscos:
  - Elíxese unha estratexia para mitigar impacto e risco.





- Determináanse as salvagardas oportunas para o obxectivo anterior.
- Determináse a calidade necesaria para as devanditas salvagardas.
- Deséñase un plan de seguridade (plan de acción ou plan director) para levar o impacto e o risco a niveis aceptables.
- Lévese a cabo o plan de seguridade.
- Como produto desta fase xérase o Plan de Seguridade.

### 3. REFERENCIAS<sup>7</sup>

- 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 da metodoloxía MAGERIT versión 2.  
[http://www.mpt.gob.es/publicaciones/centro\\_de\\_publicaciones\\_de\\_la\\_sgt/Monografias0](http://www.mpt.gob.es/publicaciones/centro_de_publicaciones_de_la_sgt/Monografias0)

**Autor: Juan Otero Pombo**

**Enxeñeiro en Informática no Concello de Ourense**

**Colexiado do CPEIG**

---

<sup>7</sup> As ligazóns foron comprobadas en novembro do 2011.

# **41. SISTEMAS DE XESTIÓN DA SEGURIDADE DA INFORMACIÓN: NORMAS DA SERIE ISO 27.000.**

## **Tema 41. Sistemas de xestión da seguridade da información: normas da serie ISO 27000**

### **ÍNDICE**

<u>1. SISTEMAS DE XESTIÓN DA SEGURIDADE DA INFORMACIÓN .....</u>	<u>1</u>
<u>1.1. Introducción.....</u>	<u>2</u>
<u>1.2. Características principais dun SXSI.....</u>	<u>3</u>
<u>1.3. Implementación dun SXSI.....</u>	<u>6</u>
<u>1.3.1 Planificar (Plan).....</u>	<u>7</u>
<u>1.3.2 Facer (Do):.....</u>	<u>10</u>
<u>1.3.3 Verificar (Check):.....</u>	<u>11</u>
<u>1.3.4 Actuar (Act):.....</u>	<u>13</u>
<u>1.4. A responsabilidade de dirección nun SXSI.....</u>	<u>13</u>
<u>1.5. Beneficios dun SXSI.....</u>	<u>14</u>
<u>2. NORMAS DA SERIE ISO/IEC 27000.....</u>	<u>16</u>
<u>2.1. As organizacións ISO e IEC.....</u>	<u>16</u>
<u>2.2. A serie ISO/IEC 27000.....</u>	<u>17</u>
<u>2.3. Contido da norma.....</u>	<u>19</u>
<u>2.3.1 ISO/IEC 27001.....</u>	<u>19</u>
<u>2.3.3 ISO/IEC 27003.....</u>	<u>22</u>
<u>2.3.4 ISO/IEC 27006.....</u>	<u>24</u>
<u>2.4. O proceso de implantación.....</u>	<u>26</u>
<u>2.1. O proceso de certificación.....</u>	<u>28</u>
<u>3. REFERENCIAS.....</u>	<u>32</u>

### **1. SISTEMAS DE XESTIÓN DA SEGURIDADE DA INFORMACIÓN**

## 1.1. Introducción

A información converteuse nun dos principais activos das empresas e as organizacións, e constitúe unha vantaxe competitiva. Por iso a seguridade da información é vital no seo de calquera organización, especialmente se está en formato electrónico.

A complexidade crecente dos sistemas de información e a súa relevancia dentro das organizacións fai que a xestión da seguridade se converta nun factor de interese que cómpre controlar.

O establecemento dun Sistema de Xestión da Seguridade da Información (SXSI)<sup>1</sup> permite manexar a xestión da seguridade dun modo ordenado e orientado á mellora continua, establecendo un conxunto de políticas de administración da información.

En síntese, un SXSI encargarase do deseño, implantación e mantemento dun conxunto de procesos orientados a xestionar eficientemente a accesibilidade da información, procurando asegurar a confidencialidade, integridade e dispoñibilidade dos activos de información minimizando ao mesmo tempo os riscos de seguridade.

A miúdo confúndese a seguridade informática coa seguridade da información. Esta confusión débese a que coa dixitalización da información foi crecendo a preocupación pola súa seguridade. Podemos dicir que o termo seguridade da información abrangue tamén a seguridade informática, xa que esta se centra nos elementos propios da infraestrutura das tecnoloxías da información e das comunicacións que a nosa organización precisa (compoñentes hardware, redes, software, etc.). Porén, a información da organización pódese atopar en diversos formatos como arquivos de texto, imaxes, contratos, documentos en papel, etc.

---

<sup>1</sup> En inglés, *Information Security Management System* (ISMS).

Xa que logo, malia que os SXSI adoitan relacionarse con sistemas dixitais, o seu alcance inclúe tamén a información que se atopa en soportes non dixitais.

A ameaza de accesos non autorizados á información almacenada en equipos conectados a unha rede é constante. Isto, unido ao continuo e vertixinoso desenvolvemento das tecnoloxías da información, que fixo posible que millóns de ordenadores separados por milleiros de quilómetros poidan estar interconectados coma se estivesen nunha mesma habitación, condúcenos a unha conclusión inmediata: a seguridade absoluta non existe.

O obxectivo de calquera sistema de seguridade será a redución dos riscos contra os activos da empresa ata un nivel (ou limiar) aceptable. Un SXSI constitúe unha valiosa ferramenta para controlar e mellorar os sistemas de seguridade mediante un proceso sistemático, documentado e coñecido por toda a organización.

## **1.2. Características principais dun SXSI**

Un **Sistema de Xestión da Seguridade da Información**, denominado habitualmente polas súas siglas **SXSI**, é unha ferramenta que implementa un conxunto de políticas de administración da información que permiten coñecer, xestionar e minimizar os posibles riscos que atenten contra a súa seguridade.

O concepto de SXSI constitúe o termo central sobre o que se define a norma **ISO 27001**.

A información é un dos principais activos das organizacións. A defensa deste activo é unha tarefa esencial para asegurar a continuidade e o desenvolvemento do negocio, así como tamén é unha esixencia legal

(protección da propiedade intelectual, protección de datos persoais, servizos para a sociedade da información), e ademais trasládalles confianza aos clientes e usuarios.

Canto maior é o valor da información, maiores son os riscos asociados á súa perda, subtracción, deterioro, manipulación indebida ou mal intencionada.

Os Sistemas de Xestión de Seguridade da Información (SXSI) son o medio máis eficaz de minimizar os riscos, ao asegurar que se identifican e valoran os activos e os seus riscos, considerando o impacto para a organización, e que se adoptan os controis e procedementos máis eficaces e coherentes coa estratexia de negocio.

Unha xestión eficaz da seguridade da información permite garantir:

- a súa confidencialidade, asegurando que só quen estea autorizado poida acceder á información,
- a súa integridade, asegurando que a información e os seus métodos de proceso son exactos e completos, e
- a súa dispoñibilidade, asegurando que os usuarios autorizados teñen acceso á información e aos seus activos asociados cando o requiran.

En moitas organizacións a maior parte da información reside en equipos informáticos, redes de datos e soportes de almacenamento, encadrados todos dentro do que se coñece como sistemas de información. Estes sistemas están suxeitos a riscos e inseguridades, tanto desde dentro da propia organización coma desde fóra. Aos riscos físicos (acceso de persoas non autorizadas á información, catástrofes naturais, incendios, etc.) haille que sumar os riscos lóxicos (accesos remotos non autorizados, virus, ataques de denegación de servizo, etc.).

A adecuada xestión da seguridade permite diminuír de forma significativa o impacto dos riscos sen necesidade de realizar grandes investimentos en software e sen contar cunha grande estrutura de persoal. Para iso faise necesario:

- Coñecer e afrontar de modo ordenado os riscos aos que está sometida a información.
- Contar coa participación activa de toda a organización, especialmente co apoio e a implicación da dirección.
- Establecer políticas, procedementos e controis de seguridade adecuados.
- Planificar e implantar controis de seguridade baseados nunha avaliación de riscos e nunha medición da eficacia daqueles.
- Realizar un proceso de avaliación e mellora continua.

Un SXSI axuda a unha organización a establecer as políticas, procedementos e controis en relación aos obxectivos de negocio da organización con obxecto de manter sempre o risco por baixo do nivel asumible pola propia organización. Ademais, proporciona unha cobertura completa da xestión da seguridade, desde o nivel estratéxico máis alto —onde a dirección definirá e aprobará as políticas de seguridade— ata o nivel máis baixo, onde, entre outras accións, se implantarán os controis técnicos e se xestionarán as incidencias do sistema.

Outra das vantaxes da implantación dun SXSI é a asistencia á organización no tratamento de aspectos clave como o cumprimento da legalidade, a adaptación dinámica e continuada ás condicións variables do contorno, a protección adecuada dos obxectivos de negocio para asegurar o máximo beneficio ou o aproveitamento de novas oportunidades de negocio.

En definitiva, mediante o uso dun SXSI, a organización coñece os riscos aos que está sometida a súa información e xestiónaos mediante un plan



definido, documentado e coñecido por todos, que se revisa e mellora constantemente.

### **1.3. Implementación dun SXSI**

Cando unha organización afronta a implantación dun SXSI debe ter presente que se trata dunha decisión de carácter estratéxico e que, daquela, afecta a toda a organización.

A tarefa da implantación non recaerá única e exclusivamente na área de tecnoloxías da información, senón que debe involucrar a toda a organización e estar apoiada e dirixida pola dirección. De feito, a primeira fase da implantación debería consistir en conseguir a aprobación e o apoio da dirección para todo o proceso.

O alcance e deseño do SXSI dependerá dos obxectivos da empresa, das súas características (actividade, tamaño, dispersión xeográfica, etc.), recursos económicos, etc. De feito, é posible que nalgúns casos o SXSI non se implante en todas as áreas da organización dun só paso, senón que se faga soamente naquelas nas que a información que se utiliza teña especial relevancia e que se complete o resto nunha implantación por fases.

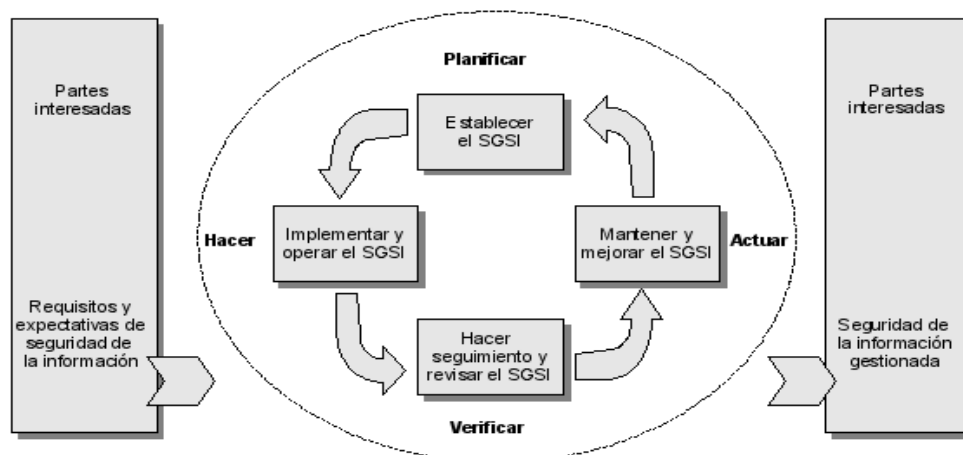
É frecuente a redefinición de políticas de seguridade da información, polo que o establecemento dun SXSI débese facer seguindo un método de implantación orientado á mellora continua. Isto pasa por unha metodoloxía cíclica que inclúa de maneira fundamental un mecanismo de retroalimentación en canto a erros e incidencias detectadas.

O método comunmente aceptado é o PDCA<sup>2</sup> (Planificar-Facer-Verificar-Actuar). Trátase dun modelo en catro fases, o cal, unha vez realizada a

---

<sup>2</sup> Siglas en inglés de *Plan-Do-Check-Act*, tamén coñecido como “Ciclo de Deming” en referencia ao estatístico Edwards Deming, quen promoveu o seu uso no ámbito do aseguramento da calidade.

última e analizados os resultados, continúa de novo na primeira fase do modelo.



**Imaxe 1: Esquema do modelo PDCA (fonte: Instituto Uruguayo de Normas Técnicas)**

### 1.3.1 Planificar (*Plan*)

Na primeira fase do modelo PDCA aplicado a SXSI realízase un estudo da situación da organización desde o punto de vista da seguridade para determinar o alcance das medidas que se van implantar en función das necesidades detectadas.

É importante realizar unha análise de riscos que valore os activos de información e as vulnerabilidades ás que están expostos, xa que non toda a información da que dispoñemos ten o mesmo valor ou está sometida aos mesmos riscos. O obxectivo é xestionar os devanditos riscos establecendo os controis axeitados que nos permitan minimizalos.

Durante esta fase realízanse as seguintes accións:

- o Estimación dos recursos económicos e de persoal que van ser necesarios para a correcta implantación e mantemento do SXSI.
- o Determinar o alcance do SXSI baseándose na información e nos procesos da organización que serán incluídos no SXSI. Deben quedar definidas as actividades da organización, as localizacións físicas que se van ver involucradas, a tecnoloxía da organización e tamén as áreas que quedarán excluídas na implantación do sistema.
- o Determinar a metodoloxía de avaliación de riscos apropiada para o SXSI e as características da nosa organización, ademais de establecer os criterios de aceptación do risco e de especificar os niveis de risco aceptables.
- o Revisar os aspectos organizativos da entidade e a asignación de novas responsabilidades. Deben existir polo menos tres roles fundamentais:
  - 1. O Responsable de Seguridade debe ser unha única persoa coa misión de coordinar todas as actuacións en materia de seguridade que se desenvolvan na organización.
  - 2. O Comité de Xestión farase cargo das accións da implantación do sistema colaborando moi estreitamente co responsable de seguridade da entidade. Este comité estará formado por persoal dos diferentes departamentos involucrados na implantación do sistema e terá potestade para asumir decisións de seguridade.
  - 3. O Comité de Dirección será o responsable de tomar e asumir decisións de alto nivel necesarias para apoiar os obxectivos do SXSI e estará formado por membros da dirección con poder executivo.

- o Establecer a **Política de Seguridade**. Trátase dun dos documentos máis importantes nun SXSI e debe estar aprobado polo comité de dirección. O seu principal obxectivo é recoller as directrices que debe seguir a seguridade da información consonte as necesidades da organización e a lexislación vixente. Ademais, debe establecer as pautas de actuación no caso de incidentes e definir as responsabilidades.

A política de seguridade plasmarase nun documento que debe estar accesible para todos os membros da organización e incluír, polo menos, os seguintes apartados:

1. Declaración de apoio por parte da Dirección aos obxectivos e principios da seguridade da información.
  2. Breve explicación das políticas.
  3. Definición da seguridade da información e os seus obxectivos globais, o alcance da seguridade e a súa importancia como mecanismo de control que permite compartir a información.
  4. Definición de responsabilidades xerais e específicas, nas que se incluírán os roles pero nunca persoas concretas dentro da organización.
  5. Referencias a documentación que poida sustentar a política.
- o Identificar e determinar as distintas opcións de xestión do risco e seleccionar aquelas que se van aplicar. Basicamente, existen tres opcións para o tratamento do risco:

1. Asumir o risco sen tomar ningunha medida. Isto é posible a condición de que non entre en conflito coa política de seguridade establecida pola organización.
  2. Transferir o risco mediante a contratación de servizos externos ou seguros. Evidentemente, isto non sempre é posible.
  3. Reducir o risco ata os niveis aceptables mediante a implantación de controis de seguridade.
- o Desenvolvemento da formación necesaria para que o persoal realice as súas actividades correctamente dentro da normativa que aplique o SXSI.
  - o Concienciación e divulgación entre o persoal da organización para que todos coñezan as accións que se están a levar a cabo e cales son as súas consecuencias e beneficios no marco da seguridade.
  - o Construír a declaración de Aplicabilidade<sup>3</sup>, que determina que controis son os que serán aplicados no sistema, cales se atopan xa implantados e cales non serán de aplicación e por que.

Como se pode apreciar, a carga de traballo nesta primeira fase do modelo PDCA para a xestión da seguridade é moi forte. Isto é algo lóxico e habitual en calquera sistema de xestión, onde a parte de planificación é un aspecto fundamental.

### 1.3.2 **Facer (Do):**

Os controis técnicos de seguridade elixidos na fase anterior son implantados nesta segunda fase do modelo PDCA desenvolvendo a

---

<sup>3</sup> Coñecida como SOA (Statement Of Applicability).

documentación necesaria. Esta fase tamén require un tempo de concienciación e formación para darlle a coñecer que se está facendo e por que ao persoal da empresa.

Nesta fase do modelo levaranse a cabo as seguintes tarefas:

- o Definir e implantar un plan de tratamento de riscos que identifique as accións, recursos, responsabilidades e prioridades na xestión dos riscos de seguridade da información. A finalidade deste plan será alcanzar os obxectivos de control identificados, incluíndo a asignación de recursos, responsabilidades e prioridades.
- o Definir un sistema de métricas que permita obter resultados reproducibles e comparables para medir a eficacia dos controis ou grupos de controis.
- o Xestionar os recursos necesarios asignados ao SXSI para o mantemento da seguridade da información.
- o Implantar procedementos e controis que permitan unha rápida detección e resposta ante os incidentes de seguridade.
- o Desenvolver programas de formación e concienciación en relación coa seguridade da información para todo o persoal.
- o Xestionar as operacións do SXSI.

### **1.3.3 Verificar (*Check*):**

A terceira fase do noso Modelo PDCA é a fase de verificación ou seguimento. Nela avalíase a eficacia e o éxito dos controis implantados.

Por iso, é moi importante contar con rexistros e indicadores que proveñan destes controis.

As tarefas que hai que realizar nesta fase son as seguintes:

- o Comprobar de modo continuo que o SXSI cumpre a política e obxectivos establecidos.
- o Medir a efectividade dos controis para verificar que se cumpren cos requisitos de seguridade.
- o Executar procedementos de monitorización e revisión para detectar incidentes e determinar se as accións levadas a cabo para solucionarlos foron efectivas.
- o Revisar regularmente en intervalos planificados as avaliacións de risco, os riscos residuais e os seus niveis aceptables, tendo en conta os posibles cambios que se puidesen producir na organización; revisar a tecnoloxía empregada, os obxectivos e procesos de negocio, as ameazas identificadas, a efectividade dos controis implantados e o contorno exterior; controlar os requisitos legais, as obrigas contractuais, etc.
- o Realizar periodicamente auditorías internas do SXSI en intervalos planificados.
- o Revisión periódica do SXSI por parte da dirección para garantir que o alcance definido segue a ser o adecuado e que as melloras no proceso do SXSI son evidentes.
- o Actualizar os plans de seguridade en función das conclusións e as novas descubertas realizadas durante as actividades de monitorización e revisión.

- o Rexistrar accións e eventos que poidan ter repercusións sobre a efectividade ou o rendemento do SXSI.

#### **1.3.4 Actuar (Act):**

Na última fase do modelo PDCA (ás veces chamada fase de mellora) lévanse a cabo os labores de mantemento do sistema. Se durante a fase anterior de seguimento se detectou algún punto débil, este é o momento de melloralo ou corrixilo, polo que esta fase se coñece ás veces como fase de mellora.

As tarefas que cómpre realizar nesta fase son as seguintes:

- o Realizar as accións preventivas e correctivas adecuadas.
- o Implantar no SXSI as melloras identificadas na fase anterior.
- o Asegurarse de que as melloras introducidas alcanzan os obxectivos previstos.
- o Comunicarlles as accións e melloras a todas as partes interesadas co nivel de detalle adecuado e acordar, se é pertinente, a forma de proceder.

Ao finalizar as catro fases, éntrase nun proceso iterativo de mellora continua partindo dos resultados da última e comézase novamente a primeira, conseguindo así unha retroalimentación do sistema coas solucións ás deficiencias atopadas.

### **1.4. A responsabilidade de dirección nun SXSI**

A implantación dun SGSI require que a dirección sexa consciente da importancia que terá dentro da organización. Se cae no erro de pensar que se trata dunha mera cuestión técnica que debe ser solucionada en solitario



pola área de tecnoloxías da información. Se o fai, a implantación do SXSI estará, de certo, condenada ao fracaso.

O apoio da alta dirección da organización debe materializarse na súa implicación no proceso asignando e proporcionando os recursos necesarios e preocupándose de formar e concienciar a toda a organización.

As tres responsabilidades principais da dirección serán:

- o A asignación de recursos, tanto económicos coma de persoal, ao desenvolvemento do SXSI, así como para o seu mantemento e adaptación se foren necesarios.
- o Revisión do SXSI para comprobar que segue a ser adecuado e eficiente para a organización. Esta revisión debe ser levada a cabo polo menos unha vez ao ano.
- o Concienciación e formación de todos os membros da organización na medida que corresponda en función da posición que ocupen.

### **1.5. Beneficios dun SXSI**

A seguridade da información é un aspecto fundamental que debe recibir unha especial consideración en toda organización. Os SXSI constitúen unha solución, case sempre de baixo custo, que axuda a controlar os riscos. Pero ademais, a mellora da seguridade trae consigo outros beneficios que se describen a continuación.

- **Cumprimento Legal:** A implantación dun SXSI serve para revisar e adaptar a nosa organización a aspectos relacionados coa lexislación do país que posiblemente no se tiveran en conta anteriormente.

- **Aforro Económico:** Un SXSI permite mellorar o uso dos recursos, o que repercute nun aforro de custos. Poder tomar decisións baseadas en datos cuantitativos e non só cualitativos permite xestionar mellor o gasto en TI. Deste xeito os investimentos en tecnoloxía axústanse ás prioridades que se impuxeron a través da Análise de Riscos, evitando os gastos innecesarios, inesperados, e sobredimensionados.
- **Redución de riscos:** é o fin último do SXSI. Partindo da Análise de Riscos ata a implantación dos controis, o conxunto de accións adoptadas reducirá os riscos de moitos aspectos da organización ata un nivel asumible.
- **Calidade da seguridade:** a implantación dun SXSI transforma a seguridade nunha actividade de xestión. Este concepto é importante, xa que deixa de lado un conxunto de actividades técnicas, máis ou menos organizadas, para se converter nun ciclo de vida metódico e controlado, no que, ao participar toda a organización, se crea conciencia e compromiso de seguridade en todos os niveis da empresa.
- **Competitividade no mercado:** contar cun SXSI é, sen dúbida, unha vantaxe competitiva, xa que contribúe a mellorar a xestión da organización e a darlle aos clientes confianza á hora de cederen a súa información á organización. Ademais, a norma ISO/IEC 27001 permite certificar a conformidade dun SXSI. Esta norma é tan importante como outras relacionadas coa calidade en diferentes áreas, por exemplo a ISO 9001. Pouco e pouco, as grandes empresas, os clientes e as administracións comezarán a esixir esta certificación para abrir e compartir os seus sistemas. Contar cunha certificación destas características convértese daquela nun importante factor

diferenciador coa competencia debido aos beneficios derivados da mellora de imaxe e vantaxe competitiva no mercado.

## **2. NORMAS DA SERIE ISO/IEC 27000**

### **2.1. As organizacións ISO e IEC**

A **Organización Internacional para a Estandarización** ISO<sup>4</sup> é unha federación de alcance mundial integrada na actualidade por institucións nacionais de estandarización de 162 países, unha por cada país. Ten a súa sede central en Xénova (Suíza), desde onde se coordinan as súas actividades. Trátase dunha organización non governamental que tenta desenvolver estándares en diferentes campos que cubran as necesidades tanto de empresas privadas como da propia sociedade en xeral.

A **Comisión Electrotécnica Internacional** IEC<sup>5</sup>, é tamén unha organización non governamental sen ánimo de lucro. Destaca por ser unha das organizacións máis importantes e activas do mundo no desenvolvemento de estándares internacionais para todo tipo de tecnoloxías relacionadas coa electricidade e a electrónica.

Algúns dos estándares con maior aceptación no mundo das tecnoloxías da información xurdiron do traballo coordinado destas dúas organizacións. Falamos de normas como a ISO/IEC 8613 (Arquitectura Open Document) ou a ISO/IEC 9945 (*Portable Operating System Interface* - POSIX) entre moitas outras, que se converteron en estándares relacionados con conceptos de tecnoloxías da información profundamente implantados e aceptados.

Existe, non obstante, un conxunto de normas que destacan pola súa relación co concepto da calidade en diferentes campos das tecnoloxías da

---

<sup>4</sup> Siglas en inglés de *International Organization for Standardization*.

<sup>5</sup> Siglas en inglés de *International Electrotechnical Commission*.

información. Trátase de ISO/IEC 15504 (SPICE), sobre a calidade nos procesos de construción do software; a serie ISO/IEC 20000, centrada na xestión de servizos de tecnoloxías da información; e a serie ISO/IEC 27000 para a xestión da seguridade de sistemas de información.

## **2.2. A serie ISO/IEC 27000**

A serie de normas ISO/IEC 27000<sup>6</sup> proporciona recomendacións de boas prácticas sobre xestión, riscos e controis no ámbito da seguridade da información, conformando o que se coñece como Sistemas de Xestión da Seguridade da Información.

O conxunto de normas é aplicable a calquera organización sen importar o seu tamaño, e segue un patrón de implantación baseado no modelo PDCA (*Plan-Do-Check-Act*), descrito anteriormente.

O deseño da serie é semellante a outras normas de aseguramento da calidade para sistemas de xestión (especialmente á serie ISO 9000). Os rangos reservados de numeración por ISO para normas desta serie van de 27000 a 27019 e de 27030 a 27044.

As seguintes normas da serie xa foron publicadas e están a ser usadas na práctica:

- ISO/IEC 27000: SXSI - Presentación e vocabulario.
- ISO/IEC 27001: SXSI - Requisitos.
- ISO/IEC 27002: Código de boas prácticas para a xestión da seguridade da información.

---

<sup>6</sup> Coñecida ás veces simplemente como ISO 27000 ou ISO27K

- ISO/IEC 27003: Guía de implantación de SXSI.
- ISO/IEC 27004: Xestión da seguridade da información – Métricas.
- ISO/IEC 27005: Xestión de riscos da seguridade da información.
- ISO/IEC 27006: Requisitos para organismos de auditoría e certificación de SXSI.
- ISO/IEC 27011: Guía sectorial de xestión da seguridade da información para organizacións de telecomunicacións.
- ISO/IEC 27031: Guía de xestión da información e as tecnoloxías das comunicacións para a continuidade do negocio.
- ISO/IEC 27033: Introducción e conceptos da seguridade na rede. Parte I.
- ISO 27799: Guía sectorial para a aplicación da norma ISO/IEC 27002 en contornos relacionados coa saúde.

Os textos traducidos ao castelán dalgunhas das normas desta serie pódense obter (pagando) da páxina web de AENOR (<http://www.aenor.es>).

A serie poderíase completar nun futuro próximo coas seguintes normas:

- ISO/IEC 27007: Guía para a auditoría de SXSI centrada nas actividades de xestión.
- ISO/IEC 27008: Guía para a auditoría de SXSI centrada nos controis de seguridade da información.

- ISO/IEC 27013: Guía para a implantación integrada de ISO/IEC 20000-1 e ISO/IEC 27001.
- ISO/IEC 27036: Guía para a seguridade de servizos externalizados (*outsourcing*).

### 2.3. Contido da norma

O número de normas incluídas na serie é bastante elevado, polo que nos centraremos unicamente na descrición do contido dalgunhas delas: 27001, 27002, 27003 e 27006.

#### 2.3.1 ISO/IEC 27001

Esta norma substituíu a antiga BS7799-2<sup>7</sup> con data de publicación 15 de outubro do 2005, e céntrase na definición dun modelo para a creación, implantación, operación, supervisión, revisión, mantemento e mellora dun SXSI. É a única norma na que unha organización se pode certificar dentro do esquema.

Dentro desta norma podemos atopar os seguintes apartados:

- o **Introdución:** xeneralidades e introdución ao método PDCA.
- o **Obxecto e campo de aplicación:** especificase o obxectivo, a aplicación e o tratamento de exclusións.
- o **Normas para consulta:** outras normas que poden servir de referencia no proceso.
- o **Termos e definicións:** breve descrición dos termos máis usados na norma.

---

<sup>7</sup> Da British Standards Institution (BSI), a organización británica equivalente a AENOR en España.

- o **Sistema de xestión da seguridade da información:** como crear, implantar, operar, supervisar, revisar, manter e mellorar o SXSI; requisitos de documentación e control da mesma.
- o **Responsabilidade da dirección:** en canto a compromiso co SXSI, xestión e provisión de recursos e concienciación, formación e capacitación do persoal.
- o **Auditorías internas do SXSI:** como realizar as auditorías internas de control e cumprimento.
- o **Revisión do SXSI pola dirección:** como xestionar o proceso periódico de revisión do SXSI por parte da dirección.
- o **Mellora do SXSI:** mellora continua, accións correctivas e accións preventivas.
- o **Anexo A: Obxectivos de control e controis.**
- o **Anexo B: Relación cos Principios da Organización para a Cooperación e o Desenvolvemento Económico (OCDE).**
- o **Anexo C: Correspondencia con outras normas.**
- o **Bibliografía:** normas e publicacións de referencia.

A norma ISO 17799, que constituía un código de boas prácticas para a seguridade da información, converteuse na ISO/IEC 27002 desde o 1 de xullo do 2007. Trátase máis dun código de boas prácticas que dunha norma coma tal. Non establece obrigatoriedade nas súas especificacións e cabe recordar que non é unha norma certificable. En lugar diso, presenta 39 obxectivos de control e desagrega os 139 controis presentados no Anexo A da ISO/IEC 27001, dando ás veces varias opcións de implantación, que poderían ser, en teoría, implantados tomando como guía as especificacións da ISO/IEC 27001.

O contido da norma ten a súa orixe nun documento do goberno do Reino Unido que se converteu en 1995 na norma BS7799 e, posteriormente, no

ano 2000, na norma ISO 17799:2000, cunha versión posterior 17799:2005. Finalmente, no 2007 publícase a norma ISO/IEC 27002, que substitúe a citada 17799:2005.

Os plans de ISO para estes estándares pasan por centrarse noutros códigos de boas prácticas sectoriais, como por exemplo, no contorno da saúde (xa publicada en forma de ISO/IEC 27799).

Dentro desta norma poderemos atopar os seguintes apartados:

- o **Introdución:** conceptos xerais de seguridade da información e SXSI.
- o **Campo de aplicación:** especificase o obxectivo da norma.
- o **Termos e definicións:** breve descrición dos termos máis usados na norma.
- o **Estrutura do estándar:** descrición da estrutura da norma.
- o **Avaliación e tratamento do risco:** indicacións sobre como avaliar e tratar os riscos de seguridade da información.
- o **Política de seguridade:** documento de política de seguridade e a súa xestión.
- o **Aspectos organizativos da seguridade da información:** organización interna; terceiros.
- o **Xestión de activos:** responsabilidade sobre os activos; clasificación da información.
- o **Seguridade ligada aos recursos humanos:** antes do emprego; durante o emprego; finalización do emprego ou cambio de posto de traballo.
- o **Seguridade física e ambiental:** áreas seguras; seguridade dos equipos.



- o **Xestión de comunicacións e operacións:** responsabilidades e procedementos de operación; xestión da provisión de servizos por terceiros; planificación e aceptación do sistema; protección contra código malicioso e descargable; copias de seguridade; xestión da seguridade das redes; manipulación dos soportes; intercambio de información; servizos de comercio electrónico; supervisión.
- o **Control de acceso:** requisitos de negocio para o control de acceso; xestión de acceso de usuario; responsabilidades de usuario; control de acceso á rede; control de acceso ao sistema operativo; control de acceso ás aplicacións e á información; ordenadores portátiles e teletraballo.
- o **Adquisición, desenvolvemento e mantemento dos sistemas de información:** requisitos de seguridade dos sistemas de información; tratamento correcto das aplicacións; controis criptográficos; seguridade dos arquivos de sistema; seguridade nos procesos de desenvolvemento e soporte; xestión da vulnerabilidade técnica.
- o **Xestión de incidentes de seguridade da información:** notificación de eventos e puntos débiles da seguridade da información; xestión de incidentes de seguridade da información e melloras.
- o **Xestión da continuidade do negocio:** aspectos da seguridade da información na xestión da continuidade do negocio.
- o **Cumprimento:** cumprimento dos requisitos legais; cumprimento das políticas e normas de seguridade e cumprimento técnico; consideracións sobre as auditorías dos sistemas de información.
- o **Bibliografía:** normas e publicacións de referencia.

### **2.3.3 ISO/IEC 27003**

A norma ISO/IEC 27003, cuxa última versión publicada data de febreiro do 2010 , constitúe a "Guía oficial de implantación dun SXSI" en calquera organización. O seu contido céntrase nos aspectos críticos necesarios para un acertado deseño e implantación dun SXSI de acordo coa norma ISO/IEC 27001:2005. Describe o proceso de delimitación dun SXSI e o deseño e posta en marcha de diferentes plans de implantación. Igualmente, inclúe o proceso para obter a aprobación da dirección para implantar un SXSI, define un alcance inicial do SXSI e proporciona unha guía de como facer desde a planificación inicial ata a implantación final dun proxecto de SXSI.

Dentro desta norma poderemos atopar os seguintes apartados:

- o                   **Alcance:** descrición do contido da norma, que na práctica abarca a totalidade do proceso de implantación dun SXSI paso por paso.
- o                   **Referencias Normativas:** outras normas e documentos de referencia.
- o                   **Termos e Definicións:** breve descrición dos termos máis usados na norma.
- o                   **Estrutura desta Norma Internacional:** descrición da estrutura da propia norma.
- o                   **Obter a aprobación da alta dirección para iniciar un SXSI.**
- o                   **Definir o alcance do SXSI, limites e políticas.**
- o                   **Avaliación dos requisitos de seguridade da información.**
- o                   **Avaliación de Riscos e Plan de tratamento de riscos.**
- o                   **Deseño do SXSI.**

- o **Anexo A: lista de recoñecemento para a implantación dun SXSí.**
- o **Anexo B: roles e responsabilidades en seguridade da información.**
- o **Anexo C: información sobre auditorías internas.**
- o **Anexo D: estrutura das políticas de seguridade.**
- o **Anexo E: monitorización e seguimento do SXSí.**

#### **2.3.4 ISO/IEC 27006**

Coñecida formalmente como *Information technology - Security techniques. Requirements for bodies providing audit and certification of information security management systems*, está composta por dez capítulos e catro anexos. Constitúese como unha guía para a acreditación de organizacións que desexen converterse en certificadores das normas da serie ISO/IEC 27000 relativas a sistemas de xestión da seguridade da información. Baséase na norma xeral de certificación ISO 17021<sup>8</sup>, á cal lle engade requisitos específicos referentes a SXSí.

Dentro desta norma poderemos atopar os seguintes apartados:

- o **Preámbulo:** presentación das organizacións ISO e IEC e as súas actividades.
- o **Introdución:** antecedentes de ISO 27006 e guía de uso para a norma.
- o **Campo de aplicación:** a quen se lle aplica este estándar.
- o **Referencias normativas:** outras normas que serven de referencia.

---

<sup>8</sup> Norma ISO que define requisitos para organismos que realizan a auditoría e a certificación de sistemas de xestión.

- o **Termos e definicións:** breve descrición dos termos máis usados na norma.
- o **Principios:** principios que rexen esta norma.
- o **Requisitos xerais:** aspectos xerais que deben cumprir as entidades de certificación de SXSI.
- o **Requisitos estruturais:** estrutura organizativa que deben ter as entidades de certificación de SXSI.
- o **Requisitos en canto a recursos:** competencias esixidas ao persoal de dirección, administración e auditoría da entidade de certificación, así como aos auditores externos, expertos técnicos externos e subcontratas.
- o **Requisitos de información:** información pública, documentos de certificación, relación de clientes certificados, referencias á certificación e marcas, confidencialidade e intercambio de información entre a entidade de certificación e os seus clientes.
- o **Requisitos do proceso:** requisitos xerais do proceso de certificación; auditoría inicial e certificación; auditorías de seguimento; recertificación; auditorías especiais; suspensión; retirada ou modificación de alcance da certificación; apelacións; reclamacións e rexistros de solicitantes e clientes.
- o **Requisitos do sistema de xestión de entidades de certificación:** requisitos do sistema de xestión de acordo con ISO 9001 e requisitos do sistema de xestión xeral.
- o **Anexo A - Análise da complexidade da organización dun cliente e aspectos específicos do sector.**
- o **Anexo B - Áreas de exemplo de competencia do auditor.**
- o **Anexo C - Tempos de auditoría.**
- o **Anexo D - Guía para a revisión de controis implantados do Anexo A de ISO 27001:2005.**

## **2.4. O proceso de implantación**

A implantación dun SXSI segundo a norma ISO/IEC 27001 realízase seguindo o xa citado modelo PDCA. A duración do proceso de implantación depende das características propias da organización, como poden ser o seu tamaño, o tipo de actividades que realice e tamén do estado de madurez en que se atopen os seus procesos de xestión e control da información. En todo caso, é fundamental realizar unha análise inicial e unha planificación do proceso completo de implantación para obter un bo resultado.

A implantación do SXSI pode ser nalgúns casos complicada e custosa, e non é estraño que se produzan desviacións respecto á planificación inicial. Isto ocorre sobre todo cando non existe unha boa planificación inicial.

Hai que ter presente, unha vez máis, que a implantación non é unha tarefa que lles incumba exclusivamente ás áreas de TI da organización, senón que todas as áreas de negocio se deben ver involucradas no proceso. É habitual que a organización designe un ou varios auditores internos que dirixirán o proceso de implantación. Estes auditores internos adoitan pertencer ao departamento de TI. Xunto a eles, representantes das principais áreas de negocio conformarán o equipo interno de implantación.

Ademais de contar con auditores internos, é bo contar coa axuda dalgunha empresa externa especializada na implantación deste tipo de sistemas. Esta empresa proporcionará auditores externos que traballarán en colaboración co equipo interno. En España, o Instituto Nacional de Tecnoloxías da Comunicación (INTECO) dispón dun catálogo de empresas que ofrecen este tipo de servizos.

É importante lembrar que a organización debe contar cunha estrutura organizativa así como cos recursos necesarios, entre outras cousas, para levar a cabo a implantación do SXSI. A implantación e o mantemento do

SXSI consumirán recursos que deben estar dispoñibles no tempo e que a organización debe prover adecuadamente. Non en balde a base de calquera Sistema de Xestión de Seguridade da Información é a continua avaliación e mellora, seguindo o modelo PDCA.

A documentación e o seu ciclo de vida teñen unha importancia capital dentro dun SXSI. A implantación e mantemento do noso SXSI debe estar documentada, e ademais existe un ciclo de vida da documentación que debe seguirse para garantir que toda ela se encontre actualizada e dispoñible para os usuarios que a requiran. ISO/IEC 27000 recolle catro tipos distintos de documentación:

- **Políticas:** sentan as bases da seguridade. Indican as liñas xerais para conseguir os obxectivos da organización sen entrar en detalles técnicos. Toda a organización debe coñecer estas Políticas.
- **Procedementos:** desenvolven os obxectivos marcados polas Políticas. Neles aparecen detalles máis técnicos e concrétase como conseguir os obxectivos expostos nas Políticas. Os Procedementos deben ser coñecidos por aquelas persoas que o precisen para o desenvolvemento das súas funcións.
- **Instrucións:** constitúen o desenvolvemento dos Procedementos. Neles descríbense os comandos técnicos que se deben realizar para a execución dos Procedementos.
- **Rexistros:** evidencian a efectiva implantación do sistema e o cumprimento dos requisitos. Entre estes Rexistros inclúense indicadores e métricas de seguridade que permitan avaliar as consecuencias dos obxectivos de seguridade establecidos.

Para os documentos xerados débese establecer, documentar, implantar e manter un procedemento que defina as accións de xestión necesarias orientadas a:

- Aprobar documentos apropiados antes da súa emisión.
- Revisar e actualizar documentos cando sexa necesario e renovar a súa validez.
- Garantir que os cambios e o estado actual de revisión dos documentos están identificados.
- Garantir que as versións relevantes de documentos vixentes están dispoñibles nos lugares de emprego.
- Garantir que os documentos se manteñen lexibles e facilmente identificables.
- Garantir que os documentos permanecen dispoñibles para aquelas persoas que os necesiten e que son transmitidos, almacenados e finalmente destruídos de acordo cos procedementos aplicables segundo a súa clasificación.
- Garantir que os documentos procedentes do exterior están identificados.
- Garantir que a distribución de documentos está controlada.
- Prever a utilización de documentos obsoletos.
- Aplicar a identificación apropiada a documentos que son retidos con algún propósito.

## **2.1. O proceso de certificación**

Unha vez que o noso SXSI estea totalmente implantado poderíamos optar a certificalo coa norma ISO/IEC 27001. Isto é, que unha entidade de certificación audite o noso sistema e obteñamos un documento que asegure que o SXSI da nosa organización é acorde coa norma. Hai que ter presente que esta certificación non proba que os controis e medidas de seguridade implantadas sexan as correctas, senón que a seguridade da

información se xestiona na forma que indica a norma. Hai unha máis que sutil diferenza.

No momento de seleccionar unha entidade certificadora, debémonos asegurar de que conta con auditores cualificados para verificar a correcta implantación do sistema segundo a norma ISO/IEC 27001. Ademais, deberemos comprobar que posúe a adecuada acreditación que a recoñece como unha entidade competente para a realización desta actividade. A entidade de certificación debe estar acreditada para a norma na que se desexa realizar a certificación, asegurando así que cumpre cos requisitos para realizar correctamente o seu traballo.

A entidade de acreditación española é a Empresa Nacional de Certificación (ENAC), aínda que existen numerosas entidades de acreditación en todo o mundo. As empresas certificadoras poderían estar acreditadas por unha entidade que non fose a española. Neste caso sería necesario que a entidade de acreditación validase as actividades tamén no territorio español, indicándoo especificamente nas súas credenciais.

Unha vez seleccionada a entidade de certificación e presentadas evidencias de que o noso SXSI se encontra implantado e funcionando, poderemos comezar realmente o proceso de certificación. Do mesmo xeito que no proceso de implantación, hai que ter presente que a organización debe contar con recursos económicos e de persoal destinados á realización do proceso de certificación, posto que os auditores necesitarán axuda e colaboración do persoal da organización para realizar as súas tarefas.

O proceso de certificación pódese dividir en tres fases principais:

- o **Xestión da solicitude de certificación:** a empresa débelle solicitar unha oferta á entidade de certificación na que se especificarán unha serie de datos sobre a organización e a



- implantación do SXSI, tales coma o alcance, o número de empregados e os centros de traballo dentro do alcance, etc. Con iso a empresa poderá presentarnos unha oferta que inclúa tempo e custo. Incluirá en todo caso o número de días de duración da auditoría así como o número de auditores que a levarán a cabo.
- o **Auditoría Documental:** a continuación ten lugar a auditoría documental, que é a primeira fase da auditoría. Nela revísase a documentación xerada durante a implantación do sistema. Incluirá, polo menos, a política de seguridade, o alcance da certificación, a análise de riscos, a selección dos controis de acordo coa declaración de aplicabilidade (SOA) e a revisión da documentación controis seleccionados pola entidade de certificación.
  - o **Auditoría In-Situ:** A segunda fase da auditoría é a auditoría in-situ. Nesta fase o equipo de auditores da entidade de certificación desprázase ás instalacións da organización. Durante o tempo planificado traballarán en colaboración con membros da empresa para realizar a revisión do SXSI en funcionamento. Durante esta fase os auditores verifican de novo a documentación revisada na fase anterior, confirman que a organización cumpre coas súas políticas e procedementos, comprobando que o sistema desenvolvido está conforme coas especificacións da norma e verifican que se están logrando os obxectivos marcados pola organización.

Como resultado de cada unha das fases da auditoría externa, a entidade certificadora emite un informe que pode conter os seguintes resultados:

- o Todo correcto. Non existe ningunha *non conformidade* e acéptase a certificación do sistema.

- o Observacións sobre o sistema que non teñen excesiva relevancia pero que deben ser tidas en conta na seguinte fase da auditoría, ben para ser revisadas in-situ ou ben para ser melloradas no seguinte ciclo de mellora.
- o No conformidades menores. Estas son incidencias atopadas na implantación e que se poden corrixir mediante a presentación dun Plan de Accións Correctivas no que se identifica a incidencia e a maneira de solucionala.
- o No conformidades maiores que deben ser corrixidas pola empresa. Sen a súa resolución e, na maior parte dos casos, a realización dunha auditoría extraordinaria por parte da entidade de certificación, non se obtería o certificado, xa que se trata de incumprimentos graves da norma. En caso de darse tras a auditoría documental é necesario a súa resolución antes de levar a cabo a auditoría in-situ.

Unha vez conseguida a certificación do sistema, este ten unha validez de tres anos, aínda que está suxeito a revisións anuais. Durante o primeiro ano realízase a auditoría inicial. Posteriormente, cada tres anos realízase unha auditoría de renovación. Nos dous anos posteriores, tanto á auditoría inicial como ás de renovación, realízanse auditorías de seguimento.

### **3. REFERENCIAS**

- Instituto Nacional de Tecnoloxías da Comunicación - Centro de Resposta a Incidentes de Seguridade. (<http://cert.inteco.es>)
- Asociación Española de Normalización e Certificación. ([www.aenor.es](http://www.aenor.es))
- O portal de ISO 27001 en Español. ([www.iso27000.es](http://www.iso27000.es))
- The ISO 27000 Directory. ([www.27000.org](http://www.27000.org))
- International Organization for Standardization (ISO). ([www.iso.org](http://www.iso.org))
- International Electrotechnical Commission (IEC). ([www.iec.ch](http://www.iec.ch))
- Instituto Uruguayo de Normas Técnicas. (<http://www.unit.org.uy/iso27000/>)

(Todas as ligazóns foron verificadas en xuño do 2011)

**Autor: Juan Otero Pombo**  
**Enxeñeiro en Informática no Concello de Ourense**  
**Colexiado do CPEIG**



## **42. VIRUS E OUTRO SOFTWARE MALIGNO. TIPOS. MEDIOS PREVENTIVOS E REACTIVOS. SISTEMAS ANTIVIRUS E DE PROTECCIÓN.**

## **TEMA 42: VIRUS E OUTRO SOFTWARE MALIGNO. TIPOS. MEDIOS PREVENTIVOS E REACTIVOS. SISTEMAS ANTIVIRUS E DE PROTECCIÓN.**

### **ÍNDICE**

<b>1. VIRUS E OUTRO SOFTWARE MALIGNO. TIPOS.....</b>	<b>2</b>
ÍNDICE.....	1
<b>2. MEDIOS PREVENTIVOS E REACTIVOS.....</b>	<b>22</b>
<b>3. SISTEMAS ANTIVIRUS E DE PROTECCIÓN.....</b>	<b>24</b>
<b>4. REFERENCIAS.....</b>	<b>30</b>

## VIRUS E OUTRO SOFTWARE MALIGNO. TIPOS.

### 1.1. Introducción

Os sistemas informáticos atópanse permanentemente expostos á ameaza dos virus informáticos cuxo nome provén da analoxía do seu comportamento cos virus biolóxicos.

Desde que apareceron os primeiros virus na década dos setenta, existiron sempre ameazas deste tipo que, nalgúns casos, chegaron a converterse en verdadeiras epidemias que infectaron millóns de ordenadores e deron lugar a perdas económicas importantes. Exemplos destas grandes epidemias foron as xeradas polo verme de *Morris*, *Melissa* ou *ILoveYou*.

En realidade os virus son un subtipo do software maligno en xeral que adoita denominarse como *malware*. Os troianos e vermes son tamén tipos de *malware* que, xunto aos virus, constitúen os tres tipos principais de software maligno que atacan os sistemas informáticos, e existen moitas outras variantes ou subtipos destes: *adware*, *spyware*, *scareware*, etc.

Na actualidade, o tipo de *malware* máis estendido son os troianos, destinados a se instalaren en sistemas de usuarios para roubar información confidencial —nomes de usuarios, números de tarxetas de crédito, etc.— e enviárllela aos atacantes. Os atacantes sérvense da rede internet para recibir e usar a información a milleiros de quilómetros, noutros países onde as leis non recollen delitos deste tipo e se encontran a salvo. Isto permítelles obter beneficios económicos, xa que a creación de programas maliciosos é un negocio lucrativo.

## **1.2. Malware**

O *malware*<sup>1</sup> é un tipo de software que ten como obxectivo infiltrarse ou danar unha computadora sen o consentimento do seu propietario. O termo *malware* é moi utilizado por profesionais da informática para se referiren a unha variedade de software hostil, intrusivo ou molesto.

Colateralmente, o *malware* adoita perseguir un lucro de modo directo ou indirecto por parte do atacante. O nivel de dano que recibe o usuario pode ir desde pequenas alarmas inofensivas a efectos desastrosos, como a perda masiva de datos. Internet resulta ser un medio moi apropiado para distribuír o *malware* de forma que se maximice o número de usuarios afectados.

Podemos establecer unha primeira clasificación de *malware* en tres tipos principais perfectamente diferenciados: virus, vermes e troianos. A partir de aí existen multitude de elementos perigosos que poderían ser catalogados nun ou noutro tipo (ou en varios á vez). Así, é común oír falar de:

- *Adware*: é un software que desprega publicidade de distintos produtos ou servizos. Estas aplicacións inclúen código adicional que mostra a publicidade en ventás emerxentes, ou a través dunha barra que aparece na pantalla simulando ofrecer distintos servizos útiles para o usuario. Normalmente, agregan iconas gráficas nas barras de ferramentas dos navegadores de internet ou nos clientes de correo, que teñen palabras clave predefinidas para que o usuario chegue a sitios con publicidade, sexa o que sexa que estea a buscar.
- *Spyware*: ou software espía, é unha aplicación que recompila información sobre unha persoa ou organización sen o seu

---

<sup>1</sup> Das palabras inglesas *malicious software*.



coñecemento nin consentimento. O obxectivo máis común é distribuírlo a empresas publicitarias ou outras organizacións interesadas. Normalmente este software envíalles información aos seus servidores, en función dos hábitos de navegación do usuario. Tamén recolle datos acerca dos sitios web polos que se navega e a información que se solicita neses sitios, así como enderezos IP e URL que se visitan. Esta información é explotada con fins de mercadotecnia, e moitas veces é a orixe doutra praga coma o SPAM, xa que pode dirixir publicidade personalizada cara ao usuario afectado. Con esta información, ademais, é posible crear perfís estatísticos dos hábitos dos internautas. Estes tipos de software adoitan “disfrazarse” de aplicacións útiles que cumpren unha función para o usuario, e a súa descarga ofrécese en moitos sitios recoñecidos.

Cabe destacar que o atacante non ten por que ser un delincuente. Por exemplo, o FBI desenvolveu a súa propia aplicación *spyware*, chamada MagicLantern, usada en investigacións criminais para obter información dos sospeitosos.

- *Crimeware*: é un tipo de programa de ordenador deseñado especificamente para cometer crimes de tipo financeiro ou semellantes e que tenta pasar desapercibido ante a vítima. Por extensión, tamén fai referencia a aplicacións web con iguais obxectivos.

Un *crimeware* pode roubar datos confidenciais, contrasinais, información bancaria, etc. e tamén pode servir para roubar a identidade ou espiar unha persoa ou empresa.

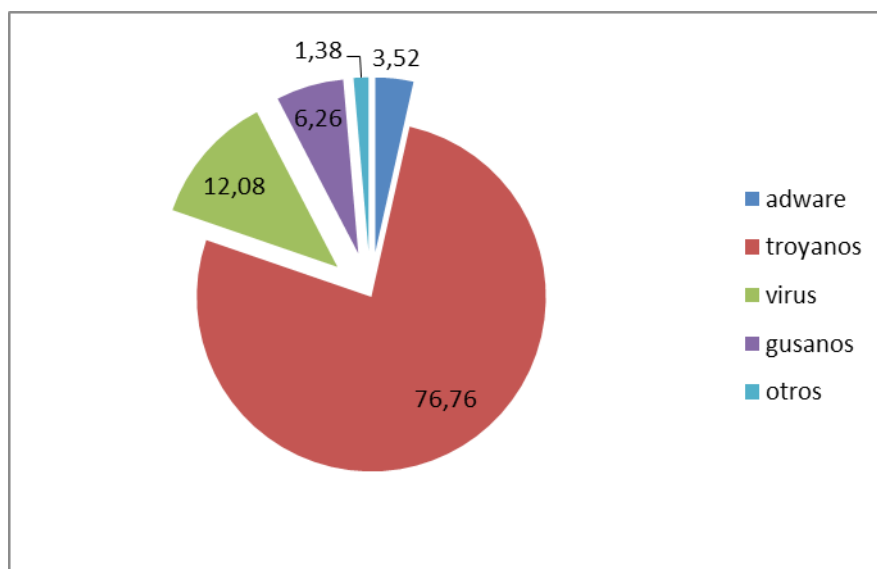
- *Scareware*: termo acuñado recentemente, é o que se coñece como “software de seguridade falso”. Normalmente este software



benefíciase da intención dos usuarios de manter os seus equipos protexidos, e especificamente emprega técnicas de enxeñería social que se basean sobre todo en crear “paranoia” neles, ofrecéndolles unha solución definitiva aos seus problemas de seguridade. Unha vez instalados, este tipo de programas dedícanse a roubar información como o faría calquera troiano bancario ou usurpador de identidade no equipo da vítima.

- Un novo tipo de *malware* comeza a aparecer con forza asociado ao crecemento das redes sociais. Trátase de aplicacións maliciosas que se moven dentro do contexto de redes sociais destinadas a roubar datos persoais, suplantar identidades, etc. Un exemplo é o verme *Koobface*, que ataca a varias redes sociais moi coñecidas, incluíndo Facebook, Twitter e Myspace.

O seguinte gráfico mostra a distribución de tipos de *malware* detectados en datas recentes<sup>2</sup>:




---

<sup>2</sup> A maioría de grandes empresas dedicadas ao desenvolvemento de antivirus ofrecen frecuentemente informes sobre os tipos de *malware* detectados, os virus máis activos, alertas especiais, etc.

## **Estatísticas de *malware* por tipos do terceiro trimestre do 2011 (fonte: Panda Security)**

LENDAS: adware / troianos / virus / vermes / outros.

### **1.3. Virus**

Os virus informáticos son porcións de código malicioso que se poden introducir nos ordenadores e sistemas informáticos de formas moi diversas, producindo efectos molestos, nocivos e mesmo destrutivos e irreparables. Ademais, o efecto inicial que o caracteriza é unha infección do equipo, seguida dunha propagación do virus a medida que se executan os arquivos onde reside. É dicir, o código do virus execútase só cando se executa o programa ou se abre o arquivo infectado. Isto é o que diferencia os virus dos vermes (que veremos máis adiante): se non se accede ao programa ou arquivo, o virus non se executa e, xa que logo, non se propaga.

#### **1.3.1. Funcionamento dos virus**

A propia denominación de virus informáticos provén da analoxía do funcionamento destes cos virus biolóxicos. Un virus biolóxico non pode sobrevivir de forma independente. En realidade, non é máis que unha cadea de ADN protexida por unha cobertura externa que se reproduce introducíndose nunha célula hóspede e usando o mecanismo reprodutor desa célula para reproducirse el mesmo.

Un virus informático tampouco é independente nin ten a capacidade de sobrevivir e reproducirse de xeito illado. Trátase dunha secuencia de código maligno que, para poder propagarse, necesita infectar un hóspede, que, neste caso, será un programa informático ou un documento.

Moitos virus escóndense dentro de arquivos de programas aparentemente limpos. Estes virus coñécense como virus de arquivo e o seu código

execútase ao cargarse na memoria principal da máquina xunto co programa que o contén. Desde alí, o código do virus pode buscar outros programas no sistema que poidan ser infectados. Se atopa un, o virus introduce o seu código nese programa, que, unha vez infectado, tamén pode ser usado para infectar a máis programas, iniciando así unha cadea infecciosa semellante a unha epidemia dun virus biolóxico.

A maioría dos virus non só se replican a eles mesmos, senón que tamén realizan outras operacións que habitualmente son daniñas para os seus hóspedes. Así, por exemplo, un virus pode eliminar certos arquivos vitais dun sistema, sobrescribir o sector de arranque dun disco duro deixando o disco inhabilitado, amosar mensaxes na pantalla, emitir ruídos, e moitas outras accións de maior ou menor poder destrutivo.

En xeral, os virus están deseñados para executar o seu código daniño no momento de seren executados. Con todo, hai outros que non atacan nese momento, senón que están deseñados para agardar a unha data concreta ou a un evento particular. Estes virus permanecen en estado latente no sistema ata que actúan.

### **1.3.2. Caracterización dos virus**

Existen moitos tipos de virus, pero podemos indicar algunhas características comúns a todos eles:

- **Latencia:** os virus teñen capacidade para permanecer inactivos, nun estado latente, ata que un evento os active. Este evento pode ser a execución dun programa, a lectura do sector de arranque, etc. Unha vez activado, o virus pode realizar as tarefas para as que estaba programado e replicarse.

- **Tipo de residencia:** os virus máis avanzados son capaces de camuflarse para evitar seren detectados e erradicados. Os virus máis básicos necesitan permanecer continuamente na memoria principal, namentres que estoutros virus máis avanzados son capaces de residir noutros lugares como a memoria secundaria. Poden chegar mesmo a modificar a táboa de asignación de arquivos para camuflar a súa presenza.
- **Forma de infección:** trátase dunha característica común de todos os virus. O medio polo que un virus infecta varía enormemente duns a outros: execución de programas, de macros, conexións mediante determinados protocolos, o simple arranque dunha máquina, etc.
- **Composición:** calquera virus informático conta con tres partes destinadas a cumprir cos seus obxectivos:
  - o **Sistema de reprodución:** encargado de infectar outros sistemas ou arquivos mediante o aproveitamento (ilícito) dos recursos da máquina hóspede.
  - o **Sistema de ataque:** en caso de existir, trátase dunha serie de rutinas destinadas a danar o sistema hóspede dun xeito ou doutro. O dano pode ir desde pequenos inconvenientes, como mensaxes molestas, ata ataques desastrosos, como a perda masiva de datos.
  - o **Sistema de defensa:** destinado a ocultar a presenza do virus mentres sexa posible e a dificultar a súa eliminación.

### **1.3.3. Ciclo de vida dos virus**

Existen unha serie de fases polas que un virus pasa ao longo da súa vida:



- **Creación:** o virus é creado por programadores que escriben o seu código.
- **Contaxio:** o contaxio inicial ou os contaxios posteriores realízanse cando o programa contaminado está na memoria para ser executado. As vías polas que se pode producir a infección do sistema son disquetes, memorias flash, redes de ordenadores e calquera outro medio de transmisión de información. Estes disquetes contaminantes adoitan conter programas de fácil e libre circulación e carecen de toda garantía. É o caso dos programas de dominio público, as copias ilegais dos programas comerciais, xogos, etc.
- **O virus activo:** Cando se di que un virus se activa significa que o virus toma o control do sistema e, ao mesmo tempo que deixa que funcionen normalmente os programas que se executan, realiza actividades non desexadas que poden causar danos nos datos ou nos programas.

O primeiro que adoita facer o virus é cargarse na memoria do ordenador e modificar determinadas variables do sistema que lle permiten “facerse un oco” e impedir que outro programa o utilice. A esta acción chámase “facerse residente”. Así, o virus permanece á espera de que se dean certas condicións —que varían duns virus a outros— para replicarse ou atacar.

A replicación, que é o mecanismo máis característico e, para moitos expertos, definitorio da condición de virus, consiste basicamente na produción polo propio virus dunha copia de si mesmo, que se situará nun arquivo. O contaxio a outros programas adoita ser a actividade que máis veces realiza o virus, xa que canto máis rápido e máis discretamente se copie, máis

posibilidades terá de danar un maior número de ordenadores antes de ser descuberto.

- **O ataque:** mentres se van copiando noutros programas, os virus comprobán se se cumpre determinada condición para atacar; por exemplo, se é cinco de xaneiro, no caso do coñecido virus Barrotes. É importante ter en conta que os virus son deseñados coa intención de non seren descubertos polo usuario e, normalmente, sen programas antivirus non son descubertos ata que se produce o dano, na terceira fase do ciclo de funcionamento do virus, coa conseguinte perda de información.
- **Descubrimento:** esta fase comeza cando o virus é detectado, identificado e documentado por vez primeira.
- **Asimilación:** as compañías fabricantes de antivirus modifican as súas solucións para conseguir detectar e eliminar as infeccións causadas polo virus.
- **Erradicación:** o uso exhaustivo de antivirus limita as infeccións do virus eliminando a súa ameaza.

Un virus pode ser catalogado en función do seu índice de perigo, que varía dependendo da fase do ciclo de vida en que se atope. O índice de perigo é unha medida do impacto que produce o seu código malicioso e da capacidade de propagación a outros sistemas. Existen varios niveis de perigo que van desde aqueles virus que causan danos leves e están pouco estendidos, ata aqueles outros que causan danos catastróficos e están moi estendidos.

O nivel de dano indica o prexuízo que un virus causa ao infectar un sistema informático. Un virus pode ser catalogado como daniño (mensaxes ou ruídos molestos, apertura de ventás involuntariamente, etc.) ou moi daniño (destrución ou modificación de arquivos, formato de discos duros, envío de información a terceiros, xeración de moito tráfico en servidores, degradación do rendemento dos sistemas, apertura de buracos de seguridade, etc.).

O grao de propagación indica o estendido que se atopa o virus. Evidentemente, canto máis estendido estea un virus, maiores son as probabilidades de estar afectado por el. A propagación dun virus determínase mediante o “cociente de infección”, que mide a porcentaxe de ordenadores infectados en relación co total de equipos explorados. O grao de propagación dun virus podería variar daquela desde “pouco estendido” ata “epidemia”.

#### **1.3.4. Tipos de virus**

En función de qué é exactamente o que un virus pode infectar, é habitual clasificalos en:

- Virus de sector de arranque mestre<sup>3</sup>: foi o primeiro tipo de virus. Agóchanse no código executable do sector de arranque de discos de memoria secundaria ou de discos de arranque externos (disquetes, CD-ROM, etc.). Ata non hai moito tempo, iniciar o ordenador desde un disco de arranque era algo bastante usual, o que significaba que os virus se espallaban rapidamente.

---

<sup>3</sup> Coñecido habitualmente polo seu nome en inglés, *Master Boot Record* (MBR).

- Virus de arquivo: caracterízanse por unirse a arquivos, onde residen, e que poden usar para propagarse entre sistemas. Adoitan infectar arquivos executables, pero tamén existen virus capaces de unirse a arquivos de código fonte, librerías ou módulos de obxectos e mesmo a arquivos de datos. O virus *Jerusalem* (tamén coñecido como *Venres 13*), un dos máis coñecidos, pertence a esta categoría.
- Macrovirus ou virus de macro: os virus de macro fan uso da capacidade que teñen certas aplicacións, como Word e Excel, para executar internamente certos códigos programados chamados macros. O virus anéxase ás devanditas macros e transmítese dun documento a outro a través delas. O virus causante dunha das maiores epidemias da historia, *Melissa*, corresponde a este tipo.
- Virus mixtos, bimodais ou multiparte: trátase dunha combinación de virus de arquivo, de macro e de sector de arranque. Realizan infeccións empregando varias técnicas para se instalar en calquera das localizacións posibles. Considéranse moi perigosos pola gran capacidade de infección que teñen.
- Virus de BIOS: alóxanse na BIOS do ordenador e, cada vez que esta se arranca, infectan os arquivos do sistema. O virus *Chernobyl* realizaba unha infección deste tipo.

Dentro dos anteriores, seguindo un criterio máis amplo, outros tipos de virus identificables serían:

- Virus de compañía: estes virus non modifican os arquivos infectados, senón que crean unha copia do arquivo orixinal e modifican esta copia. Cando o arquivo orixinal se executa, o virus fai que pase o control ao arquivo infectado. Unha variante da infección consiste en



volver nomear o arquivo orixinal e substituílo por outro co nome orixinal que contén directamente o virus.

- **Retrovirus:** trátase de virus especialmente deseñados para evitar ser detectados e infectar os programas antivirus.
- **Virus de sobrescritura:** o código do virus escríbese por riba dun ficheiro executable, destruíndoo. Se o tamaño do virus é menor que o do executable infectado, o resultado final non aumenta de tamaño, dificultando a detección do virus.
- **Virus parasitos:** os arquivos hóspede son modificados só en parte, de modo que non son destruídos e poden mesmo simular que seguen funcionando. Nestes casos o virus alóxase en lugares de arquivo, normalmente ao comezo ou ao final, onde permite que o arquivo hóspede siga parcialmente activo.
- **Virus mutantes:** cando infectan un hóspede, modifican o seu propio código para evitar que a súa “pegada” sexa detectada por programas antivirus.
- **Virus sen punto de entrada:** coñecidos como virus EPO (*Entry Point Obscuring*). Destacan porque a instrución que fai pasar o control ao virus se insire nun lugar indeterminado do arquivo hóspede. Isto fai que o virus non se manifeste ata que se realiza unha acción concreta dentro do executable infectado, o que lles permite permanecer nun estado latente durante moito tempo.
- **Virus de enlace:** caracterízanse porque a infección consiste na inserción dun enlace a algún outro lugar (por exemplo, o último clúster dun disco duro ou un clúster marcado como erróneo) onde realmente se aloxa o código do virus.

- Virus OBJ, LIB e código fonte: en lugar de infectar directamente un executable, infectan librerías ou módulos usados por outros executables. Evidentemente, a súa capacidade para actuar e reproducirse só aparecerá cando a librería sexa utilizada por outro programa.
- Virus de script: trátase de virus que actúan sobre linguaxes de script habitualmente asociadas a páxinas web. Actúan incluíndose en páxinas web ou modificando os scripts que conteñen esas páxinas.
- Virus en estado salvaxe: son aqueles que se atopan en circulación nestes momentos e que están en condicións de infectar.
- Virus de zoológico: son virus que non se encontran en liberdade ou que perderon a súa capacidade para infectar. Por exemplo, o coñecido como “virus da pelotíña”.
- Xeradores de virus: son virus que, ao mudaren, xeran novos virus.
- Virus que crean dependencia: cando un destes virus infecta unha máquina, instálase en lugares vitais, de modo que non é posible eliminalo sen facer que a máquina perda eses elementos vitais e deixe de funcionar.
- Bombas de tempo: ocúltanse nos sistemas ata que chega unha data concreta ou transcorre un determinado período de tempo. Nese momento pasan a un estado activo e realizan as súas accións de infección e replicación.

Tocante ao modo en que o virus produce a infección do sistema, podemos enumerar os seguintes:

- Engadido ou empalme: é un dos modos máis básicos e clásicos. O código do virus engádesse ao final dun arquivo hóspede (habitualmente un executable) e modifícase a estrutura de arranque deste, facendo que o virus se execute en primeiro lugar antes de pasar o control ao ficheiro orixinal. O resultado é un aumento do tamaño inicial do arquivo, permitindo así unha fácil detección.
- Inserción: é un modo máis avanzado de infección en que o virus se instala en zonas de código non utilizadas ou en segmentos de datos para que o tamaño do arquivo non varíe.
- Reordenación: introdúcese o código do virus en sectores do disco duro que quedan marcados como defectuosos e distribúense enlaces aos devanditos sectores no código doutros programas executables que quedan así infectados. A vantaxe deste método é que, ao atoparse o código do virus fóra do arquivo, este código pode ser de gran tamaño e, xa que logo, ter moita funcionalidade. En cambio, este tipo de virus é moi fácil de eliminar, simplemente sobrescribindo os sectores defectuosos.
- Polimorfismo: é probablemente o método máis avanzado. Baséase en infectar un arquivo executable, mais realizando unha compactación do código do arquivo hóspede ou do código do propio virus para evitar así un aumento do tamaño que o delate. No momento de actuar, o virus descomprime en memoria o código necesario para executarse.
- Substitución: este método, moi pouco sutil, consiste en substituír directamente o código do programa hóspede por completo polo código do virus. Deste xeito o programa orixinal simplemente desaparece e o único que se executa é o virus.

#### **1.4. Troianos**

Hai miles de anos, ante a imposibilidade de traspasar as murallas da cidade de Troia, os gregos construían un gran cabalo de madeira no interior do cal se ocultaban unha selección dos seus mellores soldados. Colocaron o cabalo diante da cidade e os troianos, cativados pola maxestade do que aparentaba un agasallo dos deuses completamente inofensivo, introduciron o cabalo na cidade.

O tipo de *malware* denominado troiano débelle o seu nome a que, para a súa propagación, utiliza a mesma estratexia que idearon os gregos para entraren en Troia. O concepto básico dun troiano consiste en introducir código malicioso dentro dun sistema que resulte atractivo para a vítima e que, ademais, pareza seguro, de modo que o conxunto parece inofensivo. Este disface podería ser desde un xogo descargado de internet ata unha mensaxe de correo electrónico de aparencia inofensiva.

Os troianos son códigos maliciosos que intentan mostrarse como algo útil ou apetecible para que unha vítima os execute. Caracterízanse porque o seu obxectivo é introducirse no sistema e pasar desapercibidos. Namentres se atopan no sistema poden dedicarse a enviar información (nese caso coñécense normalmente como *spyware*) ou a preparar o sistema para un ataque posterior mediante a instalación de *rootkits*<sup>4</sup> ou a creación de portas traseiras (*backdoors*). Ademais, a diferenza dos virus, non teñen a capacidade de replicarse e infectar outros sistemas por si mesmos.

Actualmente os troianos son moi utilizados co obxectivo de obter datos dunha vítima que os ten instalados no seu sistema sen o seu coñecemento.

---

<sup>4</sup> Conxunto de ferramentas destinadas a permitir que un atacante acceda aos privilexios de administrador do sistema de forma remota.

Isto pódeno facer de moi diversas maneiras, que van desde capturar as pulsacións de teclado (os chamados *keyloggers*) ata o acceso e manipulación das carpetas de documentos dun usuario.

#### **1.4.1. Tipos de troianos**

Os troianos poden ter características moi diversas, polo que resulta difícil catalogalos. Así e todo, en función do seu obxectivo, podemos establecer a seguinte clasificación:

- **Troianos de control remoto:** o seu obxectivo é proporcionarlle ao atacante o control da máquina onde reside o troiano. Habitualmente, o troiano tentará abrir conexións de rede clandestinas desde as que podería escoitar as ordes do atacante. Exemplos deste tipo de troianos son *Back\_orifice* ou *Netbus*.
- **Troianos que envían datos:** o seu obxectivo é enviarlle ao atacante datos confidenciais tomados da máquina atacada e da información que calquera usuario almacene nela. Polo xeral, o obxectivo é obter usuarios e claves de acceso, número de tarxetas de crédito, contas bancarias, etc. O envío de datos pódese facer de diferentes formas: mediante o envío dun correo electrónico a través dun servidor de correo público, directamente á páxina web do atacante mediante un formulario, etc. Un exemplo deste tipo é o *badtrans.b*, que é capaz de recoller as pulsacións do teclado e envialas vía correo electrónico.
- **Troianos destrutivos:** compórtanse en certo xeito como un virus, xa que o seu obxectivo é causar danos mediante a destrución de información. Poden levar a cabo esta tarefa inmediatamente trala

infección ou actuar como unha bomba lóxica que se activará cando se produza un determinado evento.

- **Troianos de ataque de denegación de servizo:** o obxectivo destes troianos é converter as vítimas en participantes involuntarios en ataques de denegación de servizo distribuídos (DDoS). A máquina infectada denomínase comunmente *botnet* ou máquina *zombi*. O atacante pode utilizar todas as máquinas infectadas para lanzar un ataque coordinado contra outro servidor ou mesmo contra unha conta de correo electrónico (cada máquina infectada podería enviar mensaxes con remitentes capturados). Un exemplo deste tipo é o *WinTrinoo*, unha ferramenta de DDoS moi estendida polo doado do seu uso.
- **Troianos Proxy:** trátase de troianos que permiten converter a máquina infectada nun Proxy a disposición do atacante. Este poderá utilizalo como punto intermedio para outros ataques, dificultando así que o ataque poida ser rastrexado ata a máquina orixinal. É común encadear varios saltos entre máquinas Proxy involuntarias para conseguir evitar que se rastrexo o ataque.
- **Troianos FTP:** caracterízanse por infectar o sistema a través do porto do protocolo FTP (o 21) e permitirlle ao atacante usar o devandito protocolo libremente contra a máquina infectada. FTP permite a transmisión bidireccional de arquivos entre equipos remotos. É dicir, o atacante terá capacidade para copiar e borrar arquivos como lle pete na máquina infectada.
- **Deshabilitadores de software de seguridade:** trátase de troianos avanzados que inclúen ferramentas para evitar ou mesmo eliminar software de protección como antivirus ou *firewalls*. Normalmente acompañan a virus e vermes e instálanse cando se produce a

infección. Coma no caso do verme *Goner*, que incluía un troiano deste tipo.

Como dicíamos, existen troianos de difícil catalogación. A realidade é que constantemente aparecen novos troianos con funcións e obxectivos cada vez máis extravagantes. Por exemplo, o *SMSlock.A*, que literalmente secuestra o equipo infectado impedindo o seu uso e pide un rescate económico a cambio da súa recuperación.<sup>5</sup>

#### **1.4.2. Modos de infección**

As dúas formas máis frecuentes polas que un troiano pode acceder e instalarse nun equipo hóspede son as seguintes:

- **Mediante adxuntos en correos electrónicos ou mensaxería instantánea:** o simple feito de abrir un arquivo adxunto a un correo electrónico ou enviado a través dunha ferramenta de mensaxería instantánea (como *Win32/SdBot*, que se instalaba a través de *MSN Messenger*) pódelle deixar a un troiano instalarse no noso sistema. Incluso algúns xestores de correo que non se atopen configurados apropiadamente poden permitir que os adxuntos se executen sen que o usuario o solicite.
- **Mediante a instalación voluntaria de software:** normalmente é software de procedencia dubidosa, *shareware*, *freeware*, versións de proba, etc. Ao descargar da rede este software e instalalo, o troiano instálase nun segundo plano sen que a vítima se decate de nada. Contra isto, cabe destacar o uso cada vez máis habitual de certificados dixitais que permiten identificar tanto o servidor ao que

---

<sup>5</sup> Este tipo de *malware* dedicado a secuestrar recursos e pedir rescate por eles é denominado tamén *ransomware*.



nos conectamos como o propio software que podemos descargar asinado. Deste xeito asegurámonos de que o estamos descargando realmente de onde pretendemos e que non foi modificado durante a comunicación.

En todo caso, a infección por troianos adoita ter un indispensable compoñente de enxeñería social. Polo xeral, os ataques sérvense de enganar para conseguir que a vítima abra os adxuntos ou chegue mesmo a executar o seu contido. Poden simular ser correos de amigos, peticións solidarias, etc. Moitas veces tamén aparentan ser programas útiles que se distribúen gratuitamente para conseguir que a vítima os descargue e instale. Incluso non é estraño atopar troianos detrás de programas antivirus gratuítos.

### 1.5. Vermes

Un verme é un programa que, unha vez executado, se replica sen necesidade da intervención humana e é capaz de enviar copias de si mesmo a través de redes de comunicacións, sen que sexa preciso que un usuario envíe un correo electrónico infectado nin estableza ningunha comunicación explícita. Propágase de anfitrión en anfitrión facendo un uso indebido de servizos desprotexidos: correo electrónico, ferramentas de mensaxería instantánea, etc. Aínda que a propagación en si non ten por que ser daniña, sucede o mesmo que cos virus: é habitual que os vermes inclúan código malicioso destinado a danar os sistemas infectados. De feito, algunhas das infeccións máis nocivas e coñecidas foron provocadas por vermes: *ILoveYou*, *Kournikova*. Algúns vermes non inclúen código malicioso, pero o seu ataque consiste no reenvío de si mesmos ata conseguir esgotar os recursos da máquina atacada.

No entanto, ao contrario que os virus, os vermes son programas completos. Non só no sentido de que son capaces de enviar copias de si mesmos a



través de internet, senón porque non necesitan de ningún programa hóspede para facelo. Non necesitan corromper outros programas e inserir o seu código alí. O seu funcionamento baséase en erros en sistemas operativos, aplicacións ou protocolos, que son aproveitados polos vermes para executarse.

### **1.5.1. Tipos de vermes**

Podemos clasificar os vermes atendendo ao medio que utilizan para a súa propagación:

- **Vermes de redes de área local:** propáganse a través dos recursos compartidos dunha rede local chegando a bloqueala ou degradando as súas medidas de seguridade. Un exemplo é o verme *Lovgate*, que pode infectar a rede local e tamén enviarse por correo electrónico a outras máquinas.
- **Vermes de redes P2P<sup>6</sup>:** usan este tipo de redes e a súa gran popularidade para incluír nelas arquivos que, ao seren descargados, traen consigo o verme. O verme *Redisto.b* utiliza este tipo de mecanismos.
- **Vermes de correo electrónico:** é probablemente o método máis habitual de propagación e realízase utilizando certos programas clientes de correo. O verme accede aos enderezos de correo da axenda dun usuario e reenvíase usando a propia conta do usuario. Algúns virus máis avanzados poden contar incluso co seu propio servidor SMTP co que enviar as súas copias. *Sircam* ou *Nimda* son exemplos de vermes de correo electrónico.

---

<sup>6</sup> *Peer to Peer.*

- **Vermes de mensaxería instantánea** (IRC, MSN Messenger): outra fonte habitual de entrada para vermes son as aplicacións de mensaxería instantánea, que ademais permiten o envío de arquivos adxuntos.
- **Vermes que se propagan directamente por internet:** os vermes máis avanzados non dependen de ningunha aplicación en particular para se propagar. A súa estratexia de infección pódese basear en atopar portos abertos nas máquinas obxectivo e conseguir introducirse na máquina sen que os usuarios se decaten. Outros vermes infectan os servidores de información, facendo que coa simple petición dunha páxina web o verme poida pasar ao cliente, como é tamén o caso de verme *Nimda* noutro dos seus modos de contaxio.

## **2. MEDIOS PREVENTIVOS E REACTIVOS**

Os medios preventivos contra o *malware* en xeral baséanse en medidas de índole técnica combinadas cunha política de seguridade que promova boas prácticas por parte dos administradores e do persoal da organización. Entre todas estas medidas destinadas á prevención de infeccións e á reacción no caso de que se chegasen a producir, poderíamos citar:

- Utilización de programas antivirus perfectamente configurados e actualizados. É a ferramenta principal na loita contra infeccións. Permiten detectar e, en moitos casos, eliminar os virus. No seguinte apartado falaremos máis en profundidade sobre eles.
- Os sistemas operativos son elementos fundamentais nos sistemas informáticos. Moitos dos métodos de infección baséanse en debilidades ou vulnerabilidades dos sistemas operativos. Xa que logo,

deben manterse sempre actualizados, especialmente coas actualizacións específicas de seguridade.

- Tamén hai que manter actualizado o resto do software instalado. Os administradores deben prestarlles atención ás noticias sobre novas vulnerabilidades do software e protexer o sistema ante ataques que se puidesen aproveitar delas.
- Controlar o software xa instalado nas máquinas e todo aquel que se vaia instalar, que, unha vez máis, debería ser soamente o necesario para as tarefas da organización. Por suposto, non se debe permitir a instalación de ningún software que non sexa orixinal. O software pirata é un dos principais puntos de propagación do *malware*.
- Os servizos activos no sistema deben manterse no mínimo número necesario. Só aqueles realmente necesarios para os obxectivos da organización deberían permanecer activos. Hai que controlar este feito periodicamente para evitar a apertura de conexións ilegais.
- Manter copias de seguridade dos datos, dos programas e dos sistemas operativos.
- Xestionar adecuadamente as cotas de uso de disco e memoria de cada usuario. Isto evitará que se un usuario provoca unha infección se consuman todos os recursos da máquina afectada, senón só os asignados ao devandito usuario.
- Tanto os administradores como os usuarios deben asumir boas prácticas de prevención: non abrir nunca arquivos adxuntos de procedencia dubidosa, desactivar as opcións de visualización de imaxes e vista previa de xestores de correo, non aceptar descargas nin instalacións de software non iniciadas voluntariamente, comprobar os certificados de procedencia do software, etc.

### **3. SISTEMAS ANTIVIRUS E DE PROTECCIÓN**

#### **3.1. Antivirus**

Os antivirus constitúen a pedra angular sobre a que descansa a maior parte da defensa contra virus, troianos, vermes e *malware* en xeral. O seu obxectivo é o de detectar, bloquear, eliminar e previr infeccións provocadas por virus informáticos. A maioría das solucións existentes hoxe en día son capaces tamén de detectar outros tipos de *malware*: troianos, vermes, *spyware*, *rootkits*, etc.

Cando un antivirus detecta unha infección, poderá actuar de dúas maneiras distintas. Se ten capacidade, podería eliminar a infección sen danar os recursos afectados. Se non é así, ha propoñer a posta en corentena dos recursos afectados (habitualmente arquivos), que quedarán illados do resto do sistema e impedirá que sexan executados. Isto último non elimina a infección, pero bloquéaa, impedindo que o virus execute o seu código malicioso e evita que se poida propagar.

Os antivirus poden detectar as infeccións seguindo unha destas dúas estratexias:

- Detección de patróns: cada virus ten un patrón de identificación, que adoita ser unha secuencia de código que o identifica. Os antivirus posúen unha base de datos de patróns de virus e compáranas cos arquivos do sistema para ver se existe algunha infección. Así e todo, os virus actuais teñen sinaturas moi pequenas. Isto dificulta a tarefa dos antivirus e pode dar lugar a falsos positivos, é dicir, deteccións que aparentan ser virus e non o son.

Os antivirus baseados en patróns obteñen moi bos resultados. Detectan un gran número de virus, pero para iso cómpre que as súas bases de datos de

patróns estean actualizadas. Todo aquel virus que non figure na base de datos será simplemente indetectable. Ademais, para funcionar dunha forma eficiente, requiren o uso de algoritmos de busca optimizados, xa que a estratexia de detección se basea en escanear o contido de todos os recursos sospeitosos.

- **Heurísticas:** usan técnicas de intelixencia artificial para lograr recoñecer secuencias de accións ou comportamentos asociados a virus. Trátase de recoñecer accións que usualmente os virus realizan (borrado de ficheiros, conexións a internet, modificar arquivos executables, etc.) ou que non realizan (abrir ventás, emitir mensaxes visibles, etc.).

As técnicas heurísticas teñen unha vantaxe fundamental: permiten detectar virus novos sen necesidade de actualizacións. Pero, por outra banda, poden dar lugar a moitos falsos positivos sobre programas que en realidade non son virus.

Existe un variado abano de solucións antivirus, dispoñibles en versións propietarias e tamén en versións ofrecidas gratuitamente ou como software libre. Entre os primeiros podemos atopar solucións moi coñecidas desenvolvidas por grandes empresas: Norton, Symantec, PandaSoftware, McAfee, Kaspersky, etc. Entre os segundos podemos citar AVG, Avast!, ClamWin, etc.

Á hora de seleccionar o antivirus máis apropiado para os nosos sistemas, deberíamos ter en conta as seguintes características:

- **Frecuencia de actualización:** canto máis actualizado estea o noso antivirus, máis preparados estaremos para loitar contra as infeccións.
- **Protección en tempo real:** é conveniente que o axente antivirus resida na memoria principal e realice un escaneamento continuo en

busca de posibles infeccións. Por suposto, isto ten un custo en recursos para a máquina que cómpre ter en conta antes de optar por unha solución deste tipo.

- Capacidade de centralización: algúns antivirus permiten ser instalados en varias máquinas, pero ser controlados e xestionados desde unha única máquina. Isto facilita a tarefa dos administradores.
- Programación de tarefas: é moi interesante que os escaneamentos, que poden consumir bastante tempo e recursos da máquina, poidan ser programados para que se executen en horas de pouca actividade (durante a noite, por exemplo).
- Protección do correo: hoxe en día, un dos puntos de entrada máis comúns para os virus é a través dos correos electrónicos e os seus arquivos adxuntos. É conveniente que o noso antivirus sexa capaz de analizar automaticamente eses arquivos adxuntos.
- Xeración de informes: é moi útil para os responsables da seguridade que o antivirus sexa capaz de xerar informes cos seus resultados e as accións que levou a cabo.

Unha vez que seleccionemos un antivirus, é conveniente ter claro como e onde utilízalo. A norma base é “un equipo, un antivirus”. É dicir, todos os equipos do sistema deberían ter o seu propio antivirus instalado. Con todo, nalgúns equipos concretos o antivirus pódelle ofrecer unha protección máis eficiente ao resto de equipos; por exemplo, en equipos que actúan como Proxy de conexión con redes externas. Un antivirus ben configurado e escaneando en tempo real protéxese a si mesmo de virus, pero tamén evita que gran parte do *malware* pase aos equipos da rede interna e, xa que logo, aos usuarios finais.

No ámbito dos antivirus, o European Institute for Computer Antivirus Research (EICAR) desenvolveu unha proba para validar a súa operatividade. O seu obxectivo é comprobar que un antivirus funciona realmente sen poñer en perigo unha máquina con virus reais. A proba **EICAR**, que así se coñece, consiste nun inofensivo arquivo de texto que debe ser gardado con extensión de arquivo executable. Unha vez feito, todo antivirus debería detectalo como un virus que ten que eliminar.

### **3.2. Outras medidas de protección**

Para protexer os nosos sistemas contra infeccións sería conveniente dispoñer dalgúns outros elementos:

#### **3.2.1. Devasas (*firewalls*)**

Os vermes propáganse pola rede conectándose a servizos con buracos de seguridade, aloxados en diferentes sistemas ao longo da rede. Ademais de asegurarse de que estes servizos vulnerables non se estean executando, o seguinte paso que debe seguir o administrador é verificar que o *firewall* non permita conexións a estes servizos. Moitos *firewalls* modernos son capaces de filtrar no tráfico da rede aqueles paquetes nos que se detecten certas sinaturas asociadas a virus ou vermes.

#### **3.2.2. NIDS (Sistemas de detección de intrusos de rede)**

Os sistemas de detección de intrusiones de rede son semellantes aos antivirus pero aplicados ao tráfico da rede. Buscan no tráfico de rede sinaturas ou patróns de comportamento relacionados con virus ou vermes. Son capaces de alertar ao usuario atacado ou de deter o tráfico de rede que tenta distribuír o *malware*.

### **3.2.3. HIDS (Sistemas de detección de intrusos de *host*)**

Os sistemas de detección de intrusión de *host*, como por exemplo as ferramentas de software libre Tripwire e Aide, son capaces de detectar cambios realizados sobre arquivos aloxados nun servidor. Baséanse na hipótese de que un arquivo executable, unha vez compilado, non necesita ser modificado. Entón, mediante o control das súas características, tales como tamaño, data de creación e control de integridade, poden detectar decontado se ocorreu algo irregular que apunte a unha infección.

### **3.2.4. Sandboxes**

O concepto de *sandbox* baséase en que unha aplicación ou programa ten o seu propio contorno para executarse e non pode afectar ao resto do sistema. Isto quere dicir que os recursos e os privilexios que a aplicación ten mentres é executada son limitados. A vantaxe dos *sandboxes* é que restrinxen o dano que un *malware* lle pode ocasionar ao sistema infectado simplemente restrinxindo os accesos dos que dispón o *malware*.

Outra opción en auxe é a virtualización, que consiste en crear unha máquina virtual completa mediante produtos como VMWare. Isto illa a máquina virtual do sistema anfitrión “real”, limitando o acceso a este segundo o configurase o administrador.

### **3.2.5. Honeypot**

Denomínase *honeypot* un sistema especialmente preparado para ser ou parecer vulnerable, de maneira que sexa fácil de infectar por *malware*. Por suposto, este sistema non contén información nin programas valiosos (e moitas veces trátase dun sistema virtualizado). Aínda así, este sistema está estritamente monitorado, de modo que o administrador pode obter



información sobre as ameazas ás que se enfronta o sistema real con antelación. Isto permítelle ao administrador xestionar as medidas de seguridade do sistema real para protexerse contra novos virus ou ataques.

#### **4. REFERENCIAS**

- RFC 4949 Internet Security Glossary, Version 2

<http://tools.ietf.org/html/rfc4949>

- Observatorio de seguridade do Instituto Nacional de Tecnoloxías da Comunicación

<http://www.inteco.es/Seguridad/Observatorio/>

- Web e enciclopedia do *malware* de PandaSoftware

<http://www.pandasecurity.com>

- Lista de virus, noticias e 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**

**Enxeñeiro en Informática no Concello de Ourense**

**Colexiado do CPEIG**



# **43. CERTIFICADOS DIXITAIS. TARXETAS CRIPTOGRÁFICAS. SINATURA DIXITAL. TÉCNICAS DE CIFRAXE. INFRAESTRUTURA DE CLAVE PÚBLICA (PKI).**



**Tema 43: Certificados dixitais. Tarxetas criptográficas. Sinatura dixital. Técnicas de cifrado. Infraestrutura de clave pública (PKI).**

**INDICE**

<b>1. TECNICAS DE CIFRADO.....</b>	<b>2</b>
<b>2. SINATURA DIXITAL.....</b>	<b>18</b>
<b>3. INFRAESTRUTURA DE CLAVE PÚBLICA (PKI).....</b>	<b>20</b>
<b>4. REFERENCIAS.....</b>	<b>32</b>

## **1. TECNICAS DE CIFRADO**

A palabra **criptografía** é unha palabra de orixe grega (krypto -oculto- e graphos -escribir-) e defínese como a arte de escribir con clave secreta ou dun modo enigmático.

### **1.1. Criptografía e criptoanálise**

A historia da criptografía remóntase a miles de anos atrás e ten unha longa tradición nas escrituras relixiosas, xa que estas podían ofender á cultura dominante ou ás autoridades políticas. A finalidade desta técnica foi sempre enviar mensaxes confidenciais coa garantía de que só o destinatario dos mesmos puidese acceder á información contida na mensaxe.

O método consiste na aplicación dunha transformación á mensaxe coñecida como **cifrado** co obxectivo de que as persoas que descoñezan a transformación realizada sexan incapaces de acceder á información contida na mensaxe.

O estudo de técnicas destinadas a atopar o sentido dunha información cifrada, sen ter acceso á información secreta requirida, é a criptoanálise . A finalidade da criptoanálise é, xa que logo, descubrir a clave de cifrado. A vulnerabilidade dos algoritmos de cifrado dependerá da dificultade da tarefa de descubrimento da clave. Unha ataque por forza bruta consiste en buscar a clave de cifrado probando un a un todos os posibles valores da mesma.

A **criptoloxía** é a disciplina que abarca a criptografía e a criptoanálise.

Outro concepto relacionado é a **esteganografía**. Do mesmo xeito que a criptografía, o que busca é ocultar unha mensaxe ante un posible atacante, pero a diferenza entre ambas técnicas estriba en como oculta a

información cada unha delas: mentres que a criptografía pretende que a información non sexa descifrada, a esteganografía o que pretende é que a información pase desapercibida (por exemplo un código secreto tatuado no coiro cabeludo e oculto polo pelo)

As técnicas criptográficas pódense clasificar seguindo varios criterios. Seguindo un **criterio temporal** pódense clasificar en clásicas ou extemporáneas e modernas ou contemporáneas.

## **1.2. Técnicas criptográficas clásicas**

As técnicas criptográficas clásicas realizan o cifrado en base á substitución e transposición dos caracteres da mensaxe. O segredo está no algoritmo aplicado á mensaxe, polo que teñen o inconveniente de que se un atacante o descubre será capaz de interpretar todas as mensaxes cifradas que capture. Como exemplos podemos citar:

- **Substitución monoalfabeto:** consiste na substitución de símbolos uno a un. Como exemplo pódese citar o *algoritmo de César*.
- **Substitución polialfabeto:** consiste na substitución dun símbolo por un dun conxunto. Como exemplo pódese citar o cifrado de Vigenère.
- **Transposición:** consiste en cambiar a orde dos símbolos.
- **Combinación de substitución e transposición** (máquinas rotoras ).

## **1.3. Técnicas criptográficas modernas**

As técnicas criptográficas modernas, a diferenza das clásicas, utilizan claves de cifrado para cifrar a información. Unha premisa fundamental da criptografía moderna é que a seguridade do método debe depender

unicamente da clave de cifrado, debendo ser os algoritmos coñecidos. Esta premisa fai que estas técnicas resulten moito máis seguras e efectivas xa que resulta máis sinxelo manter o segredo da clave e ademais cambiar a clave de cifrado sempre será menos custoso que idear un novo algoritmo resultando frecuente que a clave de cifrado se xere de forma automática.

Podemos clasificar os algoritmos de cifrado atendendo ás claves que utilizan ou ao modo en que procesan a información.

Se nos fixamos no tipo de claves que utilizan temos dous tipos de algoritmos:

- Algoritmos de cifrado **simétrico ou de clave privada**: Utilizan a mesma clave para o cifrado e o descifrado polo que debe ser secreta e compartida polo emisor e o receptor. Exemplos de algoritmos deste tipo son DES, 3DES, AES, IDEA, RC5, etc.
- Sistemas de cifrado **asimétrico ou de clave pública**: Utilizan un par de claves xeradas polo emisor. Unha das claves é pública, é dicir, coñecida por todo o mundo e a outra é privada ou secreta de forma que o que se cifra cunha clave é descifrado pola outra e viceversa. Exemplos de algoritmos deste tipo son RSA, DSA, Diffie-Hellman, ElGamal, etc.

Se nos fixamos no modo en que procesan temos 3 tipos de algoritmos:

- Técnicas criptográficas de cifrado en modo **fluxo** (*stream cipher*): estes algoritmos de cifrado baséanse na combinación dun texto en claro cun texto de cifrado obtido a partir dunha clave. A característica fundamental é que se vai cifrando un fluxo de datos bit a bit. Exemplos: RC4, SEAL.
- Técnicas criptográficas de cifrado en modo **bloque** (*block cipher*): caracterízanse porque o algoritmo de cifrado ou descifrado se aplica separadamente a bloques de lonxitude  $l$ , e para cada un deles o

resultado é un bloque da mesma lonxitude: Exemplos: DES, 3DES, AES.

- Técnicas criptográficas baseadas en funcións resumo (**hash functions**): a característica principal destes algoritmos é que permiten obter unha cadea de bits de lonxitude fixa a partir dunha mensaxe de lonxitude arbitraria: Exemplos: MD5, familia SHA.

#### **1.4. Criptografía de clave privada ou simétrica**

A criptografía de clave simétrica caracterízase porque a clave de descifrado **k**, é idéntica á clave de cifrado ou se pode obter a partir desta, residindo deste xeito a fortaleza do algoritmo no segredo da mesma.

Se **M** é a mensaxe en claro que se quere protexer, ao cifrala cun algoritmo en base a unha clave privada **E<sub>k</sub>(M)** obtense outra mensaxe chamada texto cifrado **C**. Para que este cifrado sexa útil, existe outra función **D<sub>k</sub>(C)** que a partir do texto cifrado polo emisor permite obter de novo a mensaxe en claro **M**.

$$\mathbf{C} = \mathbf{E}_k(\mathbf{M})$$

$$\mathbf{M} = \mathbf{D}_k(\mathbf{C}) = \mathbf{D}_k(\mathbf{E}_k(\mathbf{M}))$$

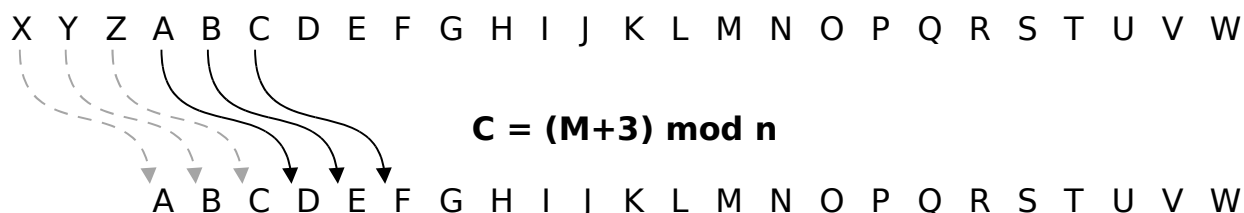
A seguridade do sistema recae pois en manter en segredo a clave **k**. O principal inconveniente da criptografía simétrica é o intercambio **de claves**. Este problema solúciónase con axuda da criptografía asimétrica.

##### **1.4.1. Substitución monoalfabeto**

Un exemplo de algoritmo de cifrado por substitución monoalfabeto é o cifrado César. É un tipo de cifrado por substitución no que cada letra no texto orixinal é substituída por outra letra que se atopa un número fixo de posicións máis adiante en o alfabeto. Por exemplo, cun desprazamento de



3, a A sería substituída por a D (situada 3 lugares á dereita de a A ), a B sería substituída por a E, etc. Este método debe o seu nome a Xulio César, que o usaba para comunicarse cos seus xenerais.



### Exemplo:

<b>Mensaxe en</b>	<b>H O L A C E S A R</b>
<b>claro:</b>	
<b>Mensaxe</b>	<b>K R O D G H V D U</b>
<b>cifrada:</b>	

O descifrado dunha mensaxe consistiría en substituír cada letra do texto pola que hai tres posicións diante no alfabeto.

A principal condición que debe cumprir a clave é que ha de ser unha permutación do alfabeto, é dicir, non pode haber letras repetidas nin faltar ningunha. Se non, a transformación non sería invertible en xeral.

#### 1.4.2. Substitución polialfabeto

O inconveniente dos algoritmos de substitución monoalfabeto é que o texto cifrado mantén a mesma distribución de frecuencia de caracteres que ten o texto claro orixinal, o que fai que sexan criptoanalizables por métodos estatísticos sinxelos. Unha posible mellora dos cifrados por substitución é intentar métodos que destrúan esa correspondencia de frecuencias entre a mensaxe en claro e o criptograma. Por exemplo, utilizando varios alfabetos ao tempo para o cifrado. Nos cifrados polialfabéticos a substitución aplicada a cada carácter varía en función da posición que ocupe este

dentro do texto claro. En realidade corresponde a unha aplicación cíclica de  $n$  cifrados de substitución monoalfabeto. Un exemplo típico de cifrado polialfabético é o **Cifrado de Vigenère**.

### **1.4.3. Cifrado en bloque**

Un algoritmo de cifrado en bloque toma como entrada un bloque de lonxitude fixa e unha clave e xera un novo bloque cifrado da mesma lonxitude que o bloque de entrada.

A técnica consiste en dividir o texto a cifrar (con lonxitude  $L$ ) en bloques de tamaño  $b$  e a continuación cifrar cada un dos bloques. Se  $L$  non é múltiplo de  $b$ , agréganse bits adicionais para conseguir que todos os bloques estean completos. Para descifrar a mensaxe procédese de xeito análogo.

Moitos dos algoritmos de cifrado en bloque baséanse na combinación de dúas operacións básicas: substitución e transposición.

- A **substitución** consiste en traducir cada bloque de bits que chegan como entrada a outro de saída seguindo unha permutación determinada. O cifrado César sería un exemplo simple de substitución no que cada grupo de bits correspondería a unha letra.
- A **transposición** consiste en reordenar a información do texto en claro segundo un patrón determinado. Un exemplo podería ser a formación de grupos de cinco letras, incluídos os espazos en branco, e reescribir cada grupo (1, 2, 3, 4, 5) na orde (3, 1, 5, 2, 4). Por exemplo:

Texto en claro: "HOLA MUNDO"

Texto cifrado: "LH OANMOUD"

A transposición non dificulta extraordinariamente a criptoanálise, pero pode combinarse con outras operacións para engadir complexidade aos algoritmos de cifrado.

O **produto de cifras**, ou combinación en cadoiro de distintas transformacións criptográficas é unha técnica moi efectiva para implementar algoritmos bastante seguros de forma sinxela. Por exemplo, moitos algoritmos de cifrado en bloque baséanse nunha serie de iteracións de produtos substitución-transposición.

Dúas propiedades desexables nun algoritmo criptográfico son a **confusión e a difusión**. A confusión consiste en esconder a relación entre a clave e as propiedades estatísticas do texto cifrado. A difusión propaga a redundancia do texto en claro ao longo do texto cifrado para que non sexa facilmente recoñecible.

A confusión consegue que, cambiando un só bit da clave, cambien moitos bits do texto cifrado, e a difusión implica que o cambio dun só bit do texto en claro afecte tamén a moitos bits do texto cifrado.

### ***Modos de operación do cifrado en bloque***

Un aspecto que hai que ter en conta cando se utiliza o cifrado é que, aínda que se pode conseguir que un atacante non descubra directamente os datos transmitidos, en ocasións é posible que se poida deducir información indirectamente. Por exemplo, nun protocolo que utilice mensaxes cunha cabeceira fixa, a aparición dos mesmos datos cifrados varias veces nunha transmisión pode indicar onde empezan as mensaxes. Para intentar contrarrestar isto, o cifrado bloque opera en varios modos:

- O modo **ECB** (Electronic Codebook): consiste en dividir o texto en bloques e cifrar cada un deles de forma separada. O inconveniente

deste método é que bloques idénticos de mensaxe sen cifrar producirán idénticos textos cifrados.

- No modo **CBC** (Cipher Block Chaining), antes de ser cifrado, a cada bloque de texto aplícaselle unha operación [XOR](#) bit a bit, co previo bloque xa cifrado. Deste xeito, cada bloque é dependente de todos os bloques de texto previos ata ese punto. Ademais, para facer cada mensaxe única pódese usar un [vector de inicialización](#). CBC é o modo usado máis a miúdo. A súa principal contrapartida é que é secuencial e non pode funcionar en paralelo.
- No modo **CFB** (Cipher Feedback), o algoritmo de cifrado non se aplica directamente ao texto en claro senón a un vector auxiliar (inicialmente igual ao IV). Do resultado do cifrado tómanse  $n$  bits que se suman a  $n$  bits do texto en claro para obter  $n$  bits de texto cifrado. Estes bits cifrados utilízanse tamén para actualizar o vector auxiliar. O número  $n$  de bits xerados en cada iteración pode ser menor ou igual que a lonxitude de bloque  $b$ . Tomando como exemplo  $n=8$ , temos un cifrado que xera un byte cada vez sen que sexa necesario esperar a ter un bloque enteiro para podelo descifrar.
- O modo **OFB** (Output Feedback) opera como o CFB pero en lugar de actualizar o vector auxiliar co texto cifrado, actualízase co resultado obtido do algoritmo de cifrado. A propiedade que distingue este modo dos demais consiste en que un erro na recuperación dun bit cifrado afecta soamente ao descifrado deste bit.

### ***Exemplos de algoritmos de cifrado en bloque: DES***

DES<sup>1</sup> é un dos algoritmos de cifrado máis usados no mundo. Foi publicado en 1977 no documento **FIPS**<sup>2</sup> PUB 46 do Instituto Nacional de Estándares e Tecnoloxía (NIST).

---

<sup>1</sup> Siglas en inglés de *Data Encryption Standard*.

<sup>2</sup> Siglas en inglés de *Federal Information Processing Standard*.

O algoritmo foi controvertido ao principio, con algúns elementos de deseño clasificados, unha [lonxitude de clave](#) relativamente curta, e as continuas sospeitas sobre a existencia dalgunha [porta traseira](#) para a NSA<sup>3</sup>. Posteriormente DES foi sometido a unha intensa análise académica e motivou o concepto moderno do [cifrado por bloques](#) e a súa [criptoanálise](#).

Hoxe en día, DES considérase inseguro para moitas aplicacións. Isto débese principalmente a que o tamaño de clave de 56 bits é curto. A finais de 2001 o algoritmo foi substituído polo novo [AES](#)<sup>4</sup>.

DES é o prototipo de algoritmo de [cifrado por bloques](#): toma un texto en claro dunha lonxitude fixa de bits e transfórmalo mediante unha serie de operacións básicas noutro texto cifrado da mesma lonxitude, dividindo para iso a mensaxe en bloques de 64 bits. O algoritmo DES utiliza unha [clave criptográfica](#) para modificar a transformación, de modo que o descifrado só pode ser realizado por aqueles que coñezan a clave concreta utilizada no cifrado. A lonxitude da clave é de 64 bits, aínda que en realidade, só 56 deles son empregados polo algoritmo. Os oito bits restantes utilízanse unicamente para comprobar a [paridade](#), e despois son descartados.

A parte central do algoritmo consiste en dividir a mensaxe de entrada en grupos de bits, facer unha substitución distinta sobre cada grupo e, a continuación unha transposición de todos os bits. Esta transformación repítese dezaseis veces: en cada iteración, a entrada é unha transposición distinta dos bits da clave sumada bit a bit (XOR) coa saída da iteración anterior. Este entrecruzamento coñécese como [esquema Feistel](#).

A estrutura de Feistel asegura que o cifrado e o descifrado sexan procesos moi similares. A única diferenza é que as subclaves se aplican en orde inversa cando desciframos. Isto simplifica enormemente a implementación, en especial sobre hardware, ao non haber necesidade de algoritmos distintos para o cifrado e o descifrado.

---

<sup>3</sup> Siglas en inglés de *National Security Agency*.

<sup>4</sup> Siglas en inglés de *Advanced Encryption Standard*.

### ***Exemplos de algoritmos de cifrado en bloque: 3DES***

Aínda que ao longo dos anos o algoritmo DES se mostrou moi resistente á criptoanálise, o seu principal problema é actualmente a vulnerabilidade aos ataques de forza bruta, por mor da lonxitude da clave, de só 56 bits. Nos anos 70 era moi custoso realizar unha procura entre as  $2^{56}$  combinacións posibles, pero a tecnoloxía actual permite romper o algoritmo nun tempo cada vez máis curto. Por este motivo, en 1999 o NIST cambiou o algoritmo DES polo “Triplo DES” como estándar oficial, mentres non estivese dispoñible o novo estándar AES. O Triplo DES, como o seu nome indica, consiste en aplicar o DES tres veces consecutivas. Isto pódese realizar con tres claves ( $k_1, k_2, k_3$ ), ou ben con só dúas ( $k_1, k_2$ , e outra vez  $k_1$ ). A lonxitude total da clave coa segunda opción é de 112 bits (dúas claves de 56 bits). A primeira opción proporciona máis seguridade, pero a costa de utilizar unha clave total de 168 bits (3 claves de 56 bits), que pode ser un pouco máis difícil de xestionar e intercambiar. Para conseguir que o sistema sexa adaptable ao estándar antigo, no Triplo DES aplícase unha secuencia cifrado-descifrado-cifrado (E-D-E) en lugar de tres cifrados:

$$\mathbf{C} = \mathbf{E}(k_3, \mathbf{D}(k_2, \mathbf{E}(k_1, \mathbf{M})))$$

$$\text{ou ben: } \mathbf{C} = \mathbf{E}(k_1, \mathbf{D}(k_2, \mathbf{E}(k_1, \mathbf{M})))$$

Deste xeito, para cifrar unha mensaxe  $M$ , primeiro cífrase con  $k_1$ , logo descífrase con  $k_2$  e finalmente vólvese cifrar con  $k_3$  (ou  $k_1$ ). Nótese que no caso de usar 2 claves se facemos que  $k_1=k_2$ , temos un sistema equivalente ao DES simple.

### ***Exemplos de algoritmos de cifrado en bloque: AES***

A lonxitude da clave do algoritmo DES foise convertendo nun problema a medida que ían aumentando as capacidades de procesamento e o algoritmo se facía cada vez máis vulnerable a un ataque por forza bruta.

En 1977, á vista de que o Triplo DES non é excesivamente eficiente cando se implementa en software, o NIST convocou á comunidade criptográfica a presentar propostas para un novo estándar que substituíse ao DES. Dos quince algoritmos candidatos que se aceptaron, escolléronse cinco como finalistas (MARS, RC6, RIJNDAEL, SERPENT e TWOFISH), e en outubro de 2000 deuse a coñecer o ganador: o algoritmo Rijndael, proposto polos criptógrafos belgas Joan Daemen e Vincent Rijmen. En novembro de 2001 publicouse o documento FIPS 197 onde AES se asumía oficialmente.

O Rijndael pode traballar en bloques de 128, 192 ou 256 bits, e a lonxitude da clave tamén pode ser de 128, 192 ou 256 bits. Dependendo desta última lonxitude, o número de iteracións do algoritmo é 10, 12 ou 14, respectivamente. Cada iteración inclúe unha substitución fixa byte a byte, unha transposición, unha transformación consistente en desprazamentos de bits e XORs, e unha suma binaria (XOR) con bits obtidos a partir da clave.

#### **1.4.4. Cifrado en fluxo**

Para algunhas aplicacións tales como o cifrado de conversacións telefónicas, o cifrado en bloques é inapropiada porque os fluxos de datos se producen en tempo real en pequenos fragmentos. As mostras de datos poden ser tan pequenas como 8 bits ou ata de 1 bit, e sería un desperdicio reencher o resto dos 64 bits antes de cifrar e transmitilos.

O funcionamento dun cifrado en fluxo consiste na combinación dun texto claro **M** cun texto de cifrado **S** que se obtén a partir a clave simétrica **k** obtendo un texto cifrado **C**. Para descifrar, só se require realizar a operación inversa co texto cifrado **C** e o mesmo texto de cifrado **S**.

A operación de combinación que se utiliza normalmente é a suma e como operación inversa e a resta. Se o texto está formado por caracteres, o algoritmo sería como un cifrado César en que a clave vai cambiando dun carácter a outro. A clave que corresponde vén dada polo texto de cifrado **S** (chamado *keystream* en inglés).

Considerando o texto formado por bits, a suma e a resta son equivalentes. Cando se aplican bit a bit, ambas son idénticas á operación lóxica “ou exclusiva”, denotada co operador XOR (eXclusive OR). Así pois:

$$\mathbf{C} = \mathbf{M} \text{ XOR } \mathbf{S(k)}$$

$$\mathbf{M} = \mathbf{C} \text{ XOR } \mathbf{S(k)}$$

Nos esquemas de cifrado en fluxo, o texto claro **M** ten unha lonxitude variable e o texto de cifrado **S** ha de ser como mínimo igual de longo. Non é necesario dispoñer da mensaxe enteira antes de empezar a cifrala ou descifrala, xa que se pode implementar o algoritmo para que traballe cun “fluxo de datos” que se vai xerando a partir da clave (o texto cifrado). De aí procede o nome deste tipo de algoritmos.

Existen varias formas de obter o texto cifrado **S** en función da clave **k**:

- Se se escolle unha secuencia **k** máis curta que a mensaxe **M**, unha posibilidade sería repetila ciclicamente tantas veces como sexa necesario para ela sumando ao texto en claro. O inconveniente deste método é que se pode romper facilmente, sobre todo canto máis curta sexa a clave.
- No outro extremo, poderíase tomar directamente **S(k) = k**. Isto quere dicir que a propia clave debe ser tan longa como a mensaxe que hai que cifrar. Este é o principio do coñecido **cifrado de Vernam**. Se **k** é unha secuencia totalmente aleatoria que non se repite ciclicamente, estamos ante un exemplo de cifrado incondicionalmente seguro. Este método de cifrado chámase en inglés *one-time-pad* (“caderno dun só uso”). Un exemplo de uso do cifrado de Vernam ocorre ás veces



entre os portaavións e os avións. Neste caso, aprovéitase que nun instante dado (antes do despegue) tanto o avión como o portaavións están no mesmo sitio, co cal, intercambiarse un disco duro de 20GB cunha secuencia pseudoaleatoria non é ningún problema. Posteriormente cando o avión despega pode establecerse unha comunicación segura co portaavións utilizando un cifrado de Vernam coa clave aleatoria que ambos comparten.

- O que na práctica utilízase son funcións que xeran **secuencias pseudoaleatorias** a partir dunha **semente** (un número que actúa como parámetro do xerador), e o que se intercambia como clave secreta ***k*** é soamente esta semente. En cada paso o algoritmo atópase nun determinado estado, que virá dado polas súas variables internas. Dado que as variables serán finitas, haberá un número máximo de posibles estados distintos. Isto significa que ao cabo dun certo período, os datos xerados se volverán repetir. Para que o algoritmo sexa seguro, interesa que o período de repetición sexa canto máis longo mellor (con relación á mensaxe que hai que cifrar), co fin de dificultar a criptoanálise.

As características deste tipo de cifrado fano apropiado para contornos nos que se necesita un rendemento alto e os recursos (capacidade de cálculo, consumo de enerxía) sexan limitados. Por iso adóitanse utilizar en comunicacións móbiles: redes sen fíos, telefonía móbil, etc.

Un exemplo clásico de cifrado en fluxo é **RC4** (Ron's Code 4). Foi deseñado por Ronald Rivest en 1987 e publicado en Internet por un remitente anónimo en 1994. É coñecido por ser o algoritmo de cifrado empregado no sistema de seguridade **WEP** (*Wired Equivalent Privacy*) recoñecido no estándar **IEEE 802.11**. [RC4](#) utiliza claves de 64 bits (40 bits máis 24 bits do vector de iniciación IV) ou de 128 bits (104 bits máis 24 bits do IV).

#### 1.4.5. Cifrado en base a funcións resumo

Ás veces os algoritmos de cifrado non só se usan para cifrar datos, senón que son utilizados para garantir a autenticidade dos mesmos. Como exemplo de algoritmo destas características pódese citar as chamadas **funcións hash**, tamén coñecidas como **funcións de resumo** de mensaxe<sup>5</sup>.

En xeral, podemos dicir que unha función resumo nos permite obter unha cadea de bits de lonxitude fixa, relativamente curta, a partir dunha mensaxe de lonxitude arbitraria:

$$H = h(M)$$

Para mensaxes **M** iguais, a función **h** debe dar resumos **H** iguais. Pero se dúas mensaxes dan o mesmo resumo **H**, non deben ser necesariamente iguais. Isto é así porque só existe un conxunto limitado de posibles valores **H**, xa que a súa lonxitude é fixa.

Para que unha función **h** se poida aplicar en sistemas de autenticación, debe cumprir unha serie de condicións que lle permitan ser considerada unha **función resumo segura**. Entre elas destacan a **unidireccionalidade e a resistencia a colisións**.

Para dificultar os ataques contra as funcións de resumo, por unha banda os algoritmos teñen que definir unha relación complexa entre os bits de entrada e cada bit de saída. Doutra banda, os ataques por forza bruta se contrarrestan ampliando o suficiente a lonxitude do resumo.

Ata hai pouco, o algoritmo de resumo máis usado era o MD5 (*Message Digest 5*). Pero como o resumo que obtén é de só 128 bits e separadamente se atoparon outras formas de xerar colisións parciais no algoritmo, actualmente recoméndase utilizar algoritmos máis seguros,

---

<sup>5</sup> *Message Digest*, en inglés.

como o SHA-1 <sup>6</sup>. O algoritmo **SHA-1**, publicado en 1995 nun estándar do NIST (como revisión dun algoritmo anterior chamado simplemente SHA), obtén resumos de 160 bits. No ano 2002, o NIST publicou variantes deste algoritmo que xeran resumos de 256, 384 e 512 bits.

### 1.5. Criptografía de clave pública ou asimétrica

Os **sistemas de cifrado de clave pública** ou **sistemas de cifrado asimétricos** inventáronse co fin de evitar por completo o problema do intercambio de claves dos sistemas de cifrado simétricos.

Nun algoritmo criptográfico de clave pública utilízanse claves distintas para o cifrado e o descifrado. Unha delas, a **clave pública**, pódese obter facilmente a partir da outra, a **clave privada**, pero o contrario é practicamente imposible. Os algoritmos de clave pública típicos permiten cifrar coa clave pública ( $k_{pub}$ ) e descifrar coa clave privada ( $k_{pr}$ ):

$$C = e(k_{pub}, M)$$

$$M = d(k_{pr}, C)$$

Pero tamén pode haber algoritmos que permitan cifrar coa clave privada e descifrar coa pública:

$$C = e(k_{pr}, M)$$

$$M = d(k_{pub}, C)$$

Na práctica, os algoritmos utilizados permiten cifrar e descifrar facilmente, pero todos eles **son considerablemente máis lentos que os equivalentes con criptografía simétrica**. Por iso a criptografía de clave pública só se adoita utilizar nos problemas que a criptografía simétrica non

---

<sup>6</sup> Siglas en inglés de *Secure Hash Algorithm-1*

pode resolver: o intercambio de claves e a autenticación con non repudio (sinaturas dixitais).

Os mecanismos de **intercambio de claves** permiten que dúas partes se poñan de acordo nas claves simétricas que utilizen para comunicarse, sen que un terceiro que estea escoitando o diálogo poida deducir cales son estas claves.

A **autenticación** baseada en clave pública pódese utilizar se o algoritmo permite utilizar as claves á inversa: a clave privada para cifrar e a clave pública para descifrar. Se A envía unha mensaxe cifrada coa súa clave privada, todo o mundo poderá descifrala coa clave pública de A e, ao mesmo tempo, todo o mundo saberá que a mensaxe só a pode xerar quen coñeza a clave privada asociada (que debería ser A). Esta é a base das **sinaturas dixitais**.

#### **1.5.1. Exemplos de algoritmos de clave pública: Diffie-Hellman**

É un mecanismo que permite que dúas partes se poñan de acordo de forma segura sobre unha clave secreta utilizando unha canle insegura. O algoritmo baséase na dificultade de calcular logaritmos discretos e úsase xeralmente como medio para acordar claves simétricas que serán empregadas para o cifrado dunha sesión.

#### **1.5.2. Exemplos de algoritmos de clave pública: RSA**

É o algoritmo máis utilizado na historia da criptografía de clave pública. O seu nome procede das iniciais das persoas que o deseñaron en 1977: Ronald Rivest, Adi Shamir e Leonard Adleman. A clave pública está formada por un número  $n$ , calculado como produto de dous factores primos moi grandes ( $n = p * q$ ) e un expoñente  $e$ . A clave privada é outro expoñente  $d$

calculado a partir de  $p$ ,  $q$  e  $e$ , de tal forma que o cifrado e o descifrado se pode realizar da seguinte forma:

$$\text{Cifrado: } \mathbf{C = M^e \bmod n}$$

$$\text{Descifrado: } \mathbf{M = C^d \bmod n}$$

Como se pode ver, a clave pública e a privada son intercambiáveis: se se usa calquera delas para cifrar, deberase utilizar a outra para descifrar. A fortaleza do algoritmo RSA baséase, por unha banda, na dificultade de obter  $M$  a partir de  $C$  sen coñecer  $d$  (problema do logaritmo discreto), e doutra banda, na dificultade de obter  $p$  e  $q$  (e, xa que logo,  $d$ ) a partir de  $n$  (problema da factorización de números grandes, que é outro dos problemas considerados difíciles).

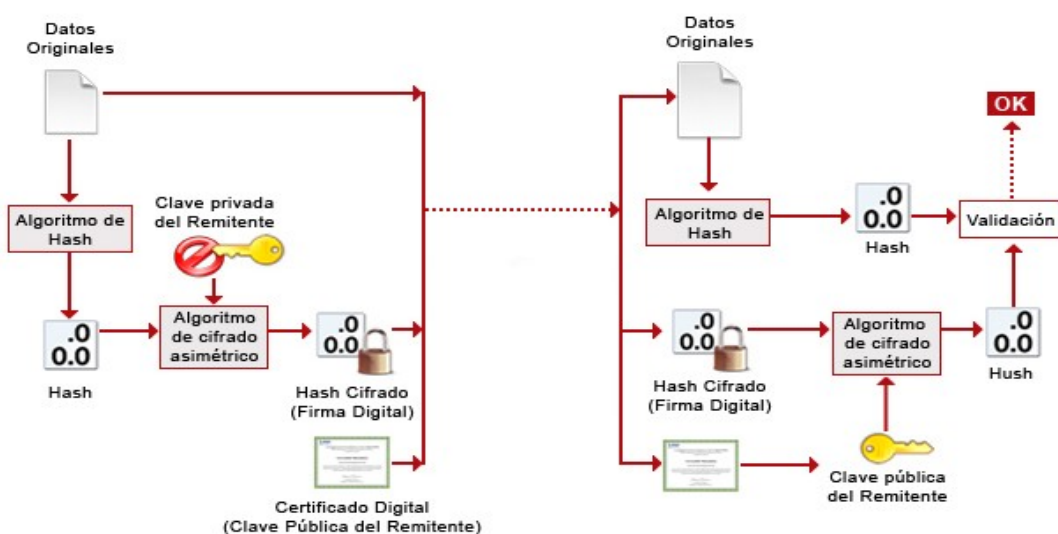
## 2. SINATURA DIXITAL

Unha sinatura dixital é, basicamente, unha mensaxe cifrada coa clave privada do asinante. Pero, por cuestións de eficiencia, o que se cifra non é directamente a mensaxe a asinar, senón soamente o seu resumo calculado cunha función *resumo* segura.

A sinatura dixital está baseada en algoritmos criptográficos asimétricos, nos que son necesarias un par de claves para o intercambio da información: unha clave pública e unha clave privada. A clave privada está baixo custodia do emisor e soamente é coñecida por el. A clave pública é distribuída entre todos os posibles destinatarios das mensaxes ou documentos asinados. O proceso para realizar unha sinatura dixital resúmese a continuación:

- O emisor obtén un resumo da mensaxe a través dunha función resumo (*Hash*). A propiedade máis importante dese resumo ou *hash* é que dous documentos diferentes sempre deben producir resumos diferentes.

- O resumo obtido cifrase coa clave privada do asinante e obtense a sinatura dixital do documento.
- O receptor da mensaxe asinada utiliza a clave pública para descifrar a sinatura, obtén o resumo do documento recibido e comproba que é igual que o resumo que lle chegou cifrado na sinatura dixital. Desta forma garántese que o contido da mensaxe non foi manipulado.



**Figura 1: Proceso de creación dunha sinatura dixital (fonte: INTECO )**

A sinatura dixital, por si mesma, non achega confidencialidade á mensaxe pero é habitual que as mensaxes asinadas electronicamente se adoiten enviar cifradas coa mesma clave privada utilizada para maior seguridade. A sinatura dixital achega:

- Identificación do asinante: a sinatura identifica ao asinante de forma única igual que a súa sinatura manuscrita.
- Integridade do contido asinado: é posible verificar que os documentos asinados non sexan alterados por terceiras partes.
- Non repudio do asinante: un documento asinado electronicamente non pode repudiarse por parte do seu asinante.

### 3. INFRAESTRUTURA DE CLAVE PÚBLICA (PKI)

Como se viu ata agora, a criptografía de clave pública permite resolver o problema do intercambio de claves, utilizando as claves públicas dos participantes. Pero preséntase outro problema: se alguén afirma ser  $A$  e a súa clave pública é  $k_{pub}$ ,

*como podemos saber que realmente  $k_{pub}$  é a clave pública de  $A$ ?*

Porque é perfectamente posible que un atacante  $Z$  xere o seu par de claves  $(k'_{pr}, k'_{pub})$  e afirme “eu son  $A$ , e a miña clave pública é  $k'_{pub}$ ”.

Unha posible solución a este problema é que exista unha entidade de confianza que nos asegure que, efectivamente, as claves públicas pertencen aos seus supostos propietarios. Esta entidade pode asinar un documento que afirme “a clave pública da é  $k_{pub}$ ”, e publicalo para que todos os usuarios o saiban. Este tipo de documento chámase **certificado de clave pública** ou **certificado dixital**, e é a base do que se coñece como **infraestrutura de clave pública ou PKI**.

Unha **PKI** está formada, entre outros, polos seguintes elementos:

- **Certificados dixitais:** Son documentos asinados electronicamente polas autoridades de certificación, que certifican que unha clave pública pertence a un determinado usuario.
- **Autoridades de certificación (AC):** Son entidades de confianza que se encargan de emitir e revogar os certificados dixitais.
- **Autoridades de rexistro (RA):** Son entidades que rexistran as peticións que fan os usuarios para obter un certificado, comprobando a veracidade e corrección dos datos que achegan os usuarios en ditas peticións e envíanas a unha AC para que sexan procesadas.

- **Autoridades de validación (VA):** fornecen información sobre a vixencia dos certificados electrónicos que, á súa vez, sexan rexistrados por unha RA e certificados pola AC.
- **Autoridades de selado de tempos (TSA):** proporcionan certeza sobre a preexistencia de determinados documentos electrónicos nun momento dado, cuxa indicación temporal xunto co hash do documento se asina pola Autoridade de selado de tempo.
- **Directorios de certificados:** proporcionan almacenamento e distribución de certificados e listas de revogación (CRLs).
- **Hardware criptográfico (HSM):** dispositivos criptográficos baseados en hardware que xeran, almacenan e protexen claves criptográficas e adoitan achegar aceleración hardware para operacións criptográficas
- **Tarxetas criptográficas (TI):** son tarxetas que inclúen un chip cun microprocesador con módulos hardware específicos para realizar operacións criptográficas.

### 3.1. Certificados Dixitais

Un certificado dixital é un documento emitido e asinado electronicamente por unha autoridade certificadora no que certifica a asociación entre unha clave pública e un participante.

O certificado garante que a clave pública pertence ao participante identificado e que o participante posúe a correspondente clave privada.

Os certificados dixitais só son útiles se existe unha *Autoridade de Certificación (CA)*, de confianza para as dúas partes, que os valide

Os certificados dixitais proporcionan un **mecanismo criptográfico** para implementar a **autenticación**. Tamén proporcionan un mecanismo seguro



e escalable para **distribuír claves públicas** en comunidades con gran número de participantes.

O formato dos certificados *X.509* é unha recomendación do *ITU*<sup>7</sup> que se publicou por primeira vez en 1988. A revisión actual do estándar foi publicada en 1996 e coñécese co nome de *X.509 v3*. Os elementos que compoñen un certificado *X.509 v3* son:

- **Versión.** É o número de versión do certificado codificado. Os valores aceptables son 1, 2 e 3.
- **Número de serie do certificado.** É un enteiro asignado pola autoridade certificadora. Cada certificado emitido por unha CA debe ter un número de serie único.
- **Identificador do algoritmo de asinado.** Especifica o algoritmo empregado para asinar o certificado (ex: *sha1withRSAEncryption*).
- **Nome do emisor.** identifica a CA que asinou e emitido o certificado.
- **Período de validez.** É o período de tempo durante o cal o certificado é válido e a CA está obrigada a manter información sobre o estado do mesmo.
- **Nome do suxeito.** Identifica o suxeito cuxa clave pública está certificada no campo seguinte. O nome debe ser único para cada entidade certificada por unha CA dada, aínda que pode emitir máis dun certificado co mesmo nome se é para a mesma entidade.
- **Información de clave pública do suxeito.** Almacena a clave pública, os seus parámetros e o identificador do algoritmo co que se emprega a clave.
- **Identificador único do emisor.** Este é un campo opcional que permite reutilizar nomes de emisor.
- **Identificador único do suxeito.** Este é un campo opcional que permite reutilizar nomes de suxeito.
- **Extensións:** As extensións do *X.509 v3* proporcionan un xeito de asociar información adicional a suxeitos, claves públicas, etc.

---

<sup>7</sup>Siglas en inglés de *International Telecommunication Union*.

- **Sinatura da AC:** Neste campo almacénase a sinatura dixital do certificado por parte da AC.

Os certificados dixitais diferéncianse **segundo a finalidade** para a que son solicitados. Así podemos ter certificados para **persoas físicas**, certificados de **servidor**, certificados para a **sinatura de código**, certificados de **entidade**, etc.

### **3.1.1. Autoridade de Certificación**

Unha Autoridade de Certificación, é unha entidade de confianza, encargada de emitir e revogar os certificados dixitais que garanten de forma unívoca e segura a identidade asociada a unha clave pública.

A Autoridade de Certificación, por si mesma ou por mediación dunha [Autoridade de Rexistro](#), verifica a identidade do solicitante dun certificado antes da súa expedición ou, en caso de certificados expedidos coa condición de revogados, elimina a revogación dos certificados ao comprobar dita identidade.

Os certificados son documentos que recollen certos datos do seu titular e a súa [clave pública](#), e están [asinados electronicamente](#) pola Autoridade de Certificación utilizando a súa clave privada.

A Autoridade de Certificación é un tipo particular de [Prestador de Servizos de Certificación](#) que lexitima ante os terceiros que confían nos seus certificados a relación entre a identidade dun usuario e a súa clave pública. A confianza dos usuarios na CA é importante para o funcionamento do servizo e xustifica a filosofía do seu emprego, pero non existe un procedemento normalizado para demostrar que unha CA merece dita confianza.

A autoridade de certificación encárgase de renovar os certificados, proporcionar servizos de backup e arquivo de claves de cifrado. Tamén

crea a infraestrutura de seguridade para a confianza dos participantes, establece políticas de operación segura e xera información de auditoría.

O mecanismo habitual **de solicitude dun certificado** de servidor web a unha CA consiste en que a entidade solicitante, utilizando certas funcións do [software](#) de [servidor web](#), completa certos datos identificativos (entre os que se inclúe o localizador [URL](#) do servidor) e xera unha parella de claves pública/privada. Con esa información o [software](#) de servidor compón un [ficheiro](#) que contén unha petición CSR<sup>8</sup> en formato *PKCS#10* que contén a clave pública e que se fai chegar á CA elixida. Esta, tras verificar por si ou mediante os servizos dunha [Autoridade de Rexistro](#) a información de identificación achegada e a realización do pago, envía o certificado asinado ao solicitante, que o instala no [servidor web](#) coa mesma ferramenta coa que xerou a petición CSR.

As CA dispoñen das súas propios [certificados públicos](#), cuxas claves privadas asociadas son empregadas polas CA para asinar os certificados que emiten. Un certificado de CA estará asinado por outra CA de rango superior establecéndose así unha xerarquía de certificación.

Existen **certificados de CA raíz** que están auto-asinados pola propia CA que os emite e que constitúen o elemento inicial da xerarquía de certificación.

Unha **xerarquía de certificación** consiste nunha estrutura xerárquica de CAs na que se parte dunha CA auto-asinada, e en cada nivel, existe unha ou máis CAs que poden asinar certificados de entidade final ([servidor web](#), persoa, [aplicación](#) de [software](#)) ou ben certificados doutras CA subordinadas plenamente identificadas e cuxa [Política de Certificación](#) sexa compatible coas CAs de rango superior.

Unha das formas polas que se establece a confianza nunha CA por parte dun usuario, consiste na "instalación" no ordenador do usuario (terceiro

---

<sup>8</sup> *Certificate Signing Request*

que confía), do certificado autoasinado da CA raíz da xerarquía na que se desexa confiar.

Cando o modelo de CA inclúe unha **xerarquía**, é preciso **establecer explicitamente a confianza nos certificados de todas as cadeas de certificación** nas que se confíe. Para iso, pódese localizar os seus certificados mediante distintos medios de publicación en internet, pero tamén é posible que un certificado conteña toda a cadea de certificación necesaria para ser instalado con confianza.

Un **certificado revogado** é un certificado que non é válido aínda que se empregue dentro do seu período de vixencia. Un certificado revogado ten a condición de suspendido se a súa vixencia pode restablecerse en determinadas condicións.

É necesario establecer un mecanismo que permita revogar un certificado antes de que este caduque para os casos de roubo, erros, cambios de dereitos, ruptura da CA, etc.

Para comprobar se un certificado está revogado xeralmente utilízanse as **CRL (Certificate Revocation List)**. Deste xeito, cando se quere verificar a sinatura dun documento, o usuario non só debe verificar o certificado e a súa validez, senón que tamén debe comprobar que o certificado non foi revogado, consultando para iso a versión máis recente da CRL .

Coas CRL opérase seguindo dous modelos:

- **Modelo pull:** o cliente que ten que facer a verificación obtén a CRL da CA cando o necesita.
- **Modelo push:** unha vez que a CA actualiza a CRL, a información é enviada aos clientes que necesitan verificar certificados.

Outro método alternativo de comprobación é o protocolo *de estado de certificado en liña* **OCSP**<sup>9</sup>. Este método permítelles aos clientes

---

<sup>9</sup> Siglas en inglés de *Online Certificate Status Protocol*.

desprendérense da xestión do estado dos certificados e obteren unha confirmación online do estado. Para iso a CA debe poñer a disposición de todos os usuarios potenciais un servizo seguro online de alta dispoñibilidade. Este protocolo está definido polo IETF no RFC 2560.

As mensaxes *OCSP* codifícanse en [ASN.1](#) e habitualmente transmítense sobre o protocolo [HTTP](#). A natureza das peticións e respostas de *OCSP* fai que aos servidores *OCSP* se lles coñeza como "*OCSP responders*". As CAs delegan a responsabilidade de proporcionar información de revogacións nos *responders* creando así unha arquitectura distribuída. Os **clientes envían unha petición de estado** a un *responder* e suspende a súa aceptación ata recibir a resposta. Este modo de funcionamento evita o uso de CRLs , reducindo así o ancho de banda consumido, o uso de CPU e evítanse os problemas asociados á xestión de información sensible que conteñen as CRLs.

### **3.1.2. Autoridade de Rexistro**

A Autoridade de Rexistro **xestiona o rexistro de usuarios e as súas peticións de certificación/revogación**, así como os certificados resposta ás devanditas peticións. Indícalle á CA se debe emitir un certificado. A Autoridade de Rexistro é a que autoriza a asociación entre unha clave pública e o titular dun certificado. Durante o ciclo de vida dun certificado, a Autoridade de Rexistro, é a que se encarga das seguintes operacións:

- Revogación.
- Expiración.
- Renovación (extensión do período de validez do certificado, respectando o plan de claves).
- Reemisión do par de claves do usuario.
- Actualización de datos do certificado.

### **3.1.3. Autoridade de Validación**

A Autoridade de Validación **fornece información de forma online acerca do estado dun certificado**. A Autoridade de Validación adoita proporcionar dous servizos de validación: o tradicional, permitindo a descarga de **CRLs** para que o usuario as interprete el mesmo, ou a través do protocolo **OCSP** (*Online Certification Status Protocol*).

Os usuarios e as aplicacións que desexen obter o estado dun certificado só teñen que realizar unha petición *OCSP* contra a Autoridade de Validación para obter dito estado. A CA actualiza a información da Autoridade de Validación cada vez que se modifica o estado dun certificado, co que, usando *OCSP*, se dispón de información en tempo real.

### **3.1.4. Autoridade de Selado de Tempos**

A Autoridade de Selado de Tempos (*TSA*) permite **asinar documentos con selos de tempo**, de maneira que permite obter unha proba de que un determinado dato existía nunha data concreta. O selo de tempo é un dos servizos máis importantes da sinatura electrónica. Co selo de tempo pódese demostrar que unha serie de datos existiron e non foron alterados desde un instante específico no tempo. Este protocolo descríbese no RFC 3161 e está no rexistro de estándares de Internet. Unha autoridade de selado de tempo actúa como terceira parte de confianza testificando a existencia dos devanditos datos electrónicos nunha data e hora concretas. Os pasos que se seguen para xerar un selo de tempo son os seguintes:

- Un usuario quere obter un selo de tempo para un documento electrónico que el posúe.
- Un resumo dixital (tecnicamente un *hash*) xérase para o documento no ordenador do usuario.
- Este resumo forma a solicitude que se lle envía á autoridade de selado de tempo (*TSA*).

- A *TSA* xera un selo de tempo con esta pegada, a data e hora obtida dunha fonte fiable e a sinatura electrónica da *TSA*.
- O selo de tempo envíase de volta ao usuario.
- A *TSA* mantén un rexistro dos selos emitidos para a súa futura verificación.

As aplicacións do selado de tempo son innumerables, xa que os certificados dixitais se emiten cun período de validez determinado e é fundamental, por exemplo: poder verificar que unha sinatura dun documento realizada hai *X* anos, efectivamente se fixo cun certificado que non estaba revogado nese instante. Exemplos de uso: factura electrónica, voto electrónico, protección da propiedade intelectual, etc.

### **3.1.5. Directorio de Certificados**

Os directorios proporcionan almacenamento e distribución de certificados e listaxes de revogación (*CRLs*). Cando unha Autoridade de Certificación emite un certificado ou *CRL*, envíao ao Directorio e, ademais, garda o certificado ou *CRL* na súa base de datos local. Xeralmente utilízase *LDAP* (*Light-weight Directory Access Protocol*) para acceder aos directorios. O usuario pode obter certificados doutros usuarios e comprobar o estado dos mesmos.

## **3.2. Hardware Criptográfico**

Os **Módulos de Seguridade Hardware** (*HSM*) son dispositivos especializados en realizar labores criptográficos. Proporcionan almacenamento seguro de claves e/ou realización de funcións criptográficas básicas como cifrado, sinatura, xeración de claves, etc. Para iso usan interfaces estándar como *PKCS#11* e *CryptoAPI*. Este tipo de dispositivos aumentan significativamente a seguridade en comparación cos certificados baseados en disco polo seguinte:

- A clave privada e as sinaturas dixitais xéranse dentro do HSM.
- A clave privada almacénase cifrada dentro do HSM.

Se se compara o hardware criptográfico coas tecnoloxías de cifrado baseado en software pódese dicir que o hardware criptográfico é moito máis rápido á hora de realizar o proceso. Dependendo do tipo de hardware *HSM*, os ratios de traballo oscilan das 600 a 4000 operacións de sinatura RSA/segundo. Ademais proporcionan seguridade física ao non poder modificar os algoritmos de cifrado e limitando o acceso ao almacenamento seguro de claves. Isto permite que estas solucións poidan ser certificadas por un terceiro en xerarquías de certificación.

### **3.3. Tarxetas e chip criptográficos**

Unha tarxeta intelixente (***smart card***), ou tarxeta con [circuíto integrado](#) (TCI), é calquera tarxeta de tipo peto con circuítos integrados que permiten a execución de certa lóxica programada. Aínda que existe un diverso rango de aplicacións, hai varias categorías de TCI : **As tarxetas de memoria** conteñen só compoñentes de memoria non volátil e posiblemente algunha lóxica de seguridade. **As tarxetas microprocesadoras** conteñen memoria e teñen capacidade de procesamento limitada. **As tarxetas con chip criptográfico** son tarxetas microprocesadas avanzadas nas que hai módulos hardware para a execución de algoritmos usados en cifrado e sinaturas dixitais.

Unha **tarxeta intelixente cun chip criptográfico** pódese definir como unha chave moi segura, non duplicable e inviolable, que contén as claves e certificados necesarios para a sinatura electrónica gravados na tarxeta e que ademais está protexida por un PIN secreto e/ou biometría. O chip **criptográfico** contén un microprocesador que realiza as operacións criptográficas coa clave privada, coa característica adicional de que non é



posible o acceso á clave desde o exterior. As características principais son as seguintes:

- Dobre seguridade: posesión da tarxeta e PIN de acceso (ou mecanismos biométricos).
- Pode ser multipropósito: Tarxeta de identificación gráfica, tarxeta de control de acceso/horario mediante banda magnética ou chip de radiofrecuencia, tarxeta moedeiro, tarxeta xeradora de contrasinais dun só uso (*OTP*).
- Precísase dun middleware (*CSP*) específico para utilizar a tarxeta, así como dun lector (*USB*, integrado en teclado ou *PCMCIA*)
- O número de certificados que se poden cargar depende do perfil de certificado, da capacidade do chip e do espazo que se reserve para os certificados.

### **3.4. 3.3. Marco legal e estándares**

#### **Lexislación Española**

- **Lei 59/2003**, de 19 de decembro, de sinatura electrónica (BOE nº 304, 20/12/2003)

#### **Directiva Europea**

- **Directiva 1999/93/CE do parlamento europeo** e do consello de 13 de decembro de 1999 pola que se establece un marco comunitario para a sinatura 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 os estándares de sinatura electrónica de acordo coa 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 os sistemas de criptografía de clave pública definidos polos 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**

- Universidade de Vigo. Materia de Seguridade en sistemas de información.  
(<http://ccia.ei.uvigo.es/docencia/SSI/>)
- Centro Criptolóxico Nacional. (<https://www.ccn.es/>)
- Instituto Nacional de Tecnoloxías da Comunicación - DNI Electrónico.  
(<http://cert.inteco.es>)
- Universidade Politécnica de Madrid - Departamento de Matemática Aplicada da Facultade de Informática.  
(<http://www.dma.fi.upm.es/java/maticadiscrreta/aritmeticamodular/>)
- Universidade Pontificia Comillas (Madrid) - Materia de Seguridade Informática. (<http://www.iit.upcomillas.es/seguridad>)

(Todas as ligazóns foron verificadas en novembro de 2011)

**Autor:** Juan Otero Pombo

Enxeñeiro en Informática no Concello de Ourense

Colexiado do CPEIG



**44. SEGURANZA EN  
CONTORNOS DE REDE  
PRIVADOS. MECANISMOS DE  
PROTECCIÓN DA  
CONFIDENCIALIDADE.  
SERVIZOS DE DIRECTORIO.  
XESTIÓN DE IDENTIDADES.  
SINGLE SIGN-ON. TIPOS DE  
CONECTIVIDADE. ACCESO  
REMOTO. VPN.**

**Tema 44. Seguridade en contornos de rede privados. Mecanismos de protección da confidencialidade. Servizos de directorio. Xestión de identidades. Single sign-on. Tipos de conectividade. Acceso remoto. VPN.**

## **ÍNDICE**

<b>1 SEGURIDADE EN CONTORNOS DE REDE PRIVADOS. MECANISMOS DE PROTECCIÓN DA CONFIDENCIALIDADE.....</b>	<b>2</b>
<b>2 SERVIZOS DE DIRECTORIO.....</b>	<b>5</b>
<b>3 XESTION DE INDENTIDADES E SINGLE SIGN-ON.....</b>	<b>12</b>
<b>4 TIPOS DE CONECTIVIDADE. ACCESO REMOTO. VPN.....</b>	<b>18</b>
<b>REFERENCIAS.....</b>	<b>29</b>

## **1 SEGURIDADE EN CONTORNOS DE REDE PRIVADOS. MECANISMOS DE PROTECCIÓN DA CONFIDENCIALIDADE**

A seguridade é unha característica de calquera sistema, informático ou non, que o protexe de todo perigo, dano ou risco ao que puidese estar exposto. No caso das redes de ordenadores, esta característica é moi difícil de conseguir (ata poderíamos dicir que é imposible) polo que cando falamos de seguridade en contornos de rede facemos referencia á fiabilidade como unha medida da probabilidade de que o sistema se comporte tal e como se espera del. Referímonos, xa que logo, a todas as medidas hardware e software, persoal, documentación e procesos dentro da infraestrutura de rede que, en conxunto, protexen a integridade e privacidade das aplicacións, datos e fluxos de información. O deseño e implementación dunha infraestrutura de seguridade é unha tarefa crítica xa que: evoluciona rapidamente, crece en complexidade e ten especial incidencia na consecución dos obxectivos da organización.

Hai unha serie de aspectos fundamentais que debemos garantir á hora de manter un sistema seguro:

- **Confidencialidade:** Consiste en protexer a información contra a lectura non autorizada explicitamente. Inclúe non só a protección da información na súa totalidade, senón tamén as pezas individuais que poden ser utilizadas para inferir outros elementos de información confidencial.

Nun contorno de rede, dispónse de dous mecanismos básicos de protección da confidencialidade:

- o **Control de acceso:** garante a confidencialidade da información almacenada nun sistema informático ao impedir o acceso a ela por parte de usuarios non autorizados.

- o Técnicas de cifrado: permiten manter a privacidade da comunicación entre 2 entidades alterando a mensaxe orixinal de modo que lle sexa incomprendible a toda persoa distinta do destinatario.
- **Integridade:** É necesario protexer a información contra a modificación sen o permiso do dono. A información que cómpre protexer inclúe non só a que está almacenada directamente nos sistemas de cómputo, senón que tamén se deben considerar elementos menos obvios como back-up, documentación, rexistros de contabilidade do sistema, tránsito nunha rede, etc. Isto abrangue calquera tipo de modificacións:
  - o Causadas por erros de hardware e/ou software.
  - o Causadas de forma intencional.
  - o Causadas de forma accidental.

Cando se traballa cunha rede, débese comprobar que os datos non foron modificados durante a súa transferencia.

- **Dispoñibilidade:** Unha boa medida para protexer a información é impedir o acceso a ela, pero resulta evidente que nese caso a información deixaría de ser útil. Xa que logo, débense protexer os servizos de cómputo de maneira que non se degraden ou deixen de estar dispoñibles para os usuarios de forma non autorizada. A dispoñibilidade tamén se entende como a capacidade dun sistema para recuperarse rapidamente en caso dalgún problema.
- **Autenticación:** consiste na confirmación da identidade dun usuario; é dicir, a garantía para cada unha das partes de que o seu interlocutor é realmente quen di ser. Un control de acceso permite garantir o acceso a recursos unicamente ás persoas autorizadas.

- **Non repudio:** constitúe a garantía de que ningunha das partes involucradas poida negar no futuro unha operación realizada.

Para termos unha visión global, é de utilidade ver en qué capa do modelo de referencia OSI se abordarían cada un dos aspectos descritos no apartado anterior. Isto pódese ver na Táboa 1. Os servizos da seguridade na rede expándense sobre as sete capas. Cada tecnoloxía pode traballar nunha ou varias capas: Por exemplo, SSL é unha tecnoloxía que traballa normalmente na capa de aplicación.

APLICACIÓN			
PRESENTACIÓN	<b>Servizos seguridade</b>  Confidencialidade Autenticación Integridade Autorización Non repudio	<b>Seguridade lóxica</b>	Seguridade proporcionada por fabricante ou provedor
SESIÓN			
TRANSPORTE			
REDE			
ENLACE			
FÍSICO		<b>Seguridade física</b>	Servizo de seguridade proporcionado na rede backbone de transporte

**Táboa 1. Seguridade na rede e Modelo de referencia OSI**

Unha vez identificados os cinco servizos básicos da seguridade na rede, pódense examinar as tecnoloxías que se definiron e desenvolveron co fin de implementar eses servizos para necesidades específicas de seguridade e baixo diferentes contornos operativos. Unha forma de clasificar estas tecnoloxías é baseándose na maneira en que implementan os servizos de seguridade:

- **Tecnoloxías básicas:** defínense como tecnoloxías básicas as que só implementan un único servizo de seguridade específico. Exemplos destas tecnoloxías son o cifrado, o uso de circuitos permanentes



virtuais (PVC) en Frame Relay para facer VPN de capa 2, ou as listas de control de acceso dos routers (ACL).

- **Tecnoloxías avanzadas:** este tipo de tecnoloxías tamén son deseñadas para implementar un único servizo de seguridade, pero son relativamente máis complexas e con frecuencia necesitan usar varias tecnoloxías básicas para conseguir os seus obxectivos. Un exemplo é a firma dixital para conseguir non repudio en orixe.
- **Tecnoloxías integradas:** este tipo de tecnoloxías son definidas utilizando outras tecnoloxías básicas, pero son deseñadas para darlle soporte a máis dun servizo de seguridade. Exemplos destas tecnoloxías son SSL e IPSEC.
- **Arquitecturas de seguridade:** son tecnoloxías de arquitectura de seguridade en rede que se definen a partir das tecnoloxías básicas, avanzadas e integradas. Proporcionan guías para implementar sistemas de seguridade dentro da arquitectura definida. O mellor exemplo para esta categoría é o uso dunha infraestrutura de clave pública (PKI).

## 2 SERVIZOS DE DIRECTORIO

Un servizo de directorio é unha ferramenta que almacena e organiza dun modo claro e efectivo a información relativa aos usuarios, aplicacións, arquivos, impresoras e outros recursos accesibles dentro dunha rede co obxectivo de mellorar a funcionalidade e a facilidade de uso e de poder facer unha xestión eficiente dos recursos da organización.

Un directorio é unha listaxe de información de obxectos que están dispostos nunha orde concreta e que achega información detallada acerca de cada obxecto concreto. Exemplos comúns son a guía de teléfonos dunha cidade ou un catálogo dunha biblioteca.

Os directorios adoitan describirse a miúdo como unha base de datos, pero realmente é unha base de datos especializada que ten unhas características de seu que a distingue das bases de datos relacionais de carácter xeral:

- Unha característica especial é que se accede con moita frecuencia mediante operacións de lectura, buscas e navegación, namentres que as operacións de escritura son moito menos frecuentes.
- Debido á característica anterior, estes sistemas están deseñados para soportar gran número de solicitudes de lectura e o acceso mediante operacións de escritura pode estar limitado a certos administradores.
- Outra diferenza coas BD de propósito xeral é que a maioría de implementacións dos servizos de directorio non son compatibles entre si.
- As consultas ás BD de propósito xeral fanse partindo dunha ferramenta estandarizada de consulta chamada SQL, namentres que os directorios adoitan utilizar un protocolo de acceso simplificado e optimizado.

Existen numerosas implementacións dos servizos de directorio de diferentes compañías. Algúns exemplos son:

- **NIS:** *Network Information Service* é unha implementación de Sun Microsystems para redes no contorno UNIX.
- **Active Directory:** é o servizo de directorio de Microsoft.
- **ApacheDS:** *Apache Directory Studio* é o servidor de directorio de Apache.

- **eDirectory:** é un servizo de directorio desenvolvido por Novell e soportado por múltiples plataformas, incluíndo Windows, NetWare, Linux.
- **OpenLDAP:** derivado da implementación orixinal de referencia LDAP da Universidade de Michigan, pero significativamente evolucionado. É compatible con practicamente todas as plataformas actuais: UNIX, Linux, Windows, etc.

Os servizos de directorio formaron parte dunha iniciativa do OSI (*Open Systems Interconnection*) para poñer de acordo aos membros da industria no establecemento duns estándares de rede comúns e así garantir a interoperabilidade. Na década dos 80, a UIT e a ISO crearon o conxunto de estándares X.500 sobre o modelo de referencia OSI para servizos de directorio. X.500 consta dos seguintes protocolos: protocolo de acceso ao directorio (DAP), protocolo de sistema de directorio, protocolo de ocultación de información e protocolo de xestión de enlaces de directorio.

## 2.1 LDAP

X.500 é un conxunto de protocolos producido pola *Unión Internacional de Telecomunicacións*<sup>1</sup> na década de 1980 que organiza as entradas no directorio de maneira xerárquica e cunha alta capacidade de almacenamento de datos, proporcionando grandes facilidades de busca e unha arquitectura facilmente escalable. X.500 especifica que a comunicación entre o cliente e o servidor debe empregar o *Directory Access Protocol* (DAP), pero DAP é un protocolo a nivel de aplicación, polo que tanto o cliente como o servidor debían implementar completamente a pila de protocolos OSI.

---

<sup>1</sup> ITU polas súas siglas en inglés.

LDAP (*Lightweight Directory Access Protocol*) xorde como unha alternativa a DAP. Trátase dunha serie de estándares do *Internet Engineering Task Force*<sup>2</sup> definidos en varios RFC. A versión máis recente é a v3 e está publicada como o RFC 4510. As claves do éxito de LDAP en comparación con DAP de X.500 son:

- LDAP utiliza TCP/IP en lugar dos protocolos OSI. TCP/IP require menos recursos e está máis dispoñible.
- LDAP representa a información mediante cadeas de caracteres en lugar de complicadas estruturas ASN.1.
- O modelo funcional de LDAP é máis simple e eliminou opcións raramente utilizadas en X.500, polo que é máis fácil de comprender e implementar.

LDAP define o contido das mensaxes intercambiadas entre un cliente e un servidor LDAP. As mensaxes especifican as operacións requiridas polo cliente, as respostas do servidor e os datos transportados na mensaxe. Un exemplo de interacción xeral entre un cliente e un servidor LDAP ten a seguinte forma:

- O cliente establece unha sesión co servidor LDAP. Coñécese como *binding*. O cliente especifica o nome de host e o porto onde escoita o servidor.
- O cliente pode proporcionar un nome de usuario e contrasinal para autenticarse contra o servidor ou establecer unha sesión anónima cos dereitos de acceso por defecto.
- O cliente realiza operacións sobre os datos do directorio. LDAP ofrece capacidades de lectura e actualización. Tamén posúe capacidades de busca de datos no directorio a través de criterios especificados polo

---

<sup>2</sup> IETF polas súas siglas en inglés.

usuario. As buscas son operacións frecuentes no directorio e lévanse a cabo con axuda dos filtros de buscas.

- Cando o cliente termina de facer peticións, pecha a sesión co servidor. Isto tamén se coñece como *unbinding*.

Ademais de definir o protocolo de acceso ao directorio, o estándar LDAP define catro modelos que permiten entender mellor o servizo de directorio.

### **2.1.1 O modelo de información**

O modelo de información describe a estrutura da información almacenada nun directorio LDAP. A unidade básica de información almacenada no directorio é a entrada (*entry*). Normalmente unha entrada representa un obxecto do mundo real (unha persoa, un servidor, etc.), pero o modelo non esixe este aspecto.

Unha entrada componse dun conxunto de atributos; cada un deles ten un tipo e un ou varios valores. O tipo define a clase de información que vai almacenar e os valores son a información en si. Ademais, os atributos teñen un identificador de obxecto (OID) e unha sintaxe que indica qué valores pode conter e cómo se fan as comparacións.

- Exemplo de atributos: cn: Manuel Rodríguez, ou: VENDAS.

Os esquemas (*schemas*) definen o tipo de obxectos que se van almacenar no directorio; tamén contén os atributos que teñen estes obxectos e se son opcionais ou obrigatorios.

Dado que cada servidor pode definir o seu propio esquema, para permitir a interoperabilidade entre distintos servidores de directorio espérase que un esquema común sexa estandarizado (RFC 2252 e RFC 2256).

### 2.1.2 O modelo de nomeado

O modelo de nomeado de LDAP define como se organizan e se referencian os datos, é dicir, define os tipos de estruturas que se poden definir utilizando as entradas. Unha vez organizadas as entradas formando unha determinada estrutura, o modelo de nomeado indícanos como referenciar estas entradas.

As entradas no directorio describen obxectos (unha impresora, un usuario, etc.), teñen asociado un identificador chamado *Distinguished Name* (DN) que os identifica univocamente e organízanse nunha estrutura de árbore coñecida como *Directory Information Tree* (DIT).

Pola súa banda, un DN consiste nunha secuencia de anacos de información máis pequenos coñecidos como *Relative Distinguished Name* (RDN). Na estrutura de árbore, o RDN corresponderíase cunha póla e o DN obteríase ao seguir toda a árbore desde a raíz a unha folla.

Polo xeral o DN represéntase mediante unha secuencia de RDN separados por comas. Exemplo:

- “cn=Pedro Pérez, ou=VENDAS, ou=empresa, c=es”.

Deste xeito, non pode haber ningunha entrada solta; só a entrada raíz pode non ter entrada pai. No caso de engadir unha entrada nun punto inexistente no directorio, o servidor devolverá unha mensaxe de erro e non realizará a operación.

Esta flexibilidade permite que o directorio almacene a información da forma máis conveniente; pódese crear un grupo que conteña todas as persoas da organización e outro que conteña todos os grupos, ou pódese escoller unha estrutura que reflicta a estrutura xerárquica da organización.

### 2.1.3 O modelo funcional

O modelo funcional describe qué operacións se poden levar a cabo sobre a información almacenada no directorio LDAP. Estas operacións pódense agrupar en tres categorías principais:

- **Autenticación:** *bind*, *unbind* son operacións utilizadas para conectar e desconectar co servidor LDAP, establecer dereitos de acceso e protexer a información. Pódese protexer unha sesión a varios niveis, elixindo entre unha sesión anónima, unha sesión autenticada e unha sesión autenticada utilizando mecanismos SASL (*Simple Authentication and Security Layer*).
- **Consultas:** é a operación máis utilizada. Pódense facer buscas e comparar información por diversos criterios especificados polo usuario. As buscas pódense acoutar establecendo un punto de partida no DIT (*baseDN*), a profundidade a buscar desde o punto de partida (*scope*), os atributos que nos interesan, etc. O elemento clave nas consultas é a definición de filtros de busca (*search Filter*). Os filtros de busca teñen unha sintaxe propia que se debe seguir: Exemplo de filtro: `(|(sn=León)(sn=Castela))` obtería as entradas nas que o apelido sexa Castela ou León.
- **Actualización:** permite as operacións de engadir, modificar e borrar as entradas (*add*, *delete*, *modify*).

### 2.1.4 O modelo de seguridade

O modelo de seguridade describe como se pode protexer a información do directorio contra accesos non autorizados. O modelo de seguridade céntrase na operación de *bind*. Hai varias formas de inicio de sesión por parte dun usuario:

- Pode iniciar unha sesión de forma anónima cos permisos por defecto.
- Pode iniciar unha sesión cun nome de usuario e contrasinal en claro.
- En LDAPv2 só se permiten sesións anónimas e autenticación mediante texto en claro; debido a isto algúns fabricantes incorporaron mecanismos de seguridade adicionais como Kerberos.
- A operación bind de LDAPv3 ten soporte para *Simple Authentication Security Layer* (SASL); ademais, definíronse operacións estendidas, unha delas relacionada coa seguridade: é a *Extension for Transport Layer Security* (TLS) para LDAPv3.

### 3 XESTION DE IDENTIDADES E SINGLE SIGN-ON

Un sistema de xestión de identidades integra políticas e procesos organizacionais destinados a simplificar e controlar o acceso aos sistemas de información e ás instalacións dunha organización por parte de empregados e outras entidades autorizadas. A xestión de identidades busca a definición dunha identidade para cada usuario (persoa ou proceso), que levará asociados unha serie de atributos.

O concepto central dun sistema de xestión da identidade é o uso do que se coñece como *single sign-on* (SSO). O SSO habilita a un usuario para acceder a todos os recursos da rede tras unha única autenticación.

Os principais aspectos que debe incluír un sistema de xestión da identidade son os seguintes:

- **Autenticación:** confirmación de que a identidade se corresponde co nome de usuario que se proporciona.



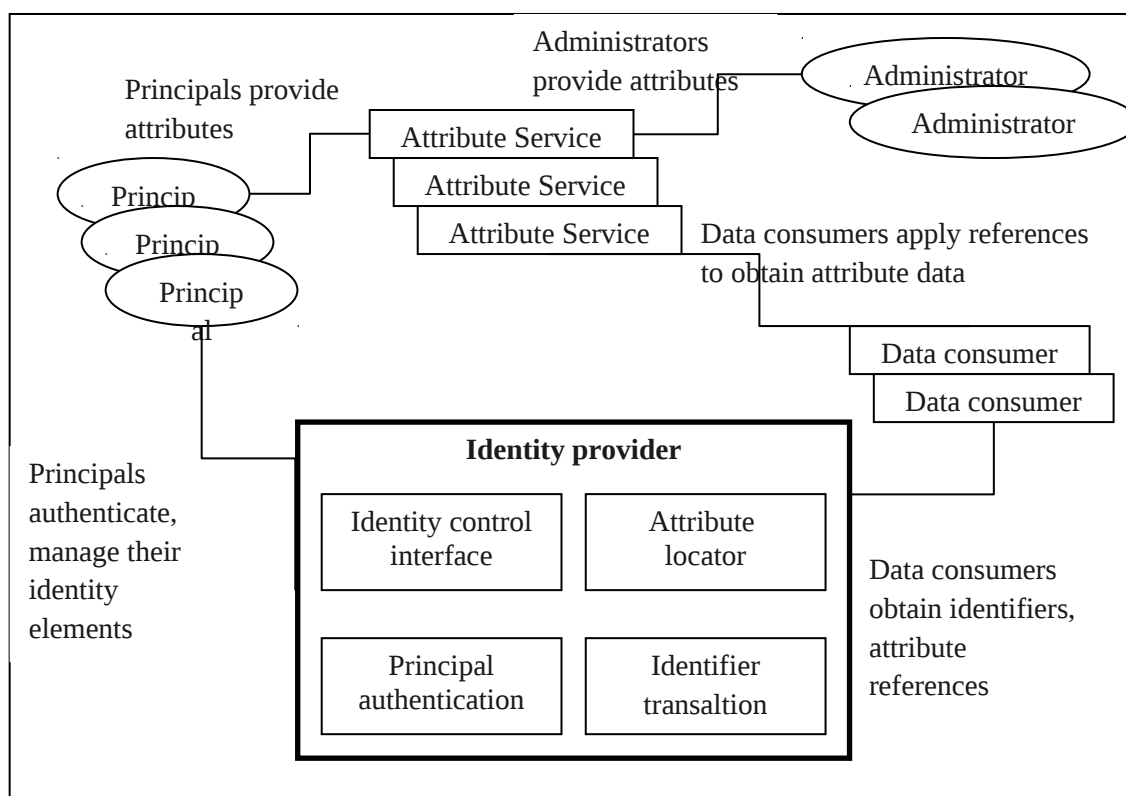


- **Autorización:** capacidade de proporcionar permisos para servizos e recursos específicos baseándose na autenticación.
- **Trazabilidade:** proceso que se encarga de rexistrar accesos e autorizacións.
- **Aprovisionamento:** inscrición de usuarios no sistema.
- **Automatización de fluxos de traballo:** movemento de datos en procesos de negocio.
- **Administración delegada:** o uso de control de accesos baseado en roles para proporcionar acceso a recursos.
- **Sincronización de contrasinais:** creación dun proceso para acceder por medio de SSO. *Single sing-on* habilita a un usuario para acceder a todos os recursos do sistema logo dunha autenticación sinxela.
- **Servizo de reseteo de contrasinais:** capacidade que permite a un usuario cambiar o seu contrasinal.
- **Federación:** proceso polo cal a autenticación e permisos son pasados dun sistema a outro, normalmente a través de diferentes organizacións, reducindo así o número de autenticacións necesarias para o usuario.

Na Figura 1, pódense ver os elementos que conforman unha arquitectura xenérica de xestión da identidade:

- **Principais:** un *principal* é un contedor de identidade. Habitualmente é un usuario que tenta acceder aos servizos e recursos da rede. Dispositivos de usuario, procesos axente e sistemas servidor poden ser tamén *principals*. Os *principals* autenticáanse contra un provedor de identidade.

- **Provedor de identidade:** asocia información de autenticación cun *principal*, así como atributos e un ou máis identificadores.
- **Servizo de atributos:** as identidades dixitais incorporan máis atributos que un identificador e información de autenticación. O servizo de atributos xestiona a creación e mantemento destes atributos. Por exemplo: un usuario que necesita proporcionar un enderezo cada vez que entra nunha Web de compras. O servizo de xestión de identidade permite proporcionar esta información unha soa vez, e será presentada aos consumidores de datos de acordo coas políticas de privacidade e autorización establecidas.
- **Consumidores de datos:** son entidades que obteñen e empregan datos xestionados e proporcionados polos provedores de atributos, e xeralmente son utilizados para levar a cabo decisións de autorización e auditoría. Por exemplo, un servidor de base de datos é un consumidor de datos que necesita as credenciais do cliente para saber que niveis de acceso lle debe proporcionar.



## **Figura 1: Arquitectura xenérica de xestión da identidade**

### **3.1 Xestión federada de identidades**

A federación de identidades é, en esencia, a extensión da xestión da identidade a múltiples dominios de seguridade. Os devanditos dominios inclúen unidades internas de negocio, socios de negocio externos e outras aplicacións e servizos de terceiros. O obxectivo é proporcionar o intercambio de identidades dixitais para que un usuario poida ser autenticado unha soa vez e despois poida acceder a recursos a través de múltiples dominios. Como estes dominios son relativamente autónomos ou independentes, non é posible un control centralizado. Así e todo, as organizacións colaboradoras deben formar unha federación, baseada en estándares e niveis de confianza mutua, para compartiren de forma segura as identidades dixitais.

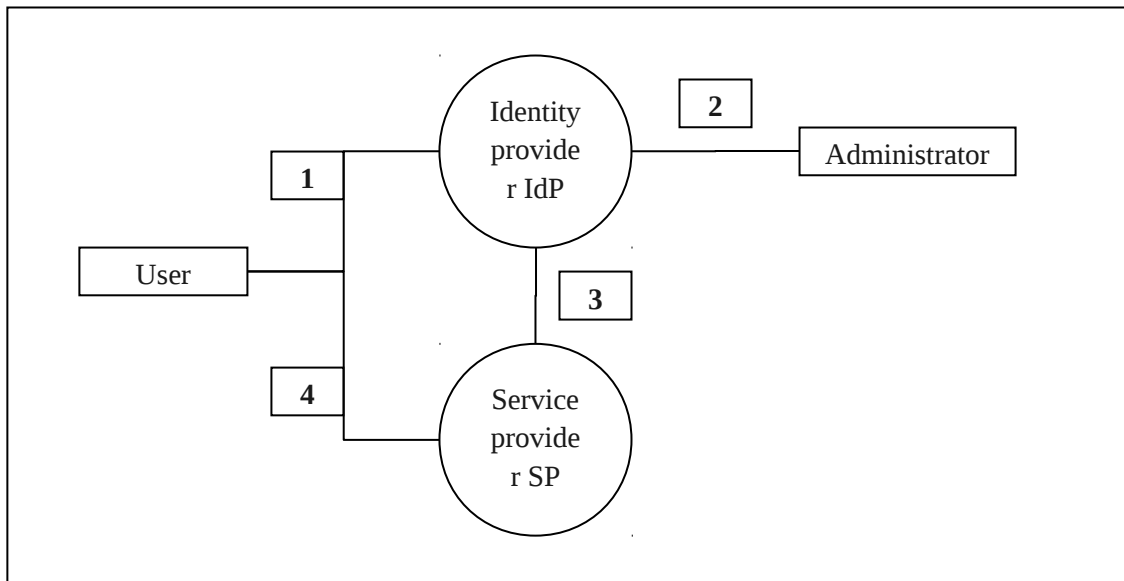
A xestión federada de identidades refírese aos acordos, normas e tecnoloxías que permiten a portabilidade das identidades, atributos de identidade e dereitos a través de múltiples organizacións e aplicacións e coa participación de moitos usuarios. Cando varias organizacións implementan un esquema de interoperabilidade de identidade federada, un empregado dunha organización pode usar un único inicio de sesión para acceder a servizos a través da federación mediante relacións de confianza asociadas á identidade.

Máis alá do SSO, a xestión de identidade federada ofrece outras capacidades: unha delas é que proporciona un medio estandarizado de representar atributos. Normalmente, as identidades dixitais incorporan máis atributos que un simple identificador e información de autenticación. Exemplos de atributos son os números de conta, roles na organización, situación física e propietarios de arquivos. Un usuario pode ter múltiples

identificadores; por exemplo, cada identificador pode estar asociado a un único rol, cos seus propios permisos de acceso.

A Figura 2 ilustra as entidades e fluxos de datos nunha arquitectura xenérica de xestión federada da identidade:

1. O navegador do usuario final ou outras aplicacións inician un diálogo cun provedor de identidade (IdP) no mesmo dominio. O usuario final tamén proporciona valores de atributos asociados coa súa identidade.
2. Algúns atributos asociados coa identidade, como por exemplo roles permitidos, poden ser proporcionados por un administrador no mesmo dominio.
3. Un provedor de servizos (SP) nun dominio remoto ao que o usuario desexa acceder obtén o identificador da identidade, información de autenticación e atributos asociados desde o provedor de identidade no dominio de orixe.
4. O provedor de servizo (SP) abre unha sesión co usuario remoto e reforza as restricións de control de acceso baseándose na identidade e atributos do usuario.



**Figura 2: Modo de operación dunha federación de identidades**

Existe un gran número de solucións no campo da xestión federada de identidades. Hai estándares abertos desenvolvidos por grandes consorcios, solucións propietarias desenvolvidas por compañías privadas e proxectos *opensource* de menor escala. Algúns exemplos son:

- **SAML:** *Security Assertion Markup Language* é un estándar baseado en XML desenvolvido por OASIS (*Organisation for the Advancement of Structured Information Standards*). A versión actual é a 2.0 e foi recoñecida como estándar en 2005. (<http://www.oasis-open.org/>).
- **OpenID:** é un estándar aberto desenvolvido pola *OpenId Foundation*. (<http://openid.net/foundation/>).
- **Shibboleth:** É un proxecto do consorcio *Internet2*, que proporciona unha arquitectura e unha implementación *opensource* dun sistema de xestión da identidade federado baseado en SAML. A versión máis recente do seu provedor de identidade é a 2.3.0 e data do 2011. (<http://shibboleth.internet2.edu/>).

- **WS-Federation:** É un Framework desenvolvido por varios fabricantes entre os que destacan IBM e Microsoft. A súa especificación máis recente é a 1.1 e data do 2006. (<http://www.ibm.com/developerworks/library/specification/ws-fed/>).
- **Liberty Identity Federation Framework (IDE-FF):** É un Framework de xestión federada da identidade, desenvolvido por un consorcio formado por máis de 150 empresas e organizacións e coñecido co nome de Liberty Alliance.

#### **4 TIPOS DE CONECTIVIDADE. ACCESO REMOTO. VPN.**

O acceso remoto é a capacidade dun usuario de obter acceso a un servidor ou a unha rede desde unha localización remota. Persoal en delegacións da organización, teletraballadores ou persoal que está a viaxar poden necesitar acceder á rede corporativa. Hai varias formas de conectar o equipo ou rede remota coa rede corporativa:

- Os usuarios que traballan desde a casa conseguen acceso a Internet a través dun provedor de servizos de Internet (ISP). Unha forma de conectarse é por medio de conexións desde un portátil ou equipo de sobremesa con axuda de liñas DSL e cable módem con axuda de VPN.
- Outra alternativa baseada no uso de VPN é a que poden utilizar os usuarios que están viaxando e non dispoñen dunha conexión cableada. Para iso pódense valer de conexións sen fíos (Wifi, Wimax) proporcionadas por dispositivos móbiles preparados para xestionar este tipo de conexións. Tamén poden acceder con axuda de conexións de datos de telefonía móbil.



- O uso dun enlace privado entre unha rede remota e a rede corporativa é unha opción útil para, por exemplo, conectar a sede dunha organización coas súas delegacións. Os enlaces privados adoitan ser máis caros, pero ofrecen maior fiabilidade e ratios de transferencia máis elevados. Exemplos de tecnoloxías que proporcionan enlaces privados son ATM, Frame Relay, Clear Channel, RDSI, Fibra óptica.
- A utilización de radio enlaces de longa distancia ou conexións vía satélite é outra forma de comunicar unha rede remota coa rede da organización.

Para acceder remotamente dunha forma segura á rede da organización son necesarias algunhas capacidades básicas relacionadas coa seguridade nos sistemas de acceso remoto:

- **Control de acceso á rede:** a primeira liña de defensa na seguridade de acceso remoto é o control de acceso para previr que accedan os intrusos non desexados. Para iso defínese unha política de seguridade que describe como se pode acceder de forma segura á rede. Exemplos disto son os portais cativos, o uso do protocolo 802.1X, etc.
- **Autenticación de usuarios e autorización:** é a segunda liña de defensa e asegura a autenticidade dun usuario mediante o uso de protocolos de autenticación.
- **Protección da conexión e integridade do tráfico:** unha vez que se establece unha sesión, é preciso garantir a confidencialidade e integridade do tráfico intercambiado entre as partes.

Non hai estándares formais definidos especificamente para explicar como debe ser unha arquitectura de acceso remoto, porque cada organización ten as súas características e requisitos de acceso remoto. No entanto, hai compoñentes funcionais que se converten en estándares de facto nun

despregamento típico de acceso remoto. Os compoñentes clave que deberían ser tidos en conta nunha arquitectura de acceso remoto típica son os seguintes:

- **Firewall:** é un conxunto de tecnoloxías hardware e software instaladas estratexicamente entre as redes privadas da compañía e unha ou máis redes non seguras (incluída Internet).
- **Zona desmilitarizada (DMZ):** é un elemento común na maioría de despregamentos de firewalls. É utilizada para proporcionar unha zona diferenciada entre os equipos da rede privada que non teñen acceso desde o exterior e os servidores que si teñen conexión exterior. Nesta rede hai servidores bastión que actúan como intermediarios entre os accesos remotos e a organización. Exemplos deste tipo de servidores son os proxies e os servidores de autenticación.
- **Servidor de acceso remoto (RAS):** é un servidor que actúa de porta de enlace entre o cliente remoto e a rede en arquitecturas de conexión mediante enlaces conmutados analóxicos e/ou dixitais (p. Ex.: RDSI). Unha vez que un usuario remoto establece a conexión por medio dunha chamada, a liña telefónica é transparente para o usuario e pode acceder aos recursos da rede interna.
- **Servidor Proxy:** é un servidor que actúa como intermediario entre un usuario remoto e as aplicacións e servizos internos da organización aos que desexa acceder. Deste xeito a empresa pode garantir a seguridade das aplicacións internas, o control administrativo e ter capacidades de *caché* (por exemplo, en accesos vía Web). A autenticación do usuario pode ser feita polo propio Servidor Proxy ou por un servidor de autenticación.
- **Servidor de autenticación:** é o encargado de verificar a identidade dos usuarios que tentan acceder á rede privada da organización.



#### 4.1 Virtual Private Networks (VPN)

As redes privadas virtuais (VPN) proporcionan unha forma segura de conectarse desde unha localización remota cunha rede de área local privada (LAN) a través de Internet ou calquera outra rede pública non segura. Unha VPN é unha conexión que ten a aparencia e moitas das vantaxes dun enlace dedicado, pero traballando sobre unha rede pública. Para isto utilízase unha técnica chamada *tunneling* que permite enrutar os paquetes de datos pola rede pública nun túnel privado que simula unha conexión punto a punto. As VPN son utilizadas frecuentemente polos traballadores remotos ou empregados nas delegacións da organización para compartir datos e recursos da rede privada. Unha rede privada virtual pode proporcionar os seguintes beneficios para a organización:

1. **Seguridade mellorada:** ao reducir o número de conexións co mundo exterior redúcese considerablemente a posibilidade dun ataque. Ademais, tamén se reduce a posibilidade de interceptación do tráfico.
2. **Rendemento previsible:** en VPN con canles dedicadas pódese garantir o ancho de banda entre os sitios e o rendemento da rede faise máis previsible.
3. **Independencia na elección das tecnoloxías de transporte para as redes de usuarios:** as posibilidades están limitadas pola elección dun provedor ou fabricante. Así, a organización pode usar Ethernet, Frame Relay, IP e outras tecnoloxías de rede para conectar os seus sitios.
4. **Espazo de enderezos IP independente:** nas redes privadas é posible utilizar calquera direccionamento. Por exemplo, case todos os servizos de VPN permiten o uso de enderezos IP privados, tales coma 10.0.0.1 ou 192.168.0.3, que non poden ser enrutados a través das redes públicas.

Estas características serán de utilidade para algúns usuarios, pero de importancia relativa para outros. As vulnerabilidades e baixo rendemento das redes públicas poden facer que a “seguridade mellorada” e o “rendemento previsible” sexan as características máis desexables dunha VPN. Recentemente, a “independencia de elección de tecnoloxía” e o “espazo de enderezos independente” parece que se volveron menos importantes: o primeiro, debido ao predominio das tecnoloxías Ethernet en capa 2 e IP en capa 3. A segunda, debido a que coa implantación de IPv6 se espera acabar co déficit de enderezos. De todos os xeitos, ter un espazo de enderezos independente mellora a seguridade, utilizando rangos de enderezos para separar sitios dentro da organización e restrinxir accesos.

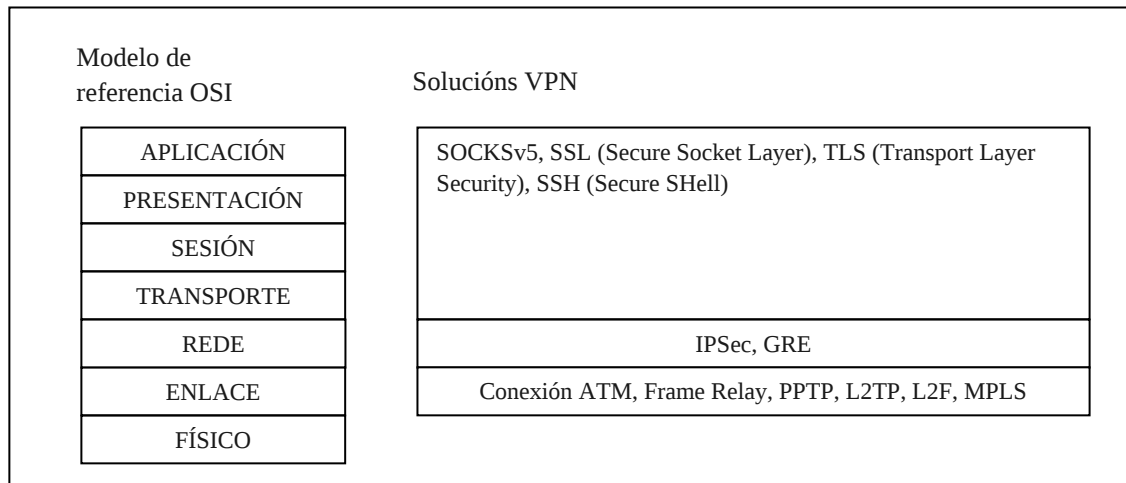
Á hora de crear unha VPN para proporcionar acceso remoto, hai que escoller a tecnoloxía que mellor se adapte ao escenario en cuestión. Esta elección de tecnoloxía abrangue técnicas de *tunneling*, autenticación, control de acceso e seguridade de datos. Polo xeral defínense tres arquitecturas principais de VPN:

- **Intranet VPN (LAN-to-LAN VPN):** neste escenario as redes remotas da organización son conectadas entre si utilizando a rede pública, converténdose deste xeito nunha única rede LAN corporativa global.
- **VPN de acceso remoto:** neste tipo de VPN situaríanse os usuarios que desde un host remoto crean un túnel para conectarse á rede privada da organización. O dispositivo remoto pode ser un equipo persoal cun software cliente para crear VPN, e usar unha conexión conmutada ou unha conexión de banda ancha permanente.
- **Extranet VPN:** este tipo de arquitecturas permiten que certos recursos da rede privada da organización sexan accedidos por redes doutras compañías, tales como clientes ou provedores. Neste escenario é fundamental o control de acceso.

Hai unha gran variedade de tecnoloxías que se poden utilizar para a implementación de VPN. Os criterios que deben cumprir estas tecnoloxías son:

- **Seguridade:** as conexións deben ser brindadas cumprindo cos requisitos de autenticación, autorización, privacidade, integridade e contabilidade.
- **Eficiencia:** os tempos de resposta deben ser adecuados e comparables coas redes consideradas “non seguras”.
- **Facilidade de administración:** os usuarios e administradores deste tipo de redes poden facer o seu traballo dunha maneira rápida e efectiva.
- **Cumprimento de estándares e interoperabilidade:** hai moitas tecnoloxías que son estándares e que participan na creación de VPN: IPSec, MD5, SOCKSv5, IKE, ISAKMP, Diffie-Hellman, X.509, RADIUS, etc.

Para clasificar as tecnoloxías que se poden utilizar na implementación dunha arquitectura de VPN, pódese tomar como referencia o modelo OSI e situalas en función do nivel en que son implementadas. A Figura 3 mostra os principais protocolos utilizados para o establecemento de conexións VPN e a súa situación no modelo de referencia OSI.



**Figura 3: Situación das solucións VPN no modelo de referencia OSI**

Á hora de implementar unha arquitectura de rede baseada en VPN hai dúas posibles opcións. Facer unha implementación por hardware ou por software.

As implementacións por Hardware realizan o proceso de encriptación e desencriptación do tráfico a nivel físico entre os extremos da liña de comunicación. Os dispositivos utilizados normalmente son routers con capacidades de VPN incorporadas. Como vantaxes desta solución pódese dicir que a instalación e configuración son relativamente sinxelas, non se necesita persoal especializado e o seu mantemento é mínimo. Pola contra, presentan o inconveniente de que o sistema de encriptación vén imposto polo fabricante e depéndese del para as actualizacións.

Doutra banda as implementacións baseadas en Software estanse impondo cada día máis. A explicación radica en que a necesidade dos usuarios pequenos e medianos de implantar sistemas de seguridade no acceso ás súas máquinas vai en aumento. As implementacións software son moito máis baratas que comprar hardware preparado para VPN e existe un gran número de VPN desenvolvidas por software. Como inconvenientes deste recurso pódese dicir que é necesaria unha máquina

para darlle soporte á solución, o sistema de claves e certificados reside en máquinas potencialmente inseguras e nos casos en que se utilice software de libre distribución poida ser que teña portas traseiras ou outras deficiencias de seguridade.

## 4.2 SSL/TLS

SSL/TLS son os acrónimos de *Secure Sockets Layer/Transport Layer Security*. O protocolo SSL é desenvolvido en 1995 por Netscape. Baséase nunha arquitectura cliente/servidor e foi deseñado orixinalmente para permitir o intercambio de información seguro entre un servidor Web e un navegador. Hoxe en día o IETF mantén o desenvolvemento de TLS como un protocolo estándar de Internet. A versión máis recente TLS 1.2 está definida no RFC 5246 e foi publicada no 2008.

SSL é un protocolo que proporciona autenticación e confidencialidade entre os extremos da comunicación mediante o uso de criptografía. Cando se establece unha comunicación por SSL, habitualmente só o servidor é autenticado, aínda que é posible a identificación mutua mediante o despregamento dunha infraestrutura de claves públicas (PKI). SSL implica unha serie de fases básicas:

- Negociar entre as partes o algoritmo que se empregará na comunicación.
- Intercambio de claves públicas e autenticación baseada en claves públicas.
- Encriptación do tráfico por medio do uso de cifrado simétrico.

Durante a primeira fase, négóciase os algoritmos criptográficos que se van usar entre o cliente e o servidor:

- Protocolos de clave pública: RSA, DSA, Diffie-Hellman, etc.

- Protocolos de cifrado simétrico: DEAS, 3DEAS, IDEA, AES, RC2, etc.
- Funcións resumo: MD5 ou familia SHA.

SSL/TLS proporcionan un amplo abano de medidas de seguridade:

- Numéranse todos os rexistros usando o número de secuencia no MAC (*Message Authentication Code*).
- Úsase un resumo de mensaxe mellorada cunha clave (só se pode comprobar o MAC coa devandita clave).
- Proporcionan protección contra varios ataques coñecidos (por exemplo: *man-in-the-middle-attack*).
- Ao finalizar a conexión envíase na mensaxe un hash de todos os datos intercambiados e vistos por ambas as partes.

SSL execútase nunha capa entre os protocolos de aplicación como HTTP, SMTP, NNTP e sobre a capa de transporte TCP do protocolo TCP/IP. Aínda que lle pode proporcionar seguridade a calquera protocolo que utilice conexións de confianza (tal como TCP), úsase na maioría dos casos xunto a HTTP para formar HTTPS. Outra aplicación na que se pode utilizar SSL é no *tunneling* dunha rede completa para poder crear así unha VPN, como se fai por exemplo con OpenVPN.

### 4.3 Secure Shell: SSH

Secure Shell ou SSH é un protocolo de rede que permite o intercambio de datos entre dous dispositivos conectados á rede utilizando unha canle segura. As dúas principais versións do protocolo son coñecidas como SSH1 e SSH2. Úsase principalmente en contornos UNIX e Linux para acceder a consolas remotas. Foi creado no ano 1995 polo investigador da Universidade de Helsinki Tatu Ylönen e o seu principal obxectivo era

proporcionar unha alternativa segura para Telnet e outros intérpretes de comandos remotos. No ano 2006 convértese nun estándar do IETF descrito no RFC 4253. A definición da súa arquitectura inclúe tres protocolos apilados nas capas de transporte e aplicación:

- *SSH Connection Protocol*: neste protocolo defínese o concepto de canles, peticións de canle e peticións globais que os servizos SSH proporcionan.
- *SSH User Authentication Protocol*: neste protocolo manéxase a autenticación de clientes e proporciónanse varios métodos de autenticación. Algúns dos métodos utilizados son: o uso de contrasinais ordinarios, autenticación de clave pública baseada en DSA, RSA e certificados X.509, Kerberos, etc.
- *SSH Transport Layer Protocol*: este protocolo manexa o intercambio inicial de claves, así como a autenticación do servidor, o establecemento do tipo de cifrado, compresión e verificación de integridade.

O uso de SSH estendeuse e pode ser utilizado por un amplo número de aplicacións sobre múltiples plataformas, incluídas UNIX, Windows, MAC VOS e Linux:

- Transferencia segura de ficheiros utilizando as aplicacións SCP e SFTP.
- Sistemas de ficheiros en rede: SSHFS. É unha alternativa a NFS, na que o cliente non necesita que o servidor exporte un directorio por NFS; abóndalle ter acceso por SSH.
- *Port forwarding*: Permite unha comunicación segura sobre rede unha insegura, moi similar a unha VPN, pero traballando cun único porto.
- *OpenSSH* desde a versión 4.3 permite facer verdadeiras VPN (todos os portos), tanto en nivel de enlace como nivel de rede.



No mercado existen diversas implementacións:

- *ssh* orixinal con licenza freeware.
- *OpenSSH*, desenvolvida orixinalmente para OpenBSD, portada a moitos outros SO, é a versión máis empregada.
- *Dropbear*, é unha versión reducida, habitual en sistemas encaixados como OpenWRT.
- En Microsoft Windows pódese utilizar o servidor *CopSSH* e o 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>).
- Apuntamentos da materia Deseño e Administración de Sistemas e Redes - Enxeñaría Informática - Universidade Rei Juan Carlos.  
([http://gsyc.escet.urjc.es/~mortuno/index\\_dasr.html](http://gsyc.escet.urjc.es/~mortuno/index_dasr.html)).

(Todas as ligazóns foron verificadas en xuño do 2011)

**Autor:** Juan Otero Pombo  
Enxeñeiro en Informática no Concello de Ourense  
Colexiado do CPEIG

**45. SEGURANZA EN REDES  
WAN E INTERNET:  
CRIPTOGRAFÍA E  
AUTENTICACIÓN.  
ARQUITECTURA DE  
SEGURANZA EN REDES.  
SISTEMAS DE AUTENTICACIÓN  
PARA SEGURANZA EN REDES.  
ELEMENTOS DE SEGURANZA  
PARA INTERNET.  
TELECOMUNICACIÓNS.**

**Tema 45. Seguridade en redes WAN e internet: criptografía e autenticación. Arquitectura de seguridade en redes. Sistemas de autenticación para seguridade en redes. Elementos de seguridade para internet.**

**ÍNDICE**

<b>1 ARQUITECTURA DE SEGURIDADE EN REDES.....</b>	<b>2</b>
<b>2 SEGURIDADE EN REDES WAN E INTERNET: CRIPTOGRAFÍA E AUTENTICACIÓN.....</b>	<b>10</b>
<b>3 SISTEMAS DE AUTENTICACIÓN PARA SEGURIDADE EN REDES.....</b>	<b>15</b>
<b>4 ELEMENTOS DE SEGURIDADE PARA INTERNET.....</b>	<b>24</b>
<b>REFERENCIAS.....</b>	<b>29</b>

## 1 ARQUITECTURA DE SEGURIDADE EN REDES

A irrupción dos sistemas informáticos nas organizacións provocou un cambio importante no modo de garantir a **seguridade da información**. Antes do uso estendido dos sistemas informáticos, a documentación sensible atopábase en soporte papel, polo que a seguridade da información para a organización era provista nun sentido físico e administrativo. Un claro exemplo disto eran os armarios con pechadura de combinación utilizados para almacenar os documentos con información sensible e os procesos de selección utilizados para incorporar novo persoal.

A implantación dos sistemas informáticos trouxo consigo a necesidade de ferramentas automatizadas para a protección de arquivos e outra información almacenada nos sistemas. Na actualidade, a información está almacenada en sistemas compartidos e distribuídos que ofrecen a posibilidade de acceder a ela a través dunha rede privada de ordenadores ou a través de internet. As **medidas de seguridade na rede** son o conxunto de medidas adoptadas para protexer os datos durante a transmisión a través de redes non seguras. Con todo, debido a que a práctica totalidade das empresas, gobernos e organizacións académicas teñen interconectados os seus sistemas informáticos cunha colección de redes que, pola súa vez, están interconectadas entre elas, dando lugar ao que coñecemos como internet, é máis frecuente o uso do termo **seguridade en internet**. A seguridade en internet abarca a prevención, detección e corrección de violacións da seguridade que poidan afectar á transmisión de información.

O *Computer Security Handbook* do NIST [NIST95] define o termo **computer security** como a protección conferida a un sistema informático co fin de alcanzar os obxectivos de preservar a integridade, dispoñibilidade e confidencialidade dos recursos de información do sistema (incluíndo

hardware, software, firmware, información/datos e telecomunicacións). Esta definición abrangue os obxectivos centrais da seguridade dos sistemas de información: confidencialidade, integridade, dispoñibilidade, autenticación e trazabilidade.

### 1.1 Arquitectura de seguridade no modelo OSI

Se a seguridade en contornos de procesamento de datos pechados é complexa, o uso de redes de área local e extensa aumenta esa complexidade de forma considerable. Por iso, o administrador responsable da seguridade dunha organización necesita algunha metodoloxía que lle permita definir os requisitos de seguridade e identificar os mecanismos que contribúan a cumprilos. Esta metodoloxía deberá facilitar a cobertura efectiva das necesidades de seguridade da organización así como a avaliación e posterior elección dos distintos produtos e políticas.

UIT-T<sup>1</sup> Recomendación X.800, *Security Architecture for OSI*, describe os servizos de seguridade básicos que poden ser aplicados cando é necesario protexer a comunicación entre sistemas. Aínda que se trata dun modelo xenérico definido nos anos noventa, os seus conceptos e definicións aínda seguen vixentes no día a día dos administradores da seguridade. A arquitectura de seguridade do modelo OSI é útil para os administradores, xa que establece un protocolo para organizar a tarefa de proporcionar seguridade. Ademais, como esta arquitectura foi desenvolvida como un estándar internacional, os fabricantes de computadoras e sistemas de comunicación engadíronlles características de seguridade aos seus produtos e servizos que se relacionan con esta definición estruturada de mecanismos e servizos. O modelo OSI de arquitectura da seguridade céntrase nos seguintes conceptos: **mecanismos de seguridade, servizos de seguridade e ataques contra a seguridade**. Pódense definir de maneira resumida:

---

<sup>1</sup> UIT-T son as siglas da Unión Internacional das Telecomunicacións, Sector de Estandarización das Telecomunicacións, que é unha axencia patrocinada polas Nacións Unidas que desenvolve estándares, chamadas “Recomendacións”, relacionadas coas telecomunicacións.

- **Mecanismos de seguridade:** son os procesos que permiten detectar, previr, ou recuperarse fronte a un ataque contra a seguridade.
- **Servizos de seguridade:** un servizo de comunicación ou procesamento que incrementa a seguridade dos sistemas de información e as transferencias de datos realizadas por unha organización. Os servizos tentan previr os ataques contra a seguridade facendo uso dun ou varios mecanismos de seguridade.
- **Ataques contra a seguridade:** calquera acción que atenta contra a seguridade da información da organización.

## 1.2 Mecanismos de seguridade

Os mecanismos de seguridade en X.800 divídense nos que se aplican a unha capa de protocolo específico e nos que non son específicos dunha capa de protocolo ou servizo de seguridade (coñecidos tamén como mecanismos de seguridade persistentes).

**Mecanismos específicos de seguridade:** poden ser incorporados nunha das capas do protocolo co fin de proporcionar algún dos servizos de seguridade OSI:

- **Autenticación:** corrobora que unha entidade, ben sexa orixe ou destino da información, é a desexada; por exemplo, A envía un número aleatorio cifrado coa clave pública de B, B descífralo coa súa clave privada e reenvíallo a A, demostrando así que é quen pretende ser. Por suposto, hai que ser coidadoso á hora de deseñar estes protocolos, xa que existen ataques para desbaratalos.
- **Control de accesos:** esforzo para que só aqueles usuarios autorizados accedan aos recursos do sistema ou á rede, por exemplo, mediante os contrasinais de acceso.

- **Sinatura dixital:** consiste en achegar unha serie de datos nunha mensaxe ou realizar unha transformación criptográfica que permita que o receptor comprobe a orixe dunha mensaxe e verifique a súa integridade.
- **Cifrado:** consiste na transformación da información por medio de algoritmos matemáticos a un formato que non é intelixible. A transformación e recuperación da información depende dun algoritmo de cifrado e/ou do uso de claves de cifrado.
- **Notarización:** o uso dun terceiro de confianza para garantir certas propiedades nun intercambio de datos.
- **Integridade:** conxunto de mecanismos para garantir que unha unidade de datos ou un fluxo de datos son correctos e completos.
- **Tráfico de recheo:** consiste en enviar tráfico espurio xunto cos datos válidos para que o atacante non saiba se se está a enviar información, nin qué cantidade de datos útiles se está a transmitir.
- **Control de encamiñamento:** permite a selección, para certos datos, de rutas físicas seguras e a variación destas, especialmente cando se sospeita dunha violación da seguridade.

Dentro dos **mecanismos de seguridade persistentes** temos:

- **Rexistro de auditoría de seguridade:** datos recollidos e potencialmente utilizables para realizar unha auditoría de seguridade.
- **Etiquetas de seguridade:** os atributos ou propiedades de seguridade asociadas a un recurso ou unidade de datos.
- **Funcionalidade de confianza:** o que se debe percibir como correcto con respecto a algún criterio (por exemplo, segundo o establecido por unha política de seguridade).

- **Detección de eventos:** detección de eventos relevantes de seguridade.
- **Recuperación da seguridade:** ocúpase das peticións dos mecanismos, tales como o manexo de eventos e a xestión de funcións, e leva a cabo tarefas de recuperación.

### 1.3 Servizos de seguridade

X.800 define un servizo de seguridade como un servizo provisto por unha capa do protocolo de comunicación e que garante a adecuada seguridade dos sistemas ou transferencias de datos. Se cadra atopamos unha definición máis clara na RFC 4949, que presenta a seguinte definición: un servizo de información ou comunicación que é proporcionado por un sistema para unha clase específica de protección de recursos informáticos. X.800 divide estes servizos en cinco categorías:

- **Confidencialidade:** require que a información sexa accesible unicamente polas entidades autorizadas. A confidencialidade de datos aplícase a todos os datos intercambiados polas entidades autorizadas ou se cadra só a porcións ou segmentos seleccionados dos datos, por exemplo, mediante cifrado. A confidencialidade de fluxo de tráfico protexe a identidade da orixe e destino(s) da mensaxe —por exemplo, enviando os datos confidenciais a moitos destinos ademais do verdadeiro—, así como o volume e o momento de tráfico intercambiado —por exemplo, producindo unha cantidade de tráfico constante ao engadir tráfico espurio ao significativo—, de forma que sexan indistinguibles para un intruso. A desvantaxe destes métodos é que incrementan drasticamente o volume de tráfico intercambiado, repercutindo negativamente na dispoñibilidade do ancho de banda baixo demanda.



- **Servizo de autenticación:** require unha identificación correcta da orixe da mensaxe, asegurando que a entidade non é falsa. Distínguense dous tipos: de entidade, que asegura a identidade das entidades participantes na comunicación mediante biométrica (pegadas dactilares, identificación de iris, etc.), tarxetas de banda magnética, contrasinais, ou procedementos semellantes; e de orixe de información, que garante que unha unidade de información procede de certa entidade, sendo a sinatura dixital o mecanismo máis estendido.
- **Control de accesos:** no contexto de seguridade informática, o control de acceso é a capacidade de controlar e limitar o acceso a través da rede aos sistemas e aplicacións. Para logralo, cada entidade que tenta conseguir acceso debe ser autenticada, polo que os dereitos de acceso se poden adaptar a cada usuario.
- **Integridade:** igual que a confidencialidade, a integridade pódese aplicar a un fluxo de mensaxes, a unha única mensaxe, ou a un conxunto de campos seleccionados dunha mensaxe. De novo, o enfoque máis sinxelo e útil é a protección total do fluxo de comunicación. Un servizo de integridade **orientado a conexión** traballa con fluxos de mensaxes e garante que as mensaxes son recibidas tal e como son enviadas, sen ser duplicadas, modificadas, reordenadas ou repetidas.
- **Non repudio:** o non repudio evita que o emisor ou receptor dunha mensaxe poida negar a transmisión. Así, cando se envía a mensaxe, o receptor pode probar que o suposto emisor fixo o envío. Do mesmo xeito, cando unha mensaxe é recibida, o emisor pode probar o feito de que a mensaxe efectivamente foi recibida.

Tanto X.800 como RFC 4949 definen a **dispoñibilidade** como a propiedade dun sistema ou recurso de ser usado e estar dispoñible baixo un sistema de autorización de entidade, de acordo coas especificacións de

rendemento para o sistema. É dicir, o sistema está dispoñible se proporciona os seus servizos de acordo co deseño do sistema cada vez que os usuarios o solicitan. Unha gran variedade de ataques poden producir a perda ou redución da dispoñibilidade. Algúns deses ataques poden ser evitados con medidas automáticas, tales como a autenticación e o cifrado, mentres que outros precisan dalgún tipo de acción física para previr ou recuperarse dunha perda de dispoñibilidade nos elementos dun sistema distribuído.

A *Táboa 1* indica a relación entre os servizos de seguridade e os mecanismos de seguridade.

#### **1.4 Ataques contra a seguridade**

Unha forma útil de clasificar os ataques contra a seguridade, utilizada tanto en X.800 como na RFC 4949, é por medio dos termos *ataque activo* e *ataque pasivo*.

Un ataque pasivo intenta coñecer ou facer uso da información do sistema pero sen afectar aos seus recursos. Os ataques pasivos son moi difíciles de detectar, xa que non provocan ningunha alteración dos datos. No entanto, é posible evitar que teñan éxito mediante o cifrado da información e outros mecanismos que se han ver máis adiante.

Un ataque activo intenta cambiar os recursos do sistema ou alterar o seu modo de funcionamento. Os esforzos contra os ataques pasivos céntranse na prevención máis que na detección, namentres que fronte aos ataques activos o máis importante é recuperarse canto antes de calquera interrupción ou atraso causado.

<b>Servizo / Mecanismo</b>	<b>Cifrado</b>	<b>Sinatura a Dixital</b>	<b>Control Accesos</b>	<b>Integridade</b>	<b>Autenticación</b>	<b>Tráfico o recheo</b>	<b>Control encamiñamento</b>	<b>Notarización</b>
Autenticación entidade	<b>X</b>	<b>X</b>			<b>X</b>			
Autenticación orixe datos	<b>X</b>	<b>X</b>						
Control de accesos			<b>X</b>					
Confidencialidade	<b>X</b>						<b>X</b>	
Confidencialidade fluxo tráfico	<b>X</b>					<b>X</b>	<b>X</b>	
Integridade	<b>X</b>	<b>X</b>		<b>X</b>				
Non repudio		<b>X</b>		<b>X</b>				<b>X</b>
Disponibilidade				<b>X</b>	<b>X</b>			

**Táboa 1. Relación entre servizos de seguridade e mecanismos de seguridade.**

## 2 SEGURIDADE EN REDES WAN E INTERNET: CRIPTOGRAFÍA E AUTENTICACIÓN

A **autenticación** é o mecanismo que permite confirmar a identidade dunha entidade (ben sexa usuario ou hardware, software, etc.). Con este mecanismo pódese controlar o acceso aos sistemas de información e, ao mesmo tempo, previr a usurpación de identidades e evitar que a información da organización se vexa comprometida.

Os mecanismos de autenticación para os seres humanos clasifícanse, polo xeral, en catro casos:

- **Algo que o usuario é:** adóitanse utilizar identificadores biométricos como a pegada dixital, o patrón da retina, a secuencia de ADN, o patrón da voz, o recoñecemento da sinatura, os sinais bio-eléctricos únicos producidos polo corpo vivo, etc.
- **Algo que o usuario ten:** unha tarxeta de identificación, o teléfono móbil, unha chave, etc.
- **Algo que o usuario sabe:** un contrasinal, unha frase ou un número de identificación persoal.
- **Algo que o usuario fai:** recoñecemento de voz, sinatura, etc.

É posible combinar distintos mecanismos, como o caso dos *tokens* criptográficos, que ademais de telos no noso poder (algo que o usuario ten) é necesario coñecer a clave (algo que o usuario sabe). Mesmo hai *tokens* criptográficos que incorporan ademais un lector de pegada dixital.

A **autenticación criptográfica** é un mecanismo mediante o cal unha entidade que se quere autenticar realiza unha serie de operacións

criptográficas sobre unha mensaxe co fin de que a súa identidade poida ser verificada. Este tipo de autenticación é moi adecuada para sistemas distribuídos en que a autenticación se realiza a distancia.

## 2.1 Mecanismos criptográficos de autenticación

Cando se realiza a transmisión dunha mensaxe entre un emisor e un receptor, os aspectos máis importantes que cómpre verificar para garantir unha comunicación segura son a non alteración da mensaxe e a autenticidade do emisor. Tamén adoita ser relevante a oportunidade dos datos (non foron adiados nin substituídos artificialmente) e verificar a secuencia relativa a outras mensaxes que flúen entre os dous extremos dunha comunicación.

A **autenticación de mensaxes** proporciona seguridade contra ataques activos tales como a falsificación de datos e as transaccións. Existen os seguintes mecanismos de autenticación de mensaxes: **checksum criptográfico, cifrado de mensaxes e funcións resumo** ou *hash*.

### 2.1.1 Checksum criptográfico

Con esta técnica as mensaxes transmítense sen cifrar, polo que non se garante a súa confidencialidade. No seu lugar xérase unha *etiqueta de autenticación* que se incorpora á mensaxe para a súa transmisión.

Este mecanismo implica a utilización dunha clave secreta coa que se xera un pequeno bloque de datos de lonxitude fixa, coñecido como *código de autenticación de mensaxe (MAC)*, que se incorpora á mensaxe.

Cando o *emisor* desexa enviar unha mensaxe, calcula o código *MAC* en función da mensaxe e da clave compartida. A mensaxe e o código lle son

transmitidos ao *receptor*, que realiza a mesma operación sobre a mensaxe recibida, utilizando a mesma clave, e verifica que o código obtido coincide co recibido. Se se asume que só *emisor* e *receptor* coñecen a clave, pódese dicir que:

- O receptor pode asegurar que a mensaxe que recibiu non foi alterada.
- A mensaxe foi enviada polo suposto emisor.
- Se a mensaxe contén un número de secuencia, entón o receptor pode estar seguro de que a secuencia é a correcta.

### 2.1.2 Técnicas de cifrado

Hai dúas técnicas básicas para cifrar información: o **cifrado simétrico** (tamén denominado cifrado de clave secreta) e o **cifrado asimétrico** (tamén denominado cifrado de clave pública).

O cifrado simétrico é a técnica máis antiga e coñecida. O emisor e o receptor coñecen a clave secreta de cifrado que se lle aplica á mensaxe dun modo determinado. Esta técnica garante que só o emisor e o receptor da mensaxe deberían ser capaces de cifralo e descifralo. O maior inconveniente do cifrado asimétrico é a distribución e custodia de claves.

O cifrado asimétrico baséase nun par de claves relacionadas entre elas de maneira que o que se cifra cunha se descifra coa outra e viceversa. Unha das claves faise pública e a outra só a coñece o seu propietario. Deste xeito, se se quere garantir que só o destinatario dunha mensaxe a poida descifrar, abonda con cifrala coa súa clave pública. Se, ademais, o emisor da mensaxe a cifra utilizando a súa propia clave privada, o receptor poderá comprobar que o emisor é quen di ser descifrando a mensaxe coa clave

pública daquel. O cifrado asimétrico resolve os problemas do cifrado simétrico, pero a cambio require máis capacidade de procesamento.

Para garantir que a mensaxe non foi alterada nin foi adiada deliberadamente durante o seu tránsito pola rede, normalmente combínanse as técnicas de cifrado co uso de códigos de detección de erros e marcas de tempo.

### 2.1.3 Funcións resumo

O uso de **funcións *hash* tampouco implica un cifrado da mensaxe enviada** e admite mensaxes de lonxitude variable.

A función *hash* acepta unha mensaxe de lonxitude variable  $M$  como entrada e produce como saída unha cadea de tamaño fixo  $H(M)$ , normalmente coñecida como resumo da mensaxe. O resumo envíase xunto á mensaxe de xeito que pode ser utilizado por parte do receptor para realizar a autenticación. Ademais da autenticación, o resumo proporciona un mecanismo de comprobación da integridade dos datos. Se no tránsito da mensaxe pola rede se altera algún bit, o resumo calculado por parte do destinatario será diferente do que vén desde a orixe, polo que a mensaxe será errónea.

Á hora de enviar a mensaxe e o resumo dunha forma autenticada, as funcións *hash* pódense utilizar de tres maneiras diferentes:

- **Utilización de criptografía simétrica para cifrar o resumo:** cífrase o resumo en orixe coa axuda dun algoritmo baseado en criptografía simétrica. Se só o emisor e o receptor coñecen a clave, pódese garantir que o resumo é auténtico.

- **Utilización de criptografía de clave pública para cifrar o resumo:** proporciona unha **sinatura dixital** da mensaxe e **autenticación**; ademais, non se require a distribución de claves aos participantes na comunicación.
- **Autenticación de mensaxes sen utilizar cifrado:** as dúas partes comunicantes comparten un segredo común. O emisor, antes de enviar a mensaxe, calcula o resumo da mensaxe concatenada co segredo. A seguir, procede a enviar a mensaxe e o resumo. A operación repítese en destino: concaténase o segredo coa mensaxe e calcúlase o resumo. Se coincide co resumo que chegou desde a orixe, conclúese que a mensaxe é auténtica. Xa que o segredo non se envía, non é posible que un atacante modifique a mensaxe interceptada. A seguridade deste sistema reside en que non se revele o segredo compartido.

As **funcións hash** son importantes, ademais de para a autenticación de mensaxes, para a realización de **sinaturas dixitais**. O propósito dunha función *hash* é producir unha “pegada” da mensaxe. Para que unha **función hash (H) se considere segura**, debe verificar as seguintes propiedades:

1. **H** debe poder ser aplicada a mensaxes de calquera tamaño.
2. **H** produce unha saída de lonxitude fixa.
3. **H(x)** é relativamente fácil de calcular para un **x** dado, facendo práctica a implementación en hardware e software.
4. Para un código dado **m**, é imposible computacionalmente atopar un **x** tal que **H(x)=m**.
5. Para un bloque dado **x**, é imposible computacionalmente atopar un **y**  $\neq$  **x** con **H(y)= H(x)**.



6. É imposible computacionalmente atopar unha parella **(x, y)** tal que **H(x)=H(y)**.

As tres primeiras propiedades son requisitos para a aplicación práctica dunha función resumo á autenticación de mensaxes. A cuarta propiedade garante a unidireccionalidade do resumo: é fácil xerar o resumo, pero imposible obter a mensaxe a partir do resumo. A quinta e sexta propiedade ten que ver coa protección contra as “colisións”, garantindo que non é computacionalmente posible atopar dúas mensaxes diferentes co mesmo resumo. Os exemplos máis coñecidos de funcións resumo son **MD5** e a familia **SHA**.

### 3 SISTEMAS DE AUTENTICACIÓN PARA SEGURIDADE EN REDES

Todos os sistemas de autenticación en redes utilizan criptografía para garantir a seguridade, o que fai necesaria a realización dunha serie de tarefas:

- **Xeración de claves:** existen diversos algoritmos de xeración de claves, inda que o máis común é utilizar unha fonte de números pseudo-aleatorios.
- **Rexistro:** as claves xeradas deben quedar ligadas de forma unívoca a unha identidade.
- **Distribución:** antes de iniciar a comunicación, é necesario que as partes implicadas coñezan tanto as claves como os algoritmos de cifrado que se van utilizar. O mecanismo de distribución de claves varía en función da técnica de cifrado utilizada.

- **Protección:** é imprescindible garantir a custodia das claves, xa que o revelalas comprometería o sistema de autenticación.
- **Mecanismos de revogación:** cando existen evidencias de que unha clave foi revelada, deben existir mecanismos para retirala.

### 3.1 Distribución de claves utilizando criptografía simétrica

A criptografía simétrica baséase nunha clave secreta compartida polo emisor e o receptor que debe ser custodiada por ambos e protexida contra o acceso por parte de terceiros non autorizados. Ademais, como prevención ante a posible vulneración do segredo, é recomendable cambiar a clave cada certo tempo. Deste xeito, a distribución das claves resulta crítica para o sistema de cifrado simétrico. Polo tanto, un dos elementos que garanten a fortaleza dun sistema de cifrado simétrico é a técnica de distribución de claves.

Para a distribución de claves entre dúas entidades, que denominaremos A e B, pódense utilizar distintas estratexias:

1. **A** pode xerar a clave e enviarlla fisicamente a **B**.
2. Un terceiro de confianza **C** xera a clave e envíallela fisicamente a **A** e **B**.
3. Nos casos en que **A** e **B** dispoñan xa dunha clave secreta común, calquera deles pode xerar unha nova clave e enviarlla á outra parte cifrando o envío coa clave establecida de antemán.
4. Se existe un terceiro de confianza **C** co que tanto **A** como **B** dispoñen dunha canle de comunicación cifrada, **C** podería xerar a nova clave e enviárllela a **A** e **B** de forma.

As opcións 1 e 2 coñécense como entrega manual da clave. Estas técnicas teñen un custo asumible en cifrados de enlace, onde toda a comunicación se cifra entre os dous mesmos elementos de comunicación. Por exemplo, poderíase intercambiar manualmente unha clave secreta dun tamaño considerable para crear unha VPN sitio a sitio entre dúas delegacións dunha organización. Así e todo, complícase para cifrados extremo a extremo en redes, onde cada orixe pode establecer comunicacións con destinos variados. Por exemplo, cando un cliente remoto ten que acceder a múltiples servizos en diversas organizacións, resúltalle inviable pedir un envío físico dunha clave por cada acceso.

A opción 3 é viable tanto para cifrados de enlace como para cifrados extremo a extremo. Ten o inconveniente de que se un atacante ten éxito e obtén a clave, todas as claves subseguintes estarán comprometidas.

A opción 4 é a máis axeitada para proporcionar claves en cifrados extremo a extremo. Nesta opción utilízanse dous tipos de claves:

- **Claves de sesión:** cando dous sistemas (*hosts*, terminais, etc.) se queren comunicar, establecen unha conexión lóxica (por exemplo, un circuíto virtual). Mentres perdure esa conexión lóxica, chamada sesión, todos os datos de usuario se cifran cunha clave de sesión dun único uso. Ao final da sesión destrúese esa clave.
- **Claves mestras:** unha clave mestra é unha clave utilizada entre entidades co propósito de distribuír claves de sesión.

Un elemento necesario para a opción 4 é o **centro de distribución de claves (KDC)**. O KDC determina que sistemas teñen permitido comunicarse entre eles. Cando se lles concede permiso a dous sistemas para comunicarse entre eles, o KDC proporciona unha clave de sesión dun só uso.

### 3.2 Distribución de claves utilizando criptografía asimétrica

Malia que na criptografía asimétrica a clave pública é coñecida por toda a comunidade, a distribución de claves presenta tamén unha problemática que cómpre abordar.

Partindo da utilización dun algoritmo amplamente aceptado como RSA, calquera participante pode xerar o seu par de claves e enviarlle a súa clave pública á comunidade. O problema desta aproximación é que resulta imposible comprobar que alguén que envía a súa clave pública asegurando ser **A** realmente o sexa. Deste xeito, se un impostor **B** fai pública unha clave dicindo que é **A**, podería ler todas as mensaxes que fosen dirixidas ao auténtico **A** en tanto non se descubrixe a fraude. A solución a este problema vén da man dos **certificados dixitais**. Un certificado dixital é un conxunto de información acerca dunha entidade, coa súa clave pública, e todo **asinado por unha terceira entidade de confianza**.

### 3.3 Protocolos e métodos de autenticación en rede

A verificación da identidade dun suxeito de forma remota presenta unha dificultade engadida, especialmente cando os datos intercambiados se transmiten a través dunha rede non segura, xa que calquera impostor se podería facer pasar por alguén que non é, conseguindo así acceder a recursos aos que, doutro xeito, non lle estaría permitido. As técnicas criptográficas constitúen unha ferramenta de grande utilidade para superar esta dificultade.

O modo de operación que utilizan os protocolos de autenticación en rede resúmese da seguinte maneira: dúas entidades *A* e *B* (coñecidas como principais) queren establecer unha conexión segura e ter acceso a datos e servizos. Para iso, un dos principais comeza a intercambiar información co outro principal ou cun Centro de Distribución de Claves fiable (KDC). Logo dunha serie de retos, conséguese unha clave de sesión única para preservar a confidencialidade dos datos intercambiados. Unha premisa fundamental é establecer unha clave de sesión nova para cada conexión e reducir así a cantidade de información comprometida no caso de que un atacante teña éxito. Hai unha ampla variedade de protocolos de autenticación en rede:

- **TACACS, RADIUS:** métodos baseados en servidores con rexistro de todos os usuarios.
- **Kerberos:** método baseado en centro de distribución de claves.
- **X.500, LDAP:** métodos baseados en servizos de directorio.
- **Certificados:** métodos baseados en certificados dixitais.
- **NIS, NIS+:** métodos baseados en *Network Information Service*.
- **EAP-TLS, EAP-TTLS, EAP-MD5, etc.:** métodos baseados no *framework* de autenticación EAP.

### 3.4 Protocolos de seguridade en internet

#### 3.4.1 Kerberos

Kerberos é un servizo de distribución de claves e autenticación de usuarios desenvolvido polo MIT (*Massachusetts Institute of Technology*). O problema que aborda Kerberos é o seguinte: nun contorno distribuído onde os

usuarios tentan acceder desde as súas estacións de traballo a servizos e servidores na rede, débese dispoñer de medios para restrinxir o acceso aos usuarios autorizados, ademais de ter a capacidade de autenticalos. Nesta situación, non se pode confiar en que as estacións de traballo autenticquen correctamente os seus usuarios para accederen aos servizos da rede. En particular, existen tres ameazas que se deben xestionar:

- Un usuario pode conseguir acceso a unha estación de traballo particular e facerse pasar por outro para realizar operacións desde esa estación.
- Un usuario pode cambiar o enderezo de rede dunha estación de traballo, polo que as peticións enviadas semellan vir dunha estación descoñecida.
- Un usuario pode realizar escoitas na rede e utilizar un ataque de repetición para conseguir acceso a un servidor ou interromper operacións.

En todos os casos, un usuario non autorizado pode conseguir acceso a servizos e datos para os que non está autorizado. No canto de construír elaborados protocolos en cada servidor, Kerberos proporciona un servidor centralizado de autenticación baseado en criptografía de clave simétrica. Para un usuario, a clave é un *hash* do seu contrasinal, gardada normalmente no KDC (**Key Distribution Center**). Para un servizo, a clave é unha secuencia xerada aleatoriamente que actúa como un contrasinal e se almacena tamén no KDC.

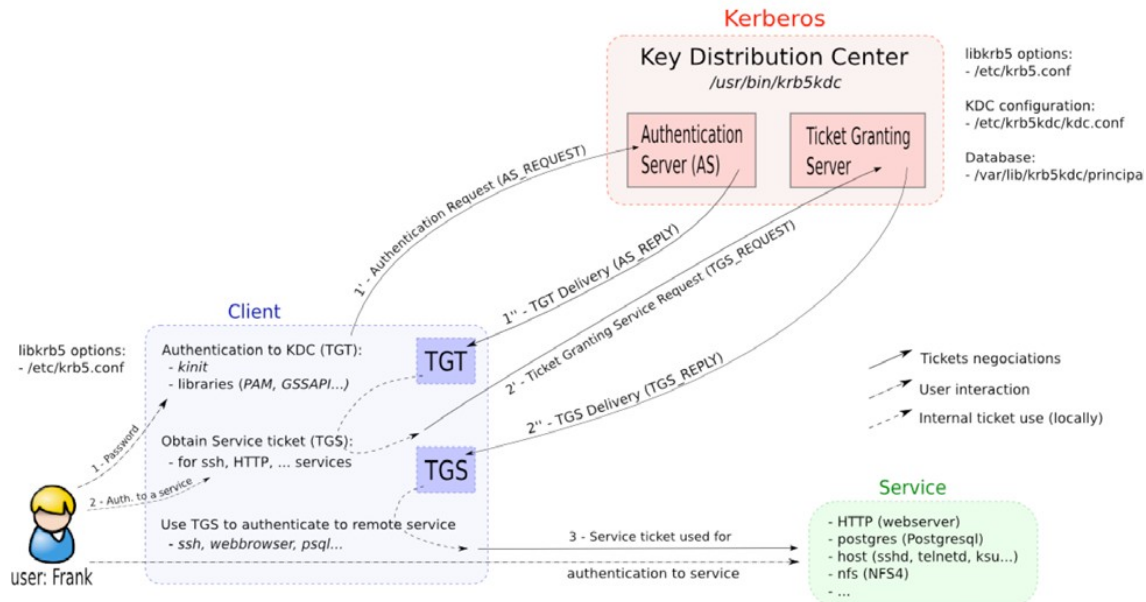
Para que o esquema de autenticación funcione, clientes e servidores teñen que confiar nunha terceira parte (o servidor Kerberos), que solicita as claves necesarias baixo demanda. A comunicación en Kerberos está

baseada no uso de **Tickets**. Os *Tickets* son un tipo de datos cifrados que se almacenan do lado do cliente.

O KDC é a parte principal dunha rede Kerberos. Consta dos seguintes elementos:

- Un servidor de autenticación, que responde as peticións de autenticación lanzadas polos clientes. Aquí é onde o cliente consegue un TGT (***Ticket Granting Ticket***), que serve para acceder aos servizos despois da autenticación.
- Un servidor de concesión de accesos (***Ticket Granting Server***), que se encarga xestionar o acceso dos clientes aos servizos. Nesta etapa, o cliente recibe un TGS (***Ticket Granting Service***) que lle permite autenticarse ante un servizo que está dispoñible na rede.
- Unha base de datos que garda todas as claves secretas (de clientes e servizos), así como información relacionada coas contas Kerberos: data de creación, políticas, etc.

## KerberosV5 Tickets Negotiation mechanism



**Figura 1: Mecanismo de negociación de Tickets KerberosV5 (fonte: MIT Kerberos consortium)**

### 3.4.2 PGP

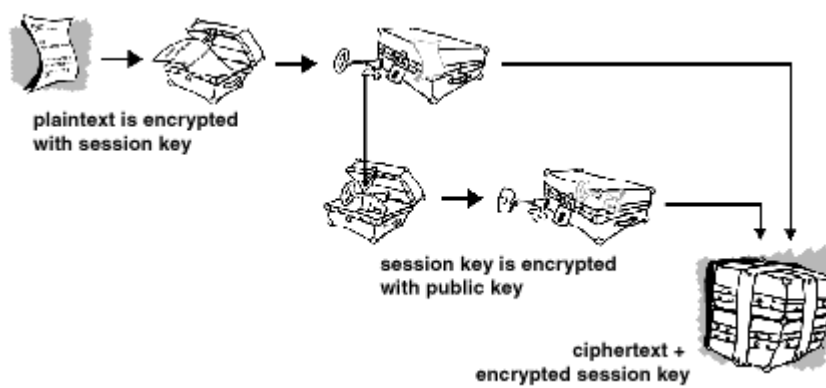
O correo electrónico é un servizo que require servizos para permitir a autenticación dos usuarios e garantir a confidencialidade das mensaxes que intercambian. PGP (*Pretty Good Privacy*) é un protocolo que proporciona confidencialidade das mensaxes que son enviadas e almacenadas. Ademais proporciona un mecanismo de autenticación que se basea na sinatura dos correos enviados.

PGP é un sistema híbrido que combina características do cifrado simétrico e do cifrado asimétrico. Cando un usuario A lle quere enviar unha mensaxe cifrada a B utilizando PGP, lévanse a cabo os seguintes pasos:

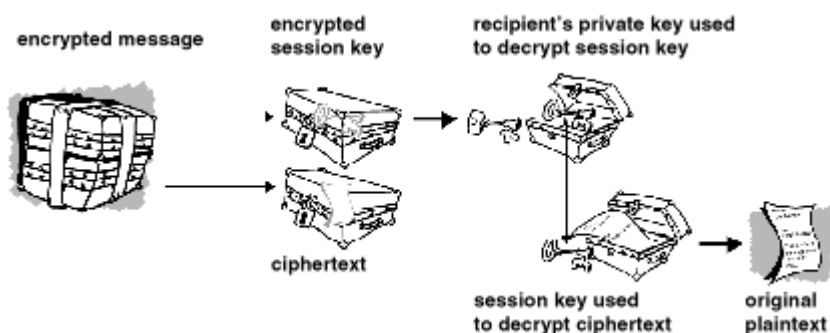
- Créase unha clave de sesión aleatoria que é utilizada para cifrar a mensaxe.



- A clave de sesión cófrase coa clave pública de B e engádeselle á mensaxe. Envíaselle a mensaxe a B.
- B descifra a mensaxe coa súa clave privada. Deste modo o que obtén é a clave de sesión en claro e a mensaxe cifrada. Para obter a mensaxe en claro, debe usar a clave de sesión e aplicar o algoritmo de descifrado baseado en criptografía simétrica.



**Figura 2: Cifrado con PGP (Fonte: International PGP Home Page)**



**Figura 3: Descifrado con PGP (Fonte: International PGP Home Page)**

Para proporcionar autenticación, PGP fai uso de sinaturas dixitais. Para iso os integrantes dunha conversa deben intercambiar as súas claves públicas. A certificación neste sistema baséase na idea de que a confianza é un

concepto social: cada persoa confía nos seus amigos. Así, pódense establecer cadeas de confianza se a clave dun terceiro descoñecido vén asinada coa clave pública dun amigo en quen se confía. Esta maneira de proceder ten o inconveniente de que non sempre se pode verificar a identidade dun terceiro, a non ser que se teña un amigo en común.

## 4 ELEMENTOS DE SEGURIDADE PARA INTERNET

Cómpre ter moi presente que ao conectar un equipo informático a internet se está a asumir un risco, xa que ese equipo pasa a estar conectado a millóns de equipos distribuídos por todo o mundo. Neste escenario débense utilizar elementos de seguridade física e lóxica que impidan accesos non autorizados e que, no caso de se produciren, faciliten a súa detección.

### 4.1 Devasas

O maior nivel de seguridade que se podería adoptar nun sistema informático consistiría en desenchufalo da rede. Con todo, esta non adoita ser unha opción aceptable xa que, a día de hoxe, a maior parte das empresas necesitan intercambiar información, ben sexa a través dunha rede local ou ben a través de internet.

Aínda que se poden ter todos os servidores e estacións de traballo protexidos con fortes medidas de seguridade, normalmente non abonda coa seguridade baseada en *host*. Unha medida complementaria —que é moi aceptada— consiste en complementar a seguridade do *host* cun **servizo de devasa**<sup>2</sup>. Unha devasa é un elemento que se sitúa entre a rede

---

<sup>2</sup> É moi común o uso do termo en inglés *firewall*.

interna e os intrusos potenciais externos constituíndo unha barreira de protección. Normalmente establécese entre a rede local e internet, facendo así de muro de protección exterior da rede local. A devasa pode ser un software nun equipo ou pode ser un conxunto de varios sistemas específicos destinados a controlar o acceso á rede interna da organización.

#### 4.1.1 Características dunha devasa

Un servizo de devasa presenta unha serie de características entre as que se poden salientar as seguintes:

- Define un punto único de control que permite afastar os usuarios non autorizados da rede protexida e proporciona protección contra ataques de *spoofing* e encamiñamento. Isto simplifica a xestión, porque as características de seguridade están centralizadas nun único sistema ou conxunto de sistemas.
- Proporciona unha localización para monitorar eventos relacionados coa seguridade. Nun sistema *devasa* pódense implementar auditorías de seguridade e alarmas.
- Proporciona unha plataforma para outras funcións de internet que non están relacionadas coa seguridade: tradución de enderezos, funcións de xestión para auditoría e rexistros de log para medir o uso de internet.
- Pode ser utilizado para implementar redes privadas virtuais (VPN).

#### 4.1.2 Tipos de devasas

Atendendo á función desempeñada polo sistema devasa podemos establecer a seguinte clasificación:

- **Devasa de filtrado de paquetes:** aplica un conxunto de regras para cada paquete IP de entrada e saída e, a seguir, reenvía ou descarta o paquete. As regras de filtrado están baseadas na

información contida en cada paquete: IP orixe, IP destino, protocolo, interface, etc.

- **Devasa de inspección de estados:** Ademais de facer o filtrado en función de paquetes, garda información das sesións e conexións abertas. Isto permite dispoñer de políticas de seguridade máis avanzadas e evita moitos ataques.
- **Proxy de aplicacións:** Actúa como intermediario no tráfico da capa de aplicación, permitindo acceder a certas características das aplicacións e reenviando a información.

#### 4.1.3 Localizacións da devasa e configuracións

Atendendo á localización da devasa, pódense obter distintas configuracións:

- **Redes DMZ:** empréganse para illar nunha ou en varias subredes (coñecidas como “zonas desmilitarizadas”) os principais servizos da organización aos que cómpre acceder desde o exterior (web, correo, DNS). A este segmento aplícanse unhas regras de filtrado para garantir unha conectividade controlada desde o exterior. Ao resto da rede interna péchase o acceso desde o exterior.
- **Redes privadas virtuais (VPN):** é unha solución que lles ofrece grandes vantaxes aos xestores de rede. Consiste en dar acceso mediante unha conexión segura a un equipo ou segmento dunha rede privada a través dunha rede considerada insegura, como pode ser internet.
- **Devasas distribuídas:** consiste en agrupar baixo un mesmo mecanismo de control centralizado a xestión de dispositivos *devasa* e a xestión de devasas baseadas en *host*. Con estas ferramentas, o administrador pode establecer políticas de seguridade e aplicarllelas

a equipos *devasa*, servidores e estacións de traballo tanto locais como remotas. Ademais proporcionan capacidades de monitorización e alertas de seguridade.

## 4.2 Sistemas de detección de intrusionés

Unha *devasa* é un mecanismo de seguridade que permite pechar todos aqueles portos de servizos que non se estean utilizando e reducir así a posibilidade de ataques por parte de intrusos. Pero inda que só se permita o acceso aos servizos básicos e teoricamente seguros, estes ás veces teñen vulnerabilidades que poden ser aproveitadas por un atacante con fins maliciosos para saltarse esta medida de protección. Facendo un símil coa protección dunha casa, a *devasa* corresponderíase coa porta de entrada, pero é necesario un sistema de alarma que se encargue de avisar no caso de que un intruso logre entrar. O elemento correspondente ao sistema de alarma no mundo da seguridade informática é o IDS (*Intrusion Detection System*). Pódese definir un IDS como un sistema que se encarga de vixiar a rede, absorbendo todo o tráfico e inspeccionándoo en busca de patróns de ataque. As características principais dos IDS son as seguintes:

- Engádelle un alto nivel de integridade ao resto da rede, xa que, en certa forma, sabemos que o resto de sistemas están ben porque o IDS non avisa do contrario.
- Pode monitorar a actividade dun atacante. Dependendo da infraestrutura de IDS, poderase monitorar esta actividade nun único segmento ou en varios.
- Alerta ante patróns de ataque comúns coñecidos.

- Automatiza a busca de novos patróns de ataque, xa que proporciona ferramentas estatísticas de busca e monitorización de tráfico anómalo.
- Pode detectar ataques en tempo real.
- Pode detectar erros de configuración nos equipos.

Os sistemas IDS constan dun equipo cunha consola central de administración e unha ou varias “sondas” que se encargan de capturar o tráfico que se debe analizar. Dependendo da arquitectura de rede da organización pódense seguir diversos criterios para situar as sondas: na DMZ, detrás da devasa, nos accesos de usuario, entre a extranet e internet, etc.

Unha variante dos sistemas de detección de intrusións son os IPS (*Intrusion Prevention System*). A diferenza con respecto aos IDS estriba en que os IPS, ademais de detectar un ataque e xerar a correspondente alerta, son capaces de actuar e intentar neutralizar o ataque. Un exemplo claro sería cando o IPS detecta actividade maliciosa por parte dun usuario conectado a un servidor a través dunha conexión remota. Unha das accións drásticas que podería tomar o IPS é cortar a conexión.

Os sistemas IPS/IDS pódense instalar como un software nun servidor (por exemplo, Snort) ou pode ser un equipo hardware co seu software completo e independente proporcionado por un fabricante de dispositivos de seguridade.

## 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/>)

(Todas as ligazóns foron verificadas en novembro do 2011)

**Autor:** Juan Otero Pombo  
Enxeñeiro en Informática no Concello de Ourense  
Colexiado do CPEIG



# **46. MODELO OSI. REDES LAN, MAN E WAN. ESTRUCTURA DE REDES: TRONCAL, DISTRIBUCIÓN ACCESO. REDES PÚBLICAS DE TRANSMISIÓN DE DATOS. PROTOCOLOS DE REDE.**



## **Tema 46. Modelo OSI. Redes LAN, MAN e WAN. Estrutura de redes: troncal, distribución acceso. Redes públicas de transmisión de datos. Protocolos de rede.**

### **INDICE**

#### **46.1 Modelo OSI**

##### 46.1.1 Introducción

##### 46.1.2 Conceptos xerais

##### 46.1.3 Transmisión entre entidades do mesmo nivel (pares)

##### 46.1.4 Conexións

###### 46.1.4.1 Establecemento de conexións

###### 46.1.4.2 Liberación de conexións

###### 46.1.4.3 Multiplexación e división

###### 46.1.4.4 Transmisión de datos

##### 46.1.5 Capas do 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 rede (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 ó modelo OSI

#### **46.2 Redes LAN, MAN e WAN**

##### 46.2.1 PAN

##### 46.2.2 LAN

##### 46.2.3 MAN

##### 46.2.4 WAN

#### **46.3 Estrutura de redes: troncal, distribución e 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 xerais

## 46.5 Protocolos de rede

### 46.5.1 Redes de conmutación de circuítos

### 46.5.2 Redes de conmutación de paquetes

## 46.6 Bibliografía

## **46.1 MODELO OSI**

### **46.1.1 INTRODUCCIÓN**

Inicialmente, os computadores eran elementos illados que almacenaban nos seus propios ficheiros e precisaban a conexión dos seus propios periféricos. A independencia era tal que, se se necesitaba imprimir un documento aloxado nunha máquina que non dispoñía de impresora, era necesario copiar o ficheiro nun disquete e levalo ata un equipo cunha impresora, conectala e imprimilo neste. Para evitar isto, a solución era instalar una impresora no computador inicial, coa conseguinte duplicación de recursos e dispositivos.

Con instalacións informáticas así, a configuración e xestión de tódolos ordenadores e periféricos a eles conectados supoñía un custo e unha tarefa moi grande, chegando a ser pouco práctica cando o número de computadores foi crescendo nas distintas empresas.

Por esta razón, apareceu a necesidade de conectar os diferentes ordenadores entre si e implantar métodos de comunicación e transferencia de datos entre eles. Nace o concepto de “redes de ordenadores” e “traballo en rede”.

A mediados dos 70 diversos fabricantes desenvolven os seus propios sistemas de redes locais. Sen embargo, a comunicación entre ordenadores pertencentes a redes distintas de distintos fabricantes era imposible, debido a que os sistemas de comunicación de cada rede eran propietarios. É dicir, estaban desenvolvidos con hardware e software propios e usaban protocolos e arquitecturas diferentes ós doutros fabricantes.

As empresas déronse de conta da necesidade de abandonar os sistemas propietarios e definir unha arquitectura de rede cun modelo común que permitise conectar varias redes sen problemas.

En 1977, a Organización Internacional de Normas (ISO, International Standard Organization), integrada por industrias representativas do sector, creou un subcomité para o desenvolvemento de estándares de comunicación de datos que permitise a interoperabilidade entre produtos de diferentes fabricantes. Tras varias investigacións acerca dos modelos de rede, elaboraron o modelo de referencia OSI (Open Systems Interconnection), en 1984.

#### **46.1.2 CONCEPTOS XERAIS**

O modelo de referencia para a Interconexión de Sistemas Abertos caracterízase por:

- Ocupase da conexión de sistemas abertos, e dicir, sistemas que permiten a comunicación con outros sistemas.
- Consta de sete capas. Por capa entendese unha (ou varias) entidade(s) que realizan por sí mesma unha función específica. As entidades do mesmo nivel denomínanse entidades pares.
- Representa o primeiro paso á estandarización internacional dos protocolos que se usan nas diversas capas.
- Non é unha arquitectura de rede en sí, xa que non especifica os servizos e protocolos exactos que se teñen que usar en cada capa, se non que só define o que debe facer cada capa.

No modelo OSI existen tres conceptos fundamentais:

- **Servizo:** Capacidade de comportamento dunha capa. Cada capa presta algúns servizos ás entidades que se atopan sobre ela, que acceden ós mesmos a través dos puntos de acceso ó servizo (SAP), intercambiando primitivas de servizo.
- **Interface:** Indica aos procesos da capa superior cómo acceder a ela, especificando cales son os parámetros e qué resultados esperar. A

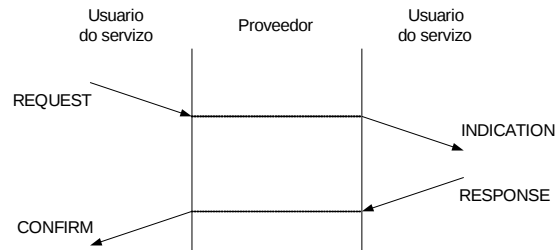
interface entre dúas capas en unha máquina non ten porque ser igual á correspondente noutra máquina.

- Protocolo: Conxunto de regras que determinan o comportamento de comunicación horizontal entre entidades pares. Pódense cambiar os protocolos dunha capa sen afectar ás demais.

#### **46.1.3 TRANSMISIÓN ENTRE ENTIDADES DO MESMO NIVEL (PARES)**

As entidades pares residentes no nivel N+1 comunícanse entre sí a través do nivel N, mediante o uso de primitivas de servizo. Sen embargo, existe unha comunicación lóxica horizontal entre entidades pares. As regras que regulan esta comunicación veñen reflexadas no protocolo de pares. Polo tanto, na especificación de cada capa existen dous documentos:

- Especificación do servizo, que informa sobre as primitivas existentes. Na descrición das primitivas indícase cuántos parámetros pode ou debe haber e qué información conteñen, pero non se especifica cómo nin con qué formato teñen que ser “pasados”. Isto é un asunto local e definir isto equivale a definir a Interface. Existen catro tipos de primitivas.
  - o De petición (REQUEST). Empregada para invocar un servizo e pasarlle os parámetros necesarios para a súa execución.
  - o De indicación (INDICATION). Usada para indicar que un procedemento foi invocado polo usuario par do servizo na conexión e pasalos parámetros asociados ou para indicar ó usuario do servizo o inicio dunha acción por parte do provedor.
  - o De resposta (RESPONSE). Empregada polo usuario do servizo para recoñecer ou completar algún procedemento previamente iniciado por unha indicación do provedor.
  - o De confirmación (CONFIRM). Usada polo provedor do servizo para recoñecer ou completar algún procedemento previamente iniciado por unha petición do usuario.

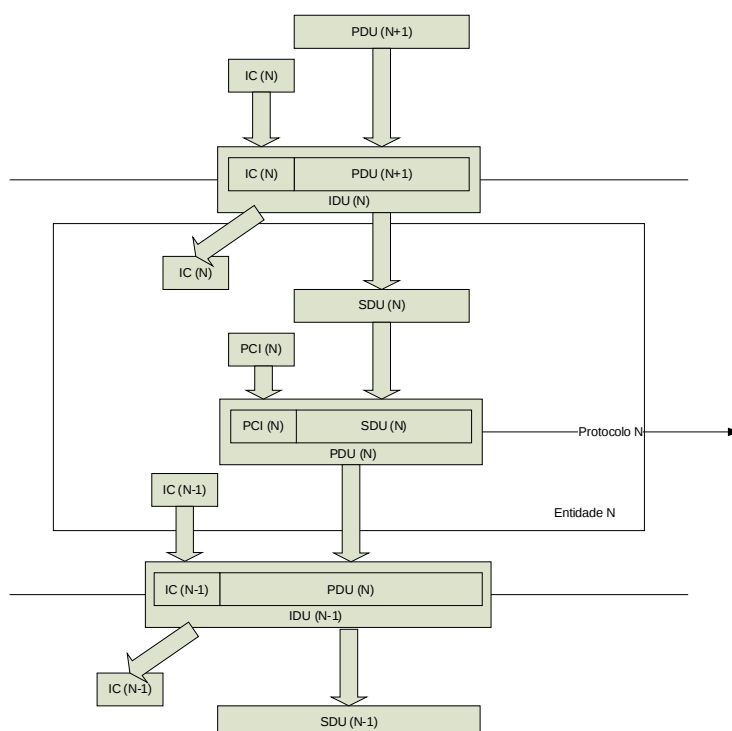


- Especificación do protocolo, que describe as PDUs (Protocol Data Units) e as regras que determinan o seu intercambio entre unidades pares. Existen dúas clases de PDUs:
  - o De datos, que contén os datos do usuario final (no caso da capa de aplicación) ou a PDU do nivel inmediatamente superior.
  - o De control, que serve para gobernar o comportamento completo do protocolo nas súas funcións de establecemento e ruptura da conexión, control de fluxo, control de erros, etc.Non conteñen información algunha proveniente do nivel  $N+1$ .

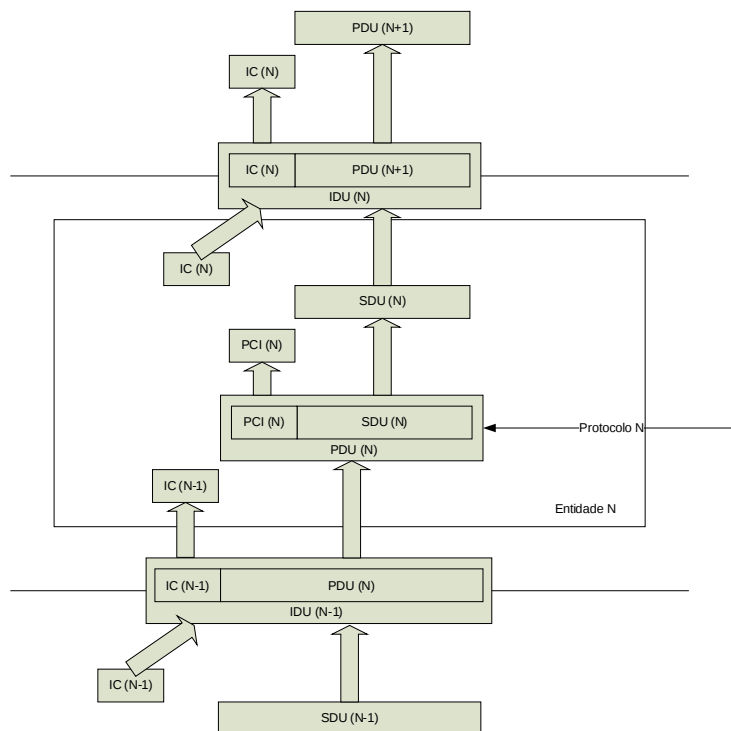
Na seguinte figura ilustrase a nomenclatura utilizada por ISO na pila que envía a información.

- PDU (N) -> Unidade de Datos do Protocolo do nivel N. Contén información de control do protocolo e, posiblemente, datos de usuario. Debe estar puntual e perfectamente definida (sintáctica e semanticamente).
- ICI (N) -> Información de Control da Interface do nivel N. É transferida entre unha entidade  $N+1$  e una entidade N para coordinar o funcionamento local conxunto. A súa sintaxe e semántica son un asunto local cando actúa como información complementaria na transferencia dunha PDU.
- IDU (N) -> Unidade de Datos da Interfaz do nivel N. É transferida a través do punto de acceso ó servizo N. Contén a ICI máis a totalidade (ou parte) da información da PDU ( $N+1$ ). A estrutura das informacións da IDU é un asunto local.
- SDU (N) -> Unidade de Datos do Servizo do nivel N. Representa a información entregada polo nivel inmediatamente superior.

- PCI (N) -> Información de Control do Protocolo do nivel N.  
Información xerada pola entidade N para coordinar o funcionamento conxunto con outra ou outras entidades do nivel N coas que está intercambiando información “horizontal”.
- UD (N) -> Datos do Usuario. Datos transferidos entre entidades do nivel N en nome das entidades do nivel N+1.



Na pila que recibe a información, a relación existente entre as unidades de datos residentes nas entidades do nivel N-1, N e N+1 é similar á representada mais arriba, só que no lugar de engadir elementos o que se producen son reducións e as frechas son ascendentes, como mostra a figura seguinte.



Cando as unidades de datos dos niveis limítrofes non teñen tamaños compatibles, recórrase a algunha das seguintes funcións:

- Segmentación de la SDU. Cando a SDU é demasiado grande, repartese en máis dunha PDU. A función simétrica no extremo receptor é o reensamblado, que consiste na identificación de varias PDUs cunha sola SDU. A PCI inclúe, neste caso, información adicional para posibilitar o reensamblado.
- Empaquetado da SDU. Cando o tamaño da SDU é máis pequeno que o da PDU, pode ser conveniente ou necesario agrupar varias SDUs nunha soa PDU. O empaquetado é o caso contrario á segmentación da SDU. A función inversa do empaquetado é o desempaquetado, que consiste en descompoñer unha PDU en varias SDUs. O caso de segmentación dase con máis frecuencia que o de empaquetado.
- Segmentación da PDU. Se a PDU é moi grande, pode ser necesario repartila en máis dunha IDU do nivel inferior. Por iso, na definición de IDU dise que contén a ICI máis a totalidade (ou parte) da PDU. Tamén neste caso deben existir informacións adicionais que posibiliten o reensamblado no extremo receptor.

- Concatenación de PDU. Se o tamaño da SDU do nivel inferior, e como resultado, da IDU do nivel inferior, é maior co da PDU, pode convir agrupar varias PDUs sobre unha soa SDU. A función inversa a esta, que se realiza no extremo receptor, é a separación. A concatenación-separación é o caso contrario da segmentación-reensamblado da PDU, sendo este último o máis frecuente.

#### **46.1.4 CONEXIÓNS**

O modelo de referencia OSI está orientado a conexión. Isto significa que, en tódolos niveis, é necesario que se estableza previamente unha conexión para que poida existir intercambio de datos. Sen embargo, existen protocolos que non requiren esta condición, son os non orientados a conexión (connectionless).

Nas comunicacións orientadas a conexión perdese tempo e recursos en establecer e liberar a conexión entre dous nodos, pero se garante que o nodo remoto está a escoitar. Polo contrario, nas comunicacións non orientadas a conexión aforrase tempo e recursos, pero á costa de non saber se o outro extremo está a escoitar.

A nivel N-1 estableceuse unha asociación, una conexión N-1, para que dúas entidades do nivel N poidan comunicarse. A conexión N-1 é un servizo ofrecido polo nivel N-1, a través do cal circulan unidades de información do nivel N.

O Punto de Acceso ó Servizo(SAP) do nivel N identifica a dirección do nivel N á que se conectan as entidades do nivel N+1. A relación entre direccións de dous niveis consecutivos pode ser 1 a 1 (1 dirección do nivel N por cada dirección do N +1), N a 1 (Varias direccións do nivel N por cada dirección do N +1) (non confundir coa multiplexación, que se explica máis adiante) ou 1 a N (1 dirección do nivel N para varias direccións do N +1).

##### **46.1.4.1 ESTABLECEMENTO DE CONEXIÓNS**

Para que dúas entidades N establezan unha conexión, é necesario:

- Dispor dunha conexión N-1 por debaixo. É necesario establecer previamente a conexión N-1 antes de intentar establecer a conexión



N, descendendo ata que se encontra unha dispoñible a nivel físico (o nivel mais baixo). Sen embargo, nos niveis altos, aprovéitase a circunstancia de establecemento da conexión N para establecer, o mesmo tempo, a conexión N+1.

- Estar ambas entidades conformes co establecemento.

Unha vez establecida a conexión, é como se a entidade dispuxese dun “tubo” a través do cal puidese enviar datos á súa entidade de comunicación correspondente.

#### **46.1.4.2 LIBERACIÓN DE CONEXIÓNS**

A liberación dunha conexión N é iniciada, normalmente, por unha das entidades N+1 que a está usando. Sen embargo, esta ruptura pode ser tamén iniciada por unha das entidades N que lle dan soporte.

Ó contrario que ocorre no establecemento, a liberación dunha conexión N-1 non implica a liberación da conexión N. Isto é así para permitir que, se a conexión N-1 rompe por dificultades da comunicación, poida intentarse reestablecela ou sustituíla por outra.

A liberación dunha conexión pode ser:

- Abrupta. Libérase de inmediato e os datos pendentes de envío pérdense.
- Suave ou diferida. Antes de rompela conexión, espérase a non ter datos pendentes.

#### **46.1.4.3 MULTIPLEXACIÓN E DIVISIÓN**

A multiplexación é a función que permite utilizar unha soa conexión N-1 para soportar varias conexións do nivel N. Tódolos “tubos” de conexión N viaxan por dentro do “tubo” de conexión N-1. Varias comunicacións entre entidades pares de nivel N realízanse apoiadas nunha soa conexión do nivel N-1. É dicir, as distintas entidades usan un só punto de acceso ó servizo N-1. A función inversa realizada no receptor denomínase demultiplexación. Non debe confundirse o concepto de multiplexación co de concatenación, xa explicado.

A división é a función que permite a utilización de mais dunha conexión N-1 por unha soa conexión de nivel N. Con elo, o fluxo de datos que soporta pode ser maior. O fluxo de datos do “tubo” correspondente á conexión N repártese entre tódolos “tubos” de conexións N-1. No extremo receptor, a función inversa denominase recombinação e debe ser capaz de recuperala orde na que as PDUs foron xeradas polo extremo emisor. Non debe confundirse o concepto de división con de segmentación, xa explicado.

#### **46.1.4.4 TRANSMISIÓN DE DATOS**

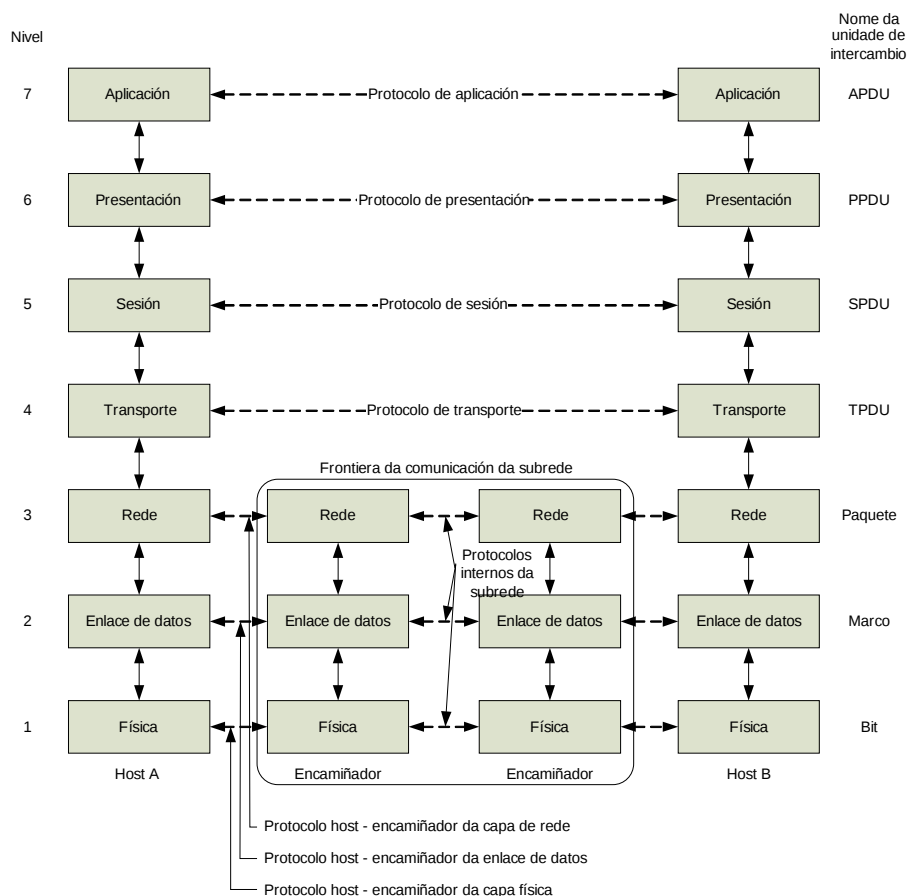
Unha capa dunha máquina non pode transferilos datos de forma directa á súa capa par noutra máquina, se non que necesita dos servizos de tódalas capas que se encontran por debaixo dela na xerarquía de capas, pasándose a información cara abaixo ata chegar ó nivel físico, onde se transmiten á máquina receptora.

Cada capa utiliza o encapsulamento para colocar a PDU da capa superior no seu campo de datos e agregar calquera encabezado e información final ca capa necesite para realizala súa función. Desta forma, a medida cos datos se desprazan cara abaixo a través das capas do modelo OSI, o tamaño da mensaxe vai crescendo. A nivel 3, a PDU chamase paquete e inclúe as direccións lóxicas orixe e destino. A nivel 2, a trama inclúe as direccións físicas. E, finalmente, a capa física codifica os datos da trama de enlace de datos nun patrón de uns e ceros para a súa transmisión a través do medio.

Na máquina receptora realizase o proceso inverso, retirando os distintos encabezados, un por un, conforme a mensaxe se propaga cara arriba po las capas.

#### **46.1.5 CAPAS DO MODELO OSI**

Como se dixo no punto anterior, o modelo de referencia OSI dividiuse en sete niveis ou capas, para poder simplificar a implementación da arquitectura necesaria.



Os principios que se aplicaron para chegar a estas sete capas son os seguintes:

- Debese de crear unha nova capa sempre que se precise un grado diferente de abstracción.
- A cada capa asignaselle unha función ben definida ou un conxunto de funcións relacionadas entre si, tratando de resolver en cada capa un problema distinto.
- A funcionalidade de cada capa débese elixir tendo en conta a posibilidade de definir protocolos normalizados a nivel internacional.
- A fronteira das capas será tal que se minimice o fluxo de información a través da interface existente entre ambas.
- O número de capas debe ser o suficientemente grande para non reunir en un mesmo nivel funcionalidades distintas e suficientemente pequeno para que a arquitectura resultante sexa manexable.

#### 46.1.5.1 CAPA FÍSICA (NIVEL 1)

A capa física está relacionada coa transmisión de bits por un canle de comunicación, de forma que só recoñece bits individuais, sen estrutura algunha. É dicir, a PDU do nivel físico correspóndese con un bit ou, dito doutro modo, cada bit considérase unha unidade de datos.

As consideracións de deseño teñen que ver coas interfaces mecánica, eléctrica e de procedemento, así como co medio de transmisión que está baixo a capa física, asegurando que cando un lado envíe un bit co valor “1”, se reciba no outro extremo o valor “1”, non coma o valor “0”.

A capa física proporciona os seus servizos á capa de enlace de datos. As súas principais funcións son:

- Definición de características materiais (compoñentes e conectores mecánicos) e eléctricas (niveis de tensión, tipo de sinal) que se van a utilizar na transmisión dos datos polo medio físico.
- Definición das características funcionais da interface en canto ó establecemento, mantemento e liberación do enlace físico.
- Definición de regras de procedemento, e dicir, a secuencia de eventos para transmitir.
- Transmisión de fluxos de bits a través do medio.
- Manexo de voltaxes e pulsos eléctricos para representar 1's ou 0's.
- Especificación de cables, polos nun enchufe, compoñentes da interface co medio, etc.
- Especificación do medio físico de transmisión (coaxial, fibra óptica, par trenzado, etc.)
- Garantía conexión física, pero non a fiabilidade da mesma. É dicir, non se realiza ningún control de erros neste nivel. Eso corresponde ó nivel superior.

#### **46.1.5.2 CAPA DE ENLACE DE DATOS (NIVEL 2)**

Posto que a capa física só acepta e transmite una corrente de bits sen preocuparse polo seu significado ou estrutura, correspóndelle ó nivel de enlace tomalo medio de transmisión en bruto e transformalo nunha liña que pareza estar libre de erros aos ollos da capa de rede.

A capa de enlace de datos pode ofrecer á capa de rede varias clases de servizo con diferentes calidades.

Algunhas das funcións máis importantes da capa de enlace son:

- Establecemento dos medios necesarios para a comunicación fiable e eficiente entre dúas máquinas da rede.
- Estructuración dos datos nun formato predefinido, denominado trama, que soe ser duns centos de bytes, engadindo unha secuencia especial de bits ó principio e ó final da mesma.
- Sincronización no envío de tramas.
- Detección e control de erros provintes do medio físico mediante o uso de bits de paridade, CRC (Códigos de Redundancia Cíclica) e envío de acuses de recibo por parte do receptor que debe procesalo emisor.
- Utilización de números de secuencia nas tramas para evitar perdas e duplicidades.
- Utilización da técnica de “piggybacking”, consistente no envío de acuses de recibo dentro de tramas de datos.
- Resolución dos problemas provocados polas tramas danadas, perdas ou duplicadas.
- Control da conxestión da rede.
- Mecanismos de regulación de tráfico ou control de fluxo, para evitar que un transmisor veloz sature de datos a un receptor lento.
- Control do acceso ó canle compartido nas redes de difusión.

#### **46.1.5.3 CAPA DE REDE (NIVEL 3)**

A capa de rede é unha capa complexa que ofrece os seus servizos á capa de transporte. Responsable da conmutación e encamiñado da información, as súas funcións pódense resumir da seguinte forma:

- Coñecemento da topoloxía da rede, é dicir, da forma en que están interconectados os nodos, con obxecto de determinar a mellor ruta para a comunicación entre máquinas que poidan estar situadas en redes xeográficamente distintas.

- División das mensaxes da capa de transporte en unidades máis complexas, chamadas paquetes (NPDUs), e asignación de direccións lóxicas ós mesmos.
- Ensamblado de paquetes no host destino.
- Establecemento, mantemento e liberación das conexións de rede entre sistemas.
- Determinación do camiño dos paquetes dende a fonte ata o destino a través de dispositivos intermedios (routers):
  - o As rutas poden basearse en táboas estáticas.
  - o As rutas pódense determinar o inicio de cada conversa.
  - o As rutas poden ser dinámicas, determinándose con cada paquete en función da carga da rede.
- Envío de paquetes de nodo a nodo usando un circuío virtual (orientado a conexión) ou datagramas (non orientado a conexión).
- Control da conxestión.
- Control de fluxo.
- Control de erros.
- Reencamiñamento de paquetes en caso de caída dun enlace.
- Con frecuencia, funcións de contabilidade, para determinar cuántos paquetes, caracteres ou bits envía cada cliente e producir información de facturación.

Esta capa só é necesaria nas redes de conmutación ou redes interconectadas. En redes punto a punto ou de difusión existe un canle directo entre os dous equipos, polo que o nivel 2 proporciona directamente conexión fiable entre os dous equipos.

#### **46.1.5.4 CAPA DE TRANSPORTE (NIVEL 4)**

Tratase dunha verdadeira capa extremo a extremo, dende a orixe ata o destino. A comunicación nos niveis inferiores é entre máquinas adxacentes.

A capa de transporte proporciona os seus servizos á capa de sesión, efectuando a transferencia de datos de maneira transparente entre dúas entidades de sesión.

O nivel 4 ten a interface mais sinxela de todo o modelo OSI, sendo a que ten menos primitivas. Non ten primitivas de confirmación, pois considerase a tódolos efectos que é un nivel fiable.

A súa función mais importante é a aceptación de datos da capa de sesión, división en unidades mais pequenas, se é preciso, denominadas segmentos, e envío desta información á capa de rede, asegurando que tódalas partes cheguen correctamente ó outro extremo de forma eficiente, onde son reensambladas.

Outras funcionalidades son:

- Establecemento, mantemento e terminación adecuados dos circuitos virtuais (conexións que se establecen dentro de una rede). Cando se inicia a conexión determinase unha ruta dende a fonte ata o destino, ruta que é usada para todo o tráfico de datos posterior.
- Determinación, no momento do establecemento da sesión, do tipo de clase de servizo de transporte que se proporcionará á capa de sesión:
  - o Canle punto a punto libre de erros, que entrega os mensaxes ou bytes na orde en que se envían.
  - o Mensaxes illados sen garantía respecto á orde de entrega.
  - o Difusión de mensaxes a múltiples destinos.
- Control de fluxo, que desempeña un papel clave nesta capa. O control de fluxo entre nodos é distinto do control de fluxo entre encamiñadores, que ten lugar na capa de rede. Os datos poden ser normais ou urxentes. Estes últimos saltan os mecanismos de control de fluxo.
- Detección e recuperación de erros de transporte.
- Control da conxestión.
- Numeración dos segmentos para previr perdas e dobre procesamento de transmisións.

- Garantía de recepción de tódolos datos e na orde adecuada, sen perdas nin duplicados.
- Asignación dunha dirección única de transporte a cada usuario.
- Illamento das capas superiores dos cambios inevitables da tecnoloxía do hardware.
- Contabilidade a través da rede.

O normal é que a capa de nivel 4 cree unha conexión de rede distinta para cada conexión de transporte que require a capa de sesión. Sen embargo, é posible crear múltiples conexións de rede, dividindo os datos entre elas para aumentar o volume, se se require un volume de transmisión alto. De igual forma, se resulta custoso manter unha conexión de rede, o nivel 4 pode multiplexar varias conexións de transporte na mesma conexión de rede para reducir o custo. Na cabeceira que engade este nivel envíase a información que identifica a qué conexión pertence cada mensaxe. En calquera caso, a capa de transporte debe facer isto de forma transparente á capa de sesión.

#### **46.1.5.5 CAPA DE SESIÓN (NIVEL 5)**

Esta capa proporciona os seus servizos á capa de presentación, facilitando o medio necesario para que as entidades de presentación de dúas máquinas diferentes organicen e sincronicen o seu diálogo e procedan ó intercambio de datos, mediante o establecemento de sesións.

Por tanto, a función principal da capa de sesión é o establecemento, administración e finalización ordenada de sesións entre dúas máquinas.

Unha sesión permite o transporte ordinario de datos, como efectuar un login nun sistema remoto ou transferir un ficheiro entre dous nodos, pero tamén proporciona servizos mellorados, útiles nalgunhas aplicacións, como os que se detallan a continuación.

- Manexo do control do diálogo (quén fala, cándoo, canto tempo, half duplex ou full duplex). As sesións poden permitir que o tráfico vaia nunha única dirección, comunicacións bidireccionais alternadas (half duplex), ou en ambas direccións ó mesmo tempo, comunicacións



bidireccionais simultáneas (full duplex). Nas comunicacións half duplex, a capa de sesión axuda a levalo control dos turnos, mediante o manexo de fichas, tamén chamadas testigos ou tokens. Só o lado que posúa a ficha pode efectual a operación.

- Sincronización do diálogo, mediante a inserción de puntos de verificación na corrente de datos (APDU), de modo que si se produce unha interrupción só é necesario repetila transferencia dos datos despois do último punto de verificación. A decisión de ónde colocar os puntos de sincronización é competencia directa do nivel de aplicación. Os puntos de sincronización poden ser de dous tipos.
  - o Maior. Necesita confirmación do outro extremo para seguir coa transferencia do seguinte bloque.
  - o Menor. Intercálanse entre dous puntos de sincronización maiores. Non necesitan confirmación. Ó confirmarse un punto de sincronización maior, danse por confirmados os puntos menores intermedios.

O bloque entre o primeiro e o último punto de sincronización maior chámase actividade. Cando se establece unha conexión de sesión, automaticamente ábrese unha actividade, para poder traballar. Só un tipo de datos concreto pode enviarse fora dunha actividade, os datos de capacidades (CD), que son datos de control. As actividades divídense en unidades de diálogo, que é o contido entre dous puntos de sincronización maior consecutivos.

Nesta capa a referencia ós dispositivos é polo nome e non pola dirección. Ademais, é aquí onde se definen as API's (Application Program Interface). O protocolo de nivel de sesión é orientado á aplicación, xa que as súas funcionalidades adáptanse ás necesidades da aplicación.

As unidades de datos do nivel de sesión, SPDUs, que regulan o diálogo, flúen horizontalmente a través do nivel 5, pero son postas en circulación por iniciativa dos correspondentes procesos de aplicación que residen no nivel 7. É dicir, a capa de sesión non é un nivel autónomo que teña

capacidade para tomar decisións sobre quen fala e quen escoita. Estas decisións están reservadas ás entidades da capa de aplicación. O nivel 5 só proporciona os mecanismos para que as entidades de aplicación poidan regularo diálogo entre si.

No parágrafo anterior falase como se a capa de aplicación residise directamente encima da de sesión. Isto non é así. Como se indica na enumeración de capa, a capa de sesión ofrece os seus servizos á capa de presentación. O que ocorre é que o protocolo de nivel 6 non é un protocolo “normal”. De feito, a maior parte das primitivas que comunican a capa de presentación co nivel 7 son translación exacta das correspondentes primitivas entre o nivel 6 e a capa de sesión.

#### **46.1.5.6 CAPA DE PRESENTACIÓN (NIVEL 6)**

A diferenza das capas inferiores, as explicadas ata agora, que se ocupan só do movemento fiable de bits dun lado a outro, a capa de presentación encargase da sintaxe e a semántica da información que se transmite. Ademais, illa de ditas capas inferiores o formato dos datos das aplicacións específicas.

As estruturas de datos a intercambiar teñense que definir de forma abstracta, mediante a codificación destes datos dunha maneira estándar acordada, facendo posible así a comunicación entre computadoras con representacións locais diferentes. A capa de presentación manexa estas estruturas de datos abstractas e convérteas da representación da computadora á representación estándar da rede e viceversa.

Ademais desta funcionalidade, a capa de presentación ofrece á capa de aplicación os servizos de:

- Garantía de que a información que envía a capa de aplicación dun sistema poida ser entendida e utilizada pola capa de aplicación doutro sistema.
- Acordo e negociación da sintaxe de transferencia na fase de establecemento da conexión. A sintaxe escollida pode ser cambiada durante o tempo que dure a conexión.

- Definición do código a utilizar para representar unha cadea de caracteres (ASCII, EBCDIC, etc.)
- Interpretación dos formatos de números...
- Compresión dos datos, se é necesario.
- Aplicación de procesos criptográficos, se así se require. É o nivel clave para o sistema de seguridade do modelo OSI.
- Formateo da información para a súa visualización ou impresión.

#### **46.1.5.7 CAPA DE APLICACIÓN (NIVEL 7)**

É a capa do modelo OSI máis próxima ó usuario. Difire das demais capas en que non proporciona servizos a ningunha outra capa OSI, se non as aplicacións que se encontran fora do modelo. Tódalas capas anteriores serven de mera infraestrutura de telecomunicacións, é dicir, manteñen en bo estado o camiño para que flúan os datos. É a capa de aplicación a que fai posible que unha rede se poida usar, a pesar de estar abstraída de tódalas restantes funcións necesarias para o establecemento da comunicación.

As aplicacións mais importantes que fan uso desta capa, para que os procesos das aplicacións accedan ó entorno OSI son, entre outras:

- Correo electrónico. Primeira aplicación que se normalizou en OSI.
- Terminal virtual de rede abstracta, que diferentes editores e programas poidan manexar.
- Transferencia de arquivos.
- Carga remota de traballos.
- Servizos de directorio.
- Login remoto (rlogin, telnet).
- Acceso a bases de datos.
- Sistemas operativos de rede.
- Aplicacións Cliente/Servidor...

Por suposto, no nivel 7 tamén hai cabida para aplicacións “particulares” deseñadas por e para un núcleo reducido de usuarios, pero carecen de demasiado interese.

As PDUs da capa de aplicación, APDUs, son de formato moi flexible e variable. Entre dúas APDUs poden encontrarse diferencias substanciais en cuanto ó seu tamaño, número de campos presentes, etc, que dependen das necesidades de cada momento.

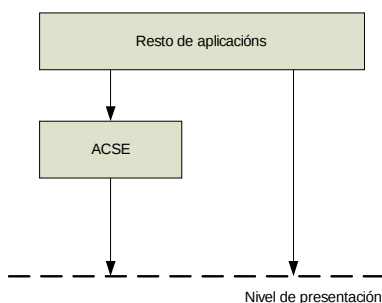
A cada unha das partes dunha aplicación que se encarga dunha tarefa específica denomínase Elemento de Servizo de Aplicación (ASE). O conxunto de tódolos ASEs que forman unha aplicación concreta e a relación entre eles forman o contexto de aplicación.

Hai ASEs válidos para varias aplicacións:

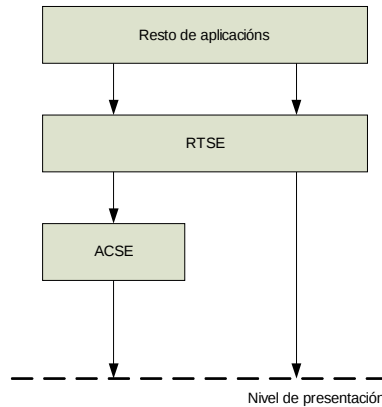
- ACSE (Association Control Service Element). Establecemento, manexo e liberación ordenada ou abrupta de conexións. Utilízanse tódalas aplicacións.
- RTSE (Reliable Transfer Service Element). Garante a fiabilidade na transferencia de datos, solucionando os problemas que se produciran do nivel 4 cara arriba. É responsable de manexar tódalas funcións de nivel 5. Utilízanse algunhas aplicacións, non todas.
- ROSE (Remote Operation Service Element). Facilita o traballo de petición de operacións remotas e devolución dos resultados.

As aplicacións compóñense dunha mestura de elementos específicos e comúns. As seguintes figuras ilustran as relacións entre ASEs comúns.

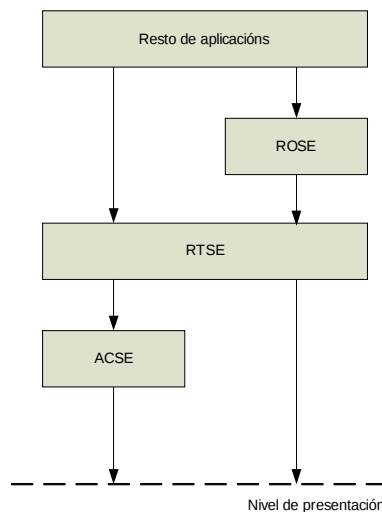
- Para aplicacións que non manexan RTSE nin ROSE. Teñen que xestionar por si mesmas os puntos de sincronización, os token, etc.



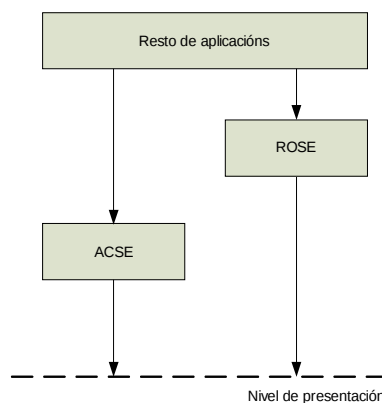
- RTSE é o que se encarga das RTSE actividades, os puntos de sincronización, etc. Neste caso, a aplicación non manexa directamente o nivel 5, se non que o fai a través de RTSE.



- Para as aplicacións que fan uso dos tres ASEs comúns.



- Neste caso, ROSE traballa directamente sobre o nivel 5.



#### 46.1.6 CRÍTICAS Ó MODELO OSI

A verdadeira razón de que o modelo OSI teña sete capas e que, no momento de deseño, IBM tiña un protocolo patentado de sete capas, chamado SNA (System Network Architecture, Arquitectura de Rede de Sistemas) e, nesa época, IBM dominaba a industria da computación. Por outro lado, o proceso de estandarización foi demasiado longo. Cando aínda se traballaba na definición de OSI, xa existían implementacións completas e gratuítas de TCP/IP e aplicacións como e-mail, telnet, ftp, etc. Algúns dos problemas ou fallos que se detectaron no modelo de referencia OSI son:

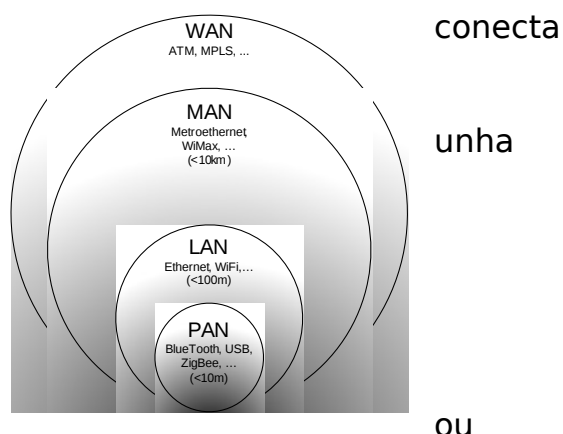
- Aínda que o modelo OSI, xunto coas súas definicións e protocolos de servizos, é moi completo; hai que recoñecer que os estándares son difíciles de implementar e ineficientes na súa operación. As implementacións iniciais foron enormes, inmanexables e lentas.
- OSI desenvolveuse antes de que se inventaran os protocolos. Así que os deseñadores non souberon ben qué funcionalidade por en cada capa.
- A capa de sesión ten pouco uso na maior parte das aplicacións.
- A capa de presentación está practicamente baleira.
- Polo contrario, as capas de rede e de enlace de datos están moi cheas, ata tal punto que chegaron a dividirse en múltiples subcapas, cada unha con funcións distintas.
- Algunhas funcións, como o direccionamento, o control de fluxo e o control de erros, reaparecen unha e outra vez en cada capa.
- Omisión da administración da rede no modelo.
- Aínda que no presente documento situouse na capa de presentación a función de cifrado e seguridade dos datos, inicialmente deixouse fora do modelo por falta de acordo sobre en qué capa colocalo.
- Na capa de rede ofrécese servizo orientado a conexión e non orientado a conexión. Sen embargo, na capa de transporte, onde o servizo é visible aos usuarios, só se ofrece comunicación orientada a conexión.

- O modelo está dominado por unha mentalidade de comunicacións. As computadoras son diferentes dos teléfonos. Moitas das decisións tomadas son inapropiadas para a forma de traballar das computadoras e o software. O modelo dun sistema controlado por interrupcións non se axusta conceptualmente cás ideas modernas da programación estruturada.

## 46.2 REDES LAN, MAN E WAN

Unha das formas clásicas de clasificar as redes é pola súa extensión física (ou alcance) da que se obteñen os seguintes tipos:

- Personal Area Network (PAN): rede que conecta elementos próximos a unha persoa.
- Local Area Network (LAN): elementos en unha área xeográfica limitada, como son casa, un edificio, etc.
- Metropolitan Area Network (MAN): algunhas veces referida como Medium Area Network conecta elementos ao largo dunha cidade espazos de similar tamaño.
- Wide Area Network (WAN): son redes de gran extensión cubrindo cidades, unha provincia ou incluso varios países.

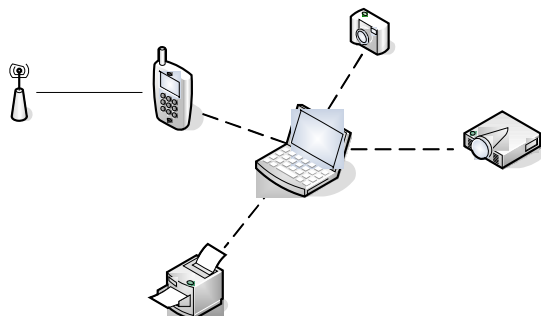


### 46.2.1 PAN

Una PAN é unha rede usada para a comunicación de ordenadores e diferentes dispositivos informáticos próximos a unha persoa. Algúns exemplos destes dispositivos usados en unha PAN son PCs, impresoras, teléfonos, PDAs ou consolas de videoxogos.

A necesidade destas redes é dobre, por un lado conectar dispositivos de uso persoal próximos coma o teléfono móbil cun mans libres ou con dispositivos de recollida de datos médicos. E polo outro permitila

mobilidade das persoas aproveitando o uso e conectividade destes dispositivos, seguindo o exemplo anterior, o móbil pode cambiar de conectarse a un mans libres no coche a conectarse a outro na casa. Unha PAN pode incluír dispositivos conectados por cable e dispositivos sen fíos alcanzando un máximo de 10 metros de distancia.

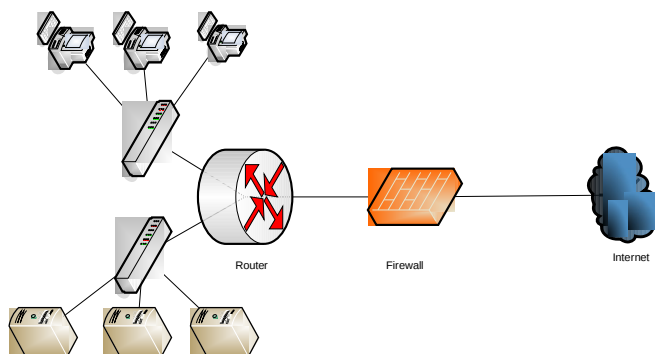


As típicas tecnoloxías nas que se basean as PAN son USB e FireWire para as cableadas e BlueTooth e ZigBee para as sen fíos.

#### **46.2.2 LAN**

Unha LAN conecta ordenadores e outros dispositivos nun espazo limitado como pode ser unha casa, un edificio, unha oficina ou un conxunto de edificios próximos entre si.

Tipicamente a distancia que abarca unha LAN non supera os 100 metros.



O exemplo máis común de LAN dáse no ámbito doméstico e das pequenas empresas onde varios equipos están conectados a un concentrador (switch), posiblemente varios servidores están conectados a outro e eses concentradores están conectados a un encamiñador (router) para a conexión a Internet.

As tecnoloxías dominantes usadas nas LAN son Ethernet (hoxe en día gigabit ethernet) e WiFi (habitualmente 802.11g) aínda que existen moitas



outras tecnoloxías que se empezan (ou continúan) a empregar, como poden ser as baseadas en PLC, por exemplo HomePlug.

#### **46.2.3 MAN**

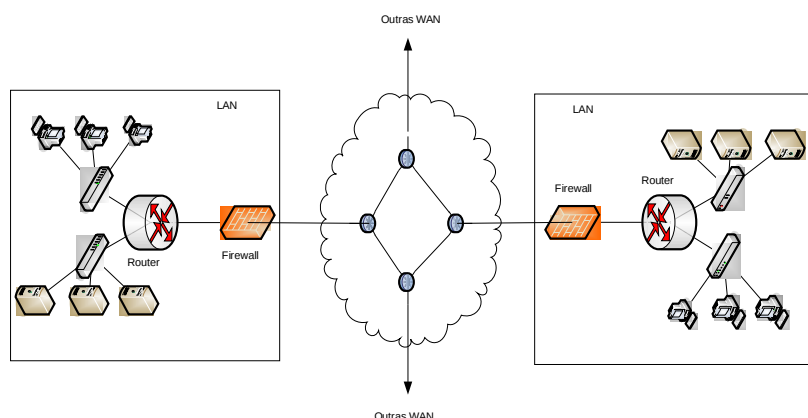
Unha MAN é unha rede optimizada para unha area xeográfica maior que unha LAN, que vai dende varios bloques de edificios ata una cidade. Unha MAN pode ser propiedade dunha organización pero normalmente é usada por moitos individuos e organizacións distintas. A súa utilidade típica e proporcionar conectividade entre varias LAN.

A distancia típica que cubre unha MAN é de 10 km.

Tipicamente estas redes están baseada sen tecnoloxías como MetroEthernet, en redes cableadas, ou Wimax, en redes sen fíos.

#### **46.2.4 WAN**

As WAN son redes de ordenadores que cobren grandes áreas e soen enlazar varias cidades, provincias ou países.



De forma análoga ás MAN a función típica das WAN é conectar varias redes de menor extensión como varias MAN ou varias LAN ademais de conectarse con outras redes WAN.

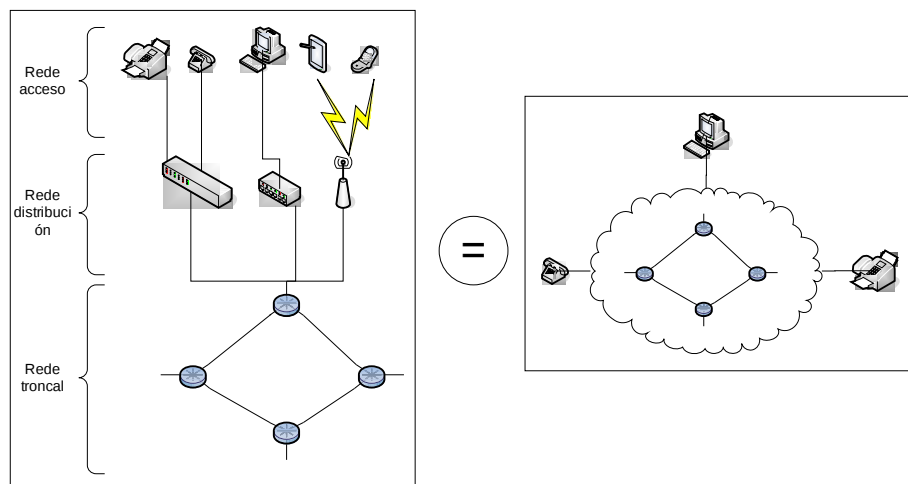
En contraste cos outros tipos de redes, as WAN non están limitadas a un tamaño máximo.

ATM ou MPLS son algunha das tecnoloxías usadas para despregar redes WAM.

### **46.3 ESTRUCTURA DE REDES: TRONCAL, DISTRIBUCIÓN E ACCESO**

As redes (xa sexa a rede dun operador ou dunha compañía) estrutúranse de forma xerárquica. Esta estrutura apórtalles modularidade, permite

aumentar os elementos dun nivel para expandir a rede sen afectar o resto da mesma (escalabilidade) e facilita a identificación e resolución de problemas.



Normalmente esta xerarquía divídese en 3 niveis (aínda que, dependendo da rede concreta, pode haber máis como, por exemplo, nas redes de cable):

- Troncal (en inglés *backbone* ou *core*): é a espiña dorsal da rede conectando os distintos elementos do nivel de distribución.
- Distribución: conecta varios elementos do nivel inferior co nivel superior e soe estar limitada a unha das zonas físicas (por exemplo unha cidade) nas que a rede está presente.
- Acceso: os elementos do nivel de acceso permite conectar os equipos finais.

#### **46.3.1 TRONCAL**

A rede troncal é o nivel xerárquico mais alto dentro da división en niveis e está formada por unha parte da infraestrutura da rede de ordenadores que conecta varias partes da mesma (subredes).

Normalmente a capacidade de transferencia de datos da rede troncal é maior que a das subredes que conecta e posúe camiños redundantes (os operadores soen usar varios aneis e nas redes corporativas soe haber varias conexións).

De tratarse dunha rede corporativa o acceso a Internet soe atoparse na rede troncal.

Un exemplo deste tipo pode ser a rede que conecta as distintas cidades onde da servizo un provedor de internet.

#### **46.3.2 DISTRIBUCIÓN**

No nivel de distribución agréganse os datos provintes dos elementos do nivel de acceso para seren enviados ao nivel superior.

Os elementos deste nivel tamén soen estar redundados pero en menor medida que no nivel superior.

De tratarse dunha rede corporativa é neste nivel onde se establecen as VLANs para cada departamento / división e onde se limitan os dominios de broadcast.

Seguindo o exemplo de antes estas poderían ser a rede que conecta os distintos nodos dentro dunha cidade.

#### **46.3.3 ACCESO**

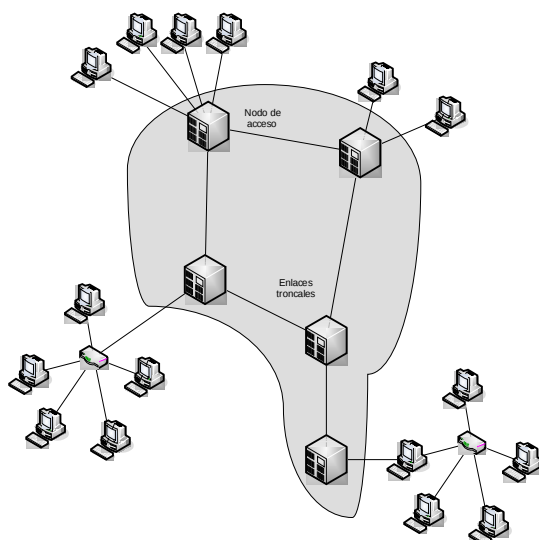
O nivel de acceso é o nivel da rede onde se conectan os equipos finais (ordenadores, teléfonos, ...).

No exemplo anterior esta sería a rede que conecta os distintos usuarios a un nodo.

### **46.4 REDES PÚBLICAS DE TRANSMISIÓN DE DATOS**

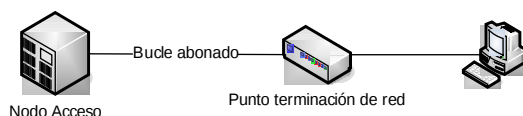
Dende o momento que naceu a necesidade de conectar dúas localizacións pasando polo dominio público, naceu a necesidade das redes públicas.

Unha rede pública é aquela a que calquera entidade pode conectarse (normalmente baixo pago dunha cuota) en orde a comunicarse con outra entidade conectada á mesma rede pero en distinta localización xeográfica. Esta dispoñibilidade de conectar calquera dúas entidades leva a que haxa varias entidades (individuos, compañías, gobernos, ...) conectadas a esta rede, como oposición a unha rede privada onde só hai unha entidades aproveitando os recursos da rede. Isto da como resultado que en moitas ocasións as entidades queiran usala rede pública como unha rede privada (xa sexa por simplicidade na configuración, seguridade ou outras razóns) dando lugar ás Redes Privadas Virtuais (VPN polas súas siglas en inglés).



#### 46.4.1 CONCEPTOS XERAIS

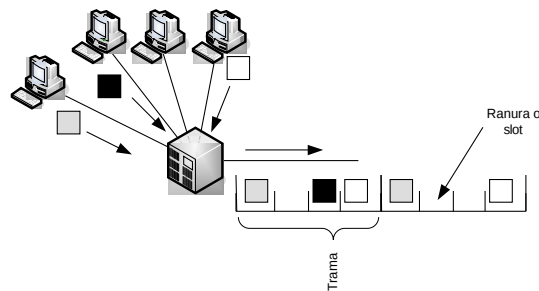
O bucle de abonado (bucle local ou lazo local) é o cableado que se estende dende os nodos de acceso (centrais de teléfonos, ...) ata o domicilio ou local do usuario.



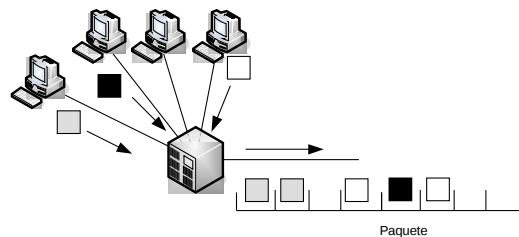
A conmutación é a conexión que realizan os diferentes nodos para lograr un camiño apropiado para conectar dous usuarios dunha rede de telecomunicacións. A conmutación permite a desconxestión entre os usuarios da rede reducindo o tráfico e aumentando o ancho de banda (comparándoa cos sistemas baseados en bus, por exemplo).

A multiplexación é a combinación de dous ou máis canles de información nun só medio de transmisión usando un dispositivo chamado multiplexor. O proceso coñécese como demultiplexación. Existen moitas estratexias de multiplexación según o protocolo de comunicación empregado pódense combinar para alcanzar o uso máis eficiente; as máis utilizadas son:

- A multiplexación por división de tempo o TDM (Time division multiplexing). Dentro de esta estratexia podemos encontrar:
  - a. Multiplexación estática ou síncrona.



b. Multiplexación estatística ou asíncrona.



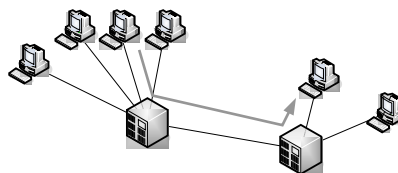
- A multiplexación por división de frecuencia o FDM (Frequency-division multiplexing) e o seu equivalente para medios ópticos, por división de lonxitude de onda ou WDM (de Wavelength).
- A multiplexación por división en código ou CDM (Code division multiplexing).

## 46.5 PROTOCOLOS DE REDE

### 46.5.1 REDES DE CONMUTACIÓN DE CIRCUÍTOS

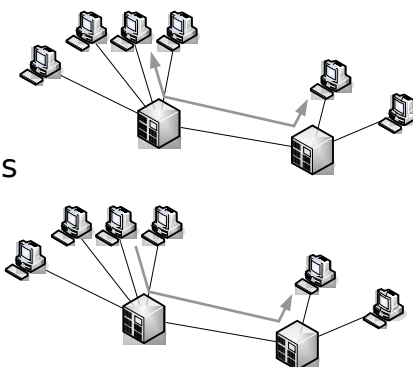
A conmutación de circuitos é un tipo de conexión que realizan os diferentes nodos dunha rede para lograr un camiño apropiado para conectar dous usuarios. Neste tipo de conmutación establece un canal de comunicacións dedicado entre as dúas estacións. Resérvanse recursos de transmisión e de conmutación da rede para o seu uso exclusivo no circuito durante a conexión.

Neste tipo de redes a comunicación ten tres fases:



1. Establecemento do circuito

## 2. Transmisión dos datos



## 3. Liberación do circuío

Este tipo de redes usa TDM, o que permite dispor dun retardo fixo e predicible. Dende o punto de vista do usuario o enlace é punto a punto. Un exemplo deste tipo de rede é a Rede Telefónica Conmutada (RTC).

### **46.5.2 REDES DE CONMUTACIÓN DE PAQUETES**

A conmutación de paquetes é o sistema máis usado para o envío de datos nunha rede de ordenadores. Un paquete é un grupo de información que consta de dúas partes: os datos propiamente ditos, e unha información de control, que especifica a ruta a seguir ó longo da rede ata o destino do paquete. Existe un límite superior para o tamaño dos paquetes; en caso de superalo é necesario dividir o paquete en outros máis pequenos. Tamén pode existir un límite inferior para o tamaño do paquete dependendo da tecnoloxía de transmisión usada.

Existen dúas técnicas para a transmisión de paquetes nas redes de conmutación de paquetes:

- A baseada en circuítos virtuais: Moi similar á conmutación de circuítos, a diferenza radica en que cos circuítos virtuais a ruta non é dedicada, se non que un único enlace entre dous nodos pódese compartir dinamicamente no tempo por varios paquetes (TDM asíncrono). Require as mesmas 3 fases que a conmutación de circuítos (Establecemento do circuío, transmisión de datos e liberación do circuío).
- A baseada en datagramas: Non debemos establecer o circuío de forma previa á transferencia de información. Cada paquete debe levar a dirección de destino e tratase de forma individualizada, sen

establecer ningún vínculo cos demais paquetes que levan datos de A a B, sexan ou non da mesma aplicación.

Os usuarios comparten os medios de transmisión por TDM estatístico. Os retardos son agora variables, dependentes da carga instantánea na rede. Cando se establece o circuíto virtual ou cada vez que se transmite un datagrama conmutador debe seleccionar por que enlace encamiña os datos usando un algoritmo de encamiñamento. Esta decisión ten que ser tomada por cada nodo da rede implicado. Esta decisión debe tomarse minimizando o custo (tempo, recursos, ...) e, con este fin, cada nodo constrúe unha táboa (usando o mencionado algoritmo), chamada táboa de encamiñamento que indica por que enlace debe transmitir os datos para chegar o destino.

No caso dos circuítos virtuais (ademais da táboa de encamiñamento que se usará para seleccionar a ruta do circuíto virtual), o nodo debe construír una táboa cos circuítos virtuais, onde se asigna o identificador dun circuíto virtual dun enlace (entrada) a outro enlace (saída).

Un exemplo de rede que usa circuítos virtuais é X.25 e un de conmutación de paquetes é 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. TECNOLOXÍAS DE ACCESO: REDES TELEFÓNICAS (RDSI, XDSL), REDES DE TELEFONÍA MÓBIL, CABLE, PLC, REDES RADIO (LMDS, WIMAX), SATÉLITE, LIÑAS PUNTO A PUNTO, METROETHERNET.**



**Tema 47. Tecnoloxías de acceso: redes telefónicas (RDSI, xDSL), redes de telefonía móbil, cable, PLC, redes radio (LMDS, Wimax), satélite, liñas punto a punto, MetroEthernet.**

**47.1 Redes telefónicas (RDSI, xDSL)**

**47.1.1 RDSI**

**47.1.1.1 Vantaxes de RDSI**

**47.1.1.2 RDSI de banda estreita**

**47.1.1.3 RDSI de banda ancha**

**47.1.1.3.1 Servizos 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 móbil**

**47.2.1 GSM**

**47.2.1.1 Arquitectura da rede 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 ou E-GPRS**

**47.2.2.2 HSCSD**

**47.2.3 Sistemas de terceira xeración: 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 Liñas punto a punto

##### 47.7.1 X.25

##### 47.7.2 FrameRelay

##### 47.7.3 MetroEthernet

#### 47.8 MetroEthernet

##### 47.8.1 MAN baseada en Ethernet

##### 47.8.2 MAN baseada en SDH

##### 47.8.3 MAN baseada en MPLS

#### 47.9 Bibliografía

### **47.1 REDES TELEFÓNICAS (RDSI, XDSL)**

Orixinalmente a única rede pública dispoñible era a Rede Telefónica Conmutada (RTC) que estaba composta por elementos analóxicos sendo o seu principal obxectivo o transporte da voz que transmitíase por liñas modulada como unha forma de onda analóxica.

Para poder transmitir datos sobre esta rede necesitábase convertela sinal dixital nunha sinal analóxica na orixe e volver a convertela en dixital no destino. Dado que as liñas de voz pensáronse só para transmitir voz usaban conmutación de circuítos. Ademais debido a que non foron deseñadas para garantir a transmisión sen perda, eran os protocolos de transmisión de datos os que debían garantir a corrección de erros, reconexión, etc.

Posteriormente, para solucionar o problema da perda de calidade do son nas chamadas a larga distancia apareceron as centrais dixitais, menos propensas a fallos, e permitiron controlar máis liñas de usuario e realizalas conexións moito máis rápido. Desta forma, unha comunicación por unha liña telefónica convencional realizase de forma analóxica no bucle de abonado, pero de forma dixital ata chegar á central onde está conectado o abonado destino. A RDSI (Rede Dixital de Servizos Integrados) supón o último avance: a comunicación dixital entre o abonado e a central telefónica.

#### **47.1.1 RDSI**

RDSI é unha rede desenvolta a partir da rede telefónica que proporciona unha conexión dixital extremo a extremo e que soporta unha gran variedade de servizos.

Denomínase “Dixital” porque basease en técnicas dixitais, garantindo a integridade da información e a transmisión da mesma libre de degradacións o perturbacións externas; e é “de Servizos Integrados” porque utiliza a mesma infraestrutura para moitos servizos que tradicionalmente requirían interfaces distintos (télex, voz, conmutación de circuítos, conmutación de paquetes, etc).

As características mais importantes son:

- A súa arquitectura está estratificada en niveis: físico, enlace e rede.
- Proporciona conexións de 64Kbps.
- A sinalización vai por un canal diferente á información propiamente dita. En certas ocasións utilízase a canle de sinalización para enviar información aínda que a unha velocidade máis baixa.
- Soporta unha gran variedade de aplicacións, independentemente de si están baseadas en conmutación de circuítos ou de paquetes.

#### **47.1.1.1 VANTAXES DE RDSI**

Entre as vantaxes que ofrece RDSI pódense destacar:

- Velocidade. Ofrece múltiples canles dixitais que poden operar simultaneamente a través da mesma conexión telefónica entre central e o usuario. Usando un protocolo de agregación de canles pódese alcanzar unha velocidade de datos sen comprimir duns 128 Kbps, no servizo de acceso básico. Este esquema permite unha transferencia de datos a una velocidade moito maior que a liña telefónica. Ademais, o tempo necesario para establecer una comunicación en RDSI é aproximadamente a metade do tempo empregado cunha liña analóxica.
- Conexión de múltiples dispositivos. É posible combinar diferentes fontes de datos dixitais e facer que a información chegue ó destino

correcto. Como a liña é dixital, é fácil controlalo ruído e as interferencias producidas ó combinar os sinais.

- Sinalización. Nunha conexión RDSI a chamada establececese enviando un paquete de datos especial a través dun canle independente dos canles para datos. Permite establecer a chamada nun par de segundos.
- Servizos. A RDSI non se limita a ofrecer comunicacións de voz. Ofrece outros moitos servizos como transmisión de datos informáticos (servizos portadores), télex, facsímile, videoconferencia (usando, por exemplo, H.320), conexión a Internet e opcións como chamada en espera, identidade da orixe, etc.

En función do ancho de banda distínguense entre RDSI de “banda estreita” que permite velocidades de 64Kbps ou agrupacións desta velocidade ata 1984Kbps e RDSI de banda ancha onde a velocidade mínima á que se traballa é 2Mbps, podendo chegar ata os 100Mbps.

#### **47.1.1.2 RDSI DE BANDA ESTREITA**

A RDSI dispón de tres tipos de canles:

- Canle B. Os canles tipo B transmiten información en modo circuíto ou en modo paquete a 64Kbps e empréganse para transportar calquera tipo de información de usuario, ben sexa voz ou datos.
- Canle D. Utilízase principalmente para enviar información de control, como é o caso dos datos necesarios para establecer unha chamada ou para liberala. Estes canles traballan a 16Kbps ou 64kbps según o tipo de servizo contratado.
- Canles H. Combinando varios canles B obtéñense canles tipo H, que tamén son canles para transportar só información de usuario pero a velocidades moito maiores. Hai varios tipos de canles H:
  - Canles H0, que traballan a 384Kbps (6 canles B).
  - Canles H10, que traballan a 1472Kbps (23 canles B).
  - Canles H11, que traballan a 1536Kbps (24 canles B).
  - Canles H12, que traballan a 1920Kbps (30 canles B).

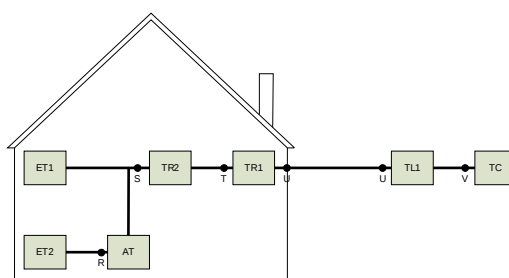
Un usuario pode contactar dous tipos de servizo diferentes co provedor telefónico según as súas necesidades:

- Acceso básico ou BRI (Basic Rate Interface). Proporciona dous canles B e un canle D.
- Acceso primario ou PRI (Primary Rate Interface). En Europa o PRI consta de 30 canles B e un canal D. Neste caso, os canles B tamén poden estar agrupados como 5 canles H0 ou un canle H12.

A RDSI ofrece a capacidade de agregar canles para realizar conexións a maior velocidade.

Nun acceso básico unha chamada a 128Kbps son en realidade dúas chamadas diferentes a 64Kbps cada una, existindo un protocolo por encima que permite ver esa chamada como unha soa. Moitos fabricantes de hardware para RDSI permiten a agregación de canles utilizando protocolos propios. Para garantir a compatibilidade entre equipos de diversos fabricantes é conveniente que o hardware soporte o protocolo MPPP (Multilink Point to Point Protocol).

A configuración de referencia defínese por agrupacións funcionais e puntos de referencia ou interfaces, como se mostra na figura:



As agrupacións funcionais son:

- TC (Terminación de Central). Situada na central de conmutación, encargase do mantemento do Acceso do Usuario.
- TL (Terminación de Liña). Situada na central, encargase dos aspectos de transmisión.
- TR1 (Terminación de Rede nº 1). Dispositivo fronteira que separa as instalacións de usuario das da rede e converte os dous fíos da interface U nos catro fíos empregados nunha interface T ou S/T.

Sempre o proporciona o provedor do servizo. En xeral, realiza funcións do nivel físico.

- TR2 (Terminación de Rede nº 2). Converte a interface T nunha interface S. Fai referencia a unha centraliña ou PABX (Private Automatic Branch Exchange). No acceso básico o TR2 non existe, co que o punto de referencia S e o T coinciden, pasándose a chamar este punto S/T.
- ET1 (Equipo Terminal nº 1). É un terminal específico para RDSI, preparado para a sinalización en modo paquete e xestión de canles de información.
- AT (Adaptador de Terminal). Trátase dun equipo RDSI que ten a capacidade de adaptar interfaces. Converte os sinais doutros equipos non RDSI a sinais adecuadas á interface correspondente, S e/ou T.
- ET2 (Equipo Terminal nº 2). Equipos non RDSI que poden conectarse mediante un AT ó bus RDSI.

Os Puntos de Referencia ou interfaces son:

- V. Representa a separación entre as funcións de conmutación e transmisión na central.
- U. Nun acceso básico está formado pola liña típica de un par trenzado de fíos procedente da rede telefónica. Nun acceso primario está formado por una liña de cable coaxial ou fibra óptica que se soe conectar directamente a unha central local de distribución ou PABX que actúa como TR2.
- T. Representa a separación entre a transmisión de liña e a transmisión no domicilio do cliente. Consta de catro fíos, dous para recibir e dous para enviar datos, permitindo tamén unha conexión full dúplex.
- S. Representa a interface de conexión física dos equipos terminais RDSI e define a estrutura da trama, a xestión do Canle D, a sincronización e as características de transmisión.
- R. Representa unha interface non normalizada en RDSI.

A RDSI estruturase en tres capas: física, de enlace e rede:

- Física. As funcións máis destacadas deste nivel son a codificación de datos dixitais para a transmisión a través da interface correspondente, transmisión full dúplex, formación da trama, activación e desactivación do circuíto físico, etc.
- Enlace. Este nivel emprega principalmente o protocolo LAP-D (Link Access Protocol ou protocolo de acceso ó enlace). Proporciona ó nivel superior un servizo orientado a conexión con transferencia de información confirmada, servizo sen conexión con transferencia de información non confirmada e servizos de administración, que permiten identificar os equipos específicos dentro do bus S/T asociado a unha conexión RDSI.
- Rede. Nesta capa, a Recomendación Q.931 especifica os procedementos para establecer, manter e liberar as conexións no interface usuario-rede. Manéxanse distintos tipos de mensaxes: de establecemento de chamada, durante a fase de transmisión de información, de liberación da chamada e outros.

#### **47.1.1.3 RDSI DE BANDA ANCHA**

A RDSI de banda ancha representa un termo medio entre a conmutación de circuítos pura e a conmutación de paquetes pura. O servizo ofrecido está orientado a conexión, pero internamente implementase con conmutación de paquetes. A RDSI-BA está baseada na tecnoloxía ATM. As razóns que levaron a elixir esta tecnoloxía foron, entre outras, que permite manexar tanto tráfico de velocidade constante como variable e que, a velocidades altas, a conmutación dixital de celdas é mais fácil que as técnicas tradicionais de multiplexación. As velocidades acadables por de RDSI-BA dependen das tecnoloxías concretas usadas na rede e van dende un mínimo de 2 Mbps ata os 155 ou 622Mbps.

En ATM, o fluxo de información organizase en bloques de tamaño fixo e pequeno (53 bytes), chamados celdas. Non se garante a entrega de tódalas

celdas, pero as que chegan fano en orde. O modelo ATM tamén se divide en capas:

- Capa física. Ten que ver co medio físico. Divídese en dúas subcapas: PDM (Physical Medium Dependent) e TC (Transmisión Convergence).
- Capa ATM. Ten que ver coas celdas e o seu transporte.
- Capa de adaptación de ATM (AAL, ATM Adaptation Layer). Permite os usuarios enviar paquetes maiores que unha celda. Divídese en dúas subcapas: SAR (Segmentation And Reassembly) e CS (Convergence Sublayer).

ATM tratarase noutro tema máis en detalle.

#### **47.1.1.3.1 SERVIZOS RDSI-BA**

Na RDSI de Banda Ancha pódense incorporar distintos tipos de servizos que podemos clasificar en servizos interactivos e servizos de distribución.

Dentro dos servizos interactivos podemos encontrar:

- Servizos conversacionais, coma poden ser:
  - o Videoconferencia
  - o Videovigilancia
  - o Fax de alta velocidade
  - o Transferenza de documentos
- Servizos de mesaxería:
  - o Video-mail
  - o Correo con contido multimedia
- Servizos de consulta:
  - o Videotex
  - o Recuperación de datos, documentos, etc.

Exemplos de servizos de distribución poderían ser:

- Servizos sen control de presentación:
  - o Televisión
  - o Televisión a la carta
  - o Distribución de documentos



- o Vídeo baixo demanda
- o ...
- Servizos con control de presentación:
  - o Vídeo

#### **47.1.2 XDSL**

Unha Digital Subscriber Line (DSL) é o nome que identifica a tódolos estándares dixitais sobre bucle de abonado, en exemplo é a RDSI. Pola súa parte xDSL identifica un conxunto de estándares para bucle de abonado sobre fío de cobre como son (entre outras):

- ADSL (Asymmetrical Digital Subscriber Line)
- SDSL (Symmetrical Digital Subscriber Line)
- HDSL (High data rate Digital Subscriber Line)
- VDSL (Very high rate Digital Subscriber Line)

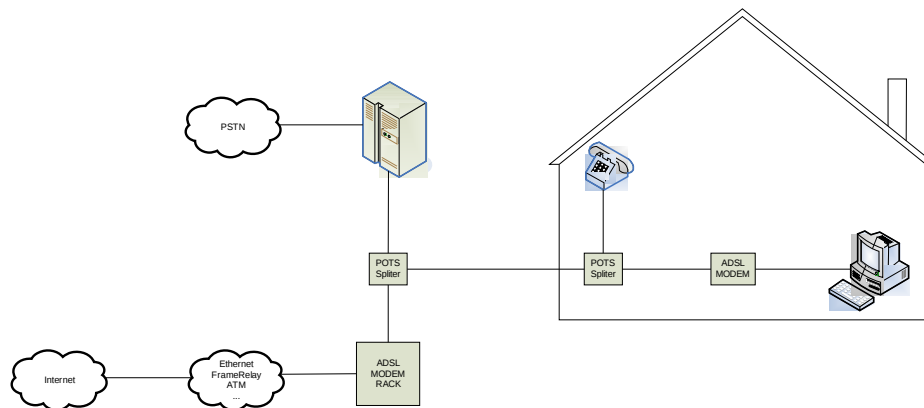
##### **47.1.2.1 ADSL**

Proporciona servizos dixitais de alta velocidade sobre redes de pares de cobre existentes. Permitindo traballar sen interferir cos tradicionais servizos de voz analóxica (POTS Plain Old Telephone Service).

Utiliza técnicas eficientes de codificación de liña como QAM. E Soporta novos servizos sobre un par trenzado simple, como o acceso a Internet de alta velocidade.

O seu ancho de banda asimétrico (64-640 kbit/s upstream, 500 kbit/s - 8 Mbit/s downstream) faina atractiva para a maioría das aplicacións cliente/servidor como o acceso a Web, acceso a LAN remotas, onde tipicamente o cliente recibe moita mais información do servidor da que xenera.

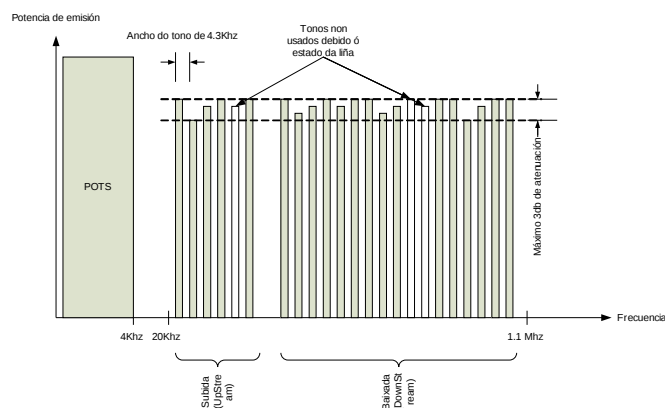
##### **47.1.2.1.1 ARQUITECTURA ADSL**



A arquitectura de ADSL fai uso de filtros tanto no domicilio do abonado coma na central para separar o sinal do teléfono e da conexión de datos, estes filtros chámanse splitters. No domicilio do abonado o teléfono conéctase directamente a saída correspondente do splitter mentres que os equipos de transmisión de datos necesitarán un MODEM ADSL. Na central a saída do splitter correspondente conéctase á PSTN (Public Switching Telephone Network ou RTC) mentres que a saída de datos conéctase a un dos modems da central que está conéctado á rede de distribución que a súa vez está conéctada a Internet.

#### 47.1.2.1.2 NIVEL FÍSICO

A canle divídese en tres bandas diferentes, utilízase DMT (Discrete Multi-Tone) que permite utilizar diferentes portadoras (codificadas en QAM) en distintas frecuencias:



DMT utiliza a codificación QAM para conseguir codificar mais bits en frecuencias

onde o sinal presenta menos interferencias. Desta forma modúlanse un número variable de bits en cada unha de esas portadoras, dependendo este número das características do cable de pares, do espectro de frecuencias e das interferencias na sinal. Deste modo, os rateos de velocidade poden ser optimizados facendo posible o uso do mesmo modem sobre bucles locais con diferentes características.

A velocidade de baixada dependen dun bo número de factores, entre eles:

- Lonxitude da liña de cobre.
- Sección do cable.
- Presencia de bobinas de carga, por atenuación en liñas analóxicas.
- Interferencias por paradiafonía.

O alcance depende da velocidade e vai dende 2,7 Km (á máxima velocidade no peor caso) ata 5,5km (á baixa velocidade no mellor caso). Actualmente este estándar evolucionou existindo ADSL2 e ADSL2+ que proporcionan maior velocidade (12 Mb no caso de ADSL2 e 24Mb no caso de ADSL2+) simplemente usando mais espectro de frecuencias.

#### **47.1.2.2 HDSL**

HDSL é simplemente unha forma mellor de transmitir circuítos T1 ou E1 (32 canles de

64 Kbs) sobre liñas de pares de cobre. Necesita un menor ancho de banda para transmitir estas liñas e non necesita utilizar repetidores.

Utilizando avanzadas técnicas de modulación, HDSL transmite 1,544 Mbps ou 2,048 Mbps utilizando rangos de frecuencia entre 80 kHz e 240 kHz, bastante menos cos 1,5 MHz necesarios para as E1/T1 tradicionais.

Sobre un cable con un calibre 24 AWG (0,5 mm) a distancia que se pode alcanzar é de aproximadamente 3,7 Km, aínda que pode chegar os 4,5 Km, sempre sobre dous pares de cobre.

Este tipo de tecnoloxía utilízase para conexións entre PBX, conexións entre estacións de antenas celulares, circuítos dixitais, servidores de Internet e

Redes de Datos Privadas. Pero non está falta de problemas, sendo os mais destacables:

- A existencia de gran cantidade de implementacións propietarias de HDSL pois o estándar só contempla as características básicas.
- Os beneficios técnicos son transparentes ós usuarios, pois eles seguen percibindo unha T1/E1 aínda se poderían alcanzar mellores rendementos en termos de velocidade e de custes.
- Para distancias maiores de 3,7 Km necesítanse repetidores.
- A necesidade de utilizar múltiples pares de fíos, reduce a dispoñibilidade do servizo T1/E1 nun área determinada entre un 50 y 66 por cento. Ademais, moitas veces existen problemas para encontrar 2 ou 3 pares libres dentro da mesma ruta.

Ó igual que con ADSL, HDSL evolucionou tratando de eliminar os problemas da primeira xeración a HDSL2 que simplemente usa menos fíos.

#### **47.1.2.3 SDSL**

SDSL (Symmetrical Digital Subscriber Line) pode referirse a:

- Nun sentido amplo a calquera tecnoloxía DSL simétrica
- Ou a un estándar concreto que proporciona servizos T1/E1 (o caso que nos ocupa)

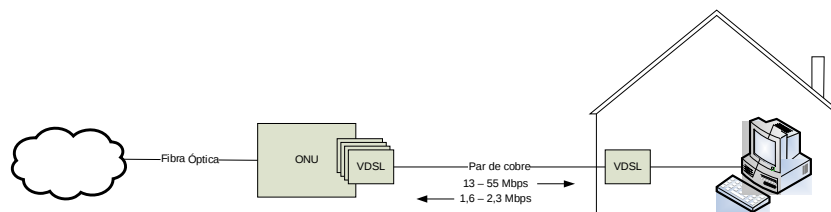
SDSL permite a transmisión de sinais T1 o E1 sobre un único par de cobre. Isto supón unha gran vantaxe sobre HDSL posto que se poden usar liñas individuais estendéndose o servizo a domicilios particulares.

A distancia máxima de SDSL é de 3 Km, distancia á que un ADSL podería operar a 6 Mbps.

#### **47.1.2.4 VDSL**

É unha das máis recentes tecnoloxías da familia xDSL, confía en que o tendido de cobre será curto xa que as operadoras están instalando cada vez máis tramos de F.O. (Fibra Óptica). Xa que as operadoras queren ofrecer novos servizos que requiran a combinación de voz, vídeo e audio, o cal, só é posible con transportes como o ofrecido por ATM. VDSL está preparado para actuar como capa física que dé soporte a redes ATM. Para

logralo, VDSL inclúe unha unidade de rede óptica (ONU) que se encarga de converter e concentrar sinais VDSL sobre unha rede de fibra.



Problemas de VDSL:

- É moi sensible ás interferencias de radio. Ás frecuencias ás que traballa, un bucle de abonado comportase como unha antena receptora para este tipo de sinais.
- VDSL foi deseñada para traballar sobre redes ATM.
- ADSL ten un custe moito menor, pois os filtros poden instalarse na propia central local. Con VDSL necesítanse ONU residenciais que deben ser instalados e mantidos pola operadora.

O igual que coas tecnoloxías xDSL anteriores VDSL ten a súa evolución en VDSL2 capaz de proporcionar 250Mbps de baixada.

## **47.2 REDES DE TELEFONÍA MÓBIL**

### **47.2.1 GSM**

A tecnoloxía GSM pertence ós sistemas de segunda xeración, que ó igual que outros como CDMA, TDMA, NADC ou PDC caracterízanse porque son dixitais. GSM implantouse en Europa e en outros países do resto do mundo, mentres que TDMA e CDMA implantouse en EEUU, e PDC en Xapón.

GSM utiliza multiplexación por división do tempo (TDM), o que posibilita que en cada frecuencia se podan transmitir varias conversas; o tempo de transmisión divídese en pequenos intervalos de tempo, cada un dos cales pode ser utilizado por unha transmisión distinta. Ademais, unha mesma conversa levase a cabo en intervalos de distintas frecuencias, co que non se pode asociar unha chamada a unha frecuencia. Isto ten a vantaxe de que se unha das frecuencias vese afectada por unha interferencia, unha conversa que utilice esta frecuencia só observará problemas nos intervalos pertencentes a dita frecuencia. Isto denomínase TDMA.

O sistema GSM ten asignadas dúas bandas de frecuencias, 900 Mhz (chamado GSM-900) e 1800 Mhz (chamado DCS-1800). En cada unha das bandas, as frecuencias mais baixas úsanse para o enlace ascendente e as mais altas para o descendente. Así, na banda dos 900 Mhz, as frecuencias comprendidas entre los 890 e 915 Mhz comprenden 125 portadoras, cada unha delas con un ancho de banda de 200 Khz para transmisións mobil-estación base. Da mesma maneira, a banda comprendida entre os 935 e os 960 Mhz subdivídese en outras 125 portadoras de 200 Khz para transmisións estación base-mobil.

Ademais, existe tamén unha terceira banda de frecuencia nos 1900 Mhz, nos que GSM opera nalgúns países como EEUU.

Cada portadora subdivide en 8 canles lóxicos ou slots, cada un deles ten o seu uso particular: sinalización, control da comunicación ou tramas de información.

En GSM, a sinalización realizase pola canle común, segundo o protocolo SS7.

GSM é un sistema baseado en conmutación de circuítos e por tanto é un servizo orientado a conexión, é dicir, en toda comunicación haberá 3 etapas diferenciadas: establecemento, comunicación e liberación. En GSM, o que se tarifica precisamente é o establecemento dun canle.

A taxa de transmisión que se alcanza con GSM é de 9'6 Kbps.

#### **47.2.1.1 ARQUITECTURA DA REDE GSM**

A arquitectura GSM basease en tres subsistemas diferenciados:

- Subsistema estación base (BSS): Agrupa as máquinas específicas aos aspectos de radio e celulares do GSM. O BSS está en contacto directo cás estacións móbiles a través do interface radio. O BSS inclúe dous tipos de elementos: a Estación de Base (BTS, Base Transceiver Station) e o Controlador de Estaciones de Base (BSC, Base Station Controller).
- Subsistema conmutación (NSS): Inclúe as funcións básicas de conmutación do GSM, así como as bases de datos necesarias para os

datos de usuario e a xestión da mobilidade. A función principal do NSS é xestionar as comunicacións entre os usuarios GSM e os usuarios doutras redes de telecomunicación. Dentro do NSS, a función básica de conmutación realizase na MSC (Mobile services Switching Centre), cuxa misión principal é coordinar o establecemento de chamadas dende e ata usuarios GSM.

- Subsistema operación e mantemento (OMS): Controla e monitoriza o estado xeral da rede. Componse dos seguintes elementos:
  - o HLR: Home Location Registry. Existe un so HLR por compañía. Nesta base de datos gárdase a información estática do abonado (servizos contratados, etc) e dinámica (ónde se localiza o móbil nun determinado momento)
  - o EIR: base de datos utilizada para comprobar a pertenza do dispositivo móbil á rede do operador, mediante o chequeo do número IMEI, que é un código que identifica univocamente o móbil, unha especie de número de serie do aparato.
  - o AUC: centro de autenticación de usuarios
  - o OMC: Centro de xestión da rede (mantemento)

#### **47.2.2 GPRS, HSCSD**

GPRS y HSCSD pertencen aos denominados sistemas da xeración 2'5, que farán de ponte entre os de segunda e terceira xeración (UMTS, que se verá mais adiante).

##### **47.2.2.1 GPRS**

GPRS significa "General Packet Radio Service". Como o seu nome indica, tratase dun servizo portador baseado na conmutación de paquetes, que se realiza utilizando a rede GSM actual, aínda que necesita terminais que a soporten.

As principais características de GPRS son as seguintes:

- Velocidade: a velocidade máxima teórica é de 171'2 Kbps, aínda que se fala dunha velocidade de conexión máxima na práctica de 115 Kbps.

- Inmediatez: GPRS facilita as conexións instantáneas tan pronto como se necesita enviar ou recibir información; pódese dicir que con GPRS estamos sempre conectados.
- Novas e mellores aplicacións: grazas á maior velocidade de GPRS.
- Tarificación: GPRS tarifícase por volume de datos intercambiado, calidade de servizo e tipo de servizo; en GSM polo contrario tarifícase por duración da chamada.

#### **47.2.2.1.1 ARQUITECTURA DE GPRS**

Coma dixemos anteriormente, o sistema GPRS despregase sobre a rede GSM existente, aínda que require dalgúns elementos novos coma:

- O nodo GGSN (Gateway GPRS Support Node): este nodo é a interface coas redes de datos externas, como X.25 e as redes IP
- O nodo SGSN (Serving GPRS Support Node): nodo de conmutación de paquetes, ó mesmo nivel que as centrais convencionais de GSM (as MSC)
- Estructura principal ou rede troncal GPRS (backbone)

#### **47.2.2.1.2 EDGE OU E-GPRS**

EDGE responde ás siglas de Evolved (ou Enhanced) Data rates for GSM Evolution. Non é en sí una nova arquitectura, se non unha mellora da modulación do canle, é dicir, é unha versión mellorada de GPRS.

Con estas técnicas conséguense ata 384 Kbps, combinando ata 8 slots.

#### **47.2.2.2 HSCSD**

HSCSD (High Speed Circuit Switched Data) é unha especificación homologada polo ETSI (European Telecommunication Standard Institute), que supón unha evolución de GSM, xa que aproveita dita infraestrutura.

Trátase dun servizo multi-slot para a transmisión de datos a alta velocidade mediante circuitos conmutados.

O HSCSD aporta un esquema de codificación mellorado que permite 14'4 Kbps, fronte ós 9'6 Kbps de GSM, o cal posibilita velocidades de transmisión de datos de ata 57'6 Kbps combinando ata 4 canles GSM.



HSCSD foi desenvolvido en paralelo con GPRS pero son servizos de alta velocidade totalmente diferentes. Como o seu propio nome indica HSCSD utiliza a conmutación de circuitos a diferenza de GPRS que utiliza a conmutación de paquetes.

A vantaxe de HSCDS sobre GPRS é a calidade de servizo garantida, proporcionada pola canle de comunicación dedicado. Isto, sen embargo, faina menos eficiente para a transmisión de datos pois a conexión ten que manterse incluso nos momentos nos que non existe transmisión de datos. GPRS fai un uso máis eficiente do ancho de banda e permite facer a tarificación en función da cantidade de contido que se recibe e non só en función do tempo de conexión.

#### **47.2.3 SISTEMAS DE TERCEIRA XERACIÓN: UMTS**

UMTS é o terceiro escalón na historia da telefonía móbil, despois da analóxica e a dixital. UMTS son as siglas de Universal Mobile Telecommunication System ou Sistema Universal de Comunicaciones Móviles. UMTS é un membro da familia global IMT-2000 do sistema de comunicacións móbiles de “terceira xeración” do UIT (Unión Internacional de Telecomunicacións). Este sistema é revolucionario xa que por primeira vez trátase dun estándar universal.

O funcionamento tamén é novedoso, xa que o usuario paga segundo a cantidade de información que se descargue da rede, e non xa polo tempo de uso do servizo. Desta forma poderemos estar constantemente conectados á rede, o que permite, por exemplo, acceder ó correo electrónico de forma instantánea.

Esta tecnoloxía permite que os teléfonos transmitan e reciban datos con una velocidade 200 veces superior á de GSM. A máxima velocidade do UMTS é 2 Mbits. Este tope pode alcanzarse soamente se a rede está ó máximo nivel, o usuario está parado e sen móbiles o seu arredor.

UMTS tamén plantexa importantes innovacións con respecto á arquitectura de rede. UMTS R'99 definiu unha arquitectura que dá cabida a redes de acceso GSM e a rede de acceso UMTS (UTRAN), e propón unha rede central

(CN, Core Network) deseñada como unha evolución da rede GSM/GPRS para facilitar a migración de redes GSM/GPRS a UMTS.

UMTS ofrece un novo interface radio denominado UTRA (UMTS Terrestrial Radio Access). Dito interface está baseado en tecnoloxía CDMA (Code Division Multiple Access) permitindo aumentar considerablemente a velocidade de transferencia de datos, e soporta dous modos de operación el FDD (Frequency Division Duplex) e o TDD (Time Division Duplex). FDD está baseada nun esquema de Secuencia Directa CDMA e soporta unha velocidade de ata 384 Kbit/s. O TDD está baseado na multiplexación en tempo e en código, deseñouse e optimizouse para ser usado en zonas con alta densidade de tráfico, e soporta unha velocidade de ata 2 Mbit/s.

Entre as cousas que nos ofrece UMTS, destacamos a súa facilidade de uso e baixos custes, novos e mellores servizos, acceso rápido, transmisión de paquetes de datos e velocidade de transferencia de datos a pedido, entorno de servizos amigable e consistente, mobilidade e cobertura e servizos UMTS dispoñibles globalmente por satélite.

A súa velocidade sumada ó soporte inherente do Protocolo de Internet (IP), combínanse para prestar servizos multimedia interactivos e novas aplicacións de banda ancha, tales como servizos de vídeo telefonía e videoconferencia.

#### **47.2.3.1 HSPA**

High-Speed Downlink Packet Access (HSDPA) é un protocolo mellorado da terceira xeración que pertence á familia High-Speed Packet Access (HSPA) tamén coñecida como 3.5G, 3G+ ou turbo 3G. HSDPA permite ás redes UMTS ter un ancho de banda de descarga maior que actualmente pode ser de 1,8, 3,6, 7,2 e 14,4 Mbps. Xa está dispoñible tamén HSPA+ que entrega ata 84Mbps gracias ó uso de varias antenas (MIMO Multiple Input Multiple Output).

High-Speed Uplink Packet Access (HSUPA) é outro dos protocolos HSPA que permite unha velocidade de subida de 5,76Mbps. O nome HSUPA foia cuñado por Nokia, o nome oficial é Enhanced Uplink (EUL).

### **47.3 CABLE**

As redes de cable actuais presenta as seguintes características: servizos integrados, alta capacidade, e redundancia. Os servizos que ofrece unha rede de cable moderna inclúen os seguintes: amplía oferta de canles de TV (terrestres, vía satélite, e de produción propia), vídeo a la carta, PPV, datos e Internet (mediante módem cable), telefonía (básica e RDSI, con opción de acceso a Internet), aluguer de liñas e fibras.

A transmisión do sinal ata o abonado levase a cabo mediante o canle denominado descendente ou directo (de 86 a 862 MHz), mentres que as que parten do abonado realízanse a través do canle ascendente ou de retorno (de 5 a 65 MHz).

A topoloxía dunha rede de cable baseada en tecnoloxía HFC (Hybrid fibre-coaxial):

- Rede troncal primaria: a nivel físico aneis redundantes de fibra óptica, a nivel lóxico topoloxía de estrela. Estes aneis comunican a cabeceira cos nodos primarios. O respaldo é activo.
- Rede secundaria ou de distribución: conecta un nodo primario con varios nodos secundarios a través de aneis con arquitectura en estrela formando lóbulos que abarcan 12.000 fogares. Cada lóbulo interconecta 5 ou 6 nodos secundarios. Hai redundancia en ruta e equipos. O servizo de telefonía a veces non se proporciona mediante a rede HFC (é dicir, no presenta telefonía integrada), se non que fai uso dunha rede paralela de tipo SDH (Synchronous Digital Hierarchy), falándose entón de telefonía superposta.
- Rede terciaria ou de dispersión: conecta cada nodo secundario con cada un dos catro nodos ópticos terminais que dependen del. Cada nodo óptico terminal cubre un área de 500 fogares. A rede de dispersión presenta una disposición en estrela sen redundancia en ruta. No nodo secundario realízase a interconexión das fibras provintes do nodo primario coas fibras que van ata os nodos terminais.

- Rede de distribución de coaxial: distribúe as sinais desde o nodo óptico terminal ata cada punto de derivación nos edificios aos que da servizo. A distribución realízase con estrutura en árbore, de forma que cada nodo óptico terminal da lugar a 4 ramas duns 125 fogares aproximadamente. Os nodos ópticos terminais ubícanse fisicamente en armarios de exterior. O nodo óptico terminal realiza a conversión óptico-eléctrica dos sinais transportadas en sentido descendente. De el vai aos amplificadores que atacan as catro ramas de coaxial que parten do nodo óptico. Cada rama de coaxial alimenta (se é necesario, mediante amplificadores) a unha rede de derivadores, cuxas saídas están conectadas ás acometidas individuais de abonado. Para o camiño de retorno utilízase a mesma infraestrutura de rede, equipando adecuadamente aos amplificadores.
- Rede de acometida de abonado: conecta a rede de distribución de coaxial co punto de terminación de rede. Existen dúas arquitecturas:
  - o Estrela: un mesmo derivador da servizo a tódalas vivendas das diferentes plantas dun edificio.
  - o Árbore: colócase un derivador en cada planta, do que parten os coaxiais que dan servizo aos abonados desa planta.A rede de acometida de abonado pódese dividir en dúas partes: cableado de edificio ou verticais, e cableado de vivenda.

As redes HFC teñen os seguintes puntos singulares:

- Cabeceira: está equipada para a prestación do servizo de difusión de televisión. Pódese descompoñer en catro bloques:
  - o Sistemas de recepción e transmisión analóxica: composto por antenas de recepción, equipos de recepción, equipos para banda base, etapa de codificación, e etapa de modulación e saída.
  - o Sistemas de recepción e transmisión analóxica de reserva: antenas de recepción, equipos de recepción, e etapa de modulación.
  - o Sistemas de monitorización.

- o Sistemas de transmisión óptica.
- Nodo primario: recibe o sinal da rede troncal primaria provinte da cabeceira de rede. O nodo primario presenta dous módulos independentes:
  - o O módulo do camiño descendente.
  - o O módulo do camiño ascendente.
- Nodo secundario: encamiñan os sinais procedentes do nodo primario (mediante a rede troncal secundaria) ata os nodos ópticos terminais (a través da rede terciaria). Ubicanse fisicamente nunha arqueta, habitualmente xunto a un dos seus nodos ópticos terminais.
- Nodo óptico terminal: dan servizo a áreas de aproximadamente 500 fogares. Ubicanse en armarios de exterior. Pódense descompor en dous grandes bloques:
  - o Canle descendente.
  - o Canle ascendente.
- Terminal direccionable de abonado: permite ó cliente acceder aos servizos TV da rede e é instalado no propio domicilio do abonado. Descodifica os canles correspondentes ó servizo contratado polo abonado e permite o cliente interactuar co sistema.
- Subredes de telefonía e datos:
  - o Subred de datos:
    - Servizos ofrecidos: portadores (aluguer de circuítos dixitais), de transmisión de datos (baséanse en conmutación de circuítos e conmutación de paquetes ou celdas), de acceso a redes (acceso a Internet e a outros provedores de contido multimedia ), e de valor engadido.
    - Estructura: os equipos que conectan a rede de datos con Internet están situados na cabeceira. O nodo primario que reside xunto a esta é o encargado do funcionamento dos módems cable, a través dos cales o abonado ten acceso á rede. Os seus elementos son:

- Router: encamiña o tráfico IP entre a rede de datos e Internet.
  - Servidor Proxy: actúa a modo de caché.
  - Firewall (cortafuegos): protexe a rede de datos de ataques externos.
  - Servidores: encárganse de dar diversos servizos: WWW, FTP, IRC, e-mail, DNS, etc.
  - Conmutador ATM multiservizo: permite a interconexión de equipos de diferentes tecnoloxías.
  - Conmutador LAN: conecta os servidores co conmutador ATM multiservizo.
  - Conmutador ATM de acceso: como o conmutador ATM multiservizo , pero de menor capacidade.
  - Cabeceira de modems cable: a cabeceira de modems e os modems cable, compoñen a rede de acceso a datos integrada en HFC.
  - Modems cable: sitúase no domicilio do abonado, e permite acceso á rede de datos mediante HFC.
- o Rede de telefonía:
- Servizos ofrecidos: telefonía analóxica tradicional, acceso dixital RDSI básico, acceso dixital RDSI primario.
  - Estructura: A rede soporta tanto telefonía integrada como superposta.
    - Centro de conmutación: canaliza todo o tráfico de chamadas.
    - Rede de acceso mediante telefonía integrada: aproveita a rede HFC de distribución de TV e datos para chegar ata o cliente. Para realizar o interface coa rede HFC, son necesarios dous equipos específicos (HDT y MDU).
    - Rede de acceso mediante telefonía superposta: non usa a rede HFC. Dende a cabeceira distribúese o sinal, mediante

fibra óptica ata os nodos primarios, e dende eles, ata os lóbulos de 12.000 fogares da rede SDH.

- Cableado de vivendas.

#### **47.4 PLC**

A tecnoloxía Power Line Communications, "PLC", posibilita a transmisión de voz e datos a través dos cables eléctricos, convertendo calquera enchufe da casa en conexión potencial a tódolos servizos de telecomunicacións. O cliente só necesitará conectar un pequeno módem para acceder a Internet, telefonía e datos ó mesmo tempo e a alta velocidade (banda ancha).

A rede eléctrica transporta electricidade a unha frecuencia de 50 Hz. En PLC engádense frecuencias na banda que vai dende 1,6MHz ata 30MHz para o transporte dos datos. Uns filtros instalados no transformador de baixa tensión separan as frecuencias altas de datos, da frecuencia de 50Hz da electricidade.

Power Line Communications emprega unha rede coñecida como High Frequency Conditioned Power Network (HFPCN) para transmitir simultaneamente enerxía e información. Unha serie de unidades acondicionadoras son as que se encargan do filtrado e separación de ambos sinais.

Na actualidade non existen estándares tecnolóxicos para o PLC de acceso. Este é un dos principais problemas desta tecnoloxía, ó non permitila interoperabilidade entre os equipos suministrados polos distintos fabricantes. Tampouco existía unha regulación en canto á utilización de frecuencias, ata o 2005. Garantindo agora a coexistencia de sistemas domésticos (como HomePlug) e as tecnoloxías de acceso.

É posible que o prezo da tecnoloxía PLC sexa bastante inferior ó dos actuais ADSL e Cable no mesmo rango de velocidades o que a converte nunha tecnoloxía interesante.

Os servizos típicos de telecomunicacións que poderían ser proporcionados son:

- Telefonía

- Acceso rápido a Internet
- Vídeo baixo demanda

#### Vantaxes de PLC:

- Como a PLC posicionouse coma un servizo de tipo IP utilizará routers de paquetes en vez dos de conmutación de circuítos típicos, dos subministradores de telecomunicacións tradicionais, mantendo así os custes dos equipos de IT baixos.
- As compañías eléctricas poderían pois comercializar un servizo básico de conexión a Internet con unha suscripción mensual de tarifa plana.
- Esta tecnoloxía ponse virtualmente ó alcance de calquera,
- Xa existen varias tecnoloxías que transforman os cables eléctricos existentes nun cableado LAN (Local Area Network)
- PLC podería facilitar ás compañías eléctricas a oportunidade de ofrecer servizos de valor engadido.

#### Inconvenientes de PLC:

- O número máximo de fogares por transformador. Como os sinais de datos de Power Line non poden sobrevivir o seu paso por un transformador, só se utilizan na última milla. O modelo europeo de rede eléctrica soe colocar un transformador cada 150 fogares aproximadamente.
- Polo que é necesario que tódolos transformadores veñan dotados de servidores de estación base PowerLine.
- Calquera liña conductora é, por definición, unha antena polo que a instalación eléctrica dunha casa actúa como tal, e é moi sensible ás interferencias que se produzan nas frecuencias de transmisión de datos, o redor dos 30 MHz.

## **47.5 REDES RADIO (LMDS, WIMAX),**

### **47.5.1 LMDS**

LDMS nace no contexto das emerxentes tecnoloxías sen fíos e a crecente interese en IP como unha alternativa para proporcionar servizos multimedia



ó usuario final, xunto co aumento da demanda de novos servizos de telecomunicación orientados a voz y datos (acceso rápido a Internet, etc) LDMS (Local Multipoint Distribution Service) é unha tecnoloxía de acceso sen fíos de banda ancha ou bucle de abonado sen cable. Os sistemas LDMS utilizan ondas radioeléctricas de alta frecuencia para ofrecer servizos multimedia e de difusión a usuarios finais en distancias similares ás alcanzadas coas tecnoloxías de cable.

Entre as vantaxes que ofrece LDMS podemos sinalar:

- Rápido despregue, comparado coas tecnoloxías de cable: LDMS permite instalar redes rapidamente xa que, por exemplo, o emprazamento das antenas é moi sinxelo dado o pequeno tamaño destas.
- Posibilidade de integrar distintos tipos de tráfico (voz, vídeo, datos,...)
- Alta velocidade de acceso a Internet
- Flexibilidade y modularidade

Como outras características de LDMS, podemos sinalar que require LoS (Line of Sight), é dicir, visión directa entre os dous puntos que se comunican. As velocidades de acceso que se alcanzan encóntranse no entorno dos 512 Kbps - 2 Mbps.

O servizo LDMS prestase en dúas bandas:

- Banda S: esta banda traballa nos 3,5 GHz. É a que se utiliza para o despliegue do bucle de abonado. Ten un alcance de o redor de 15 Km e posúe un ancho de banda de 20 Mhz.
- Banda K: traballa nos 26 GHz. É a banda utilizada para o acceso de banda ancha. Dispón dun alcance menor que a banda S (o redor de los 3 Km), pero un maior ancho de banda (uns 56 Mhz).

A comunicación en LDMS establececese mediante radiodifusión punto-multipunto: os sinais viaxan dende ou ata unha estación central, ata ou dende os diferentes puntos de recepción distribuídos na zoa de cobertura. LDMS utiliza modulación QPSK (Cuadratura Phase Shift Keying), que permite reducirlas interferencias e aumentala reutilización do espectro, alcanzando un ancho de banda cercano a 1 Gbps.

### **47.5.2 WIMAX**

WiMAX (Worldwide Interoperability for Microwave Access) é un protocolo de telecomunicacións que provee acceso a Internet en puntos fixos ou móbiles.

A actual revisión de WiMAX permite ata 40Mbps, coa nova versión (IEEE 802.16m) se esperan velocidades de ata 1 Gbps.

O nome WiMAX foi creado polo WiMAX Forum que foi fundado en xuño de 2001 para fomentar a interoperabilidade do estándar. Este foro describe WiMAX como unha tecnoloxía baseada en estándares permitindo o acceso de banda ancha de última milla como alternativa ó cable e ás xDSL.

O estándar 802.16 Broadband Wireless Access (BWA) define:

- **Capa 1 - Capa física:** A versión orixinal de IEEE 802.16 especifica unha capa física que operan o rango entre os 10 e os 66Ghz. 802.16a (actualización do 2004) engadiu a posibilidade de operar entre 2 e 11 Ghz. En 2005 a versión 802.16e-2005 viu a luz usando SOFDMA (Scalable Orthogonal Frequency-Division Multiple Access) en vez da orixinal OFDM (Orthogonal Frequency División Multiplexing). 802.16e tamén define o uso de varias antenas con MIMO.
- **Capa 2 - Capa de acceso o medio (MAC):** Usa un algoritmo de planificación para o que a estación do abonado necesita competir só unha vez: para conectarse á rede. A ventá de tempo pode alargarse ou contraerse, pero permanece asigna ó abonado. O algoritmo é estable en situacións de sobrecarga e gran número de abonados permitindo á estación base o control da calidade do servizo (QoS).
- **Mobilidade**
- **Características opcionais e obrigatorias do enlace de radio**

### **47.6 SATÉLITE**

O acceso a Internet por satélite pode obterse en calquera parte do mundo usando satélites LEO (Low Earth Orbit) aportando unha relativamente baixa latencia pero baixa velocidade ou satélites geoestacionarios aportando maior velocidade pero tamén maior latencia e non podendo chegar a certas

partes dos polos. As desvantaxes deste sistema non se quedan ahí (alta latencia) se non que tamén inclúen problemas de cobertura cando chove, ademais require liña directa de visión ó satélite (nun terreo escarpado esto pode ser un problema).

O equipo do cliente para unha comunicación de satélite require a instalación dunha antena parabólica dun tamaño dependente da tecnoloxía concreta, do satélite e do modo en que se use (comunicación uni ou bidireccional, ...) ademais dun MODEM específico.

Existen distintas técnicas usadas para compartir cada portadora (TDMA, SCPC, ...) aportando velocidades de ata 40Mbps de descarga.

Os típicos modos de comunicación son:

- Comunicación bidireccional por satélite. Neste caso tanto a subida como a baixada prodúcese usando ó satélite, requirindo unha moi precisa orientación da antena.
- Comunicación unidirección mais conexión terrestre. Neste caso a antena só recibe o sinal do satélite, e o envío de datos prodúcese por unha liña terrestre (RTC, GSM, GPRS, ...). Ten a vantaxe sobre o modelo anterior de que a antena non necesita estar tan precisamente orientada e que, polo tanto, é mellor para instalación móbiles.
- Comunicación unidireccional / multicast, sen retorno. Dentro desta modalidade temos os servizos de multicast por IP que non requiren retorno (ademais da transmisión de audio e vídeo).

#### **47.7 LIÑAS PUNTO A PUNTO**

Unha liña punto a punto ou liña privada (coma contraposición a unha VPN) é unha liña física entre dúas ubicacións de forma transparente, de forma que unha liña punto a punto dende unha ubicación remota funciona da mesma forma que se estivese conectada na ubicación de destino.

Tradicionalmente cando se contrataba unha liña punto a punto especificábase as características e velocidade da mesma usando múltiplos do DS0, dende un DS0 (64Kbps) ata un T1/E1 (1,5Mbps) ou DS-3 (672

canles de 64Kbps). Os operadores usaban conmutación de circuítos ou circuítos virtuais con tecnoloxías coma X.25.

Na actualidade estas liñas sóense crear coma unha VPN dentro das redes do operador, por exemplo usando MetroEthernet e MPLS.

#### **47.7.1 X.25**

X.25 é un estándar para o acceso a redes públicas de conmutación de paquetes. Non especifica cómo está implementada a rede interiormente aínda que o protocolo interno soe ser parecido a X.25. Implementa un servizo de circuito virtual externo.

O servizo que ofrece é orientado a conexión, fiable, no sentido de que non duplica, nin perde nin desordena, e ofrece multiplexación, isto é, a través dun único interfaz mantéñense abertas distintas comunicacións.

Os elementos usados por X.25 denomínanse:

- DTE (Data Terminal Equipment): É o equipo final de usuario (PC con placa X.25 por exemplo).
- DCE (Data Circuit Terminating Equipment): Podemos interpretalo coma un nodo local. A nivel de enlace (LAPB) as conexións establécense DTE-DCE. Co nivel de rede, ampliamos as comunicacións mais ala do DCE, que fai de interconexión.

X.25 define 3 niveis:

- Nivel Físico:

Existen dúas posibilidades:

- X.21: Utilízase para o acceso a redes de conmutación dixital. (Similares ás de telefonía dixital.)
- X.21bis: Empregase para o acceso a través dun enlace punto a punto. (Similar a RS-232 en modo síncrono.)

En canto as características mecánicas, úsanse conectores Canon de 15 pines ou de 25 pines.

As velocidades van entre os 64kbps e os 2Mbps, velocidades que poden parecer baixas e, de feito, así son. X.25 presenta un problema

de baixa eficiencia pola esaxerada protección contra erros que implementa e que coas redes actuais non ten sentido.

- Nivel de Enlace (LAP-B):

En X.25, este nivel queda implementado co protocolo LAP-B (Link Access Procedure - B) que é un protocolo de enlace con rexeitamento simple e no cal as tramas de información poden ser utilizadas como tramas de control.

- Nivel de Paquete (PLP):

Este nivel está especificado polo PLP (Packet Layer Protocol) que é un protocolo de acceso a nivel de rede e que proporciona servizos ó nivel superior.

Permite establecer circuitos virtuais (CV): Que poderíamos definir como a asociación lóxica entre usuarios para comunicarse entre eles. Existen dous tipos de CV:

- Conmutados (CVC) : Hai que realizar un diálogo previo á transmisión co nodo local para establecelos.
- Permanentes (CVP): Están establecidos de antemán (por contrato), así que non fai falla fase de establecemento. Son moi útiles se se transmite moito e con moita frecuencia cara un mesmo destino.

#### **47.7.2 FRAMERELAY**

É posible usar FrameRelay como tecnoloxía de soporte para conseguir redes punto a punto. Esta tecnoloxía explícase noutro tema.

#### **47.7.3 METROETHERNET**

É posible usar MetroEthernet como tecnoloxía de soporte para conseguir redes punto a punto. Esta tecnoloxía explícase máis adiante neste mesmo tema.

#### **47.8 METROETHERNET**

MetroEthernet é unha rede tipo MAN (está deseñada para cubrir unha área metropolitana) baseada no moi coñecido estándar Ethernet. O uso habitual de MetroEthernet é servir de rede de acceso para conectarse a Internet ou servir de rede de interconexión de varias oficinas dunha compañía.

Tipicamente o proveedor dunha conexión MetroEthernet proporcionará a mesma por fibra óptica terminando nun equipo que habitualmente ten capacidades non só de nivel 2 se non de nivel 3 (rede).

Esta tecnoloxía pode despregarse de varias formas atendendo á base usada para MAN que a soporta:

- Ethernet pura, toda a rede está baseada en Ethernet, sen ningunha outra tecnoloxía de soporte. Esta opción aporta unha gran simplicidade e baixo custe, pero ten graves problemas de fiabilidade e de escalabilidade polo que está limitada a pequenos despregues.
- MetroEthernet baseadas en redes SDH xa existentes, coas restricións que impón SDH no manexo do ancho de banda.
- E, por último, MetroEthernet baseadas en MPLS. Esta é a opción mais cara pero a mais escalable e fiable sendo a típica que a despregar por operadores (de non ter unha rede SDH existente).

#### **47.8.1 MAN BASEADA EN ETHERNET**

Un despregue baseado unicamente en Ethernet fai so uso de switches de nivel 2. Isto permite un deseño e configuración moi simples a un baixo custo.

Este tipo de despregue so foi posible tras a incorporación das VLAN (Virtual LAN) aportando a posibilidade de “punto a punto” e “multipunto a multipunto” combinadas con VLAN Stacking (tamén coñecida como VLAN Tunneling) e VLAN Translation xa que previamente non era posible illar o tráfico de cada usuario (dada a natureza de Ethernet) para formar circuítos. VLAN Stacking permite o uso de varias LANs virtuais sobre o mesmo circuito da rede troncal gracias ó uso de dous identificadores: un para rede troncal e outro para a rede Ethernet (existindo 4096 identificadores distintos segun o estándar 802.1Q, que non 4096 VLAN distintas) . VLAN Translation permite converter un identificador de VLAN noutro de forma que o identificador usado nunha parte da rede sexa distinto ó usado noutra, evitando desta forma posibles conflitos entre identificadores de distintos usuarios.

#### **47.8.2 MAN BASEADA EN SDH**

Unha Ethernet MAN baseada en SDH (Synchronous Digital Hierarchy) é un paso intermedio entre redes tradicionais (baseadas en división de tempos) e redes máis modernas (como Ethernet). Neste modelo a infraestrutura SDH existente é usada para transportar conexións Ethernet de alta velocidade aportando unha gran fiabilidade grazas aos mecanismos intrínsecos das redes SDH (cun tempo de recuperación inferior a 50 ms). Este tipo de implantacións limítanse aos casos onde xa existe unha rede SDH debido ó alto custo dos equipos SDH e as limitacións de SDH para xestionar o tráfico (velocidade, ruta, ...) levando moitas veces á instalación de switches Ethernet na fronteira SDH para aliviar parte destas limitacións

#### **47.8.3 MAN BASEADA EN MPLS**

Neste caso as tramas Ethernet enviadas polo usuario son empacquetadas en MPLS que transmite os seus datos sobre (habitualmente) Ethernet, creando unha pila Ethernet sobre MPLS sobre Ethernet (aínda que podería haber outro protocolo por debaixo).

Este despregue usa LDP (Label Distribution Protocol) punto a punto para a etiqueta interna (etiqueta do VC) e RSVP-TE (Resource reSerVation Protocol-Traffic Engineering) ou LDP para a etiqueta externa usada na rede. Un dos mecanismos de restrición de MetroEthernet baseadas en MPLS é Fast ReRoute (FRR) que permite un tempo de restoración inferior ós 50ms. Isto é unha das cousas que máis hai que ter en conta á hora de decidirmos por MetroEthernet baseadas en MPLS fronte aquelas baseadas en Ethernet, xa que se temos un tempo de restoración equivalente usando unha solución Ethernet pura non merece a pena introducir unha baseada en MPLS.

#### **47.9 BIBLIOGRAFÍA**

José Manuel Huidrobo. Todo sobre comunicacións. 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. TECNOLOXÍAS DE TRANSPORTE: FRAME RELAY, ATM, DWDM, MPLS. REDES DE FIBRA ÓPTICA. REDES DE NOVA XERACIÓN (NGN).**

## **Tema 48. Tecnoloxías de transporte: Frame Relay, ATM, DWDM, MPLS. Redes de fibra óptica. Redes de nova xeración (NGN).**

### 48.1 Tecnoloxías 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 da conxestión

###### 48.1.1.1.4 Tipos de tráfico transportado

###### 48.1.1.1.5 Vantaxes

#### 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 do tráfico

###### 48.1.2.2.2.2 Clases de servizo

###### 48.1.2.2.2.3 Asignación de ancho de banda e control da conxestión

###### 48.1.2.2.3 Capa de adaptación (AAL)

###### 48.1.2.2.3.1 Estructura da 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 Funcions de MPLS

##### 48.1.4.2 LSRS e 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 Xerarquía Dixital Plesiócrona (PDH)

#### 48.2.2 Xerarquía Dixital Síncrona (SDH) / SONET

##### 48.2.2.1 Frame SDH / SONET

##### 48.2.2.1.1 Framing

##### 48.2.2.1.2 Estructura do frame STM-1

### 48.3 Redes de nova xeración (NGN)

#### 48.3.1 Tecnoloxías de soporte

### 48.4 Bibliografía

## **48.1 TECNOLOXÍAS DE TRANSPORTE**

### **48.1.1 FRAME RELAY**

Frame relay é un protocolo de transmisión de paquetes de datos en ráfagas de alta velocidade a través dunha rede dixital fragmentados en unidades de transmisión chamadas Frames. Require unha conexión exclusiva durante o período de transmisión.

Frame relay é unha tecnoloxía de paquete-rápido xa que o chequeo de erros non ocorre en ningún nodo da transmisión. Son os extremos os responsables deste chequeo de erros. (Sen embargo debido a que os erros en redes dixitais son extremadamente menos frecuentes en comparación coas redes analóxicas, isto non supón un verdadeiro inconveniente).

A diferenza dos paquetes que son de tamaño fixo, Frame Relay transmite Frames que son de tamaño variable (mil ou mais bytes ).

O estándar de Frame Relay (ITU-T I.122) é unha extensión do estándar ISDN. Implementa varios interfaces físicos como V.35 para velocidades menores de 2 Mb e G.703 para 2 Mb.

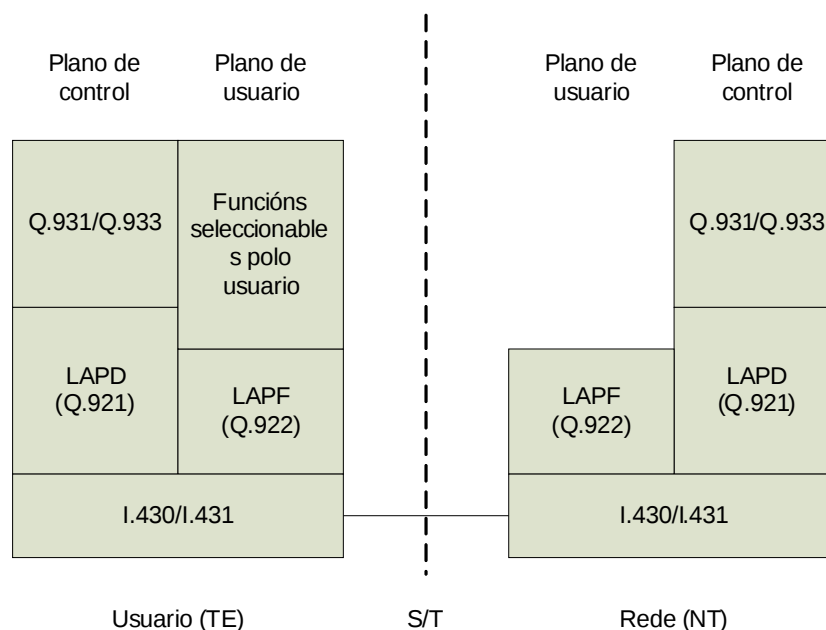
Unha conexión Frame Relay é coñecida como unha conexión virtual. Unha conexión virtual permanente é exclusiva ó par orixen-destino e pode transmitir por encima de 1,544 Mbps, dependendo das capacidades do par

orixen-destino. É posible tamén unha conexión virtual conmutada usando a rede pública e pode proporcionar elevados anchos de banda.

#### 48.1.1.1 ARQUITECTURA DE PROTOCOLOS

En Frame Relay considéranse dous planos de operación:

- Plano de control (C): Involucrado no establecemento e liberación de conexións lóxicas. Os protocolos deste plano implementanse entre o usuario e a rede. É similar á sinalización en canles de servizos de conmutación de circuítos, xa que usa un canal lóxico separado para a información de control. Na capa de enlace usase o protocolo LAPD (Q.921) para proporcionar un servizo de control de datos fiable, mediante un control de fluxo e de erros entre a rede e o usuario. Este servizo de enlace de datos usa para o intercambio de mensaxes de control o protocolo Q.931.
- Plano de usuario (U): Responsable da transferencia de datos extremo a extremo mediante o protocolo LAPF (Procedemento de Acceso ó Enlace para Servizos en Modo Trama) definido no estándar Q.922.



##### 48.1.1.1.1 PROTOCOLO LAPF

Permite a retransmisión de tramas como un servizo orientado a conexión da capa de enlace cás seguintes propiedades:

- Envío secuencial das tramas a partir da información de direccionamento existente na cabeceira de control de cada trama.
- Existe unha probabilidade pequena de perda de tramas.
- Reduce ó mínimo o traballo da rede.

El formato de trama de LAPF de funcionamento mínimo (coñecido como protocolo central LAPF) é similar ó LAPD e LAPB con unha salvedade: non existe campo de control, o que ten as seguintes implicacións:

- Existe un único tipo de trama, usada para transportar datos de usuario. Non existen tramas de control.
- Non é posible o uso de sinalización en banda; unha conexión lóxica só pode transmitir datos de usuario.
- Non é posible levar a cabo control de erros dado que non existen números de secuencia.
- Os campos indicador e secuencia de verificación de trama (FCS), actúan como en LAPD y LAPB. O campo de información contén datos de capas superiores. Si o usuario decide implementar funcións adicionais de control de enlace de datos extremo a extremo, debe incluírse neste campo unha trama de enlace de datos.

#### **48.1.1.1.2 DIRECCIONAMIENTO**

O campo de dirección ten implícitamente unha lonxitude de 2 octetos, e pode ampliarse a 3 ou 4 octetos (indicase mediante os bits de ampliación do campo de dirección (EA)). Este campo contén un identificador de conexión de enlace de datos (DLCI) de 10, 17 ou 24 bits. O DLCI proporciona a mesma función que o número de circuíto virtual en X.25: permite a multiplexación de varias conexións lóxicas de retransmisión de tramas a través dun único enlace físico. Como en X.25, o identificador de conexión só ten significado local.

A función realizada por calquera rede que soporte a técnica de retransmisión de tramas, consiste no encamiñamento das tramas de acordo co seus valores DLCI. Para esta función existe un xestor de tramas

encargado de tomar as decisións de encamiñamento. Esta operación pode involucrar a múltiples xestores de tramas interconectados.

#### **48.1.1.1.3 CONTROL DA CONXESTIÓN**

Utilízanse dous tipos de sinalización para o control da conxestión:

- Sinalización implícita: prodúcese cando a rede descarta tramas, feito que é detectado polos protocolos de nivel superior no interface de usuario.
- Sinalización explícita: é de carácter opcional e constitúe unha sinalización da rede ó interface de usuario mediante dous bits. Ambos bits permiten que os dispositivos finais regulen a velocidade de transmisión de información á rede ata que a conxestión desapareza. Os bits son o BECN (conxestión no sentido oposto á trama) e o FECN (conxestión no sentido da trama).

Adicionalmente, existe outro mecanismo de control da conxestión (CLLM, “Consolidated Link Layer Management”), consistente en mensaxes que a rede envía aos dispositivos de acceso con códigos indicadores das causas da conxestión, así como unha lista de tódolos DLCI’s que deben reducir o seu tráfico para diminuír o nivel de conxestión.

En Frame Relay defínense dúas clases de tráfico por Circuito Virtual Permanente:

- Clase de Caudal ou CIR (Committed Information Rate): defínese como o caudal de información que a Rede comprométese a transmitir expresado en bit/sg. Nun dimensionamiento correcto, debe corresponder a un tráfico “normal” ou promedio. Recomendase que non supere o 75 % da velocidade da liña, aínda cando hai pouca simultaneidade entre os Circuitos Virtuais, pódese superar coa sobrecontratación que se recomenda non exceda do 200%.
- Exceso de Tráfico ou EIR (Excess Information Rate): sen contratación, e que vai dirixido a permitirla transmisión de ráfagas de gran intensidade de tráfico, sen custe adicional: defínese como a cantidade de información en exceso do CIR contratado, que a Rede é

capaz de xestionar durante un período de tempo definido. Esta clase de tráfico, expresado en bit/sg, é sinalada pola Rede como de menor prioridade ( $DE=1$ ), e en condicións normais será retransmitida e en condicións de conxestión pode ser descartada.

Para os Circuitos Virtuais Commutados defínese un CIR e un EIR Total Agregado que engloba a tódolos CVC establecidos.

#### **48.1.1.1.4 TIPOS DE TRÁFICO TRANSPORTADO**

A necesidade de novas facilidades para as comunicacións de área extendida, en particular para as comunicacións de datos entre redes locais, impulsou enormemente o desenvolvemento e utilización de Frame Relay, debido a que satisfai as dúas características predominantes deste tipo de tráfico:

- Tráfico a ráfaga e impulsivo, que esixiría dimensionar en exceso o enlace para atender os picos de demanda. Frame Relay soluciona este problema, xa que require unha pequena cantidade de ancho de banda permanentemente reservada vía un circuítio virtual permanente, mentres que dinamicamente, e sempre que exista ancho de banda dispoñible, é posible asignar maior velocidade á conexión para atender picos de demanda.
- A necesidade de interconexión remota de LANs incrementa a necesidade de mallado das redes WAN resultantes. Frame Relay evita a necesidade de numerosos enlaces físicos, permitindo a definición de múltiples circuítos virtuais permanentes a diferentes destinos, a través dun mesmo porto dedicado a un enlace físico.

#### **48.1.1.1.5 VANTAXES**

Aforro nos custes de telecomunicacións: Co servizo Frame Relay os usuarios poderán transportar simultaneamente, compartindo os mesmos recursos de rede, o tráfico pertencente a múltiples comunicacións e aplicacións, e cara diferentes destinos.

Tecnoloxía punta e altas prestacións: Frame Relay proporciona alta capacidade de transmisión de datos pola utilización de nodos de rede de

alta tecnoloxía e baixos retardos, como consecuencia da construción de rede (backbone) sobre enlaces a 34 Mbps. e dos criterios de encamiñamento da Rede de Datos, orientados a minimizar o número de nodos de tránsito.

Flexibilidade do servizo : Frame Relay é unha solución adaptable ás necesidades cambiantes, xa que se basea en circuítos virtuais permanentes (CVP), que é o concepto de Rede Pública de Datos, equivalente ó circuíto punto a punto nunha rede privada. Sobre unha interface de acceso á rede pódense establecer simultaneamente múltiples circuítos virtuais permanentes distintos, o que permite unha fácil incorporación de novas sedes á Rede de Cliente.

Servizo normalizado: Frame Relay é un servizo normalizado según os estándares e recomendacións de UIT -T, ANSI e Frame Relay Forum, co que queda garantida a interoperatividade con calquer outro produto Frame Relay asimesmo normalizado.

#### **48.1.2 ATM**

Asynchronous Transfer Mode (ATM) é unha técnica de conmutación que leva a cabo a transmisión de datos por medio de paquetes (celdas), permite a multiplexación de varias conexións lóxicas sobre unha única interface física e tratase dunha técnica de conmutación de paquetes orientada a conexión.

O protocolo de ATM ten unha mínima capacidade de control de erros, de fluxo e un tamaño de paquete fixo (celda) co que facilita o uso de nodos de conmutación a velocidades elevadas.

As súas principais características son:

- Capacidade de integración de diverso tipo de tráfico.
- Asignación dinámica e flexible do ancho de banda.
- Optimización do compromiso entre caudal e latencia.
- Ganancia estatística: capacidade de optimizar a relación entre a suma das velocidades de pico das fontes e a velocidade do enlace.

##### **48.1.2.1 PRINCIPIOS DE OPERACIÓN**



As conexións lóxicas en ATM están relacionadas coas conexións de canais virtuais (VCC, “Virtual Channel Connection”). Unha VCC é a unidade básica de conmutación en un rede ATM. Unha VCC establecece entre dous usuarios finais a través da rede, intercambiándose celdas de tamaño fixo a través da conexión de un fluxo full-duplex e de velocidade variable. As VCC utilízanse tamén para sinalización de control e xestión de rede e encamiñamento.

Introducíuse unha segunda capa de procesamento en ATM para xestionar o concepto de camiño virtual. Unha conexión de camiño virtual (VPC, “Virtual Path Connection”) é un conxunto de VCC cos mesmos extremos, de maneira que tódalas celdas fluíndo a través das VCC dunha mesma VPC conmútanse conxuntamente.

A técnica de camiño virtual axuda a conter o custo de control agrupando nunha soa unidade conexións que comparten camiños comúns a través da rede. As accións da xestión de rede poden ser aplicadas a un pequeno número de grupos de conexións, en lugar de a un gran número de conexións individuais.

#### **48.1.2.2 CAPAS DE ATM**

As normalizacións ITU-U para ATM baséanse nunha arquitectura onde contéplanse os seguintes niveis:

- Capa física: Especifica o medio de transmisión e un esquema de codificación do sinal. Dividíndose en dúas capas:
  - Subcapa dependente do medio físico (PMD): que leva a cabo funcións de transmisión e temporización de bits.
  - Subcapa de Converxencia de Transmisión (TC): responsable das funcións relacionadas coa transmisión de células como control de HEC, delimitación de celdas, etc..
- Capa ATM: Define a transmisión de datos en celdas de tamaño fixo, ó tempo que establece o uso de conexións lóxicas. Realiza funcións de multiplexación de celdas e control de fluxo.

- Capa de adaptación ATM (AAL): Capa de adaptación para admitir compatibilidade con protocolos de transferencia de información non baseados en ATM. Divídese en dous:
  - Subcapa de Converxencia (CS).
  - Subcapa de Segmentación e reensambrado (SAR).

#### **48.1.2.2.1 CAPA FÍSICA**

A función básica do nivel físico é a codificación/decodificación da información en formato eléctrico ou óptico para a transmisión/recepción sobre o medio físico de comunicación utilizado. Outras funcións proporcionadas por este nivel son a desalineación de celdas e xeneración e proceso do checksum para o control de erros na cabeceira.

As recomendacións ITU-T detallan a velocidade de transmisión e as técnicas de sincronización para a transmisión de celdas ATM. As principais propostas de capas físicas en redes ATM son as seguintes:

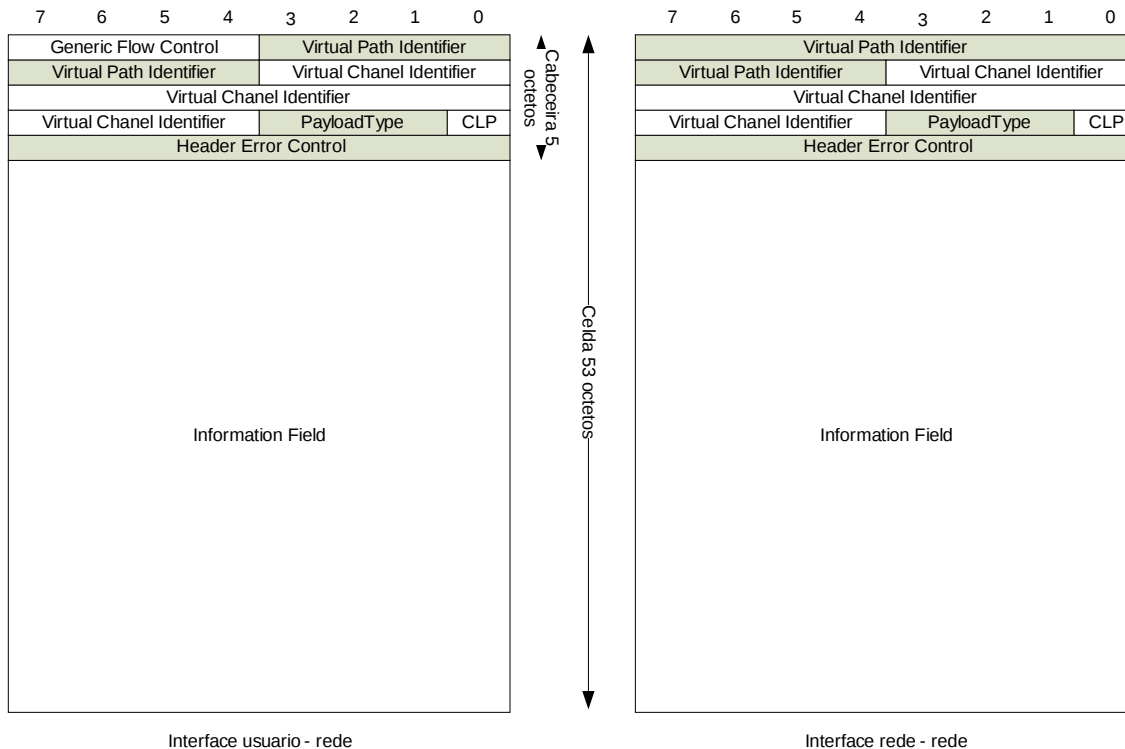
- ATM sobre SDH: STM-1 (155,52) e STM-4 (622,08)
- ATM sobre PDH: E1 (2,048), DS1 (1,548), DS2 (6,312), E3 (34,368), E4 (139,264) e DS3 (44,736).
- ATM a 100 Mbps sobre FDDI.
- ATM a 25,6 Mbps (proposta por IBM).

#### **48.1.2.2.2 CAPA ATM**

O modo de transferencia asíncrono utiliza celdas de tamaño fixo, que constan de 5 octetos de cabeceira e un campo de información de 48 octetos. A capa ATM é a encargada de incorporala cabeceira de 5 octetos ó campo de información. A cabeceira ten o seguinte formato:

- Control de Fluxo Xenérico (GFC, "Generic Flow Control"). Utilízase unicamente no interface UNI (User-Network Interface).
- Identificador de Camiño 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 se se trata de datos de usuario, información de xestión, información OAM, etc...

- Prioridade de Perda de Celda (CLP, “Cell Loss Priority”). As celdas marcadas son as primeiras en ser descartadas en caso de conxestión.
- Control de Erros de Cabeceira (“Checksum”).



#### **48.1.2.2.2.1 PARÁMETROS DE TRÁFICO**

Cando se establece unha conexión ATM constitúese un “Contrato de tráfico” no que se especifican os parámetros de tráfico e os de QoS, entre os máis significativos están:

- PCR (“Peak Cell Rate”): Taxa máxima de celdas permitida sobre o circuíto.
- MCR (“Minimun Cell Rate”): Mínima taxa de celdas sobre o circuíto garantida polo proveedor do servizo.
- CDVT (“Cell Delay Variation Tolerance”): Nivel de tolerancia para a diferenza entre la celda co mínimo retardo e a celda co máximo retardo.
- SCR (“Sustained Cell Rate”): Taxa media de transmisión de celdas que se manterá durante a duración dunha transmisión.

- BT (“Burst Tolerance”): Límite que a transmisión pode alcanzar no seu nivel máis alto (PCR).

Garántese unha calidade de servizo con respecto a un mínimo ancho de banda dispoñible, a cantidade de retardo que afectará á transmisión e a máxima perda de celdas que se producirá nesta.

#### **48.1.2.2.2.2 CLASES DE SERVIZO**

A partir destas especificacións iniciais do ITU, definíronse cinco clases de servizo que a rede ATM debería proporcionar (non é obrigatorio):

- CBR (“Constant Bit Rate”): É un servizo determinístico, deseñado para soportar emulación de circuítos, tráfico de voz e vídeo (por exemplo, MPEG/JPEG) en taxa constante de bits. Proporciona ancho de banda reservado, garantido mínima perda de celdas e mínimas variacións en retardos. O servizo CBR proporciona ancho de banda reservado ata o PCR especificado para o circuíto. Con CBR o usuario debe declarar o PCR e o CDTV no momento de establecela conexión.
- VBR (“Variable Bit Rate”): Definíronse dous tipos:
  - VBR-RT (“Real Time”), proporciona un estreito control dos retardos para a transmisión de información como vídeo e voz sen silencios.
  - VBR-NRT (“Non Real Time”) ten menos esixencias que o anterior, respecto ás variacións en retardos e desenvolveuse para a transmisión de datos transaccionais.

O servizo VBR tamén require a especificación do PCR, se ben con un comportamento diferente: o usuario pode utilizar a canle por enriba do SCR (ata o PCR) só durante curtos períodos de tempo determinados polo parámetro BT, pero debe manter o SCR como unha taxa media. Se o usuario excede o SCR durante un período de tempo, a isto seguiralle un período similar por debaixo do SCR. Se o usuario excede o PCR, esto seguirase por un período de inactividade antes de que o usuario poda exceder o SCR de novo. Con VBR o usuario debe declarar PCR, CDVT, SCR y BT.

- UBR (“Unspecified Bit Rate”): Diseñouse para permitir o uso de ancho de banda excedente non utilizado para os servicios CBR e VBR. Non ofrece garantías en canto á perda de celdas ou variacións en retardos; é dicir, non inclúe ningún mecanismo de control no caso de conxestión na rede. Con UBR non hai descritores de tráfico, nin garantías de calidade de servizo nin mecanismos de realimentación en caso de conxestión na rede. A estación pode enviar tráfico cando o necesite e a rede o aceptará; iso si, en caso de conxestión, a estación non é notificada de ningún modo e o conmutador eliminará celdas cando os seus buffers estén cheos. Isto significa que a taxa potencial de perda de celdas con UBR pode ser inaceptablemente alta.
- ABR (“Available Bit Rate”): Ó igual que UBR diseñouse para aproveitalo ancho de banda excedente pero, ó contrario que aquel, implementa mecanismos de control e control en caso de conxestión na rede. ABR concebiuse para transportar o tráfico a ráfagas sen as limitacións de calidade de servizo de UBR, basicamente aplicacións que non funcionen en tempo real e polo tanto pouco sensibles a retardos. Utiliza basicamente os descritores PCR y MCR; o usuario comprométese a non enviar información mais rápido que o PCR e a rede a proporcionar como mínimo o MCR requirido. O usuario non está obrigado a especificar PCR e MCR; en ausencia de tal especificación, os valores por defecto serían o PCR a velocidade de acceso e o MCR a cero. Se se cumpren estes parámetros descritores de tráfico, garántese a calidade de servizo en canto a mínimo nivel de perda de celdas e mínimo ancho de banda asegurado; o retardo de celdas será minimizado, pero non existe garantía absoluta respecto ó retardo para o servizo ABR. Hai outro tipo de servizo en estudio polo ATM Forum (VBR+) que, como o ABR, contempla un sistema de realimentación para control da conxestión na rede pero,

adicionalmente, proporciona ademais garantías en canto a os retardos.

#### **48.1.2.2.3 ASIGNACIÓN DE ANCHO DE BANDA E CONTROL DE CONXESTIÓN**

Unha rede ATM debe garantir uns determinados parámetros de QoS, ademáis de proporcionar ganancia estatística. Para conseguilo utiliza métodos preventivos, denominados Control de Admisión de Conexión e de monitorización posterior, mediante una función de policía (UPC) que emprega diversos algoritmos para este fin.

Tamén existen métodos reactivos como o CLP (Cell Loss Priority) ou o GFC (Generic Flow Control) que controla o tráfico do usuario á rede.

Para o control da conxestión existen dúas opcións:

- Control baseado en créditos: o extremo receptor emite créditos, que indican o número de celdas que pode enviar o emisor, útil en entornos de área local.
- Control baseado na velocidade: baseado en mensaxes EFCI (Explicit Forward Congestion Indication) , as estaciones e conmutadores axustan a velocidade dinamicamente. Esta é a técnica máis amplamente utilizada.

#### **48.1.2.2.3 CAPA DE ADAPTACIÓN (AAL)**

A función básica do nivel de adaptación ATM (AAL) é proporcionar o enlace entre os servizos requiridos polos niveis superiores de rede e o nivel ATM.

Ata o momento, o ITU-T definiu para a AAL catro clases de servizo, respondendo esta

clasificación a tres parámetros básicos: a relación de tempo entre a fonte e o destino, taxa de bits constante ou variable e modo de conexión. As clases definidas son as seguintes:

<b>Clase</b>	<b>A</b>	<b>B</b>	<b>C</b>	<b>D</b>
<b>Relación orixe / destino</b>	Si	Si	No	No
<b>Velocidade</b>	Constante	Variable	Variable	Variable

<b>Orientado a conexión</b>	Si	Si	Si	No
---------------------------------	----	----	----	----

#### **48.1.2.2.3.1 ESTRUCTURA DA CAPA AAL**

A capa AAL está organizada en dúas subcapas:

- Subcapa de segmentación e reensambrado (SAR): Segmenta a información das capas superiores para construíla carga útil das celdas ATM e reciprocamente, reensambla os campos de información das celdas en unidades de información para as capas superiores.
- Subcapa de converxencia (CS): ten como misión realizar funcións específicas para cada servizo, como o tratamento da variación do retardo de celda, sincronización extremo a extremo, tratamento de celdas mal insertadas ou perdidas. Existen, por tanto, diferentes CS sobre a subcapa SAR. Debido á gran cantidade de servizos propostos sobre ATM, foi necesario distinguir entre unha parte común CS (CPCS) e unha parte específica de servizo (SSCS).

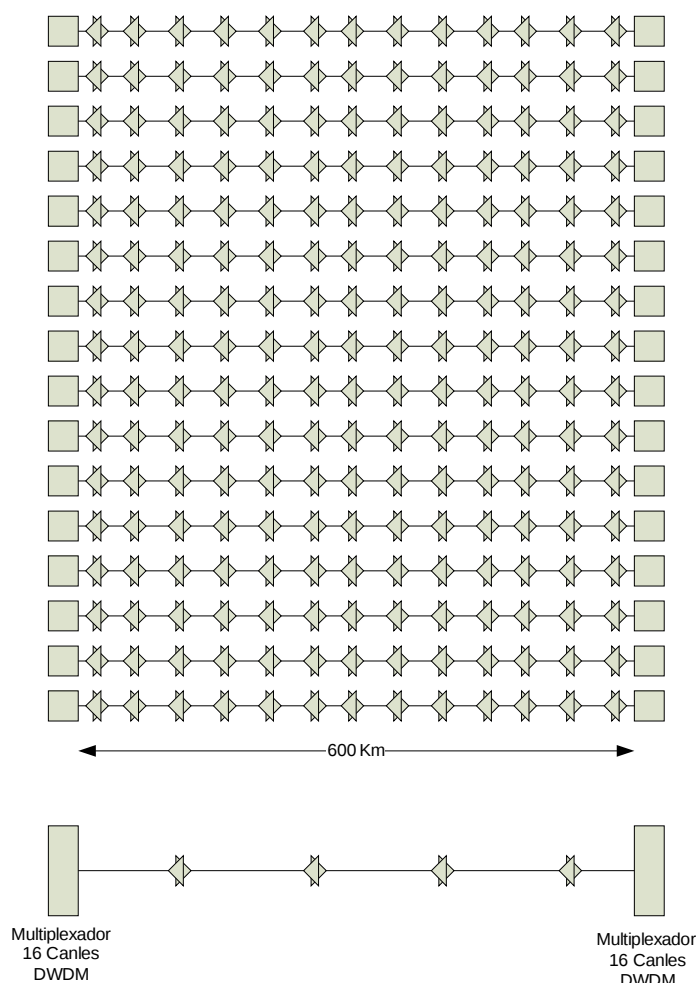
Inicialmente, el ITU-T recomendou catro tipos de protocolos AAL para soportar as catro clases de servizo definidas, os protocolos AAL de tipo 1, 2, 3, e 4. Así, o tráfico de clase 1 utilizará o protocolo AAL-1, o de clase 2 o AAL-2, e os de clase 3 e 4 o protocolo AAL-3/4. Sendo os protocolos das clases 3 e 4 un protocolo único.

Debido á complexidade do protocolo AAL-3/4 propúxose como alternativa o AAL-5, a veces denominado SEAL ("Simple and Efficient Adaptation Layer"). En consecuencia, as clases de tráfico 3 e 4 poden utilizar o protocolo AAL-3/4 ou o AAL-5.

#### **48.1.3 DWDM**

A tecnoloxía DWDM usa unha composición óptica do sinal de distintos fluxos de datos cada un dos cales na súa propia lonxitude de onda óptica. A pesar de que a división e multiplexado usando o espectro óptico é unha tecnoloxía que se coñece dende hai tempo, as súas primeiras aplicacións restrinxían o seu uso a prover dous lonxitudes de onda moi grosos e moi separados ou a construción de compoñentes capaces de ata 4 canles. So

recentemente a tecnoloxía evolucionou ata o punto de poder empacar e integrar nun sistema de transmisión unha alta densidade de canais paralelos, simultáneos, a unha frecuencia extremadamente alta (192 - 200 Terahertz). Conforme ó plan de canles do ITU, este sistema asegura a interoperabilidade con outros equipos e permite os operadores posicionarse ben para despregar solucións ópticas na súa rede. O sistema de 16 canles proporciona basicamente un cable virtual con 16 fibras.



Para transmitir 40Gb/s a 600 Kms usando un sistema tradicional requirimos 16 pares de fibra óptica con rexeneradores cada 35 kms cun total de 272 rexeneradores. Un sistema DWDM de 16 canles usa só un par de fibra óptica e 4 amplificadores posicionados cada 120Km.

A forma mais común de DWDM usa un par de fibra (unha para transmitir e outra para recibir). Aínda que existen sistemas que só usan unha fibra para transmitir e recibir, estes sistemas deben sacrificar un pouco da



capacidade da fibra óptica para unha banda de garda e evitar así a mestura de canles reducindo tamén o rendemento dos amplificadores.

Adicionalmente, existe un gran risco de que os reflexos producidos durante o mantemento ou reparación podan danar os amplificadores.

A dispoñibilidade de tecnoloxías maduras de soporte como os multiplexadores precisos e os EDFA (Erbium Doped Fiber Amplifiers) permitiu a dispoñibilidade comercial de sistemas DWDM con oito, dezaseis, ou incluso un maior numero de canles.

#### **48.1.3.1 DEMULTIPLEXADORES**

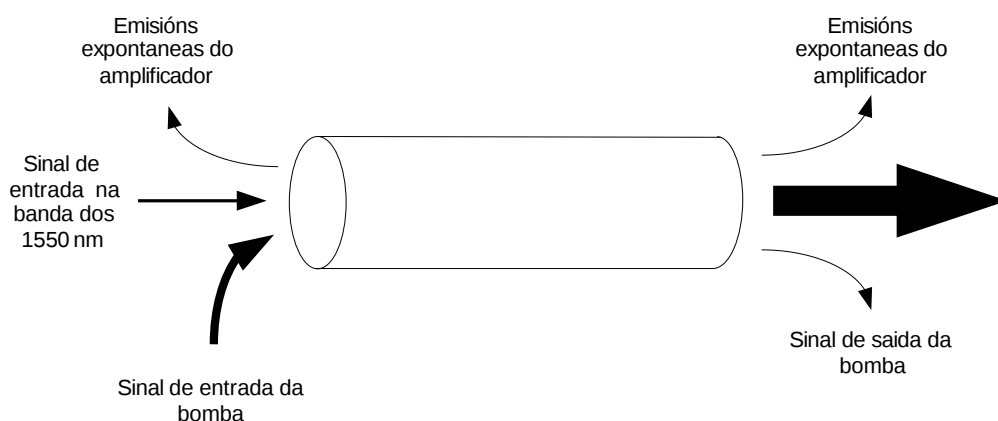
Con sinais tan precisos e densos como os usados en DWDM, ten que existir unha forma que aporte unha precisa separación dos sinais, ou filtrado, no receptor óptico. Esta solución tamén ten que ser fácil de implementar e non requirir mantemento. Os sistemas primitivos de filtrado eran ou demasiado imprecisos para DWDM ou demasiado sensibles a variacións de temperatura e polarización, demasiado vulnerables a cruces de comunicacións en canles adxacentes ou demasiado caros. Isto restrinxiu a evolución de DWDM. Para conseguir satisfacer os requisitos de alto rendemento, desenvolveuse unha nova tecnoloxía de filtrado que fixo DWDM posible a un custo aceptable: a fibra con rexilla de Bragg.

O novo compoñente de filtro (fibra con rexilla) consiste nunha determinada lonxitude de fibra óptica onde o índice de refracción do núcleo foi permanentemente modificado en puntos equidistantes, xeralmente por exposición a un patrón de interferencia ultravioleta. O resultado é un compoñente que reflecta a luz dependendo da lonxitude de onda e é útil para separar lonxitudes de onda. Noutras palabras, a rexilla crea un filtro altamente selectivo para unha lonxitude de onda moi estreita que funciona de forma similar a un espello e aporta maior selectividade de lonxitude de onda que calquera outra tecnoloxía. Como este é un dispositivo pasivo, fabricado en fibra de vidro, é robusto e durable.

#### **48.1.3.2 ERBIUM DOPED FIBER AMPLIFIER**

A chegada do EDFA permitiu o desenvolvemento de sistemas DWDM comerciais provendo unha forma de amplificar toda as lonxitudes de onda

ó mesmo tempo. Esta amplificación óptica faise incorporando ións de Erbium no núcleo dunha fibra especial nun proceso coñecido como dopado. Úsanse bombas ópticas láser para transferir altos niveis de enerxía á fibra especial, enerxizando os ións de Erbium que logo aumentan os sinais ópticos que pasan pola fibra. A estrutura atómica do Erbium proporciona amplificación ós grandes rangos do espectro que se requiren para DWDM.



En vez de múltiples rexeneradores electrónicos, que requiren que o sinal óptico sexa convertido a sinal electrónico e viceversa, o EDFA amplifica directamente os sinais ópticos. Desta forma o sinal pode ser enviado ata 600 Km sen rexeneración e ata 120Km entre amplificadores nun sistema DWDM dispoñible comercialmente.

#### **48.1.4 MPLS**

MPLS (MultiProtocol Label Switching) é unha solución versátil para resolver os problemas que afrontan as redes actuais de velocidade, escalabilidade, xestión da calidade de servizo (QoS) e enxeñería do tráfico. MPLS emerxeu coma unha solución elegante para aportar a xestión de ancho de banda e requirimentos de servizo para a nova xeración de redes troncais baseadas en IP. MPLS resolve problemas relacionados coa escalabilidade e encamiñamento (baseados en QoS e métricas da calidade de servizo) e pode existir sobre redes ATM e Frame Relay xa existentes.

##### **48.1.4.1 FUNCÍONS DE MPLS**

MPLS realiza as seguintes funcións:

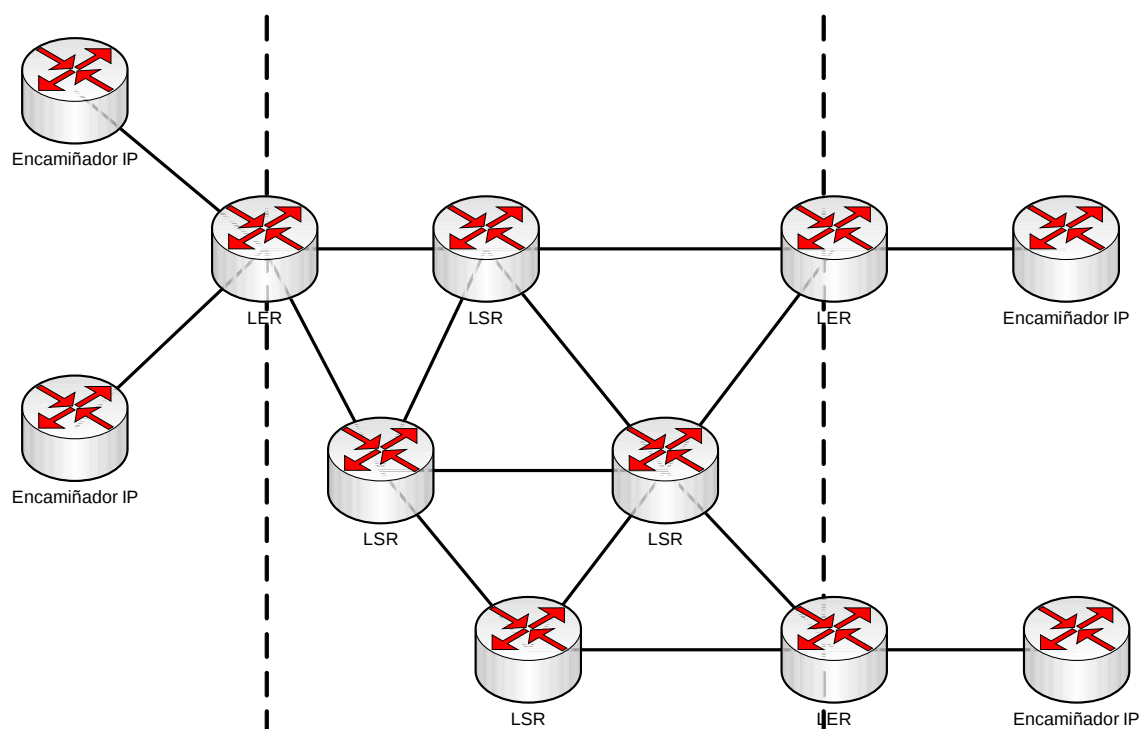
- Especifica mecanismos para xestionar os fluxos de tráfico de varias granularidades, coma os fluxos entre diferente hardware, maquinas ou incluso entre diferentes aplicacións.
- Mantense independente dos protocolos das capas 2 e 3.
- Aporta un método para mapear direccións IP a simples etiquetas de tamaño fixo, usadas por diferentes tecnoloxías.
- Intégrase con protocolos existentes coma RSVP (Resource Reservation Protocol) e OSPF (Open Shortest Path First).
- Da soporte a IP, ATM e Frame Relay.

En MPLS a transmisión de datos prodúcese en LSPs (Label Switching Paths). Un LSP é unha secuencia de etiquetas para cada un dos nodos ó longo do camiño, desde a orixe ata o destino. Os LSPs establécense antes da transmisión dos datos (establecemento por control) ou ante a detección dun determinado fluxo de datos (establecemento por datos). As etiquetas (que son identificadores específicos dos protocolos subxacentes) distribúense usando LDP (Label Distribution Protocol) ou RSVP ou acompañando os datos de protocolos de encamiñamento como o BGP (Border Gateway Protocol) e OSPF. Cada paquete de datos encapsula e transporta as etiquetas durante o seu traxecto dende a orixe ata o destino. A alta velocidade de conmutación é posible pola lonxitude fixa das etiquetas e por que estas son insertadas ao principio do paquete ou celda e isto permite que hardware específico as use para conmutar paquetes a alta velocidade entre distintos enlaces.

#### **48.1.4.2 LSRS E LERS**

Os dispositivos que participan nos mecanismos do protocolo MPLS poden clasificarse en LERs (Label Edge Routers) e LSRs (Label Switching Routers). Un LSR é un encamiñador de alta velocidade no núcleo dunha rede MPLS que participa no establecemento dos LSPs usando o protocolo de sinais adecuado e proporciona conmutación de alta velocidade dos datos baseándose nos camiños establecidos.

Un LER é un dispositivo que opera no límite entre a rede de acceso e da rede MPLS. LERs soportan múltiples portos conectados a diferentes redes (Frame Relay, ATM, Ethernet, ...) e envía o tráfico á rede MPLS despois de establecer o seu LSP, tamén distribúe o tráfico á rede de acceso no proceso inverso. O LER xoga un rol moi importante na asignación e renovación de etiquetas, cando o tráfico entra ou sae dunha rede MPLS.



#### **48.1.4.3 FEC**

A FEC (Forward Equivalent Class) é a representación dun grupo de paquetes que comparten os mesmos requisitos de transporte. Todos os paquetes deste grupo reciben o mesmo tratamento na súa ruta cara o destino. Ó contrario que IP, en MPLS, a asignación dun determinado paquete a un FEC realízase só unha vez, cando o paquete entra na rede. Os FECs están baseados nos requisitos do servizo para un conxunto de paquetes ou simplemente nun determinado prefixo de rede. Cada LSR constrúe unha táboa para saber como un paquete debe ser enviado. Esta táboa, chamada LIB (Label Information Base) componse de relacións FEC – etiqueta.

#### **48.1.4.4 ETIQUETAS**

Unha etiqueta na súa forma mais simple, identifica o camiño que debe recorrer un paquete. As etiquetas encapsulanse nunha cabeceira de nivel 2 xunto co paquete. O encamiñador que o recibe, examina o paquete para obtela súa etiqueta para determinalo seguinte salto. Unha vez que o paquete esta etiquetado, o resto do camiño pola rede troncal basease en conmutación por etiquetas. Os valores das etiquetas só teñen valor local, esto quere dicir que so pertencen a saltos entre LSRs concretos.

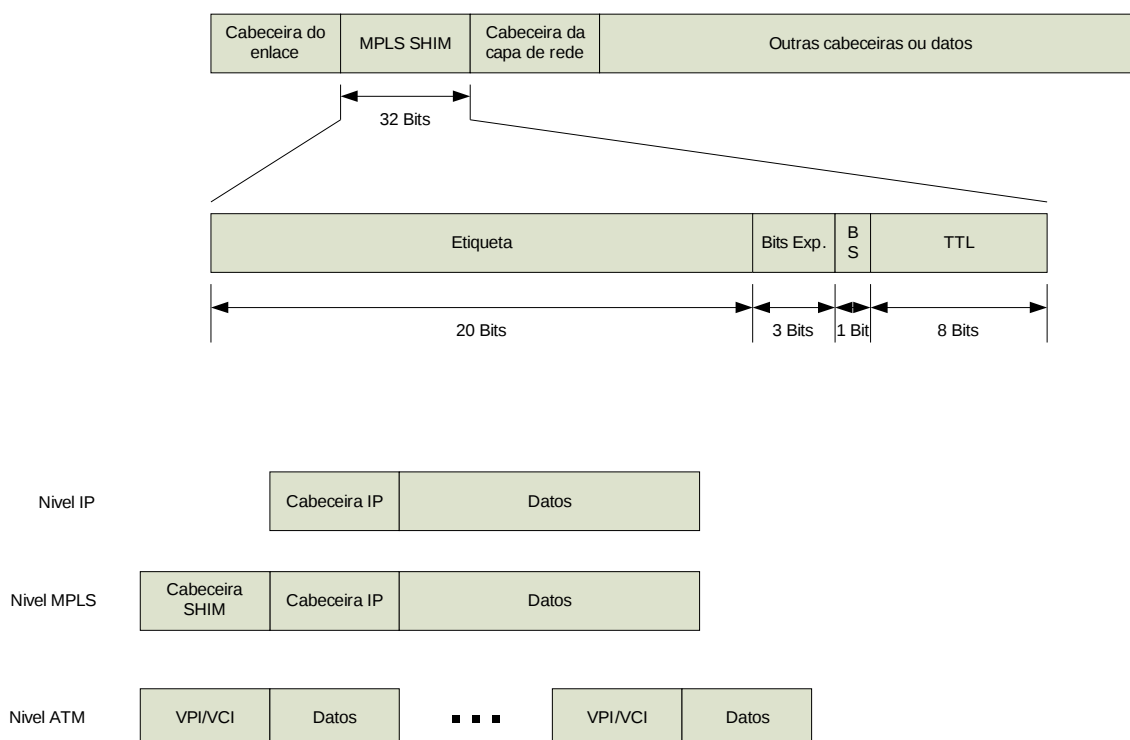
Cando un paquete se clasifica como un FEC novo ou existente, asignáselle unha etiqueta. Os valores da etiqueta derívanse da capa de enlace inferior (DLCI para Frame Relay, VPI/ VCI para ATM, ...).

As etiquetas enlázanse cos FEC como resultado dun evento ou política que indica a necesidade dese enlace. Estes eventos poden ter como orixe as sinais de control ou as propias transmisión de datos sendo esta última a mellor opción polas súas propiedades de escalado.

A asignación de etiquetas basease en criterios de encamiñado coma:

- Destino Unicast
- Enxeñaría de tráfico
- Multicast
- VPN (Virtual Private Network)
- QoS

Na seguinte imaxe podemos ver a estrutura dunha etiqueta MPLS e un exemplo do proceso dende IP ata a capa de enlace (neste caso sobre ATM).



#### 48.1.4.5 DISTRIBUCIÓN DE ETIQUETAS

MPLS non impón un só método de distribución de etiquetas. Existen protocolos de encamiñado, como BGP e RSVP que foron mellorados para poder incorporar (usando o método pogyback) a información das etiquetas xunto coa información do protocolo. O IETF (Internet Engineering Task Force) tamén definiu un protocolo chamado LDP (Label Distriution Protocol) para xestionar as etiquetas. Extensións de LDP permiten definir rutas explícitas baseadas en requisitos de Qos. Estas extensións están recollidas na definción do protocolo CR-LSP (Constrint-based Routing-LDP). Un resumo dos varios esquemas para o intercambio de etiquetas é o seguinte:

- LDP: mapea direccións de unicast IP a etiquetas.
- RSVP, CR-LDP: úsanse para enxeñaría do tráfico e reserva de recursos.
- PIM (Protocol Independent Multicast): usase para mapear multicasts a etiquetas.
- BGP: etiquetas externas (VPN)

#### 48.1.4.6 LSP

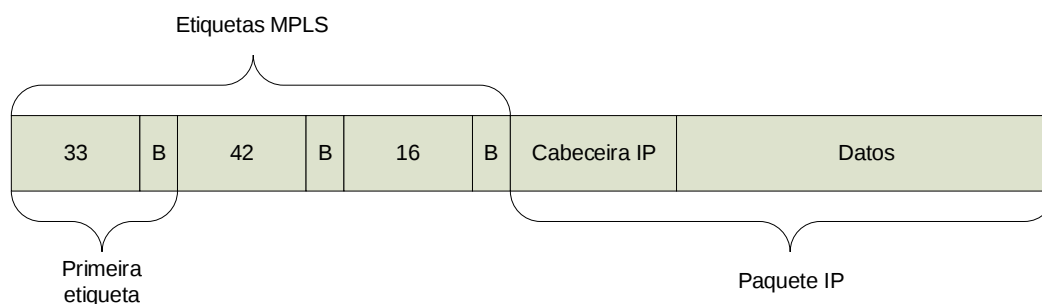
Unha colección de dispositivos MPLS defínese coma un dominio MPLS. Dentro dun dominio MPLS, fíxase un camiño para un paquete baseándose no seu FEC. O LSP fíxase antes da transmisión dos datos usando unha destas dúas opcións:

- Encamiñado salto a salto (hop-by-hop): cada LSR selecciona independentemente o seguinte salto para un FEC determinado. Esta é unha metodoloxía moi similar á usada en redes IP. O LSR usa os protocolos de encamiñamento dispoñibles coma OSPF, etc.
- Encamiñado explícito (ER-LSP): O LSR de entrada (o LSR onde o fluxo de datos comeza na rede) especifica unha lista de nodos que o ER-LSP atravesará. O camiño podería ser non óptimo. Os recursos necesarios poderían ser reservados para garantir QoS. Isto facilita a enxeñaría de tráfico na rede, e permite que servizos diferentes sexan dados usando fluxos baseados en métodos de políticas ou xestión de rede.

Un LSP para un determinado FEC é unidireccional en natureza, o tráfico de retorno terá que usar outro LSP.

#### **48.1.4.7 PILA DE ETIQUETAS**

O apilado de etiquetas (Label Stack) é un mecanismo que permite a operación xerárquica dentro dun dominio MPLS. Basicamente permite a MPLS ser usado simultaneamente para o encamiñado a nivel fino (entre encamiñadores individuais dentro dun ISP) e nun nivel groso (dominio a dominio). Cada nivel, nunha pila de etiquetas, pertence a un nivel xerárquico. Isto facilita o uso de túneles en MPLS.



## **48.2 REDES DE FIBRA ÓPTICA**

### **48.2.1 XERARQUÍA DIXITAL PLESIÓCRONA (PDH)**

A PDH (Plesiochronous Digital Hierarchy) é unha tecnoloxía usada en redes de telecomunicacións para transportar unha gran cantidade de datos sobre redes de fibra óptica ou radioenlaces. O termo alude a que as diferentes partes da rede funcionan de forma case sincronizada, pero non totalmente. A maior parte dos operadores están a actualizar PDH a SDH ou SONET (capaces de transmitir a maior velocidade) se non a reemplazan directamente por unha tecnoloxía completamente distinta.

PDH permite a transmisión de datos a unha velocidade similar entre as transmisións pero permitindo variacións sobre a velocidade nominal, xa que non hai unha sincronización exacta dentro da rede.

A velocidade de transferencia básica é de 2 Mb/s, para a transferencia de voz esta é dividida en 30 canles de 64Kb/s e dous canles para sinalización e sincronización; ademais todo o enlace (2Mb/s) pódese usar para transmitir datos.

A velocidade de transmisión está controlada por un reloxo no equipo que envía os datos, esta velocidade pode variar 50 ppm dende os 2 Mb/s isto quere dicir que as distintas transmisións poden estar sucedendo a diferentes velocidades (e probablemente o están).

Para transmitir varios fluxos de datos dende unha orixe, estes se multiplexan en grupos de 4 de forma que primeiro se transmite o bit 1 do fluxo 1, logo o bit 1 do fluxo 2, logo o bit 1 do fluxo 3, logo o bit 1 do fluxo 4 e así sucesivamente. O transmisor tamén engade información para poder reconstruír o fluxo cando se recibe. Como os fluxos de datos transmitidos poden non estar a ser recibidos á mesma velocidade no multiplexador de orixe, este supón que os está a recibir á máxima velocidade posible. Esta suposición provoca que as veces non se haxa recibido o bit correspondente dun fluxo, esta situación debe ser notificada ó multiplexador de destino para que este poda reconstruír os fluxos á velocidade correcta.

A velocidade resultante da multiplexación descrita é de 8.448 kbit/s, técnicas similares permiten combinar 4 streams de 8 Mb/s máis bit de recheo (proporcionando 34 Mb/s), 4 streams de 34Mb/s (proporcionando 140Mb/s) e 4 streams de 140 Mb/s (proporcionando 565Mb/s). 565 Mbit/s é



a velocidade típica para transmitir datos sobre fibra óptica para longas distancias.

#### **48.2.2 XERARQUÍA DIXITAL SÍNCRONA (SDH) / SONET**

Synchronous optical networking (SONET) e Synchronous Digital Hierarchy (SDH) son protocolos de multiplexación que transmiten varios streams sobre unha rede de fibra óptica, aínda que tamén se poden usar sobre interfaces eléctricos (a menor velocidade). Esta técnica desenvolveuse para reemplazar PDH na tarefa de transportar un largo número de chamadas de teléfono e tráfico de datos sobre a mesma fibra en problemas de sinalización. A maior diferenza con PDH é que SDH / SONET está sincronizada usando reloxos atómicos reducindo a necesidade de buffers na rede e aproveitandoa mellor.

SONET e SDH, son basicamente idénticos, e, aínda que SONET (ANSI T1.105) é anterior, dado que só é usado en Canada e EEUU mentres que SDH (ITU G.707, G.783, G.784 e G.803) é usado no resto do mundo, SONET considerase unha variación de SDH. Dada a gran similitude entre eles é extremadamente fácil a interconexión entre os dous a calquera velocidade.

##### **48.2.2.1 FRAME SDH / SONET**

Á unidade básica para a transmisión en SDH é a Synchronous Transport Module, level 1 (STM-1), que é transmitida a 155,52Mb/s. SONET cambia o nome desta estrutura a Synchronous Transport Signal 3 concatenated (STS-3c) ou OC-3c dependendo se o sinal se transporta electricamente (STS) ou opticamente (OC) pero a súa funcionalidade, velocidade e tamaño son iguais a STM-1.

SONET proporciona outra unidade STS-1 ou OC-1 que opera a 51,84Mb/s (un tercio de STM-1) esto busca poder transmitir unha canle DS-3 estándar (672 canles de 64Kb/s para voz) .

##### **48.2.2.1.1 FRAMING**

En tecnoloxías como Ethernet a trama consiste nunha cabeceira e un conxunto de datos, a cabeceira é transmitida primeiro, seguida dos datos e posiblemente dunha cola contendo o CRC ou equivalente. En SDH esto

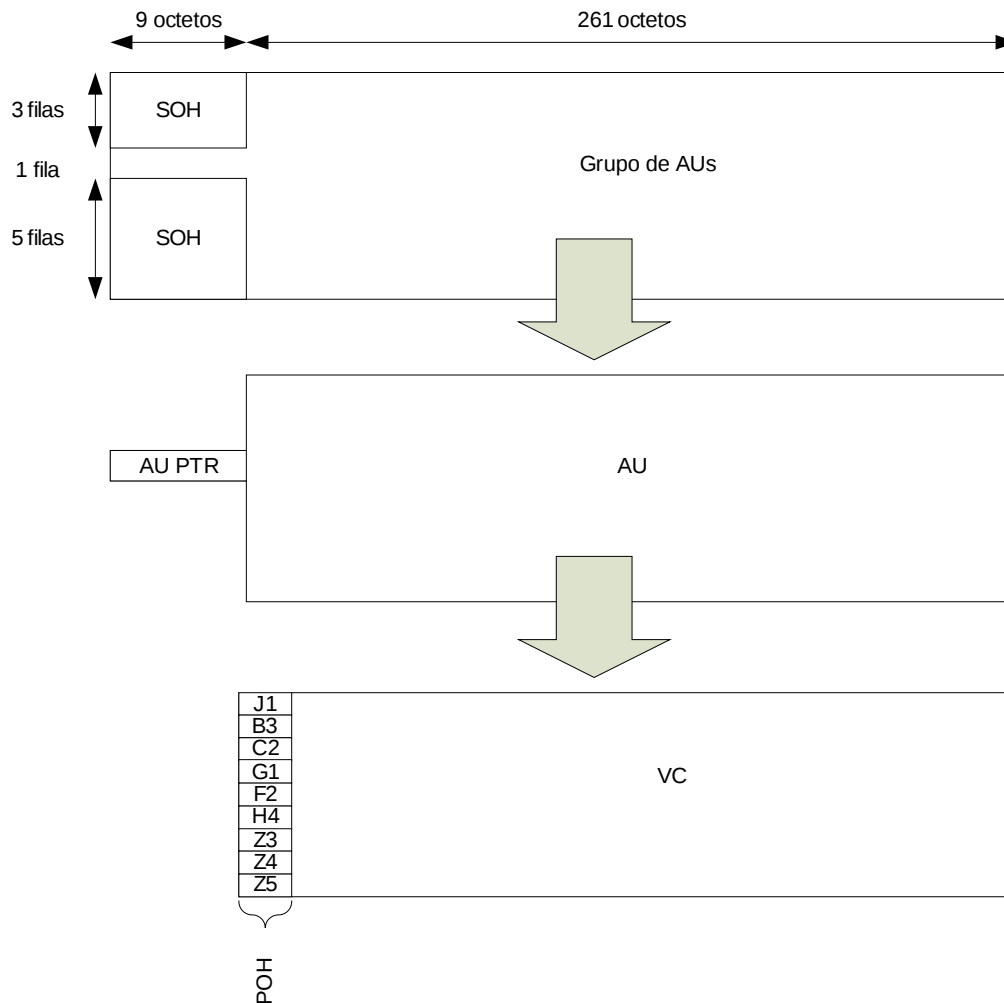
modifícase lixeiramente, a cabeceira denominase overhead e en vez de ser transmitida antes que o resto dos datos é entrelazada con eles durante a transmisión: transmítese parte da cabeceira, logo parte dos datos, ... ata que se transmite todo o frame.

No caso de STS-1, cada frame está composto de 810 octetos, mentres quen o caso de STM-1/STS-3 cada frame está composto de 2.430 octetos. STS-1 transmite 3 octetos de overhead seguidos de 87 de datos durante nove veces ata transmitir os 810 octetos en 125 microsegundos. No caso de STM-1 (que opera a tres veces a velocidade de STS-1) transmítense 9 octetos de overhead e 261 de datos, tamén 9 veces ata que se transmite nos 2.430 octetos levando tamén 125 microsegundos. Isto soe representarse graficamente dibuxando o frame como un bloque de 90 columnas e 9 filas para STS-1 e 270 columnas e 9 filas para STM-1 desta forma a representación alínea toda a overhead e todos os datos da payload.

A estrutura interna da overhead e dos datos transmitidos dentro do frame varían lixeiramente para SONET e SDH, usando tamén diferentes nomes para describir estruturas.

#### **48.2.2.1.2 ESTRUCTURA DO FRAME STM-1**

A Overhead Section e os Administrative Unit Pointers ocupan as 9 primeiras columnas do frame. Estes punteiros (os bytes H1, H2 e H3) identifican AUs (Administrative Units) dentro da carga útil. Cada unha destas unidades administrativas pode albergar un ou varios Virtual Containers (VC) que a súa vez conteñen unha descrición do camiño (Path OverHead, POH) e datos. A primeira columna é para o POH e o resto son para datos que poden ser á súa vez outros VC. As unidades administrativas poden ter calquera tipo de alineación e é esta alineación a que é indicada polo punteiro da fila 4.



Os compoñentes do frame son:

- Overhead contendo:
  - o SOH (Section OverHead) contén información para o sistema de transmisión (para control de calidade, detección de fallas, ...) e está dividida en dúas partes:
    - RSOH (Regenerator Section Overhead) tamén coñecida como Section overhead: composta por 27 octetos contendo información sobre a estrutura do frame.
    - MSOH (Multiplex Section Overhead) tamén coñecida por Line overhead : está composta 45 octetos contendo información sobre corrección de erros e mensaxes Automatic Protection Switching (como poderían ser: alarmas e mensaxes de mantemento)

- o Punteiro AU: Apunta á localización do byte J1 nos datos (o primeiro byte do VC).
- Datos Path: os datos transmitidos de extremo a extremo chámanse datos path e están compostos de 2 elementos:
  - o POH (Path OverHead): nove octetos para sinalización extremo a extremo.
  - o Datos de usuario: 2340 octetos de datos

### **48.3 REDES DE NOVA XERACIÓN (NGN)**

Segundo o ITU-T, unha NGN é unha rede baseada en paquetes que pode prover servizos, incluíndo servizos de telecomunicacións, e capaz de usar varias tecnoloxías de banda ancha que incorporen capacidades de calidade de servizo. Nestas redes as funcións relacionadas co servizo deben ser independentes da tecnoloxía de transporte usada. Ofrecen un acceso sen restriccións ó usuario a diferentes provedores de servizo. Soporta a mobilidade o que permitirá una provisión de servizo consistente e ubicua aos usuarios.

Dende un punto de vista práctico, NGN implica tres cambios na arquitectura:

- Na rede troncal, NGN implica a consolidación de diversas redes de transporte, cada un das cales construída historicamente para un servizo diferente nunha soa rede troncal de transporte (normalmente baseada en IP e Ethernet). Implica entre outras, a migración da voz dende unha arquitectura de conmutación de circuítos (RTC) a VoIP, e tamén a migración de servizos como X.25 e Frame Relay (xa sexa unha migración comercial a nivel de usuario con servizos como VPN sobre IP, ou a migración técnica emulando estes servizos pero sobre a NGN).
- Na rede de acceso por par de cobre, NGN implica a migración dende o sistema dual cá voz independente do xDSL na central á que chega o bucle de aboado a unha configuración onde os DSLAMs (Digital Subscriber Line Access Multiplexer, o punto onde se concentran todas

ás conexións DSL da central) integran portos de voz ou VoIP, posibilitando a eliminación da infraestrutura de conmutación de voz.

- Na rede de acceso de cable, a converxencia NGN implica a migración da voz de servizos CBR a estándares de VoIP e SIP.

Nunha NGN existe unha maior distancia entre a parte da rede que proporciona o transporte (conectividade) e os servizos que se executan sobre este. Isto ten como consecuencia que cada vez que un operador quere dar un novo servizo só ten que definir o nivel da capa de servizos sen preocuparse polo transporte. Cada vez mais os servizos (incluíndo os de voz) tenden a ser independentes da rede de acceso e residen mais nos equipos de usuario final (PC, Set-Top Box, ...).

#### **48.3.1 TECNOLOXÍAS DE SOPORTE**

As redes de nova xeración están baseadas en tecnoloxías coma IP e MPLS. A nivel de aplicación SIP (Session Initiation Protocol) está a reemprazar a H.323. Aínda que orixinalmente H.323 era o protocolo de VoIP / videoconferencia / ... sobre redes IP máis popular, ás súas limitacións para atravesar NAT (Network address translation) e firewalls reducen a súa implantación a nivel do bucle de aboado. Son estas algunhas das razóns (xunto coa complexidade de H.323) que están levando á implantación de SIP, sobre todo no bucle de aboado. Sen embargo, nas redes de operador (onde todo está baixo o seu control) moitos de eles usan H.323 para ás súas redes troncais.

Cos novos cambios introducido sen H.323 é posible que dispositivos H.323 atravesen NAT e firewalls facilmente, esta circunstancia pode propiciar que H.323 poda volver a ser usado en entornos onde isto sexa necesario.

Como contrapartida moitos operadores están á investigar e dar soporte a IMS (IP Multimedia Subsystem, unha arquitectura estandarizada para servizos multimedia en Internet definida polo ETSI e a 3GPP) que daría a SIP a oportunidade de ser o protocolo máis usado.

Para aplicacións de voz o dispositivo mais importante da NGN é o Softswitch (este nome e ás súas funcións aínda son moi dependentes do

fabricante), un dispositivo que controla as chamadas VoIP permitindo a correcta integración de diferentes protocolos dentro da NGN. A súa función principal é crear a interface ás redes telefónicas existentes (RTC).

Un dos termos máis comunmente usados é o de GateKeeper, que orixinalmente referíase a un dispositivo que transformaba voz e datos dende os seus formatos analóxicos a IP. Cando este dispositivo comezou a usar Media Gateway Control Protocol pasou a chamarse Media Gateway Controller (MGC).

Un Axente (Call Agent, SIP Agent, ...) é un nome xeral para dispositivos capaces de controlar chamadas.

#### **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. TECNOLOXÍAS SEN FÍOS: BLUETOOTH, WIBREE, WIRELESS USB, WI-FI. RFID. TECNOLOXÍAS MÓBILES.**

## **Tema 49. Tecnoloxías sen fíos: Bluetooth, WiBree, Wireless USB, Wi-Fi. RFID. Tecnoloxías móbiles**

### **49.1 Tecnoloxías sen fíos**

#### **49.1.1 Bluetooth**

##### **49.1.1.1 Funcionamento de Bluetooth**

##### **49.1.1.1.1 Especificacións e características**

###### **49.1.1.1.1.1 Versión 1.0 e 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 interface de rádio**

###### **49.1.1.1.2.2 Capa do protocolo de xestión de enlace (LMP)**

###### **49.1.1.1.2.3 Interface de controlador Host (HCI)**

###### **49.1.1.1.2.4 Capa do protocolo de adaptación e control do enlace lóxico (L2CAP)**

###### **49.1.1.1.2.5 Capa do protocolo de descubrimento de servizos (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 Descrición do sistema**

###### **49.1.3.1.1 Topoloxía**

###### **49.1.3.1.1.1 USB host**

###### **49.1.3.1.1.2 Dispositivos Wireless USB**

###### **49.1.3.1.1.3 Interface física**

###### **49.1.3.1.1.3.1 Velocidades da capa física**



- 49.1.3.1.1.3.2 Soporte de canles
          - 49.1.3.1.1.3.3 Selección de canle
          - 49.1.3.1.1.4 Xestión de enerxía
          - 49.1.3.1.1.5 Protocolo de bus
          - 49.1.3.1.1.6 Robustez
            - 49.1.3.1.1.6.1 Xestión dos erros
          - 49.1.3.1.1.7 Seguridade
          - 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 fluxos de datos
          - 49.1.3.1.1.10 Dispositivos Wireless USB
            - 49.1.3.1.1.10.1 Características dos dispositivos
            - 49.1.3.1.1.10.2 Dispositivos e capa MAC
          - 49.1.3.1.1.11 Hardware e software do host
  - 49.1.4 Wi-Fi
    - 49.1.4.1 Descrición do sistema
      - 49.1.4.1.1 Capa física(PHY)
        - 49.1.4.1.1.1 Infravermellos
        - 49.1.4.1.1.2 FHSS
        - 49.1.4.1.1.3 DSSS
        - 49.1.4.1.1.4 Tramas da capa física
      - 49.1.4.1.2 Capa de acceso ó medio (MAC)
        - 49.1.4.1.2.1 Tramas do nivel MAC
- 49.2 RFID
  - 49.2.1 Principios de RFID
  - 49.2.2 Compoñentes e operación
- 49.3 Tecnoloxías móbiles
  - 49.3.1 Android

49.3.2 Meego

49.3.3 Symbian

49.3.4 Windows Phone 7

49.4 Bibliografía

## **49.1 TECNOLOXÍAS SEN FÍOS**

### **49.1.1 BLUETOOTH**

É unha tecnoloxía sen fíos de curto alcance (PAN) deseñada para substituír os cables entre dispositivos que se converteu na solución sen fíos ideal para conectar teléfonos móbiles con portátiles para súa conexión a Internet, ou para que outros organizadores de mano, como PDAs poidan conectarse ó PC para coordinar os seus contactos, e incluso para poder imprimir desde un ordenador sen necesidade de cables.

As características intrínsecas das tecnoloxías con bluetooth permiten establecer conexións seguras, con capacidade de encriptación da canle, autenticación da rede e outros parámetros de seguridade como a localización e dispositivo do usuario.

#### **49.1.1.1 FUNCIONAMENTO DE BLUETOOTH**

Bluetooth traballa no rango de frecuencias de 2.4 a 2.48 Ghz, con espectro ensanchado (widespread) e saltos de frecuencia (frequency hopping), con posibilidade de transmitir en full-duplex con un máximo de 1600 saltos/seg. Os saltos de frecuencia realízanse entre un total de 79 frecuencias con intervalos de 1Mhz, o cal permite brindar seguridade e robustez. A frecuencia na cal traballa permítelle atravesar paredes, polo cal é ideal tanto para o móbil, como en oficinas.

A potencia de saída para transmitir a unha distancia máxima de 10m é 1-2,5 mW, mentres que a versión de largo alcance, ata 100m, transmite a 100 mW.

Para lograr alcanzar o obxectivo de baixo consumo e baixo custe, deseñouse unha solución integrada nun só chip. Desta maneira, logrouse crear unha solución de 9x9mm e que consume aproximadamente 97% menos enerxía que un teléfono celular común.

Cada unha das catro canles de voz na especificación Bluetooth pode soportar unha taxa de transferencia de 64 Kb/s en cada sentido, o cal é suficientemente adecuada para a transmisión de voz. Unha canle de datos asíncrono pode transmitir 721 Kb/s nunha dirección e 56 Kb/s na dirección oposta, sen embargo, para unha conexión asíncrona é posible soportar 432,6 Kb/s en ambas direccións se o enlace é simétrico.

Para relacionarse e intercambiar información os dispositivos Bluetooth ofrecen distintos servicios, chamados tecnicamente Perfiles, entre estes perfiles encóntranse o Acceso a Redes locais (LAN), Acceso Telefónico, Fax, Transferencia de Archivos, Sincronización, Intercomunicador, ou Telefonía sen fíos, entre outros. Desta

forma cando dous dispositivos se comunican por primeira vez intercambian esta información para coñecer as súas posibilidades de intercomunicación. As compañías mais destacadas no desenvolvemento desta tecnoloxía foron Ericsson e Nokia. A primeira versión do estándar Bluetooth lanzouse en maio de 1998. Esta tecnoloxía sen fíos tiña unha velocidade de transferencia de datos de 1Mbps e conta con un alcance máximo de 100 metros. Sen embargo a versión mais utilizada é a de alcance 10 metros, xa que o consumo eléctrico aumenta rapidamente con unha maior potencia de transmisión.

#### **49.1.1.1.1 ESPECIFICACIÓN E CARACTERÍSTICAS**

Tras o deseño da primeira especificación en 1994 a especificación foi ratificada polo SIG (Bluetooth Special Interest Group) en 1998 e dende entón evolucionou en varias versións ata a actualidade. Todas as versións inclúen a compatibilidade cos dispositivos das versións anteriores.

##### **49.1.1.1.1.1 VERSIÓN 1.0 E 1.0B**

Estas versións tiveron moitos problemas sobre todo no que a interoperabilidade entre fabricantes se refire.

Tamén obrigaba a incluír a dirección física na transmisión durante o proceso de conexión o cal era contraproducente para algúns dos servizos planificados.

##### **49.1.1.1.1.2 VERSIÓN 1.1**

Foi establecida como estándar 802.15.1-2002 polo IEEE corrixindo moitos erros da versión 1.0B e engadindo soporte para canle son encristados e RSSI (Received Signal Strength Indicator).

#### **49.1.1.1.1.3 VERSIÓN 1.2**

As melloras desta versión inclúen:

- Maior velocidade de conexión e busca (Discovery).
- Uso de AFH (Adaptive Frequency-Hopping) que mellora a resistencia a interferencias evitando o uso de frecuencias moi ocupadas na secuencia de saltos.
- Maior velocidade de transmisión, na práctica ata 721 kbit/s.
- Uso de eSCO (Extended Synchronous Connections) que mellora a calidade dos enlaces de voz permitindo a retransmisión de paquetes corruptos e, opcionalmente, podendo incrementala latencia para mellorar o soporte para a transferencia de datos concorrente.
- Soporte do HCI (Host Controller Interface) para UARTs de 3 fíos.
- Estandarizado coma IEEE 802.15.1-2005.
- Introducción de modos de control de fluxo e retransmisión para L2CAP.

#### **49.1.1.1.1.4 VERSIÓN 2.0 + EDR**

A principal diferenza coa versión anterior é a posibilidade de uso de EDR (Enhanced Data Rate) como modo de transferencia rápido sendo a velocidade nominal de 3 Mbit/s aínda que a velocidade práctica real sexa de 2.1 Mb/s. EDR é opcional na especificación polo que poden existir dispositivos da versión 2.0 que non soporten EDR.

#### **49.1.1.1.1.5 VERSIÓN 2.1 + EDR**

Esta versión foi adoptada polo SIG no 2007 sendo a súa maior aportación ao estándar o SSP (Secure Simple Pairing) que mellor a experiencia de emparellamento dos dispositivos Bluetooth mentres mellora a seguridade.

#### **49.1.1.1.1.6 VERSIÓN 3.0 + HS**

Esta versión é do 2009 soportando en teoría velocidades de ata 24Mb/s, pero non sobre o enlace Bluetooth se non que Bluetooth usase para

negociar o establecemento dun enlace 802.11 sobre o que se transfiren os datos.

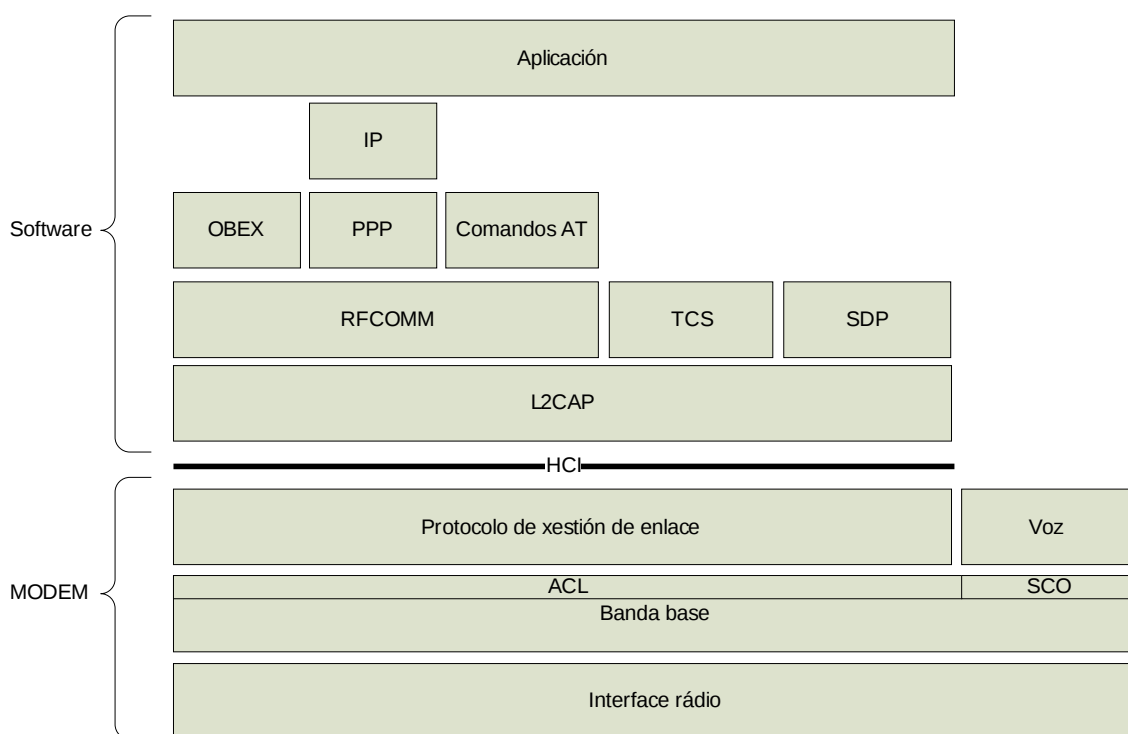
#### **49.1.1.1.1.7 VERSIÓN 4.0**

Esta versión data de xuño de 2010 e inclúe tres sabores do protocolo: Classic Bluetooth, Bluetooth high speed e Bluetooth low energy. Bluetooth high speed está baseado en WiFi e Classic Bluetooth está composto polos protocolos de versións anteriores.

Pola súa parte Bluetooth low energy define unha nova pila de protocolo para a creación rápida de enlaces simple e foi deseñado para executarse en dispositivos de moi baixo consumo.

#### **49.1.1.1.2 PILA DE PROTOCOLOS**

Dunha forma básica podemos ver a pila de protocolos Bluetooth na imaxe seguinte.



##### **49.1.1.1.2.1 CAPA DE BANDA BASE E INTERFACE DE RADIO**

Na base da pila de protocolos Bluetooth encóntranse a capa de banda base e o interface de radio. A súa función principal é permitir o enlace físico por radiofrecuencia (RF) entre unidades Bluetooth realizando tarefas de

modulación e demodulación dos datos en sinais RF que se transmiten polo aire.

O nivel de banda base proporciona dous tipos de enlace físico:

- ACL (Asynchronous ConnectionLess) para enlaces asíncronos sen conexión.
- SCO (Synchronous Connection-Oriented) para enlaces síncronos orientados a conexión.

#### **49.1.1.1.2.2 CAPA DO PROTOCOLO DE XESTIÓN DE ENLACE (LMP)**

A capa LMP é a responsable da configuración e control do enlace entre dispositivos Bluetooth, incluíndo o control e negociación do tamaño dos paquetes.

#### **49.1.1.1.2.3 INTERFACE DE CONTROLADOR HOST (HCI)**

A capa HCI (Host Controller Interface) actúa como fronteira entre as capas de protocolo relativas o hardware (módulo Bluetooth) e as relativas ó software (host Bluetooth). Proporciona unha interface de comandos para a comunicación entre o host e o firmware do módulo Bluetooth e permite dispoñer dunha capa de acceso homoxénea para tódolos módulos Bluetooth, aínda que sexan de distintos fabricantes.

#### **49.1.1.1.2.4 CAPA DO PROTOCOLO DE ADAPTACIÓN E CONTROL DO ENLACE LÓXICO (L2CAP)**

A especificación Bluetooth inclúe o protocolo L2CAP (Logical Link Control and Adaptation Protocol), que se encarga da multiplexación de protocolos, xa que o protocolo de banda base non soporta un campo tipo para identificar o protocolo de nivel superior o que quere transmitir a información, por exemplo SDP, RFCOMM e TCS.

Outra función que se realiza no nivel L2CAP é a segmentación e recomposición de paquetes, necesaria para permitirla utilización de protocolos que utilicen paquetes de maior tamaño que os soportados pola capa de banda base.

#### **49.1.1.1.2.5 CAPA DO PROTOCOLO DE DESCUBRIMENTO DE SERVICIOS (SDP)**

O descubrimento de servizos fai referencia á capacidade de buscar e encontrar servizos dispoñibles en dispositivos Bluetooth. A través dos servizos, dos dispositivos poden executar aplicacións comúns e intercambiar datos.

#### **49.1.1.1.2.6 CAPA RFCOMM**

O protocolo RFCOMM (Radio Frequency Communication) é un protocolo de emulación de liña serie baseado no estándar ETSI TS 07.10. Proporciona unha emulación dos portos serie RS-232 sobre o protocolo L2CAP.

#### **49.1.1.1.2.7 COMANDOS AT**

Os comandos AT son instrucións codificadas que conforman unha linguaxe de comunicación entre o home e un terminal módem. Os comandos AT denomínanse así por la abreviatura de attention.

#### **49.1.2 WIBREE**

En 2001, investigadores Nokia determinan que existen varios escenarios non cubertos polos sistemas sen fíos da época. Para solucionar este problema Nokia Research Center comezou a desenvolver unha tecnoloxías en fíos adaptada dende o estándar Bluetooth que proporcionase un dispositivo de mais baixo consumo e prezo pero sen ser moi distinto a un Bluetooth. O resultado foi publicado en 2004 usando o nome Bluetooth Low End Extension, e tras mais desenvolvemento a tecnoloxía foi publicada co nome de WiBree en outubro de 2006. Tras unha negociación co SIG de Bluetooth, en xuño de 2007 acordouse que WiBree sería incluído nunha futura especificación de Bluetooth coma Bluetooth ultra-low-power que hoxe se coñece coma Bluetooth low energy (presenta na especificación Bluetooth 4.0).

BLE (Bluetooth Low Energy) opera no mesmo rango de frecuencias que Classic Bluetooth (2402-2480 MHz) pero usa un conxunto de canles distinto, en vez de usar os 79 canles de 1Mhz. BLE usa 40 canles de 2 Mhz. BLE foi deseñado para permitir dúas alternativas: modo simple e modo dual. Os dispositivos sinxelos, coma sensores, reloxos, etc. están baseados no modo simple permitindo só BLE, mentres que os dispositivos de modo dual combinan BLE con Classic Bluetooth na mesma circuitería.

A pesar de que Classic Bluetooth e BLE poden coexistir non son compatibles entre sí. Podemos velas principais diferencias na seguinte taboa.

	Classic Bluetooth	Bluetooth Low Energy
Alcance	100 m	200 m
Velocidade da transmisión	1-3 Mb/s	1 Mb/s
Velocidade aproveitable	0.7-2.1 Mb/s	0.26 Mb/s
Latencia típica	100 ms	6 ms
Capacidade para voz	Si	Non
Topoloxía	Malla	Etrella - Bus
Consumo	1mW	0,01 a 0,5mW
Pico de consumo de corrente	<30mA	<20mA

### **49.1.3 WIRELESS USB**

Wireless USB é un protocolo de comunicación sen fíos de alta velocidade e reducido alcance baseado na plataforma común de radio UWB (Ultra-WideBand) e sendo capaz de transmitir a 480Mb/s ata unha distancia de 3 metros e a 11Mb/s ata unha distancia de 10 metros. Foi deseñado para operar no rango de frecuencias entre 3.1 e 10.6 Ghz aínda que as regulacións de cada país poden limitar este rango.

Sen embargo, a pesar de que existe unha gran excitación sobre Wireless USB e soporte dos grandes fabricantes, non acaba de despegar. A pesares de que tecnicamente Wireless USB ten moitas vantaxes sobre BlueTooth e WiFi (os seus principais competidores) estas outras tecnoloxías xa tiñan a súa posición no mercado e non había espacio para unha nova.

#### **49.1.3.1 DESCRICIÓN DO SISTEMA**

Un sistema USB esta composto por un host e un número indeterminado de dispositivos funcionando na mesma conexión lóxica e pode ser descrito por 3 áreas:

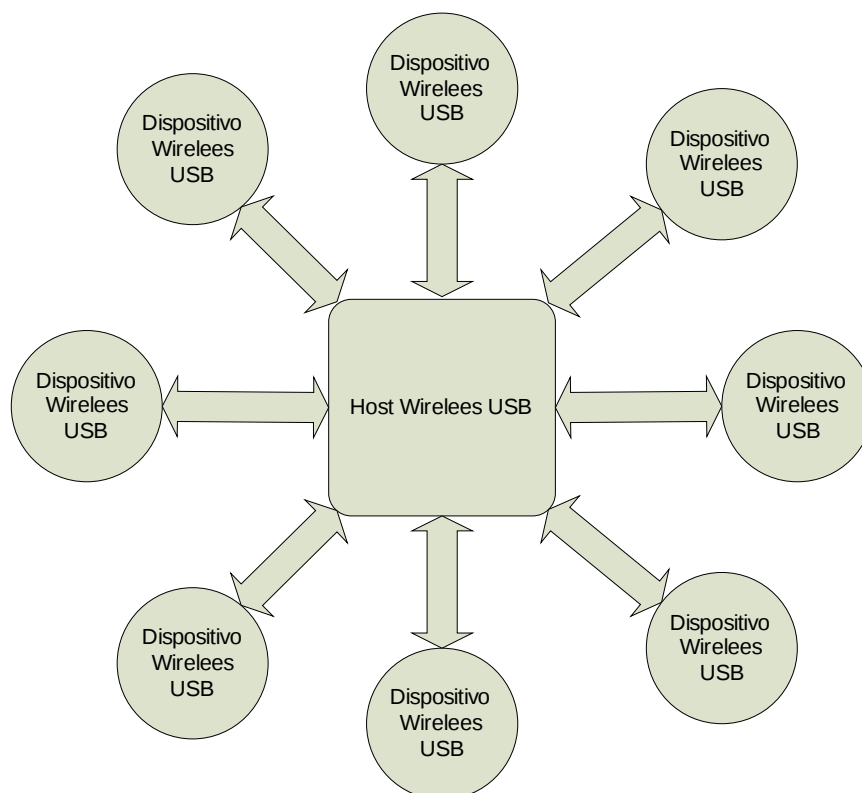
- Interconexión USB
- Dispositivos USB
- Host USB



Neste documento centrarémonos na descrición da Interconexión USB.

#### **49.1.3.1.1 TOPOLOXÍA**

Wireless USB conecta dispositivos usando un modelo de “conectarse ó concentrador e falar” (“hub and spoke”). O host é o concentrador no centro da topoloxía e cada dispositivo encontrase ó final dunha conexión punto a punto co host. Un host pode soportar ata 127 dispositivos debido a que Wireless USB non ten un interfaz físico para cada porto (conector como o de o USB) non hai necesidade de instalar ningún dispositivo para expandilos portos.



##### **49.1.3.1.1.1 USB HOST**

Solo hai un host en calquera sistema USB. A interface co ordenador host chamase Host Controller e tipicamente están conectados aos PCs usando buses internos como o PCI. O Host Controller pode estar implementado coma unha combinación de hardware, firmware e software.

Os adaptadores que usan cables e se conectan directamene ó PC usando USB coñécense como Host Wire Adapter, estes dispositivos proporcionan capacidade de Host Wireless USB ó PC.

Os adaptadores que proporcionan conexións USB pero se conectan a o host usando Wireless USB chamanse Device Wire Adapters e típicamente usan conectores USB tipo A.

Hai que ter en conta que cada un destes adaptadores crea un novo sistema USB con un host (o adaptador) e un ou varios dispositivos USB.

#### **49.1.3.1.1.2 DISPOSITIVOS WIRELESS USB**

Os dispositivos USB poden adoptar unha das seguintes formas:

- Funcións: provén capacidades ao sistema coma impresoras, cámaras dixitais, ...
- Device Wire Adapter: xa descrito mais arriba

Os dispositivos Wireless USB proporcionan unha interface estándar en termos de:

- A súa comprensión do protocolo Wireless USB
- A súa resposta a operacións USB estándar como confirmación ou reinicialización
- A súa capacidade de proporcionar información descriptiva

#### **49.1.3.1.1.3 INTERFACE FÍSICA**

##### **49.1.3.1.1.3.1 VELOCIDADES DA CAPA FÍSICA**

A capa física de Wireless USB esta descrita na especificación UWB PHY da WiMedia Alliance e soporta velocidades de transmisión de 53,3, 80, 106,7, 200, 320, 400, e 480Mb/s con múltiples canles.

PHY aporta tamén esquemas de detección e corrección de erros para prover unha canle de comunicación tan robusta como sexa posible.

As velocidades de 53,3, 106,7 e 200 son obrigatorias para os dispositivos Wireless USB o resto de velocidades son opcionais.

Os host Wireless USB están obrigados a implementar tódalas velocidades descritas.

##### **49.1.3.1.1.3.2 SOPORTE DE CANLES**

Todas as implementacións Wireless USB deben soportar as canles PHY da 9 á 15 (Band Group 1, Códigos TF 1-7) se está permitido polas regulacións

nacionais. Na versión 1.1 débense soportar Band Group 3 ou Band Group 6 (tódolos códigos TF) e no caso dos hosts tamén ás usadas na versión 1.0.

#### **49.1.3.1.1.3.3 SELECCIÓN DE CANLE**

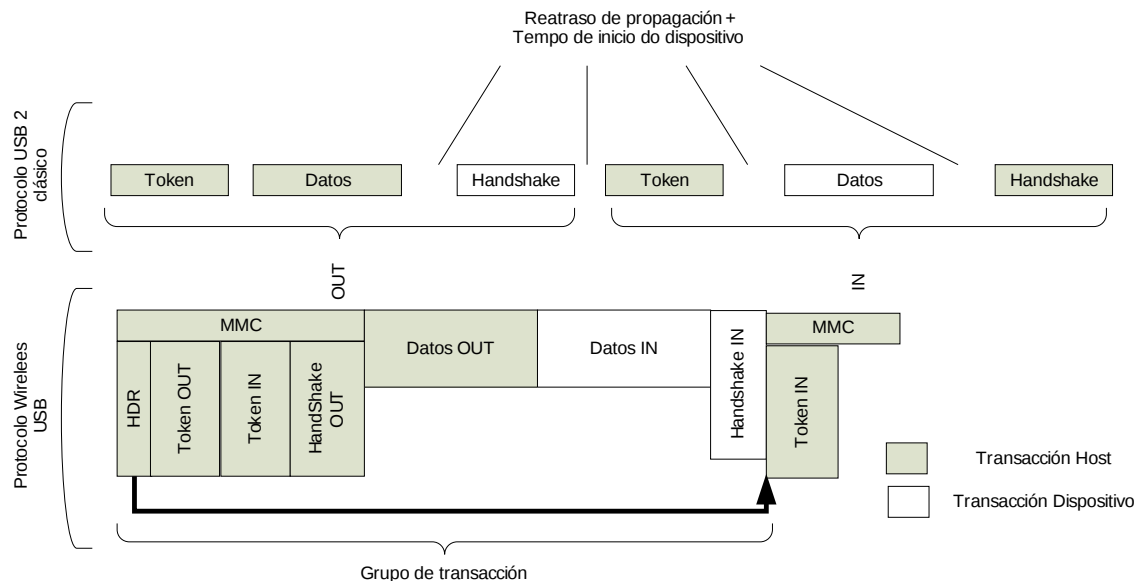
As implementacións de Wireless USB deben soportar un canle inicial para encontrar outros dispositivos e, despois desta busca, poden moverse a outra canle.

#### **49.1.3.1.1.4 XESTIÓN DA ENERXÍA**

Un host Wireless USB pode ter un sistema de xestión da enerxía independente do USB. O software do sistema USB interactuará co xestor de enerxía do host para procesar os eventos tales como a suspensión. Ademais os dispositivos USB implementarán características adicionais para a xestión da enerxía que poden ser usadas polo software do sistema.

#### **49.1.3.1.1.5 PROTOCOLO DO BUS**

Loxicamente Wireless USB é un protocolo baseado en TDMA similar ao de USB. O Host Controller inicia todas as transmisión de datos. Da mesma forma que no USB de cable, cada transferencia esta composta de 3 “paquetes”: token, datos e handshake. Sen embargo, para melloral a eficiencia da capa física eliminando transmisións constantes entre o emisor e o receptor, os hosts combinan información de múltiples tokens nun so paquete. Nese paquete o host indica o tempo apropiado para que os dispositivos escoiten un paquete OUT ou para que transmitan un paquete IN ou handshake.



Da mesma forma que en USB, o modelo de transferencia de datos entre unha orixe e un destino chamase pipe.

Wireless USB define un novo máximo tamaño de paquete para algunhas transmisións co obxectivo de mellorar o rendemento e o consumo.

#### **49.1.3.1.1.6 ROBUSTEZ**

Hai varios atributos de Wireless USB que contribúen á súa robustez:

- A capa física está deseñada para unha comunicación fiable e robusta con detección e corrección de erros.
- Detección de conexións e desconexións e configuración de recursos no sistema
- Autorecuperación no propio protocolo usando timeouts para paquetes perdidos e corruptos
- Control de fluxo metendo nun buffer e reintentando

##### **49.1.3.1.1.6.1 XESTIÓN DOS ERROS**

O protocolo permite a xestión de erros tanto en hardware como en software.

A xestión de erros en hardware incue o reporte e envío de transferencias fallidas. Un host reintentará unha transmisión na que se encontren erros ata un número limitado de veces antes de informalo software do fallo.

O software pode recuperarse dese fallo nunha forma que é dependente da implementación.

#### **49.1.3.1.1.7 SEGURIDADE**

Tódolos hosts e tódolos dispositivos Wireless USB deben soportar o nivel de seguridade definido na especificación. O mecanismo de seguridade asegúrase de que ambos, host e dispositivo, son capaces de autenticarse un ao outro (impedindo un ataque de man-in-the-middle) e de que as comunicacións son privadas.

Á seguridade básease en encriptación AES-128/CCM, as comunicacións entre o host e o dispositivo usan claves que só o host e o dispositivo posúen unha vez que están autenticados un no outro.

#### **49.1.3.1.1.8 CONFIGURACIÓN**

De igual forma que co USB, Wireless USB soporta dispositivos conectándose e desconectándose do host polo que o software do sistema debe soportar esta circunstancia.

##### **49.1.3.1.1.8.1 CONEXIÓN DE DISPOSITIVOS WIRELESS USB**

A diferenza de USB, un dispositivo Wireless Usb conectase a un host enviando unha mensaxe nun momento determinado. O host e o dispositivo auténtícanse entre eles usando os seus identificadores únicos e as claves de seguridade apropiadas.

Despois de que o dispositivo e o host se haxan autenticado e autorizado, o host asígnalle unha dirección USB única ó dispositivo e notifica ó software do sistema da conexión do dispositivo.

##### **49.1.3.1.1.8.2 DESCONEXIÓN**

A desconexión dos dispositivos pode ser realizada de forma explícita polo host ou o dispositivo usando os mecanismos definidos no protocolo. A desconexión tamén se produce se o host non pode comunicarse co dispositivo por un longo período de tempo.

##### **49.1.3.1.1.8.3 ENUMERACIÓN**

Esta actividade permite identificar e asignar direccións únicas a os dispositivos conectados ó bus lóxico. Dado que Wireless USB permite aos dispositivos conectarse ou desconectarse do bus lóxico en calquera

momento, a enumeración é unha tarefa continua do software do sistema USB. Adicionalmente a enumeración de Wireless USB permite tamén a detección e procesado das desconexións.

#### **49.1.3.1.1.9 TIPOS DE FLUXOS DE DATOS**

Wireless USB soporta os mesmos tipos de transferencia e “pipes” que USB. Debido ó seu maior nivel de erro (por razóns do medio de transmisión), o protocolo de Wireless USB define diferentes mecanismos para realizalas transmisións, estes mecanismos inclúen handshakes durante a recepción de datos e o uso de buffers para permitir unha certa confianza no pipe. A asignación de ancho de banda realízase de forma similar a USB.

#### **49.1.3.1.1.10 DISPOSITIVOS WIRELESS USB**

Da mesma forma que os dispositivos USB, os dispositivos Wireless USB están divididos en clases de dispositivos tales coma interface humana, impresoras ou dispositivos de almacenamento. Os dispositivos Wireless USB teñen que almacenar a información necesaria para a súa identificación e configuración. Tamén se require deles que mostren un comportamento consistente cos estados USB definidos.

Unha cousa importante é que os concentradores, non son dispositivos Wireless USB xa que o propio host soporta 127 dispositivos.

##### **49.1.3.1.1.10.1 CARACTERÍSTICAS DOS DISPOSITIVOS**

Da mesma forma que en USB, todos os dispositivos Wireless USB son accesibles usando unha dirección USB que é asignada cando o dispositivo se conecta e sofre o proceso de enumeración. Cada dispositivo USB soporta adicionalmente un ou varios “pipes” polos que o host pode comunicarse con el. Todos os dispositivos deben soportar un “pipe” especial ao que se conectara o “pipe” de control USB do dispositivo. Tódolos dispositivos soportan un mecanismo de acceso á información a través deste “pipe” de control. Asociado a este “pipe” está a información requirida para describir por completo o dispositivo USB.

##### **49.1.3.1.1.10.2 DISPOSITIVOS E CAPA MAC**

Os dispositivos deben implementar unha capa MAC que se comporte adecuadamente.

#### **49.1.3.1.1.11 HARDWARE E SOFTWARE DO HOST**

O host posúe unhas responsabilidade maiores que no caso de USB. O host Wireless USB debe comportarse de forma responsable con respecto á capa MAC e pode que teñan que compartir a UWB con outras aplicacións do host, por exemplo nun PC ó acceso radio pode ser compartido entre Wireless USB e a conexión de rede.

Os hosts son tamén responsables de conectarse a outros dispositivos UWB (incluíndo outros hosts Wireless USB) de forma ordenada para reducil a interferencia e mellorar o uso de ancho de banda.

Á especificación de hosts Wireless USB cubre hosts implementados coma parte de Pcs, no caso doutros dispositivos que non se conforman a este estándar (dispositivos portátiles, embebidos, ...) poden elixir implementar un subconxunto dos requisitos.

#### **49.1.4 WI-FI**

Hoxe en día existen varias tecnoloxías e estándares para as comunicacións de redes de área local sen fíos.

Estes estándares, definen unha rede formada por un medio inalámbrico compartido e transmisión encriptada da información.

IEEE 802.11 é un estándar para redes inalámbricas definido pola organización Institute of Electrical and Electronics Engineers (IEEE), instituto de investigación e desenvolvemento, de gran recoñecemento e prestixio, cuos membros pertencen a decenas de países entre profesores e profesionais das novas tecnoloxías.

O estándar IEEE 802.11 é un estándar en continua evolución, debido a que existen cantidade de grupos de investigación, traballando en paralelo para melloralo estándar, a partir das especificacións orixinais.

Na actualidade coexisten principalmente os seguintes estándares:

- 802.11b: Este estándar especifica transmisións na banda de frecuencias dos 2.4GHz, con velocidades de ata 11 Mbps.
- 802.11a: Este estándar, posterior ó 802.11b, especifica transmisións na banda dos 5 GHz (unha banda con menos ruído que a dos 2.4 GHz)

) e con unha velocidade de ata 54 Mbps. Posúe unha menor cobertura que 802.11b.

- 802.11g: Especifica transmisións de ata 54 Mbps na banda dos 2.4GHz e asegura a compatibilidade cos dispositivos 802.11b.
- 802.11n: Aprobado no 2009 especifica velocidades de transmisión de ata 600Mb/s.

A alianza WI-FI (Wireless Fidelity) é unha organización sen ánimo de lucro formada en 1999 para certificar a interoperabilidade dos produtos 802.11 e para promocionalos con un estándar global de WLAN en tódolos segmentos de mercado. Hoxe en día, existen mais de 500 produtos certificados, principalmente en 802.11b/g.

Trátase dunha especificación en continua evolución con posibilidade de adaptarse a novos requirimentos e demandas de usuario no futuro.

#### **49.1.4.1 DESCRICIÓN DO SISTEMA**

O estándar permite o uso de varios medios e técnicas para establecer conexións. Incluso o estándar orixinal permite usar infravermellos e espectro ensanchado, tanto en salto de frecuencias como secuencia directa, coa vantaxe de usar unha capa de acceso ó medio (MAC) común. Isto proporciona moita flexibilidade aos desenvolvedores e investigadores, que poden esquecerse de certos aspectos xa que non existe dependencia directa entre eles.

Os estándares de IEEE 802.11 son de libre distribución e calquera persoa pode ir á páxina Web do IEEE e descargarlos. Estes estándares só definen especificacións para as capas físicas e de acceso ao medio e para nada tratan modos ou tecnoloxías a usar para a implementación final.

Esto debe permitir e facilitar a interoperabilidade entre fabricantes de dispositivos IEEE 802.11 e para asegurarse diso creouse unha alianza denominada WECA para crear e definir procedementos para conseguir certificados de interoperabilidade e de cumprilas especificación, todo dentro dun estándar chamado WiFi (Wireless Fidelity). O nome ademais é un indicativo do enfoque doméstico e moi enfocado cara o usuario final.



O bloque constructivo básico dunha rede inalámbrica 802.11 é o denominado conxunto de servizo básico (BSS, Basic Service Set), que é un área xeográfica na que as estacións sen fíos se poden comunicar.

O tipo mais sinxelo de BSS consiste en dous ou mais equipos que entran dentro das áreas de transmisión respectivas. Este proceso polo que os dispositivos entran nun BSS denomínase asociación.

#### **49.1.4.1.1 CAPA FÍSICA (PHY)**

A capa física en calquera rede define a modulación e características de sinalización para a transmisión de datos nese medio. Para poder transmitir en redes sen fíos en bandas sen licenza necesítanse usar técnicas de espectro ensanchado, definidas nos requirimentos de case tódolos países. No estándar IEEE 802.11 defínense tres medios de nivel físico. Un usa sinais de infravermellos e os outros dous utilizan sinais de radio frecuencia (RF).

Os medios de RF 802.11 funcionan na banda de 2.4Ghz, con un ancho de banda de 83Mhz entre 2.400 e 2.483 GHz, aínda que en España tan só temos 23Mhz, como Francia e Xapón. Ademais hai definicións de potencia máxima de transmisión definidas polos distintos organismos de regulación. En EEUU defínese unha potencia máxima de 1W, para Europa 10mW cada 1 Mhz e para Xapón 10mW.

As definicións para a transmisión por radiofrecuencia nos estándares son de espectro ensanchado por salto en frecuencias (FHSS) e espectro ensanchado por secuencia directa (DSSS). Ambos están definidos para traballar na banda de 2.4Ghz, e DSSS ademais ten unha variante na banda dos 5Ghz, que consegue maiores velocidades de transmisión.

##### **49.1.4.1.1.1 INFRAVERMELLOS**

As comunicación por infravermellos utilizan frecuencias entre 850 e 950 nanómetros, xusto por debaixo do espectro da luz visible. A implementación IEEE 802.11 de infravermellos, a diferenza da maioría dos medios infravermellos, non require comunicación de visión directa, pode funcionar mediante sinais reflexadas.

Sen embargo, debido o seu limitado alcance comparado cos medios de RF e a que só pode funcionar adecuadamente nun ambiente interior cando as superficies proporcionan unha boa reflexión dos sinais, é raro que se implemente nas redes sen fíos. Ademais impón mais restriccións na ubicación física do dispositivo que FHSS ou DSSS.

#### **49.1.4.1.1.2 FHSS**

FHSS (Frequency-Hopping Spread Spectrum) refírese a un sistema que periodicamente cambia as frecuencias nas que transmite. Utilízase a banda enteira o que contribúe a aumentala seguridade fronte a escoitas á vez que axuda a suprimir o ruído ou as interferencias.

FHSS ten 22 patróns de saltos predefinidos usando 79 canles de 1Mhz a un mínimo de 2.5 saltos por segundo, e para resolver os problemas de sincronización, para que tanto transmisor como receptor salten á vez, defínense paquetes de sincronización.

A velocidade dos cambios de frecuencia é independente da velocidade de bit de transmisión de datos. Se a velocidade do salto de frecuencia é menor que a velocidade de bit do sinal, a tecnoloxía denomínase sistema de salto lento, e se é maior denomínase sistema de salto rápido.

Para a modulación FHSS usa FSK gaussiano de 2 ou 4 niveis. As velocidades típicas conseguidas son de 1 e 2 Mbps para FHSS.

#### **49.1.4.1.1.3 DSSS**

DSSS (Direct Sequence Spread Spectrum) traballa nun canle fixo e preconfigurado, o que lle permite obter maiores taxas de transferencia, pero coa desvantaxe de ser mais sensible a interferencia e a sinais procedentes de outros dispositivos usando a mesma frecuencia. É posible ter tres puntos de acceso con tres canles diferentes, sen solapar en un mesmo emprazamento e sen ter en conta ningún tipo de planificación. Aínda para mais de tres puntos de acceso é necesaria certa planificación, para poder mantelas velocidades, posto que o solape de celdas e frecuencias terá un deterioro sobre o rendemento.

As modulacións usadas para DSSS son BPSK e DQPSK para o estándar orixinal. Para 11b, que permite conseguir 11Mbps, utilízase CCK.

Ademais definiuse una variante de IEEE 802.11, que permite conseguir 54Mbps na banda de 5Ghz, con un ancho de banda de ata 300MHz e usando una modulación OFDM.

Esta mesma modulación é a usada por 802.11g e 802.11n.

#### **49.1.4.1.1.4 TRAMAS DA CAPA FÍSICA**

En lugar de ter un esquema de sinalización relativamente sinxelo coma en Ethernet e Token Ring que utilizan Manchester e Manchester diferencial respectivamente, os medios que funcionan en 802.11 teñen o seu propio formato de tramas, que encapsulan as tramas xeradas no nivel de enlace de datos.

A trama de FHSS contén os seguintes campos:

- Preámbulo (10 bytes): contén 80 bits de 1 e 0 alternos utilizados polo receptor para detectalo sinal e sincronizalos tempos.
- Delimitador de comezo de trama (SFD) (2 bytes): indica o comezo da trama.
- Lonxitude (12 bits): indica o tamaño do campo de datos.
- Sinalización (4 bits): contén un bit para indicar se se está utilizando a velocidade de 1 ou 2 Mbps. Os outros 3 bits resérvanse para uso futuro. Só o campo de datos se pode transmitir a 2 Mbps.
- CRC (2 bytes): contén un valor de comprobación de redundancia cíclica.
- Datos (de 0 a 4.095 bytes): contén a trama do nivel de enlace de datos que se transmite.

A trama DSSS contén os seguintes campos:

- Preámbulo (16 bytes): contén 128 bits que o sistema receptor utiliza para axustarse á sinal entrante.
- Delimitador de comezo de trama (SFD) (2 bytes): indica o comezo da trama.
- Sinal (1 byte): especifica a velocidade de transmisión.
- Servizo (1 byte): contén o valor hexadecimal 00 que indica que o sistema cumpre co estándar 802.11

- Lonxitude (2 bytes): indica o tamaño do campo de datos.
- CRC (2 bytes): contén un valor de comprobación de redundancia cíclica.
- Datos (variable): contén a trama do nivel de enlace de datos que se transmite.

A trama de infravermellos contén os seguintes campos:

- Delimitador de comezo de trama (SFD) (2 ranuras): indica o comezo da trama.
- Velocidade de datos (3 ranuras): especifica a velocidade de transmisión.
- Axuste do nivel de DC (DCLA) (32 ranuras): utilizado polo receptor para estabilizar o nivel DC despois de transmitir os campos precedentes.
- Lonxitude (12 bits): indica o tamaño do campo de datos.
- CRC (2 bytes): contén un valor de comprobación de redundancia cíclica.
- Sincronización (SYNC) (entre 57 y 73 ranuras): utilizadas polo sistema receptor para sincronizalo tempo e opcionalmente para estimar a relación sinal/ruído.
- Datos (de 0 a 2.500 bytes): contén a trama do nivel de enlace de datos que se transmite.

#### **49.1.4.1.2 CAPA DE ACCESO Ó MEDIO (MAC)**

A especificación da capa MAC do IEEE 802.11 ten moitas similitudes co estándar de Ethernet cableado (IEEE 802.3). O protocolo do 802.11 é un esquema de protocolo coñecido como detección de portadora, acceso múltiple, evitando colisións (CSMA/CA). Este protocolo evita as colisións, en vez de detectalas como o algoritmo de 802.3 (CSMA/CD). É extremadamente difícil detectar colisións nunha rede de transmisión de radiofrecuencias e de ahí que se trate de evitalas colisións.

A capa MAC opera xunto coa capa física muestreando a enerxía do medio de transmisión de datos. O protocolo CSMA/CA permite opcións para que se

poda minimizalas colisións usando tramas de transmisión RTS/CTS (Request-to-send/Clear-to-send), datos e recoñecementos dunha maneira secuencial. Nestas tramas sóense incorporar datos de duración dos envíos co obxectivo de asegurar que eses envíos non van a ser interrompidos: os demais nodos saben que deben estar calados durante ese intervalo de tempo. Todo elo ademais se asegura e confirma con tramas de recoñecemento (ACK).

Pero un problema común a calquera WLAN é o problema dos nodos ocultos. Isto pode chegar a reducilas prestacións nun 40% nunha WLAN con alta carga. Producese cando un nodo non pode escoitar transmisións dun nodo e trata de transmitir a un nodo que si pode escoitalos, alí se pode xerar moitas colisións.

Algunhas melloras incluíronse para evitalo problema co uso de RTS/CTS dunha maneira intelixente.

Ademais utilízanse tempos entre tramas para evitar colisións isto, a parte de evitar colisións, permite ademais certo uso de clases de calidade ou polo menos de preferencia dun tráfico sobre outro, utilizando funcións de coordinación puntual e de permitilo acceso ó medio de tráfico prioritario antes que aos demais.

#### **49.1.4.1.2.1 TRAMAS DO NIVEL MAC**

O estándar 802.11 define tres tipos básicos de tramas neste nivel:

- Tramas de datos: úsanse para transmitir datos dos niveis superiores entre estacións.
- Tramas de administración: úsanse para o intercambio de información para realizar funcións de rede como a autenticación e a asociación.
- Tramas de control: úsanse para regularo acceso ó medio e para recoñecemento das tramas de datos transmitidas.

Unha trama MAC xenérica contén os seguintes campos:

- Control da trama (2 bytes): contén 11 subcampos que habilitan as distintas funcións do protocolo:

- Versión do protocolo (2 bits): especifica a versión do estándar que se está a usar.
- Tipo (2 bits): indica se a trama é de administración (00), control (01) ou datos (00).
- Subtipo (4 bits): identifica a función específica da trama.
- A DS (1 bit): un valor de 1 indica que a trama transmítese ó sistema de distribución a través dun punto de acceso.
- Dende DS (1 bit): un valor de 1 indica que a trama recibíuse dun sistema de distribución.
- Mais fragmentos (1 bit): un valor de 1 indica que o paquete contén un fragmento dunha trama e que hai mais fragmentos para a súa transmisión.
- Reintento (1 bit): un valor de 1 indica que a trama se está retransmitindo debido a unha falta de recepción dun ack.
- Administración de enerxía (1 bit): un valor de 0 indica que a estación está funcionando en modo activo; un valor de 1 en modo aforro de enerxía.
- Mais datos (1 bit): se vale 1 indica que o AP ten mais paquetes almacenados para a estación e en espera de transmisión.
- WEP (1 bit): se vale 1 indica que o corpo da trama cifrouse utilizando WEP.
- Orde (1 bit): se vale 1 indica que a trama de datos se está transmitindo utilizando a clase de servizo estritamente ordenado.
- Duración/AID (2 bytes): nas tramas de control de sondeo de enerxía contén a identidade de asociación (AID) da estación transmisora. No resto de tramas contén o tempo (en microsegundos) necesario para transmitir unha trama máis o intervalo entre tramas.
- Dirección 1 (6 bytes): contén unha dirección que identifica ó receptor da trama, dependendo dos valores dos subcampos A DS e Dende DS.
- Dirección 2 (6 bytes): contén unha dirección, dependendo dos valores dos subcampos A DS e Dende DS.

- Dirección 3 (6 bytes): contén unha dirección, dependendo dos valores dos subcampos A DS e Dende DS.
- Control de secuencia (2 bytes): contén dous subcampos:
  - Número de fragmento (4 bits): contén un valor que identifica un fragmento particular nunha secuencia.
  - Número de secuencia (12 bits): contén un valor que identifica os fragmentos da secuencia que compoñen o conxunto de datos.
- Dirección 4 (6 bytes): contén unha dirección, dependendo dos valores dos subcampos A DS e Dende DS.
- Corpo da trama (0 a 2.312 bytes): contén a información que se está transmitindo á estación receptora.
- Secuencia de verificación de trama (4 bytes): contén un valor CRC.

Os cinco tipos de dirección do subnivel MAC son:

- Dirección do emisor (TA): unha dirección MAC individual que identifica ó sistema que transmitiu a información que vai no corpo da trama no medio sen fíos actual (un AP).
- Dirección do receptor (RA): unha dirección MAC individual ou de grupo que identifica ó receptor inmediato da información no corpo da trama no medio inalámbrico actual (un AP).
- Dirección destino (DA): unha dirección MAC individual ou de grupo que identifica ó receptor final dunha unidade de datos de servizo.
- Dirección orixe (SA): unha dirección MAC individual que identifica ó sistema que xenerou a información que vai no corpo da trama.
- ID do conxunto de servizo básico (BSSID): nunha rede ad hoc o BSSID é un valor xenerado aleatoriamente durante a creación do BSS; nunha rede con infraestrutura é a dirección MAC da estación que funciona como AP do BSS.

## **49.2 RFID**

RFID (Radio-frequency identification) é unha tecnoloxía que usa a comunicación mediante ondas de radio para transferir datos entre un lector

e unha etiqueta electrónica adherida a un obxecto co propósito de identificación ou seguimento.

Unha etiqueta pasiva de RFID (unha sen alimentación propia) pódese ler cun lector RFID se se aproxima suficientemente.

#### **49.2.1 PRINCIPIOS DE RFID**

Existen moitos tipos de RFID, pero no maior nivel de abstracción podemos dividilas en dous clases: activo e pasivo.

As etiquetas activas requiren enerxía de unha fonte, están ou conectadas á rede eléctrica ou a unhas baterías. No caso de usar baterías a vida da etiqueta está limitada pola duración destas contra o número de lecturas que sufrirá o dispositivo. Un exemplo de etiqueta activa é o transpondedor dun avión que identifica á súa nación de procedencia.

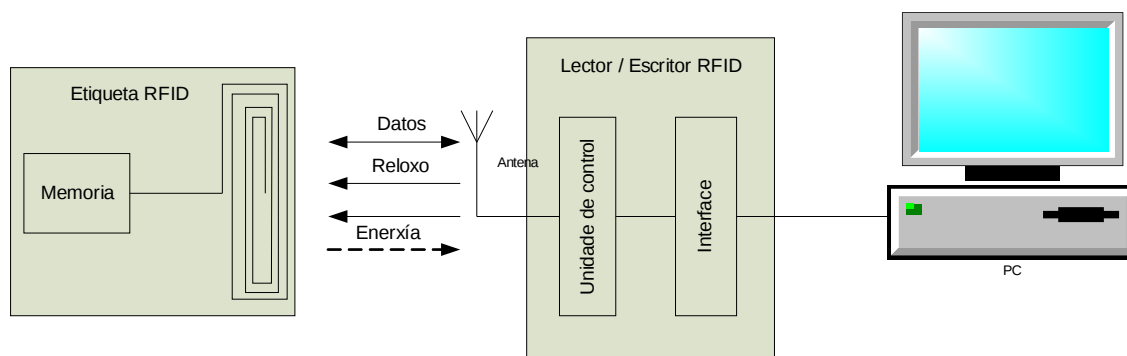
Sen embargo as baterías fan que o custo, tamaño e duración das etiquetas activas sexa pouco práctica. As etiquetas RFID pasivas son interesantes porque non necesitan mantemento, teñen un período de vida indeterminado e son suficientemente pequenas como para caber nunha etiqueta adhesiva.

Unha etiqueta pasiva esta composta por 3 elementos: unha antena, un chip conectado á antena e algún tipo de encapsulación. O lector de etiquetas é o responsable de aportala enerxía e comunicarse coa etiqueta para ler o seu ID (o chip da etiqueta coordina este proceso). A encapsulación mantén integridade física da etiqueta e protexe a antena e o chip das condicións ambientais. Esta encapsulación pode ser un cristal ou unha lamina de plástico con adhesivo por unha das caras para permitir a súa adherencia a una superficie.

Existen dúas aproximacións fundamentais distintas para transmitir enerxía á etiqueta dende o lector: inducción magnética e captura de onda electromagnética (EM). Estes dous deseños toman coma vantaxe as propiedades EM asociadas cunha antena cunha potencia típica de desde 10 microvatios ata 1 milivatio (podemos comparalo co consumo dun procesador Intel XScale que é de 500 milivatios ou co consumo dun procesador Intel Pentium 4 de 50 vatios).



### 49.2.2 COMPOÑENTES E OPERACIÓN



Un sistema RFID ten os seguintes compoñentes:

- Unha etiqueta RFID que almacena certa información (ás mais típicas son de 2KB pero hainas de moitos tamaños)
- Un lector RFID que emite nunha determinada frecuencia e é capaz de detectar a resposta da etiqueta
- Un equipo capaz de interpretar a información da etiqueta

A operación do sistema é moi sinxela:

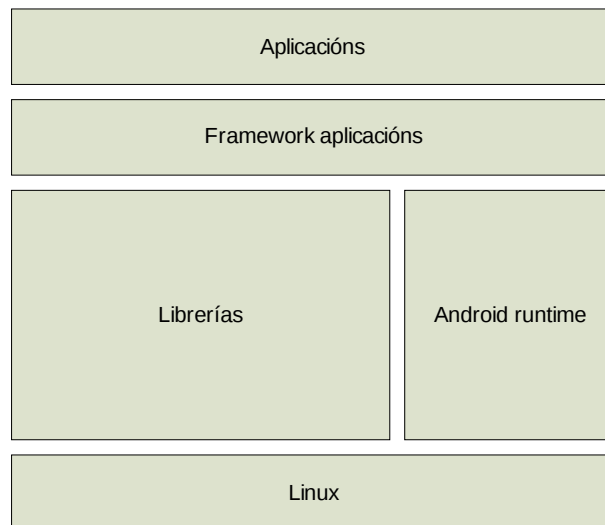
- O lector RFID emite sinais de radio a unha determinada frecuencia co obxectivo de activar a etiqueta RFID e ler ou escribir nela
- Cando unha etiqueta RFID pasa polo rango de acción do lector RFID, este detecta o sinal da etiqueta
- O lector comunícase coa etiqueta (co propósito concreto para o que se crease ese sistema, identificación do produto, pago sen fíos, ...)

## 49.3 TECNOLOXÍAS MÓBILES

### 49.3.1 ANDROID

Android é unha pila de software para dispositivos móbiles que inclúe o sistema operativo baseado en Linux, un middleware e aplicacións clave sendo a plataforma para móbiles mais vendida.

Google comprou a compañía que comezou o desenvolvemento do produto en 2005 e xunto con outros membros da Open Handset Alliance colaborou no seu desenvolvemento e publicación e na actualidade AOSP (Android Open Source Project) leva o seu mantemento e desenvolvemento futuro. A grandes trazos a estrutura de Android pode verse na figura seguinte.



- Aplicacións: Android permite desenvolver aplicacións e interfaces de usuario específicas para produtos específicos
- Framework aplicacións: Permite estender a funcionalidade por enriba da de un dispositivo de man dando soporte ás aplicacións e permitindo definir clases específicas para unha industria ou produto.
- Librerías: Optimizadas para un hardware determinado.
- Android runtime: Optimización da VM Dalvik de Java para distintas CPU's e SoC.
- Linux: Sistema operativo base preparado para distintas CPU's e chipsets.

#### **49.3.2 MEEGO**

MeeGo é un sistema operativo baseado en Linux e orientado a dispositivos móbiles. Aínda que está principalmente orientado a dispositivos móbiles e appliances no mercado de electrónica de consumo MeeGo esta deseñado para actuar como sistema operativo para outras plataformas hardware coma netbooks, tablets, televisions, ... Na actualidade MeeGo está amparada pola Linux Foundation.

#### **49.3.3 SYMBIAN**

Symbian é outro sistema operativo e plataforma computacional para smartphones mantido por Nokia. A plataforma Symbian é a sucesora de Symbian OS. Se do Nokia Series 60, a diferenza de Symbian OS, que requiría

unha interface de usuario adicional Symbian inclúe compoñentes de interface de usuario baseados na 5ª edición de S60. A última versión de Symbian (Symbian ^3) lanzouse a finais do 2010 co Nokia N8.

Symbian so está preparado para executarse en procesadores ARM aínda que existe unha versión para procesadores x86 que non foi lanzada.

Os dispositivos Symbian inclúen un 29,2% dos smartphones.

#### **49.3.4 WINDOWS PHONE 7**

Windows Phone 7 (anteriormente Windows Phone 7 Series) é un sistema operativo mobil desenvolto por Microsoft e é o sucesor da súa Windows Mobile platform. A diferenza do seu predecesor esta orientado ó mercado de consumo en vez de ó mercado empresarial.

Con Windows Phone 7 Microsoft ofrece un novo interface de usuario coa súa nova linguaxe Metro, integra o sistema operativo con servizos de terceiras partes e da propia Microsoft e controla o hardware no que se executa.

#### **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:  
ENDEREZAMENTO E SISTEMAS  
DE NOMES DE DOMINIO.  
PROTOCOLOS IP, ICMP, TCP,  
UDP. ENCAMIÑAMENTO.  
APLICACIÓNS BÁSICAS:  
TELNET, FTP (TFTP) E SMTP.**

**Tema 50. Protocolo TCP/IP: Enderezamento e sistemas de nomes de dominio. Protocolos IP, ICMP, TCP, UDP. Encamiñamento. Aplicacións básicas: Telnet, FTP (TFTP) e SMTP.**

50.1 Protocolo TCP/IP

50.1.1 Enderezamento e sistemas de nomes de dominio

50.1.1.1 Enderezamento IP

50.1.1.1.1 Subredes

50.1.1.1.2 Máscaras de rede

50.1.1.1.3 Direccións IPV6

50.1.1.2 DNS

50.1.1.2.1 Estructura do DNS

50.1.1.2.2 Sintaxe de nomes de dominio

50.1.1.2.3 Servidores de nomes

50.1.1.2.4 Resolución de nomes

50.1.1.2.4.1 Dependencias circulares

50.1.1.2.4.2 TTL

50.1.1.2.4.3 Busca inversa

50.1.1.2.5 Estructura dos rexistros DNS

50.1.2 Protocolos IP, ICMP, TCP, UDP

50.1.2.1 Capas do 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 mexases de Internet

50.1.2.4 ARP. Protocolo de resolución de direccións

50.1.2.5 RARP. Protocolo de resolución de direccións inverso

50.1.2.6 Protocolo TCP

50.1.2.6.1 Segmento TCP

50.1.2.6.2 Conexións TCP

50.1.2.6.3 Detección de erros

50.1.2.6.4 Control de fluxo

50.1.2.6.5 Control de conxestión

#### 50.1.2.7 Protocolo UDP

##### 50.1.2.7.1 Datagrama UDP

#### 50.1.3 Encamiñamento

##### 50.1.3.1 CIDR

##### 50.1.3.2 OSPF

##### 50.1.3.3 BGP

#### 50.1.4 Aplicacións básicas: Telnet, FTP (TFTP) e 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**

O alumbramento do modelo TCP/IP remontase á rede ARPANET. Esta era unha rede de investigación controlada polo Departamento de Defensa de EE.UU. Pouco a pouco foron conectándose institucións, mediante o uso de liñas da rede telefónica. A necesidade de buscar unha arquitectura de referencia nova xurdiu cando empezaron a engadirse redes de satélite e radio cos conseguíntes problemas de interactuar cos protocolos existentes. Un dos principais obxectivos desta nova arquitectura foi a capacidade de conexión de múltiples redes entre si desembocando no que hoxe coñecemos como modelo TCP/IP.

TCP/IP ten unha maior aplicación que o modelo OSI, xa que se desenvolveu antes e implantouse TCP/IP mentres se esperaba ao protocolo OSI.

Ademais, como tódalas especificacións asociadas aos protocolos TCP/IP son de dominio público, e polo tanto non hai que pagar nada para usalos, foron utilizados extensivamente por entidades comerciais e públicas para crear entornos de redes abertos.

As vantaxes de TCP/IP son:

- Agrupa redes, creando unha rede maior chamada Internet.

- É independente do hardware dos nodos, do sistema operativo e da tecnoloxía do medio e do enlace.
- Ofrece capacidade de encamiñamento adaptativo, transparente ó usuario.
- É o software de rede mais dispoñible universalmente.

As diferenzas co modelo OSI son:

- Mentres que en OSI a distinción entre os conceptos de servizo, interface e protocolo é clara, en TCP/IP non existía esta distinción inicialmente. Posteriormente, intentouse axustar isto para acercarse máis a OSI.
- OSI desenvolveuse antes de que se definiran os protocolos, mentres que TCP/IP foi, en realidade, o resultado dos protocolos existentes.
- Unha diferenza clara é que OSI conta con sete capas ben definidas e TCP/IP só ten 4.
- O modelo OSI considera os dous tipos de comunicación, orientada e non orientada a conexión, na capa de rede. Sen embargo, na capa de transporte, ofrece unicamente orientada a conexión. Por outro lado, o modelo TCP/IP na capa de rede só soporta comunicacións non orientadas a conexión pero considera ambos modos na capa de transporte.

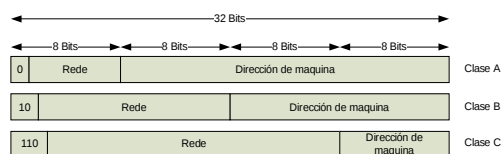
### **50.1.1 ENDEREZAMENTO E SISTEMAS DE NOMES DE DOMINIO**

#### **50.1.1.1 ENDEREZAMENTO IP**

Cada nodo da rede ten unha dirección IP única, formada polo número da rede e o número do nodo. A asignación de direccións IP esta regulado pola ICANN (Internet Corporation for Assigned Names and Numbers) para evitar que unha mesma dirección sexa usada por varias máquinas.

Unha dirección IP na súa versión 4 consta de 32 bits de lonxitude e xeralmente escríbese como concatenación de 4 bytes en formato decimal separados por puntos.

Tradicionalmente as direccións agrúpanse en clases que podemos ver na seguinte imaxe.



Ademais historicamente existen as clases D (para multicast) e E (orixinalmente reservada para uso futuro).

Hai determinadas direccións reservadas, estas son:

- 0.0.0.0 Esta IP usase polas estacións cando aínda non teñen unha IP asignada.
- A dirección da rede representase por unha dirección IP onde a primeira parte é a parte de rede e o resto de bits están a 0.
- 127.X.X.X Rede se loopback (acceso á propia maquina dende a propia máquina) sendo a dirección predilecta para este fin 127.0.0.1 aínda que todas funcionan da mesma forma.
- 255.255.255.255 É a dirección de broadcast (normalmente non retransmitido polos encamiñadores). De forma equivalente a dirección de broadcast para a rede e da dirección da rede co resto de bits a 1.

Cando o número de rede vai todo a ceros asúmese que esa dirección se refire á rede actual.

Non tódalas direccións son únicas na rede (estas direccións son coñecidas como IPs públicas) se non que existe nunha serie de rangos reservados para o seu usos en rexistro:

- Para a clase A: de 10.0.0.0 a 10.255.255.255 (8 bits rede, 24 bits estación).
- Para a clase B: 172.16.0.0 a 172.31.255.255 (16 bits rede, 16 bits estación). 16 redes clase B contiguas, uso en universidades e grandes compañías.
- Para a clase C: 192.168.0.0 a 192.168.255.255 (24 bits rede, 8 bits estación). 256 redes clase C contiguas, uso de compañías medias e pequenas.

#### **50.1.1.1.1 SUBREDES**



Tódolos ordenadores dunha rede deben ter o mesmo número de rede. Esta característica pode chegar a ser un problema a medida que crecen as redes. A solución a este problema é a división dunha rede en varias partes ou subredes. Desde o punto de vista do mundo exterior as subredes non son visibles, se non que se ve a rede como un todo.

A parte da dirección que define o número de rede permanece igual unha vez dividida, pero o número de estación divídese en número de subrede e número de estación.

#### **50.1.1.1.2 MÁSCARAS DE REDE**

A ferramenta que permite obter a dirección de rede dunha dirección IP dada é a máscara de rede. É unha especie de dirección IP especial que, en binario, ten tódolos bits que definen a rede postos a 1 e os bits correspondentes ó host postos a 0. Así, as máscaras de rede dos diferentes tipos de redes principais son:

- Rede de clase A: Máscara de rede = 255.0.0.0
- Rede de clase B: Máscara de rede = 255.255.0.0
- Rede de clase C: Máscara de rede = 255.255.255.0

A máscara de rede posúe a propiedade de que cando se combina, mediante unha operación AND lóxica, coa dirección IP dun host obtense a dirección propia da rede na que se encontra o mesmo.

Nas redes onde existen definidas subredes aplicase o concepto de máscara de subrede, que é o resultado de por a 1 tódolos bits que representan rede ou subrede e a 0 tódolos bits que representan una estación.

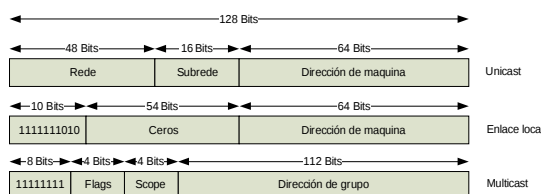
#### **50.1.1.1.3 DIRECCIÓNS IPV6**

A diferenza de IPv4, que utiliza unha dirección IP de 32 bits, as direccións IPv6 están compostas de 128 bits, ampliando enormemente a capacidade de direccións do protocolo IP.

De similar forma que as direccións IPv4 as direccións IPv6 agrúpanse en 8 números de 4 díxitos hexadecimais separados entre si por dous puntos (:). Cando un destes números é todo ceros, pódese omitir na escritura da dirección.

Existen 3 tipos de direccións:

- Unicast que identifica un único interface de rede. O protocolo IP entrega os paquetes enviados a unha dirección unicast á interface específico.
- Anycast que é asignada a un grupo de interfaces, normalmente de nodos diferentes. Un paquete enviado a unha dirección anycast entregase unicamente a un dos membros, tipicamente o host con menos custe, según a definición de métrica do protocolo de encamiñamento. As direccións anycast non se identifican facilmente pois teñen o mesmo formato que as unicast, diferenciándose unicamente por estar presente en varios puntos da rede. Case calquera dirección unicast pode utilizarse como dirección anycast.
- Multicast que tamén é usada por múltiples hosts, que conseguen a dirección multicast participando do protocolo de multidifusión (multicast) entre os routers de rede. Un paquete enviado a unha dirección multicast é entregado a tódolos interfaces que se uniron ó grupo multicast correspondente.



### 50.1.1.2 DNS

O sistema de nomes de dominio (DNS, polas súas siglas en inglés: Domain Name System) é un sistema de nomes xerárquico e distribuído para equipos, servizos ou calquera tipo de recurso conectado a Internet. A súa función máis importante é traducir os nomes comprensibles polos usuarios a direccións IP numéricas co propósito de localizalos na rede.

#### 50.1.1.2.1 ESTRUCTURA DO DNS

O espazo de nomes está organizado en árbore con cada nodo ou folla na arbore contendo cero ou máis rexistros de recursos (sendo estes os que almacenan a información correspondente ó nome de dominio).

Unha zoa DNS consiste nun ou varios dominios e subdominios dependendo da autoridade delegada nese xestor. Esta autoridade pode dividirse

creando mais zoas (que normalmente ocuparanse de subdominios) cuxa autoridade será asumida por outra entidade, perdendo a orixinal a autoridade sobre estas novas zoas.

#### **50.1.1.2.2 SINTAXE DE NOMES DE DOMINIO**

A descrición das regras de nomeado para os dominios aparece nos RFC 1035, RFC 1123, e RFC 2181. Un nome de dominio consiste nunha ou varias partes, chamadas etiquetas, que son concatenadas de forma xerárquica e separadas entre si por puntos.

As regras para construír o nome son:

- A etiqueta situada ao final dereito do nome chamase TLD (Top-Level Domain) e ten que pertencer a un dos TLD definidos.
- A xerarquía descende de dereita a esquerda, de forma que con cada etiqueta se especifica unha división na arbore. Existe un límite de 127 niveis na árbore xerarquía.
- Cada etiqueta pode ter ata 63 caracteres e o nome completo do dominio non pode exceder os 255 octetos (incluíndo un punto como representación do máximo nivel o que fai que o nome de dominio mais grande poda conter 253 caracteres).
- Os nomes de dominio almacenados en DNS poden estar compostos de calquera carácter almacenable nun octeto. Aínda que os nomes que se permiten na zona raíz e na maioría das subzonas limitan isto, permitindo só un subconxunto dos caracteres ASCII que inclúe da a á z, da A á Z, do 0 ó 9 e o guión. Os nomes de dominio non distinguen entre maiúsculas e minúsculas e as etiquetas non poden comezar nin acabar nun guión.
- Un nome de equipo é aquel nome de dominio que ten asociada polo menos unha IP, independentemente do seu nivel.

#### **50.1.1.2.3 SERVIDORES DE NOMES**

O Sistema de Nomes de Dominio esta soportado por unha base de datos distribuída e xerárquica accesible usando o paradigma cliente-servidor. Os nodos desta base distribuída chámanse servidores de nomes.

Cada dominio ten os seus datos almacenados nun servidor de nomes autoritativo que contén os datos dese dominio e os servidores de dominio subordinados a él. Na cúspide da xerarquía están os servidores de nomes raíz (contendo a información dos TLD).

Existen dous tipos de servidores de nomes:

- Servidor de nomes autoritativo: este tipo de servidor responde cos datos configurados por unha fonte orixinal (como pode ser o administrador do dominio ou algún método dinámico, pero non por consultas a outro servidor de nomes). Dependendo da fonte que se use para actualizarse, existen dous tipos de servidores:
  - Mestres: Recollen a configuración directamente do administrador do dominio.
  - Escravos: Manteñen unha copia da base de datos do seu servidor mestre que obteñen usando un mecanismo automático do protocolo DNS.

Toda zoa DNS debe ter polo menos un servidor de nomes autoritativo que debe estar almacenado nun rexistro DNS na zoa pai. Normalmente úsanse dous servidores (referidos coma Primario e Secundario) para cada zoa so distinguidos pola prioridade almacenada nos seus rexistros (a especificación técnica DNS en si non ten ningunha referencia a estes termos) e que soen corresponder a un mestre (o Primario) e a un escravo (o Secundario). Cando un servidor autoritativo responde a unha petición dun dos seus dominios marca a resposta co bit AA (Authoritative Answer) para indicalo.

- Servidores recursivos e de cache: Aínda que teoricamente os servidores autoritativos deberían ser suficientes, se so existisen estes unha petición debería viaxar de forma recursiva dende a zoa raíz. A forma para corrixir isto e reduci-lo tráfico DNS e mellorar o rendemento foi a creación de servidores de nomes que almacenan unha cache cos resultados previos e que teñen a capacidade de recorrer recursivamente os servidores autoritativos para resolver peticións.

#### **50.1.1.2.4 RESOLUCIÓN DE NOMBRES**

Como xa se comentou anteriormente o proceso para resolver un nome implica realizar unha serie de peticións comezando coa etiqueta á dereita. Mais en detalle este proceso implica:

1. Un equipo debe ter configurada unha cache inicial (chamada hint) coas direccións dos servidores raíz. Esta cache debe ser actualizada a man polo administrador dos equipos.
2. Unha petición a un dos servidores raíz para obtela dirección do servidor de nomes do TLD.
3. Unha petición ao servidor de nomes do TLD para obter a dirección do servidor de nomes autoritativo do dominio no seguinte nivel.
4. O paso anterior repetirase para cada etiqueta no nome ata que no último paso obtemos a dirección IP.

##### **50.1.1.2.4.1 DEPENDENCIAS CIRCULARES**

Os servidores de nomes aos que se delega una zoa identifícanse por nome, non por IP (no rexistro NS), provocando que haxa que resolver outro nome. Isto pode levar a que se produza unha dependencia circular (por exemplo: tratar de resolver un dominio para o que se ten que resolver o nome do seu servidor de nomes, que está dentro dese dominio). Para resolver isto, os servidores de nomes almacenan rexistros denominados “glue” (pegamento) que almacenan unha ou varias IP's deses servidores de nomes autoritativos, o servidor que delega provee este “pegamento” coma rexistros na sección adicional da resposta DNS peor co nome do servidor de nomes ao que se delega no campo correspondente da resposta.

##### **50.1.1.2.4.2 TTL**

Para evitar peticións continuas do mesmos nome, deseñouse un mecanismo para gardar unha cache dos rexistros DNS durante un tempo limitado, este tempo chamase TTL (Time To Live) e está asociado a tódolos rexistros DNS podendo ir dende non permitilo cache ata 68 anos.

Unha consecuencia desta característica e que un cambio nun rexistro DNS non se propaga de forma automática a toda a rede, se non que tarda o tempo expresado no TTL en actualizarse.

A correcta forma de seleccionar o TTL para un determinado rexistro esta definida no RFC 1912.

Existe tamén a posibilidade de facer cache negativa (gardala non existencia dun determinado rexistro), o TTL desta cache negativa esta determinado polo servidor de nomes autoritativo para esa zoa, que inclúe na resposta negativa o rexistro SOA (Start Of Authority) no que se especifica o mínimo tempo de TTL que combinado co TTL do propio rexistro SOA define o TTL da cache negativa.

#### **50.1.1.2.4.3 BUSCA INVERSA**

Existe a posibilidade de buscar o nome asociado a unha determinada dirección IP. Hai que ter en conta que pode haber varios nomes asociados a unha dirección IP. Os servidores DNS manteñen a información das direccións IP en rexistros PTR (Pointer) dentro do TLD arpa (in-addr.arpa para IPv4 e ipv6.arpa para IPv6) invertindo a orde dos números da IP (193.144.100.12 esta estará almacenada como 12.100.144.193.in-addr.arpa).

#### **50.1.1.2.5 ESTRUCTURA DOS REXISTROS DNS**

A base de datos dos rexistros DNS segue unha estrutura de lista de rexistros, onde cada rexistro contén:

- Nome: o nome completo do dominio na arbore. Te nun tamaño variable.
- Tipo: indicando o tipo de rexistro que define o formato e o posible uso dos datos do rexistro. Te nunha lonxitude de 2 octetos. Os tipos máis importantes son:
  - o A: Rexistro de dirección (IP), asocia un nome a unha dirección IP.
  - o MX: Rexistro de correo electrónico asocia un nome de dominio a un nome do servidor de correo electrónico para ese dominio.
  - o CNAME: Rexistro de alias. Asocia un nome a outro (cadea que debería acabar nun rexistro de tipo A).
  - o NS: Rexistro de delegación dunha zoa a un nome de servidor.
- Clase: Indica a clase do rexistro. Ten unha lonxitude de 2 octetos e soe ter o valor de IN (para os rexistros de Internet) pero tamén pode ter os

valores CN (Chaos) e HS (Hesiod). Cada clase é independente no que o espazo de nomes se refire.

- TTL: Time To Live. Ten unha lonxitude de 4 octetos.
- Datos: Contén os datos relevantes para ese rexistro, dependendo do tipo de rexistro estes datos son distinto se teñen distinto formato. Ten unha lonxitude variable.

### **50.1.2 PROTOCOLOS IP, ICMP, TCP, UDP**

#### **50.1.2.1 CAPAS DO MODELO TCP/IP**

A arquitectura do modelo TCP/IP consta de 4 capas:

- Aplicación. Proporciona comunicación entre procesos ou aplicacións en ordenadores distintos. Contén tódolos protocolos de alto nivel.
- Transporte. O igual que a capa de transporte de OSI, permite que se poida establecer unha comunicación entre as entidades pares dos nodos orixe e destino. Proporciona, por tanto, transferencia de datos extremo a extremo, asegurando que os datos chegan no mesmo orde en que foron enviados e sen erros. Esta capa tamén pode incluír mecanismos de seguridade. Pódese resumir a funcionalidade da capa de transporte como calidade de servizo. Neste nivel defínense dous protocolos importantes, que se explican en detalle máis adiante:
  - o TCP : Protocolo orientado a conexión que proporciona entrega fiable de mensaxes entre máquinas. Realiza control de fluxo para que un emisor rápido non poida saturar a un receptor lento.
  - o UDP: Protocolo sen conexión e non fiable. Utilízase en aplicacións onde a entrega rápida é máis importante que a entrega precisa, como transmisión de voz e vídeo, e en aplicacións de consulta de petición e resposta.
- Rede. Esta capa é o eixo da arquitectura e permite que os nodos inxecten paquetes en calquera rede e os fagan viaxar de forma independente o seu destino, sen importar se está na mesma rede, ou se hai outras redes entre elas. A súa misión principal, por tanto, é o encamiñamento dos paquetes, pero sen garantía de que cheguen ó

extremo final nin de que o fagan no mesmo orde no que se enviaron. Se se desexa unha entrega ordenada, as capas superiores deben reordenalos paquetes. Neste nivel defínese un formato de paquete e o protocolo IP, que se detalla seguidamente.

- Capa do nodo á rede. O modelo TCP/IP non dí moito do que sucede baixo a capa de rede, existe un gran baleiro. Esta abstracción da topoloxía de rede pon en relieve a capacidade da capa de rede de soportar calquera tipo de rede por debaixo. O que está claro é que debe permitir que un nodo se conecte á rede para que poida enviar por ela paquetes IP. O protocolo que regula esta conexión pode variar de un nodo a outro.

#### **50.1.2.2 PROTOCOLO IP**

IP proporciona un servizo de distribución de paquetes caracterizado por:

- Transmisión de datos en datagramas (paquetes IP).
- Non é orientado a conexión, polo que os paquetes son tratados de forma independente e cada un pode seguir una traxectoria diferente na súa viaxe cara o host destino.
- Non é fiable, polo que non garante a entrega dos paquetes, nin a entrega en secuencia, nin a entrega única. Isto é responsabilidade do protocolo TCP da capa superior.
- Non implementa control de erros nin control de conxestión.
- Pode fragmentalos paquetes si é necesario.
- Direcciona os paquetes empregando direccións lóxicas IP de 32 bits (en IPv4).
- Verifica a integridade do paquete en sí, non dos datos que contén.

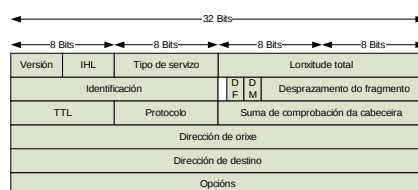
##### **50.1.2.2.1 DATAGRAMA IP**

Os datos proporcionados pola capa de transporte son divididos en datagramas e transmitidos a través da capa de rede. Ao longo do camiño poden ser fragmentados en unidades máis pequenas para atravesar unha rede ou subrede cuxa MTU (Unidade de Transferencia Máxima) sexa máis pequena que o paquete. Na máquina destino,



estas unidades son reensambladas para volver a ter o datagrama orixinal que é entregado á capa de transporte.

Un datagrama IP está formado por un corpo e una cabeceira. O corpo corresponde co segmento TCP/UDP da capa de transporte. A cabeceira ten unha parte fixa de 20 bytes e unha parte opcional de lonxitude variable. Na seguinte figura pode verse a estrutura de dita cabeceira.



- **Versión (4 bits).** Indica a versión do protocolo ó que pertence o datagrama. O propósito deste campo é permitirla evolución do protocolo e que durante a transición entre as versións se poida executar nunhas máquinas a versión vella e noutras a versión nova. Actualmente hai dúas versións: a 4 (Ipv4) e a 6 (Ipv6).
- **IHL (Internet Header Length) (4 bits).** Indica a lonxitude da cabeceira en palabras de 32 bits, xa que esta non ten unha lonxitude constante. Se non hai opcións, este valor é mínimo e igual a 5. O valor máximo é 15 (4 bits a "1", "1111"=15 en decimal). Como cada palabra equivale a 4 bytes, o tamaño máximo da cabeceira é de 60 bytes e, por tanto, de 40 bytes o campo de opcións.
- **Tipo de servizo (8 bits).** A subrede ofrece distintos graos de confiabilidade e seguridade. Con este campo o host pode indicarlle á subrede o tipo de servizo que quere, combinando fiabilidade e seguridade. Este campo contén, a súa vez, de esquerda a dereita:
  - o Campo de precedencia (3 bits): Indica a prioridade, de 0 (normal) a 7 (paquete de control de rede).
  - o Tres bits indicadores: D (Delay=retardo), T (Throughput=rendemento) e R (Reliability=fiabilidade), que permiten especificar qué interesa mais.
  - o Dous bits non usados.

- Lonxitude total (16 bits). Lonxitude total en octetos do datagrama, incluíndo cabeceira e datos. A lonxitude teórica máxima é 65535 bytes (64 Kbytes) pero na práctica os datagramas son de uns 1500 bytes. Este tamaño máximo será insuficiente nas redes futuras de alta velocidade. Internet non limita os datagramas a un tamaño específico pero suxire que redes e encamiñadores estean preparados para manexar datagramas a partir de 576 octetos.
- Identificación (16 bits). Cando se transmite un datagrama a través de Internet pode ser necesario fragmentalo en unidades máis pequenas ao longo do camiño. Este campo permite ó host destino determinar a qué datagrama pertence un fragmento recen chegado, xa que tódolos fragmentos dun mesmo datagrama conteñen o mesmo valor de identificación.
- 1 bit sen uso actualmente.
- Bit DF (Don't Fragment). Posto a "1", indica aos encamiñadores que non poden fragmentalo datagrama porque o destino no vai a poder unilas pezas de novo. Se é demasiado grande e non se pode enviar, descartase e envíase á orixe un mensaxe de error.
- Bit MF (More Fragment). Este bit está a "1" en tódolos fragmentos dun datagrama excepto no último. Desta forma, sábese cándo chegaron tódolos fragmentos.
- Desprazamento do fragmento (13 bits). Indica en qué posición do datagrama orixinal, medido en unidades de 8 octetos (64 bits), se encontra o fragmento actual. Todos os fragmentos, menos o último do datagrama, deben ter unha lonxitude múltiplo de 8 bytes. Pode haber 8192 fragmentos como máximo por datagrama.
- TTL o tempo de vida (8 bits). Contador que serve para limitala vida dun paquete. Teoricamente, conta o tempo en segundos, permitindo unha vida máxima de 255 segundos ("11111111"=255 en decimal). Debe diminuírse en cada salto. Na práctica, simplemente conta saltos. Cando o contador chega a 0 o paquete descartase e envíase ó host orixe un

paquete de aviso. Este campo evita que os paquetes estean dando voltas eternamente pola rede.

- Protocolo (8 bits). Indica a entidade da capa de transporte á que debe entregarse o datagrama unha vez que a capa de rede do host destino o ensambla por completo.
- Suma de comprobación da cabeceira (16 bits). Verifica só a cabeceira e é útil para a detección de erros xerados por palabras de memoria en mal estado nun encamiñador.
- Dirección de orixe e dirección de destino (32 bits, cada unha). Indican a dirección IP orixe e a dirección IP destino.
- Opcións (de 0 a 40 bytes). As opcións son de lonxitude variable. Empezan con un código de 1 byte, que identifica a opción. A continuación, só para algunhas opcións, 1 byte que indica a lonxitude da opción. Finalmente, un ou máis bytes de datos. O campo de opcións enchese para obter palabras completas ou, o que é o mesmo, múltiplos de 4 bytes. As opcións elixenas as aplicacións de orixe aínda é bastante raro usalas. Actualmente hai 5 opcións definidas:
  - o Seguridade: Permite engadir unha etiqueta para indicalo secreta que é a información que contén o datagrama. Na práctica, os encamiñadores ignoran esta opción.
  - o Encamiñamento estrito dende a orixe: Indica a traxectoria completa a seguir como secuencia de direccións IP. Esta opción é usada polos administradores para facer medicións de tempo.
  - o Encamiñamento libre dende a orixe: Indícase unha lista de encamiñadores polos que ten que pasalo paquete, na orde especificada, pero pode pasar a través doutros encamiñadores no camiño. É de utilidade cando as consideracións políticas ou económicas dictan pasar ou evitar certos países.
  - o Rexistrar ruta: Indica aos encamiñadores polos que pasa o datagrama que agreguen a súa dirección IP de 32 bits no campo de opcións para coñecer a ruta que seguiu o datagrama.

- o Marca de tempo: Como a opción anterior, pero ademais o encamiñador tamén ten que rexistrar unha marca de tempo de 32 bits, expresada en milisegundos, de acordo a cada reloxo local. Ambas opcións utilízanse principalmente para a busca de fallos nos algoritmos de encamiñamento.

### **50.1.2.3 ICMP PROTOCOLO DE CONTROL DE MENSAXES DE INTERNET**

Cando ocorre algún suceso, ICMP (Internet Control Message Protocol) é o protocolo encargado de informar do mesmo. Non toma ningunha decisión ó respecto, esto é tarefa das capas superiores. Os mensaxes de ICMP encapsulanse dentro do campo de datos dos paquetes IP.

A mensaxe ICMP ten tres campos fixos e a continuación, o corpo da mensaxe que varía en función do tipo. Os campos obrigatorios son:

- Tipo (8 bits). Utilízase para distinguilos tipos de mensaxes ICMP, descritos máis abaixo, e determinar o seu formato.
- Código (8 bits). Nalgunhas mensaxes ICMP utilízase este campo para distinguir distintos subtipos dentro dun tipo de mensaxe, é dicir, para ofrecer unha descrición concreta do error que se produciu.
- Checksum (16 bits). Código de protección contra erros de transmisión.

Existen diversos tipos de mensaxes ICMP. Por un lado, están as mensaxes informativas. Todos eles conteñen, ademais dos 3 campos fixos, un identificador de 16 bits e un número de secuencia, tamén de 16 bits. As mensaxes informativas máis importantes son as seguintes:

- Solicitude de eco (Tipo 8). Permite detectar se un destino concreto é alcanzable e está vivo. Cando se envía unha mensaxe de este tipo esperase que o destino devolva unha mensaxe de resposta de eco. Leva un campo de Datos opcional con un número de bytes variables que fixa o host peticionario.

- Resposta de eco (Tipo 0). Mensaxe que se devolve cando se recibe unha mensaxe de Solicitud de eco contendo os datos enviados polo peticionario.
- Solicitud de marca de tempo (Tipo 13). Mesma funcionalidade que a mensaxe Solicitud de eco pero indica ó receptor que debe engadir información adicional de tempos na mensaxe de resposta.
- Resposta de marca de tempo (Tipo 14). Parecido á mensaxe de Resposta de eco pero ademais almacena o tempo de chegada da mensaxe de Solicitud de marca de tempo e o tempo de partida da mensaxe de resposta.
- Solicitud de máscara de dirección (Tipo 17). Utilízao un host cando se reinicia nunha rede e non coñece cuántos bits asignáronse á máscara de subrede.
- Resposta de máscara de dirección (Tipo 18).

O resto son mensaxes de erro. Todos eles conteñen, ademais dos 3 campos fixos, o encabezado e os 8 primeiros bytes do datagrama que ocasionou o erro. As mensaxes de erro máis importantes son as seguintes:

- Destino inalcanzable (Tipo 3). Este tipo de mensaxe utilízase ante varias situacións. O campo de código describe o erro concreto que se produciu.
  - o Código=0: non se pode encontrara rede destino da mensaxe.
  - o Código=1: host ou aplicación destino inalcanzable.
  - o Código=2: campo de protocolo do datagrama non coincide con ningún dos protocolos do host destino.
  - o Código=3: non se pode chegar ó porto destino ou a aplicación destino non está libre.
  - o Código=4: cando unha rede non pode transportar un paquete IP demasiado grande para ela pero leva o bit DF activado, indicando que non se permite fragmentación.
  - o Código=5: ruta de orixe non é correcta.
  - o Código=6: non se coñece a rede destino.

- o Código=7: non se coñece o host destino.
- o Código=8: o host orixe está illado.
- o Código=9: a comunicación coa rede destino está prohibida por razóns administrativas.
- o Código=10: a comunicación co host destino está prohibida por razóns administrativas.
- o Código=11: non se pode chegar á rede destino debido ó Tipo de servizo.
- o Código=12: non se pode chegar ó host destino debido ó Tipo de servizo.
- Tempo excedido (Tipo 11). Cando existe unha alta conxestión na rede ou os paquetes están vagando pola rede en bucle, chega un momento en que o contador de tempo de vida do paquete chega a 0.
  - o Código = 0: tempo excedido (TTL alcanzou 0)
  - o Código = 1: finaliza o tempo sen que se recibiran tódolos fragmentos dun datagrama
- Problema de parámetro (Tipo 12). Indica que algún campo da cabeceira ten un valor ilegal, que o tamaño do datagrama é incorrecto ou que falta algún campo obrigatorio, debido a un fallo do software de IP no host emisor ou en algún dos encamiñadores polos que pasou a mensaxe. Este mensaxe inclúe un campo Indicador de 8 bits que apunta ó campo do encabezado IP que xenerou o problema.
- Supresión de orixe (Tipo 4). Cando un host envía moitos paquetes envíaselle unha mensaxe deste tipo coa intención de que reduza. Na actualidade apenas se usa xa que incrementa a posibilidade de conxestión na rede.
- Redireccionamento (Tipo 5). Cando un encamiñador detecta que unha paquete pode estar mal encamiñada envía unha mensaxe deste tipo ó host emisor do paquete para avisarlle do posible erro e para que modifique a súas táboas de encamiamento, se procede.

#### **50.1.2.4 ARP. PROTOCOLO DE RESOLUCIÓN DE DIRECCIÓN**

O hardware da capa de enlace de datos non entende as direccións IP, é necesario que sexan traducidas a direccións físicas. Unha posible solución é ter un arquivo de configuración nalgún lugar do sistema que proxecte as direccións IP en direccións físicas. Sen embargo, en organizacións con miles de hosts, o mantemento e xestión destes arquivos suporía moito tempo e sería moi susceptible a erros.

Unha solución máis sinxela ofrécea o protocolo de resolución de direccións, ARP (Address Resolution Protocol). Cando un host quere enviar un paquete a outro, do cal so coñece a dirección IP, envía un paquete ARP á rede coa dirección IP que se quere resolver. A difusión chegará a cada host da rede, que revisará a súa propia dirección IP, e só aquel que coincida responderá con súa dirección física. O host de orixe engade esta nova entrada á súa táboa ARP.

#### **50.1.2.5 RARP. PROTOCOLO DE RESOLUCIÓN DE DIRECCIÓNS INVERSO**

As veces prodúcese o caso inverso ó anterior. É dicir, necesítase coñecer a dirección IP dada unha dirección física. Isto ocorre, por exemplo, cando se inicia unha máquina sen disco que normalmente recibe a imaxe binaria do seu sistema operativo dun servidor de arquivos remoto, pero descoñece a súa dirección de IP.

O protocolo de resolución de direccións inverso RARP (Reverse Address Resolution Protocol) permite que un host recién iniciado difunda a súa dirección física para preguntar se alguén na rede coñece a dirección IP asociada a ela. Cando o servidor RARP recibe esta solicitude busca a dirección física nos seus arquivos de configuración e envíalle a dirección de IP correspondente.

#### **50.1.2.6 PROTOCOLO TCP**

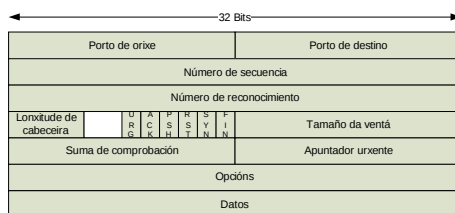
TCP (Transmisión Control Protocol) deseñouse especificamente para enviar unha secuencia de bytes fiable a través dunha rede non fiable. As súas características principais son:

- É un protocolo orientado a conexión. TCP establece unha conexión entre un socket da máquina transmisora e un socket da máquina receptora. Un socket é un punto terminal ó que se lle asigna un número de socket formado pola dirección IP do host e un número de 16 bits local a ese host, chamado porto. Unha vez establecida a conexión pódense transferir datos entre a orixe e o destino. Aínda que cada paquete enviado desde o host orixe pode viaxar por un camiño ou ruta diferente ata chegar ó host destino, por medio do protocolo IP, TCP consegue que pareza que existe un único circuíto de comunicación entre ambos hosts.
- É un protocolo fiable.
- É un protocolo de fluxo non estruturado, con posibilidade de enviar información de control xunto aos datos.
- É un protocolo con transferencia de memoria intermedia. Co obxecto de minimizar o tráfico de rede e conseguir unha transferencia eficiente, vanse almacenando os datos do fluxo de transmisión ata completar un paquete o suficientemente largo como para ser enviado. No destino, almacénanse os datos recibidos ata completar unha secuencia completa e correcta para pasala ó proceso de aplicación destino.
- Usa conexións full-dúplex, é dicir, o tráfico pode ir en ambos sentidos ó mesmo tempo.

#### **50.1.2.6.1 SEGMENTO TCP**

Cada segmento comeza con unha cabeceira de formato fixo de 20 bytes. Esta pode ir seguida de opcións de cabeceira. Tras as opcións, se as hai, encóntranse os datos. Tamén pode haber segmentos sen datos, usados normalmente para acuses de recibo e mensaxes de control. O formato da cabeceira TCP é a seguinte:





- Porto de orixe e porto de destino (16 bits cada uno). Identifican os puntos terminais locais da conexión. Cada host pode decidila forma de asignar os seus propios portos, comezando polo 256.
- Número de secuencia (32 bits). Indica o primeiro byte de datos que hai no segmento.
- Número de acuse de recibo (32 bits). Especifica o seguinte byte esperado, non o último byte recibido correctamente. Para que este campo se teña en conta o bit ACK debe estar activado ("1").
- Lonxitude de cabecera TCP. Cantidade de palabras de 32 bits. É precisa, xa que o campo de opcións é de lonxitude variable. O tamaño da cabecera completa pode oscilar entre 5 y 60 bytes.
- 6 bits que non se usan. O seu valor é "0" e están reservados para usos futuros.
- 6 indicadores de 1 bit con funciones de control:
  - o URG: A "1" indica que o segmento contén datos urxentes. O Apuntador urxente (16 bits) indica o seguinte byte do campo de Datos que sigue a os datos urxentes, é dicir, indica cal é o último byte de datos que é urxente.
  - o ACK: A "1" indica que o Número de acuse de recibo é válido. Se ACK=0 ignórase o campo de Número de acuse de recibo.
  - o PSH: Indica datos "empuxados". Actívese para solicitar ó receptor que entregue os datos á aplicación á súa chegada e non os almacene no buffer ata a recepción dun buffer completo.
  - o RST: Serve para reestablecer unha conexión e para rexeitar un segmento non válido ou un intento de abrir unha conexión.

- o SYN: Campo para a sincronización dos números de secuencia, que se utiliza ó establecela conexión. SYN indica o primeiro número de secuencia co que se vai a empezar a transmitir. Pode ser distinto de 0.
- o FIN: Utilízase para liberar conexións.
- Tamaño da ventá (16 bits). Indica a cantidade de bytes que poden enviarse a partir do último byte do que se recibiu acuse de recibo. O receptor pon o valor da ventá a 0 cando non pode recibir máis datos.
- Suma de comprobación (16 bits). Suma de comprobación da cabeceira, os datos e unha pseudocabeceira conceptual.
- Opcións. Permite agregar características extra non cubertas na cabeceira normal.
- Para completar o tamaño do segmento TCP ata que sexa múltiplo de 32 bits úsanse bits de recheo.

#### **50.1.2.6.2 CONEXIÓNS TCP**

Para establecer unha conexión un dos lados espera pasivamente unha conexión entrante e o outro executa unha primitiva de conexión, especificando a dirección e o porto IP co que se desexa conectar, o tamaño máximo de segmento TCP que está disposto a aceptar e, opcionalmente, algúns datos de usuario. Esta primitiva xera un segmento TCP co bit SYN a 1 e o bit ACK a 0. Ó chegar o segmento ao destino a entidade TCP revisa se hai algún proceso escoitando no porto indicado no campo de porto de destino. Se non o hai, envía una contestación co bit RST a 1 para rexeitala conexión. En caso contrario, o proceso recibe o segmento TCP entrante e pode aceptar ou rexeitala conexión. Se a acepta, envíase de volta un segmento de acuse de recibo.

Cando se cae un host, por seguridade, non pode reiniciarse durante o tempo máximo de paquete (120 seg.) para asegurar que no haxa paquetes de conexións previas vagando por Internet.

Para liberar unha conexión, calquera das partes pode enviar un segmento TCP co bit FIN activado, indicando que non ten máis datos que transmitir. Ó recoñecerse o FIN, ese sentido apágase. Sen embargo, o fluxo de datos no outro sentido pode continuar. Cando ambos sentidos se apagan libérase a conexión. Nalgunhas implementacións de TCP existe un temporizador de seguir con vida (keepalive timer). Cando unha conexión esta ociosa durante demasiado tempo este contador pode esgotarse. Se isto ocorre, un lado da conexión comproba se o outro aínda responde. Se non se recibe resposta se termina a conexión.

#### **50.1.2.6.3 DETECCIÓN DE ERROS**

As técnicas máis efectivas e usadas son as seguintes:

- Detección de erros. Consiste en engadir un ou mais bits de información a cada segmento de forma que indiquen claramente se se alterou algún dos bits do mesmo no camiño dende emisor ó receptor (Paridad, CheckSum, CRC, ...).
- Confirmacións positivas. O receptor devolve un acuse de recibo positivo por cada un dos segmentos recibidos correctamente. Usase para detectar e solicitar o reenvío de segmentos perdidos. Esta é a técnica que se utiliza no sistema de parada e espera.
- Expiración de intervalos de tempo. O emisor inicia un contador de tempo tras enviar un segmento (o temporizador de retransmisión). Se este contador se esgotase sen que se reciba un ACK positivo o emisor volve a transmitir o mesmo segmento.
- Confirmación negativa e transmisión. O receptor só confirma os segmentos recibidos erroneamente para que o emisor os volva a enviar. Por tanto, utilízase para solicitar o reenvío de segmentos danados.

#### **50.1.2.6.4 CONTROL DE FLUXO**

O control de fluxo máis simple é o que se leva a cabo mediante o sistema de parada e espera. O transmisor garda un rexistro de cada segmento que envía, esperando un ACK antes de enviar o seguinte. Tamén arranca un

temporizador cando envía o segmento. Se o temporizador expira antes de recibilo acuse de recibo, retransmite o segmento e reinicia o temporizador. Este mecanismo é o máis barato e o máis usado cando se transmiten tramas moi grandes pero é ineficiente xa que está a canle de transmisión desaproveitado a maior parte do tempo.

O control de fluxo mediante ventá deslizante permite que o transmisor envíe varios segmentos sen esperar os ACK correspondentes. Neste sistema o emisor e o receptor póñense de acordo no número de segmentos sen procesar que pode gardar este último, dependendo do tamaño dos seus buffers. Tamén se poñen de acordo no número de bits a utilizar para numerar cada segmento. Cando a ventá ten un tamaño cero o emisor non pode enviar máis segmentos, salvo en dous casos excepcionais: cando se trata de datos urxentes e cando o emisor envía un segmento de 1 byte para provocar que o receptor xere un novo acuse de recibo con un novo tamaño de ventá, evitando así un bloqueo indefinido da conexión.

Unha variedade mellorada do sistema de ventá deslizante é o sistema de control de fluxo con adiante-atrás-N, no que cando a estación destino encontra un segmento erróneo devolve un ACK negativo, rexeitando tódolos que lle cheguen ata que non reciba outra vez o segmento incorrecto en boas condicións. O emisor, ó recibir o ACK negativo, sabe que ten que volver a transmitir ese segmento e tódolos seguintes.

Por último, existe outro sistema denominado sistema de control con rexeitamento selectivo, que se basea en que os únicos segmentos que se volven a retransmitir son aqueles rexeitados polo receptor ou aqueles cuxo temporizador expira sen confirmación. Este método é máis eficiente que os anteriores pero precisa que o receptor dispoña dun buffer intermedio de gran capacidade no que gardar tódolos segmentos recibidos tras o rexeitamento dun dado ata recibir de novo o segmento.

#### **50.1.2.6.5 CONTROL DE CONXESTIÓN**

Cando a carga ofrecida á rede é maior que a que pode xestionar prodúcese conxestión. Tódolos algoritmos TCP supoñen que as terminacións de

temporización son causadas por conxestións e as revisan en busca de problemas.

Cada transmisor mantén dúas ventás diferentes:

- Ventá negociada co receptor ó establecerse a conexión, cuxo tamaño está baseado no tamaño do buffer de memoria de destino. Isto permite que o transmisor non envíe máis datos dos que o receptor pode almacenar evitando así que o saturar.
- Ventá de conxestión, determinada polo tamaño dos datos que se poden enviar sen que se produza timeout.

O transmisor só pode mandar un número de segmentos limitado polo tamaño da ventá máis pequena. Ó establecerse unha conexión, o transmisor asigna á ventá de conxestión o tamaño de segmento máximo usado pola conexión. Cada envío recoñecido con éxito duplica a ventá de conxestión. Este algoritmo chamase arranque lento (slow start) e permite que o tamaño da ventá de conxestión creza exponencialmente ata que se produza unha terminación de temporización (timeout) ou se alcance o tamaño da ventá receptora.

Este crecemento exponencial pode producir saturación. Para evitalo, introdúcese outro parámetro, denominado umbral, que toma como valor inicial 64 KBytes. Cando se produce o timeout cámbiase o valor do umbral á metade do tamaño da ventá de conxestión, establecece o valor da ventá ó do tamaño dun segmento máximo e inicialízase outra vez o proceso de arranque lento. Agora, cando o tamaño da ventá chega ó do umbral esta crece soamente en saltos dun segmento máximo, é dicir, con un progreso lineal ata que se produza unha nova terminación de temporización.

#### **50.1.2.7 PROTOCOLO UDP**

O UDP (User Data Protocol) ofrece ás aplicacións un mecanismo para enviar datagramas IP en bruto, encapsulados sen ter que establecer unha conexión. É unha alternativa a TCP e usase cando unha entrega rápida é máis importante que unha entrega garantida, ou cando a información a enviar cabe nun único datagrama. As súas características son:

- UDP non admite numeración dos datagramas e tampouco utiliza mensaxes de confirmación de entrega. Polo que é posible que os datagramas cheguen duplicados e/ou desordenados o seu destino.
- É un protocolo do tipo best-effort (mellor esforzo) porque fai o que pode para transmitirlos datagramas cara o destino, pero non pode garantir que este os reciba.
- UDP non utiliza mecanismos de control de erros. Cando se detecta un erro nun datagrama, en lugar de entregalo á aplicación destino, descartase.

#### **50.1.2.7.1 DATAGRAMA UDP**

O datagrama UDP consiste nunha cabeceira de 8 bytes seguida dos datos. A cabeceira presenta o seguinte aspecto.

- Porto de orixe e porto de destino (16 bits cada uno). Ó igual que en TCP, serven para identificalos puntos terminais das máquinas de orixe e destino.
- Lonxitude UDP (16 bits). Indica a lonxitude do datagrama UDP en bytes, incluíndo a cabeceira de 8 bytes e os datos.
- Suma de comprobación UDP (16 bits). Esta suma é opcional. Se non se calcula, o seu valor é 0.

#### **50.1.3 ENCAMIÑAMENTO**

Para encamiñar os paquetes dunha rede a outra utilízanse uns dispositivos denominados encamiñadores ou routers. Son os encargados de determinar o camiño concreto que seguirá cada paquete na súa viaxe dende o host orixe ata o host destino.

Cada encamiñador posúe no seu interior unha táboa de encamiñamento para alcanzar redes distantes e outra para alcanzar redes locais. Na primeira almacénanse direccións IP de redes e subredes distintas da actual, así como a máscara e interface de saída asociada a cada unha delas. E na segunda táboa as direccións dos hosts da subrede actual, xunto coa dirección da tarxeta de rede de dito host. Desta forma, cada encamiñador só ten que levar o rexistro de outras redes/subredes e dos host locais. As

táboas de direccionamiento deben estar ordenadas dende as direccións máis específicas ata as máis xenerais e recorrerse nesa orde.

As táboas de encamiñamento poden ser fixas e conter rutas alternativas que serán utilizadas cando algún dispositivo de encamiñamento non esté dispoñible. Tamén poden ser dinámicas de forma que o router pode ir modificándoas de acordo co estado da rede e dos encamiñadores que se comunican con el. Este é o motivo polo que os paquetes pertencentes a unha mesma comunicación poden seguir camiños diferentes.

Os hosts tamén posúen táboas de encamiñamento (dende simples táboas ARP ata táboas mais complexas). De feito, cando un host desexa enviar datos a outro o primeiro que fai é comprobar se o host destino aparece nas súas táboas de encamiñamento. En caso afirmativo os datagramas sonlle enviados directamente mediante a súa dirección física (a dirección da súa tarxeta de rede). En caso contrario envía un mensaxe de petición ARP, que será respondido polo host destino enviando a súa dirección física. A partir de aquí procedese como no caso afirmativo. En ambos casos o proceso recibe o nome de entrega directa. Se ningún host da rede/subrede responde á mensaxe de petición os datagramas son enviados ó router para que este se encargue do seu direccionamento. Neste caso falase de entrega indirecta.

Cando un paquete IP chega a un encamiñador, extraese a dirección do host destino e comprobase, pasándolle as diferentes máscaras almacenadas na táboa de encamiñamento, se pertence a algunha das redes que dito router une. En caso afirmativo, o encamiñador comportase como un host mais e segue o proceso de entrega directa explicado no párrafo anterior. Se o host destino non pertence a ningunha das redes que conecta o router, reenvíase o seguinte encamiñador pola interface dada na táboa de encamiñamento. Desta forma, o paquete vai saltando dun a outro router, ata chegar a un que si esté conectado á rede destino.

#### **50.1.3.1 CIDR**

CIDR (Classless Inter-Domain Routing) lanzouse en 1993 para melloralo sistema de encamiñamento aproveitando mellor as direccións dispoñibles.

En vez de nas clásicas clases de rede, CIDR basease en VLSM (Variable-Length Subnet Masking) que define a máscara de subrede cun número de bits de prefixo, por exemplo 10.0.0.0/7 define una máscara de subrede onde os 7 primeiros bits son 1 e o resto 0. Ademais CIDR tamén define a agregación de subredes con prefixos contiguos en redes de maior tamaño, reducindo así a táboa de encamiñamento.

CIDR define o concepto de bloque sendo un conxunto de direccións IP contiguas que seguen un patrón A.B.C.D./N, onde A, B, C e D son números do 0 a o 255 representando unha dirección IP e o N e o número de bits (polo tanto de 0 a 32) que se considera que definen a rede. Unha determinada dirección IP pertence a un determinado bloque CIDR cando os N primeiros bits da mesma son idénticos a os N primeiros bits de A.B.C.D. Seguindo o exemplo anterior 10.0.0.0/7 define unha rede onde os 7 primeiros bits teñen que ser iguais ós 7 primeiros bits da IP 10.0.0.0. Dunha forma similar a máscara de subrede está constituída por N uns seguidos de  $32 - N$  ceros, que se dividen en 4 bytes e se separan por puntos.

A agregación de subredes, proceso coñecido coma superneting, permite que, por exemplo, 128 redes contiguas do tipo 192.168.X.0/24 se agregen nunha soa 192.168.Z.0/20. O proceso require que as redes sexan do mesmo nivel (mesmo número N) e contiguas (que a diferenza se produza nos bits menores a N) e que, se a diferenza se produce no bit N estean presentes as dúas variantes para poder establecer un bloque con N-1, é dicir, se hai M bits de diferenzas (sempre nos últimos bits distintos de cero da máscara de subrede) téñense que agregar as  $M^2$  subredes nunha “superrede” N-M.

### **50.1.3.2 OSPF**

OSPF (Open Shortest Path First) estandarizouse en 1990 desbancando ó protocolo de vector de distancia RIP, que só funcionaba ben en sistemas pequenos.

Os requisitos que se pretendían cubrir cando se deseñou OSPF eran:



- O algoritmo non podía ser propiedade dunha compañía se non que tiña que publicarse como literatura aberta.
- O novo protocolo tiña que recoñecer distintas métricas de distancia, incluídas distancia física e retardo.
- Tiña que ser un algoritmo dinámico que se adaptara aos cambios de topoloxía de forma rápida e automática.
- O novo protocolo tiña que recoñecer o encamiñamento baseado no tipo de servizo, diferenciando entre o tráfico de tempo real e o resto.
- O protocolo tiña que efectuar equilibrio de cargas, dividíndoa entre varias liñas.
- Recoñecemento de sistemas xerárquicos de modo que ningún encaminador tivera que coñecela topoloxía completa.
- Requiríase un mínimo de seguridade para evitalo envío de información de encamiñamento falsa aos routers.

OSPF funciona mapeando o conxunto de redes, encamiñadores e liñas nun grafo dirixido, no que a cada arco ten asignado un custe, e calculando a traxectoria máis curta desde cada dispositivo de encamiñamento a tódolos demais en base aos pesos dos arcos.

OSPF manexa áreas numeradas, onde un área é unha xeneralización dunha subrede. A topoloxía e detalles de un área non son visibles dende fora da mesma.

### **50.1.3.3 BGP**

Todo o que ten que facer un protocolo coma OSPF, é mover paquetes coa maior eficiencia posible dende orixe ao destino sen necesidade de preocuparse pola política. Sen embargo BGP (Border Gateway Protocol), deseñouse para permitir moitos tipos de políticas de encamiñamento.

As políticas típicas comprenden consideracións políticas, valga a redundancia, de seguridade ou económicas. Configúranse manualmente en cada encamiñador BGP e non son parte do protocolo mesmo.

BGP ten especial interese no tráfico de tránsito. As redes agrúpanse en tres categorías:

- Redes de punta. Só ten unha conexión ao grafo BGP.
- Redes multiconectadas. Poden utilizarse para o tráfico de tránsito excepto que se neguen a facelo.
- Redes de tránsito. Están dispostas a manexar os paquetes de terceiros, posiblemente con algunhas restriccións.

Dous enrutadores BGP considéranse conectados se comparten unha rede común. Os pares de routers BGP comunícanse entre eles establecendo conexións TCP, proporcionando comunicación fiable e ocultando tódolos detalles da rede pola que pasa.

BGP é fundamentalmente un protocolo de vector de distancia, no que cada dispositivo de encamiñamento mantén o custe a cada destino e, ademais, a traxectoria seguida. Do mesmo modo, en lugar de dar periodicamente a cada veciño os seus custes estimados a tódolos destinos posibles, cada enrutador BGP dille os seus veciños a traxectoria exacta que está usando. A esencia de BGP é o intercambio de información de encamiñamento entre dispositivos de encamiñamento.

#### **50.1.4 APLICACIÓNS BÁSICAS: TELNET, FTP (TFTP) E SMTP**

##### **50.1.4.1 TELNET**

Este “protocolo” permite aos usuarios conectarse a ordenadores remotos e utilízalos dende o sistema local mediante a emulación de terminal sobre unha conexión TCP. Interconecta o cliente local dunha máquina co servidor co que se comunica.

Os caracteres que se teclean nun cliente local son enviados pola rede e procesados no ordenador remoto. O resultado da súa execución transmítese de volta e mostrase na pantalla do ordenador local.

Este protocolo foi un dos primeiros que se definiu e foi deseñado para traballar con terminais en modo texto. Impleméntase en dous módulos:

- O módulo cliente, que é un programa que ofrece un entorno non gráfico, é dicir, modo carácter e é o encargado de entenderse co programa servidor.

- O módulo servidor, que permanece escoitando no porto adecuado, por defecto o porto 23 de TCP, á espera de peticións por parte dos clientes.

#### **50.1.4.2 FTP**

Permite a transferencia de arquivos de texto ou binarios dende un ordenador a outro sobre unha conexión TCP.

FTP (File Transfer Protocol) implementa un sistema estricto de restriccións baseadas en propiedades e permisos sobre os arquivos. Hai un control de acceso dos usuarios e, cando un usuario quere realizala transferencia dun arquivo, o FTP establece unha conexión TCP para o intercambio de mensaxes de control. Desta maneira pódese enviar o nome de usuario, a password, os nomes dos arquivos e as accións que se querenrealizar. Unha vez aceptada a transferencia do arquivo, unha segunda conexión TCP establece para a transferencia de datos. O arquivo transfírese sobre a conexión de datos sen a utilización de ningunha cabeceira ou información de control na capa de aplicación. Cando se completa a transferencia, a conexión de control usase para sinalizar que a transferencia completouse e para aceptar novos comandos de transferencia.

##### **50.1.4.2.1 TFTP**

TFTP (Trivial FTP) é un protocolo de transferencia de arquivos moi sinxelo que poderíamos dicir é unha versión simplificada de FTP. TFTP utilízase con frecuencia para transferir pequenos arquivos entre ordenadores nunha rede, como cando un cliente lixeiro arranca dende un servidor de rede (por que non ten un sistema operativo instalado).

As principais características de TFTP es as principais diferencias con FTP son:

- Utiliza UDP (no porto 69) como protocolo de transporte (a diferenza de FTP que utiliza o porto 21 TCP).
- Non pode listar o contido de directorios.
- Non existen mecanismos de autenticación ou cifrado.
- Utilízase para ler ou escribir arquivos dun servidor remoto.

- Soporta tres modos diferentes de transferencia, "netascii", "octet" e "mail", dos que os dous primeiros corresponden a os modos "ascii" e "binario" do protocolo FTP.

#### **50.1.4.3 SMTP**

SMTP (Simple Mail Transfer Protocol) É o protocolo dedicado á transmisión de mensaxes electrónicas sobre unha conexión TCP. Implementouse sobre unha sinxela sesión do terminal virtual de rede (NVT, Network Virtual Terminal) de Telnet.

O protocolo especifica o formato das mensaxes, definindo a estrutura da información acerca do remitente, o destinatario, datos adicionais e naturalmente o corpo das mensaxes.

Este protocolo non especifica cómo as mensaxes deben ser editadas. É necesario ter un editor local ou unha aplicación nativa de correo electrónico. Unha vez a mensaxe está creada, o SMTP a acepta e usa o protocolo TCP para enviala a un módulo SMTP doutra máquina. TCP é o encargado de intercomunicar os módulos SMTP das máquinas implicadas. Existen extensións de SMTP, ESMTP, definidas nun conxunto mais recente de normas, que permiten transportar calquera tipo de información (imáxenes, vídeos, sons, 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.  
TOPOLOXÍAS. REDES  
ETHERNET. REDES  
CONMUTADAS E REDES  
VIRTUAIS. XESTIÓN DE REDES.  
SISTEMAS DE CABLEADO.  
ELECTRÓNICA DE REDE:  
REPETIDORES,  
CONCENTRADORES, PONTES,  
CONMUTADORES,  
ENCAMIÑADORES,  
PASARELAS.  
INFRAESTRUTURA DE  
SISTEMAS.**

**Tema 51. Redes de área local. Topoloxías. Redes Ethernet. Redes conmutadas e redes virtuais. Xestión de redes. Sistemas de cableado. Electrónica de rede: repetidores, concentradores, pontes, conmutadores, encamiñadores, pasarelas.**

**51.1 Redes de área local**

**51.1.1 Funcións dos niveis especificados polo IEEE 802**

**51.1.1.1 Tramas LLC**

**51.1.2 Exemplos de redes locais**

**51.1.2.1 Técnicas de contenda en bus**

**51.1.2.2 Técnicas de contenda en anel**

**51.2 Topoloxías**

**51.2.1 Bus**

**51.2.2 Anel**

**51.2.3 Estrela**

**51.2.4 Árbore**

**51.2.5 Malla**

**51.2.6 Mixta**

**51.3 Redes Ethernet**

**51.3.1 Operación dunha rede Ethernet**

**51.3.2 Control de acceso ó medio**

**51.3.2.1 Transmisión dunha trama**

**51.3.2.2 Recepción dunha trama**

**51.3.2.3 Algoritmo de BackOff**

**51.3.2.4 Formato de trama MAC**

**51.3.2.4.1 Direccións 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 e redes virtuais**

#### 51.4.1 VLAN

##### 51.4.1.1 Tipos de VLAN

#### 51.5 Xestión de redes

##### 51.5.1 Modelo OSI de xestión de rede

##### 51.5.2 SNMP

###### 51.5.2.1 Funcionamento de SNMP

###### 51.5.2.2 Especificacións técnicas SNMP mínimas requiridas

##### 51.5.2 TMN

#### 51.6 Sistemas de cableado

##### 51.6.1 Estructura do cableado estruturado

##### 51.6.2 Instalacións comúns de telecomunicacións

##### 51.6.3 Medios de transmisión

###### 51.6.3.1 Fibra óptica

###### 51.6.3.2 Par trenzado

#### 51.7 Electrónica de rede

##### 51.7.1 Repetidores

##### 51.7.2 Concentradores

##### 51.7.3 Pontes

##### 51.7.4 Conmutadores

##### 51.7.5 Encamiñadores

##### 51.7.6 Pasarelas

#### 51.8 Bibliografía

### **51.1 REDES DE ÁREA LOCAL**

Unha LAN conecta ordenadores e outros dispositivos nun espazo limitado como pode ser unha casa, un edificio, unha oficina ou un conxunto de edificios próximos entre si.

Tipicamente a distancia que abarca unha LAN non supera os 100 metros. A familia de estándares (que leva o mesmo nome que o comité que os propuxo) no que se basea a maioría das tecnoloxías usadas en LAN e a IEEE 802 que se ocupa de redes de area local e de area metropolitana nas

que o tamaño de trama é variable (como oposición a outros tipos de redes onde se transmiten celdas de tamaño estándar, ou fluxos continuos, ...). Veremos agora unha introducción ás tecnoloxías LAN a través da visión da estrutura que estandariza e dalgúns exemplos desta familia.

### **51.1.1 FUNCIONS DOS NIVEIS ESPECIFICADOS POLO IEEE 802**

No nivel físico o IEEE 802 define:

- A codificación e sinalización (Manchester, 4B/5B, etc...).
- A xeración de preambulos para sincronización.
- Transmisión e recepción de bits.

No nivel de enlace (subnivel MAC):

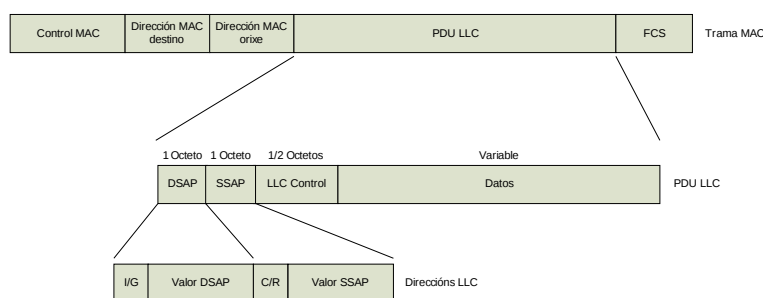
- A capa de control de acceso ó medio encargase de controlala forma en que as estacións que comparten o medio físico acceden a el. Este control pode ser centralizado nunha estación monitora (lóxica de acceso sinxela, pódense establecer prioridades, etc.) ou distribuído entre tódalas estacións (mellora as prestacións e evita conxestións).
- En cuanto a cómo controlar o acceso ó medio, este pode ser síncrono (dedicase unha capacidade fixa a cada estación) ou asíncrona (asígnase a capacidade de transmitir de maneira dinámica). Dentro das técnica asíncronas podemos nomear:
  - o Rotación circular: A cada estación se lle proporciona a posibilidade de transmitir dunha maneira ordenada e cíclica. Útil cando moitas estacións necesitan realizar transmisións largas.
  - o Reserva: O tempo divídese en ranuras, as estacións reservan ranuras para transmitir. Adecuada en tráfico continuo.
  - o Competición: Tódalas estacións compiten nun momento dado por obtela posibilidade de transmitir. Útil en tráfico a ráfagas.
- Esta capa é a responsable da detección de erros e rexeitar tramas erróneas (o control de erros e retransmisión de tramas corresponde o subnivel LLC).

No nivel de enlace (subnivel LLC):



- Responsable do interface con capas superiores, ofrecendo aos mesmos servizos con ou sen conexión. Tamén se encarga do control de fluxo e de erros na transmisión de tramas. A mesma capa LLC pode ofrecer varias opcións MAC.
- Ofrece ós niveis superiores, os seguintes servizos:
  - o Non orientado a conexión sen confirmación: Servizo de tipo datagrama, non inclúe mecanismos de control de fluxo e de erros, polo que a recepción de datos non está garantida. É o mais frecuente en LANs, e pode encontrarse facilmente para IP ou IPX sobre Token Ring ou FDDI.
  - o Modo orientado a conexión: Establecese unha conexión lóxica entre dous usuarios con control de erros e de fluxo. Similar ó ofrecido por HDLC. É empregada por NetBEUI ou MS-LAN Manager.
  - o Non orientado a conexión con confirmación: É unha mestura dos anteriores, os datagramas son confirmados, pero non se establece unha conexión lóxica.

#### 51.1.1.1 TRAMAS LLC



Significado dos bits I/G e C/R:

- I/G. Bit de dirección individual ou grupo de destinos SAP.
- C/R. Bit que indica se se trata dun comando ou unha resposta.

Existen os seguintes tipos de tramas:

- Non numeradas (U): Formato 11 MM P/F MMM onde MM\_MMM indica a 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 non numerada (datagrama).
- o 11\_110: SABME -> Establecer modo de conexión balanceada asíncrona.
- o 11\_000: DM -> Modo desconexión.
- o 00\_010: DISC -> Cerre de conexión.
- o 00\_110: UA -> Confirmación non numerada a un SABME o DISC.
- o 10\_001: FRMR: Rexeite dunha trama incorrecta.
- Información (I): Formato 0 N(S) P/F N(R).
- Supervisión (S): Formato 10 SS 0000 P/F N(R) onde SS indica a función.
  - o 00: RR -> Receptor preparado.
  - o 10 RNR -> Receptor non preparado.
  - o 01 REJ -> Demanda de retransmisión de tramas dende N(R).

### **51.1.2 EXEMPLOS DE REDES LOCAIS**

#### **51.1.2.1 TÉCNICAS DE CONTENDA EN BUS**

Mais adiante neste mesmo tema veremos en detalle como funciona Ethernet.

#### **51.1.2.2 TÉCNICAS DE CONTENDA EN ANEL**

Imos ver algún detalle de IEEE 802.5 (Token Ring) para exemplificar as técnicas de contenda en anel.

Este tipo de topoloxía, consta de varios repetidores que copian e rexeneran cada bit que circula polo anel, retrasando, no tempo de transmisión de un bit, a circulación da trama.

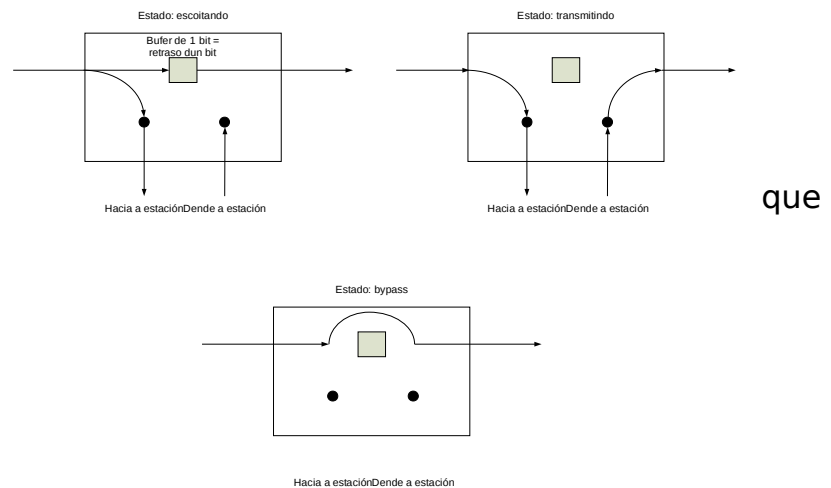
Nunha topoloxía en anel, debe controlarse a eliminación de tramas. Esta tarefa pode realizala o destino ou máis comunmente, a orixe. Seguindo este último convenio, facilítase o uso de direccionamento múltiple e confirmacións automáticas de recepción da trama.

Esta topoloxía presenta os seguintes problemas:

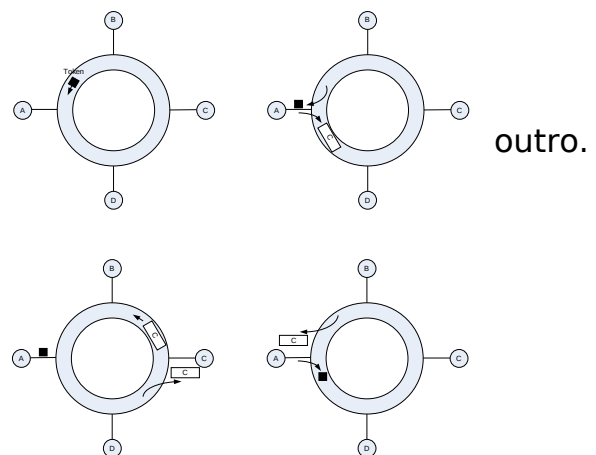
- Problemas derivados da perda dun enlace ou estación.

- Inserción dunha nova estación (necesidade de identificación por parte dos seus veciños).
- Perda ou duplicidade do testigo.

A topoloxía en estrela-anel soluciona moitos destes problemas, ó existir un nodo central se encarga de monitorizar e illar fallos. Na seguinte imaxe podemos ver como funciona 802.5 con respecto a unha estación.



Na seguinte imaxe podemos ver un exemplo de funcionamento da transmisión dunha trama dun nodo a

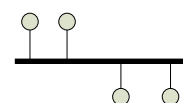


## 51.2 TOPOLOXÍAS

A topoloxía de rede defínese coma a cadea de comunicación usada polos nodos que conforman una rede para comunicarse entre si.

### 51.2.1 BUS

Nas redes onde se usa unha topoloxía en bus cada un dos nodos conectase ó mesmo cable. Un sinal enviado un dos ordenadores conectado á rede viaxa en ambas direccións do cable ata chegar os extremos alcanzando a tódolos nodos no seu camiño.

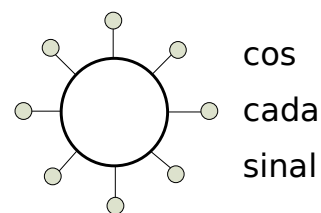


Podemos considerar dous tipos de redes en bus:

- Bus lineal: onde só existen dous extremos finais e tódolos equipos están conectado ó mesmo cable.
- Bus distribuído: cando existen máis de dous extremos finais e o bus configúrase basicamente conectando máis cables ó mesmo e formando ramas.

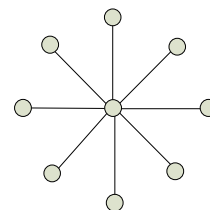
### 51.2.2 ANEL

Unha topoloxía en anel constrúese en forma circular datos circulando ó redor do anel nunha soa dirección e cada dispositivo actúa coma un repetidor para manter o a un nivel adecuado.



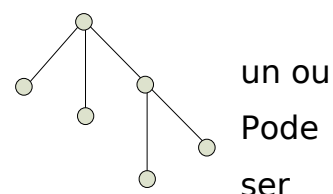
### 51.2.3 ESTRELA

Nesta topoloxía cada ordenador conectase a un dispositivo central usando unha conexión punto a punto. Todo o tráfico que viaxa pola rede pasa polo dispositivo central que actúa coma un repetidor.



### 51.2.4 ÁRBORE

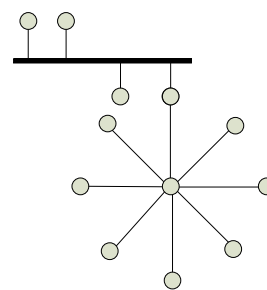
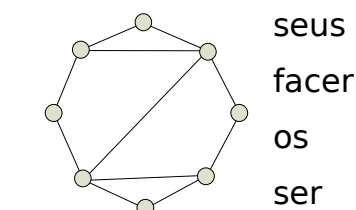
Nesta topoloxía os nodos estrutúranse de forma xerárquica, cun nodo no nivel superior conectado a varios nodos no seguinte nivel e así sucesivamente. haber un número fixo de nodos fillos por nodo pai ou



completamente libre. Durante unha transmisión, os datos soben na xerarquía dende o nodo emisor ata ó primeiro nodo común entre o emisor e receptor baixando logo ata o receptor.

### 51.2.5 MALLA

É un tipo de topoloxía onde cada nodo debe enviar os propios datos, se ten un enlace directo ó destino, ou uso doutros nodos intermedios para que retransmitan datos de non ter un enlace directo. As mallas poden total (tódolos nodos teñen un enlace directo ós



demais nodos) ou parcialmente (non tódolos nodos teñen un enlace directo ós demais nodos) conectadas.

### **51.2.6 MIXTA**

As topoloxías mixtas usan unha combinación de dúas ou mais das topoloxías anteriores adoptando formas que poden ter unha elevada complexidade.

### **51.3 REDES ETHERNET**

Ethernet (IEEE 802.3) é a máis común das redes de área local existindo interfaces (tarxetas, ...) para case calquera tipo de maquina. Á súa velocidade orixinal era de 10 Mbps, actualmente existen solucións comerciais a 100 Mbps (FastEthernet) e 1000 Mbps (Gigabit Ethernet). Ethernet utiliza un método distribuído de acceso ó medio para tódalas máquinas conectadas. Non existe unha estación mestra que controle a rede. Non existen tampouco niveles de prioridade para transmitir. O modo de transmisión é semi-duplex (orixinalmente Ethernet montábase usando unha topoloxía de bus), aínda que os conmutadores actuais permiten full-duplex.

O estándar Ethernet describe as capas física e MAC.

#### **51.3.1 OPERACIÓN NUNHA REDE ETHERNET**

Ethernet basease, coma comentamos anteriormente, nun acceso distribuído ó medio (Carrier Sense Multiple Access with Collision Detection, CSMA/CD polas súas siglas en ingles) no que calquera equipo pode por si mesmo decidir o inicio da transmisión e ocupalo medio cos seus datos sempre e cando non exista outra estación transmitindo. Poden ocorrer colisións debidas ó retardo da propagación (tempo que tarda o sinal en alcanzar todo o medio).

O transporte de datos ten lugar mediante a emisión de paquetes (tramas) emitidas sobre o medio físico. Estas tramas terán unha lonxitude entre 64 e 1518 bytes (con un campo de datos entre 46 e 1500 bytes).

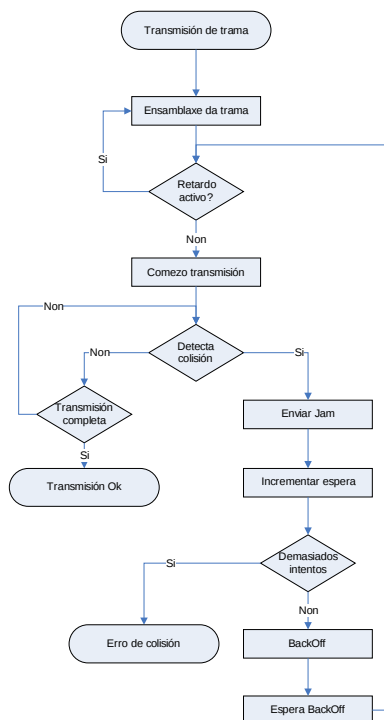
A tarxeta de rede do computador xestiona as funcións MAC inherentes a Ethernet e comunícase coa capa LLC superior.

A eficiencia global de Ethernet é xeralmente alta, aínda que difícil de cuantificar e dependente do número e tipo de estacións conectadas. Ethernet ten unha gran eficiencia en redes onde existe un equipo que xenera a maior parte do tráfico e o resto dedícanse a recibir e transmitir pequenas cantidades.

### 51.3.2 CONTROL DE ACCESO Ó MEDIO

Como xa mencionamos anteriormente, Ethernet usa CSMA/CD para o control de acceso ó medio. Nas figuras seguintes podemos ver de forma gráfica os principais algoritmos implicados.

#### 51.3.2.1 TRANSMISIÓN DUNHA TRAMA

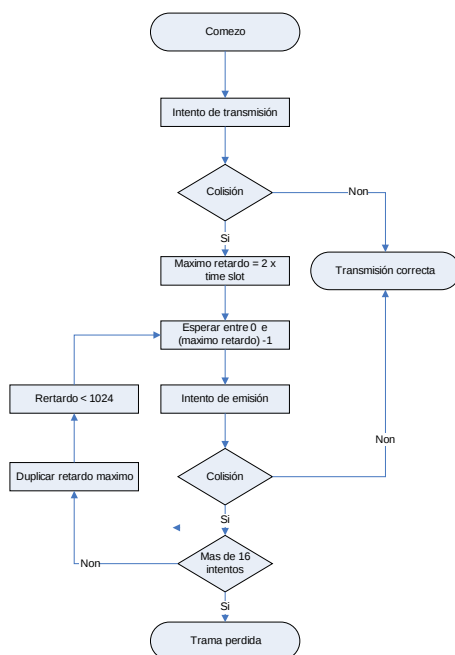


#### 51.3.2.2 RECEPCIÓN DUNHA TRAMA

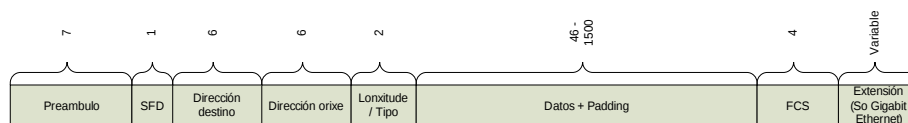


- Runt (anana): Trama demasiado curta, menor de 64 bytes. Pode haber sido truncada por unha colisión. Normalmente será una trama desaliñada cun FCS erróneo.
- Jabber: Trama demasiado longa, mais de 1518 bytes. Normalmente non existirán tramas de este tipo na rede, a non ser que se trate de:
  - o Unha superposición de dúas tramas.
  - o Ristra sen estrutura de frame enviada por un equipo que funciona incorrectamente.
- Trama desaliñada: Unha trama cun número de bits non divisible entre oito.
- Trama con FCS erróneo: Trama para a cal o receptor calculou un CRC que non concorda cos últimos 4 bytes.

O algoritmo de backoff define o tempo que a estación debe esperar para o seguinte intento de emisión dunha trama no caso dunha colisión no anterior intento, tendo en conta os intentos xa realizados.



### 51.3.2.4 FORMATO DE TRAMA MAC



O formato MAC para 802.3 consta dos seguintes campos:

- **Preámbulo:** O receptor utiliza 7 bytes co patrón 10101010 para sincronización.
- **SFD:** Delimitador de comezo de trama 10101011.
- **Dirección destino:** Indica unha estación ou estacións á que vai dirixida a trama. Pode ser individual, de grupo ou global.
- **Dirección orixe** da estación que emite a trama.
- **Lonxitude** do campo de datos LLC.
- **Datos LLC.**
- **Recheo (Padding):** Octetos engadidos para construír tramas o suficientemente longas que aseguren un correcto funcionamento da técnica CD.
- **Secuencia de comprobación de trama (FCS)** Código de redundancia cíclica de 32 bits en base a tódolos campos excepto os de preámbulo, SFD e o propio FCS.



- A maiores, no caso de Gigabit Ethernet, requírese engadir bytes extra ás tramas menores de 512 bytes para garantir que se detectan as colisións

#### **51.3.2.4.1 DIRECCIÓN MAC 802.3**

A dirección MAC é unha dirección única (con respecto a tódalas tarxetas de rede existentes) que posúe a tarxeta de rede. Poden ser de 16 ou 48 bits.

As de 48 bits son 6 bytes onde:

- Os 3 primeiros constitúen o código do vendedor. O primeiro byte do código de vendedor ten dous bits especiais:
  - o O bit menos significativo é o que indica se a dirección é individual ou de grupo (multicast, bit a uno).
  - o O bit mais significativo indica se se trata dunha dirección global (visible a través dunha ponte) ou local (bit a uno).
- Os 3 últimos o identificador do dispositivo.

Existe unha dirección global (broadcast), representada polos 6 bytes a un. Tamén existen 247 direccións diferentes, mantidas polo IEEE.

Exemplos:

- 08:00:20:0a:ef:31 (dirección individual)
- 09:00:20:00:00:00 (multicast a todas as máquinas 08:00:20)
- 89:00:20:00:00:00 (multicast local)
- 00:80:C2 (Prefixo usado polo 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 os que poderemos montar Ethernet, dependendo da velocidade que queremos alcanzar.

##### **51.3.3.1 10 MBPS**

	10BASE5	10BASE2	10BASE-T	10ANCHA36	10BASEF-P	10BASEF-L
Medios de	Coaxial 50	Coaxial 50	UTP	Coaxial 75 Ohms.	Par Fibra 850 nm	Par Fibra

transmisión	Ohms.	Ohms.				850 nm
Topoloxía	Bus	Bus	Estrela	Bus / Arbore	Estrela	Punto a punto
Lonxitude 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
Topoloxía	Estrela	Estrela	Estrela	Estrela
Lonxitude máxima / segmento	100	100	100	100

### 51.3.3.3 1000 MBPS

	1000BASET	1000BASET X	1000BASEC X	1000BASES X	1000BASEL X
Medios de transmisión	4 Pares UTP5	2 Pares UTP6	STP	Par Fibra 850 nm	Par Fibra 1300 nm
Topoloxía	Estrela	Estrela	Estrela	Estrela	Punto a punto
Lonxitude máxima / segmento	100	100	25	275 - 62,5 550 - 50	550 - MMF 5 km - SMF

## 51.4 REDES CONMUTADAS E REDES VIRTUAIS

Os modelos de rede baseados na compartición de ancho de banda, presentes nas arquitecturas LAN dos primeiros noventa, carecen da potencia suficiente como para proporcionar os cada vez maiores anchos de banda que requiren as aplicacións multimedia. Neste tipo de LANs os usuarios comparten un único canle de comunicacións, de modo que todo o ancho de banda da rede asignase ó equipo emisor de información quedando o resto dos equipos en situación de espera. Seguindo a filosofía de compartición do ancho de banda e para aumentar o ancho de banda dispoñible para cada usuario, pódese optar pola segmentación dos buses e aneis. Sen embargo, estas técnicas non ofrecen boas prestacións, debido principalmente as dificultades que aparecen para xestionala rede. Cada segmento soe conter de 30 a 100 usuarios.

A técnica idónea para proporcionar elevados anchos de banda é a conmutación. Mediante esta técnica, cada estación de traballo e cada servidor posúe unha conexión dedicada dentro da rede, co que se consegue aumentar considerablemente o ancho de banda a disposición de cada usuario.

As LANs baseadas en compartición de ancho de banda constrúense mediante concentradores e encamiñadores. Nunha LAN conmutada, unha das funcións tradicionais do encamiñador pasa a ser realizada polo conmutador LAN, quedando o encamiñador destinado a funcións relacionadas coa mellora das prestacións no que respecta á xestión da rede e a conexión con outras redes. Con este novo modelo pódense conectar de 100 a 500 usuarios. O decremento nos prezos de conmutadores Ethernet foi un dos principais empuxes a que un bo número de empresas se inclinen por unha LAN conmutada.

Sen embargo, a continua instalación de conmutadores, dividindo a rede en máis e máis segmentos (con menos e menos usuarios por segmento) non reduce a necesidade de broadcast. As VLANs representan unha solución alternativa ós encamiñadores con función de xestores da rede.

#### **51.4.1 VLAN**

Unha VLAN (Virtual Local Area Network) é unha rede lóxica creada sobre unha rede física. As súas principais características son:

- Permite xestionar os segmentos dunha LAN como dominios de emisión lóxicos. Restrínxese desta forma o tráfico multicast e broadcast.
- Non importa a ubicación topolóxica ou física das estacións (xa que en caso de ser necesario prodúcese unha comunicación entre conmutadores).
- Se se configura adecuadamente poderase mover unha estación dunha VLAN a outra sen necesidade de modificala dirección IP.
- Os encamiñadores só se usarán agora para comunicar VLANs.

#### **51.4.1.1 TIPOS DE VLAN**

- Nivel 1: Configuradas usando o porto do conmutador (incluso entre conmutadores). É a forma mais sinxela de definir VLANs. Se se move a estación haberá que reconfigurar manual da VLAN. Ten a limitación de que un porto non pode pertencer a máis dunha VLAN.
- Nivel 2: Configuradas usando a dirección MAC da estación. Estas VLAN defínense en base a un conxunto de direccións MAC. Un porto unicamente é rexistrado nunha VLAN cando se constata que un paquete con unha determinada MAC orixe foi transmitido por ese porto. Para identificar a que grupo pertence unha trama debe inspeccionarse a mesma polo que esta técnica é mais lenta que a anterior. Esta técnica representa mais traballo ó principio xa que necesítase rexistrar nalgunha VLAN todas as MAC.
- Nivel 3: Configuradas polo tipo de protocolo ou por subrede IP. O particionado por protocolo permite o movemento sen reconfiguración, e elimina a necesidade de etiquetado de tramas. Pero esta técnica obriga a analizar o paquete de rede por completo polo que ten un menor rendemento cas técnicas de nivel 2.
- Técnicas de maior nivel: Configuradas polos protocolos de nivel superior baseándose en aplicacións e / ou servizos. Permite crear unha VLAN con tódalas máquinas que utilicen o servizo de e-mail, por

exemplo. A maioría dos fabricantes non a implementan, pois consideran suficiente a técnica de nivel 3.

IEEE 802.1Q só define os tipos de nivel 1 e 2. A partir dese nivel o establecemento de

VLANs non se encontra estandarizado e cada fabricante implementao de maneira propietaria resultando algunhas implementacións incompatibles con outras.

## **51.5 XESTIÓN DE REDES**

### **51.5.1 MODELO OSI DE XESTIÓN DE REDE**

ISO, seguindo as directrices do grupo OSI, definiu o modelo de xestión de rede como a forma máis importante para entender a funcións principais dos sistemas de xestión de rede.

O modelo OSI de xestión de rede categoriza as funcións en 5 áreas que as veces se denominan modelo FCAPS (Fault, Configuration, Accounting, Performance e Security):

- **Falla (Fault):** Sendo o obxectivo desta área detectar, illar, corrixir e rexistrar as fallas que se produzan na rede.
- **Configuración (Configuration):** Os obxectivos desta área son recoller/fixar/facer seguimento da configuración dos dispositivos. A xestión da configuración ocupase de monitorizar a información de configuración do sistema e calquera cambio que se produzan a mesma. A importancia deste área ven dada por que moitas incidencias na rede son o resultado de cambio sen arquivos de configuración, actualización de versións, etc. Unha adecuada xestión da configuración obriga a rexistrar tódolos cambios na configuración software e hardware.
- **Contabilidade (Accounting):** Sendo o obxectivo principal recoller estatísticas. A xestión da contabilidade preocupase por manter a información referida á utilización da rede, de forma que se poda facturar a usuarios individuais, departamentos, etc.
- **Rendemento (Performance):** O obxectivo deste área é dobre: por un lado preparar a rede par ao futuro e por outro medir a eficiencia actual

da mesma asegurándose que está dentro dos niveis aceptables. A xestión do rendemento preocupase de recoller regularmente a información de rendemento da rede como son os tempos de resposta, rátios de perda de paquetes, utilización de enlaces de datos, etc.

- **Seguridade (Security):** O obxectivo da xestión da seguridade é controlalo acceso ós recursos da rede. Este área non so se preocupa de que a rede sexa seguras e non de recadar e analizar a información referida á seguridade. Ás funcións típicas dentro deste área son a autenticación, autorización, auditoría, de forma que os usuarios (tanto internos como externos) teña no acceso adecuado ós recursos da rede.

### **51.5.2 SNMP**

SNMP (Simple Network Management Protocol) é o protocolo definido polos comités técnicos de Internet para ser utilizado coma ferramenta de administración dos distintos dispositivos en calquera rede. O funcionamento de SNMP é sinxelo, como o seu propio nome indica, aínda que a súa implementación pode chegar a ser tremendamente complexa. SNMP utiliza a capa de transporte de TCP/IP mediante o envío de datagramas UDP (os axentes escoitan no porto 161 e as estacións xestoras no 162). Sen embargo, o feito de usar UDP fai que o protocolo no sexa fiable (en UDP non se garante a recepción dos paquetes enviados, como en TCP).

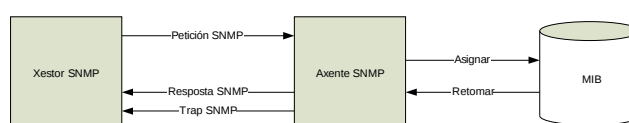
O protocolo SNMP está definido nun gran número de RFCs (Request For Comments), entre eles o RFC 1157, 1215 (que definen a versión 1), do 1441 ao 1452 (que definen a versión 2), do 2271 ao 2275 e do 2570 ao 2575 (para SNMP v3).

#### **51.5.2.1 FUNCIONAMENTO DE SNMP**

Cada axente (pódese ver a un axente coma unha máquina na que queremos monitorizar algún dos seus estados) ofrece unha determinada serie de variables, que poden ser lidas ou modificadas. Ademais, un axente pode enviar “alarmas” (Traps) a outros axentes para avisar de eventos que teñen lugar. O normal é que o axente encargado de recibir os eventos se

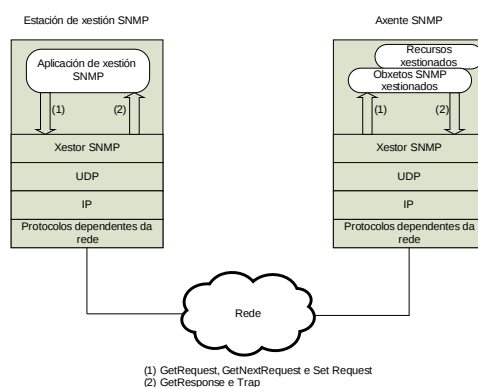
denomine “xestor” (podemos ver a este como á maquina que monitoriza o estado de toda a rede). De forma moi resumida podemos ver as capacidades expostas:

- GET : A estación xestora extrae (lee) o valor dun obxecto do axente
- SET : A estación xestora fixa (escribe) o valor dun obxecto do axente
- TRAP : Permite a un axente notificar á estación xestora eventos significativos



As variables ofrecidas para a consulta nos axentes SNMP defínense a través dunha MIB (Management Information Base, Base de Información de Xestión ). A MIB é unha forma de determinala información que ofrece un dispositivo SNMP e a forma en que se representa. A versión da MIB actual é MIB-II e está definida no RFC 1213, aínda que hai múltiples extensións definidas noutros RFCs. A MIB está descrita en ASN.1 para facilitalo seu transporte transparente pola capa de rede.

Cada axente SNMP ofrece información dentro dunha MIB, tanto da estándar (definida nos distintos RFCs) como de aquelas extensións que desexe prover cada un dos fabricantes.



ASN.1 (Abstract Syntax Notation One) é un estándar de notación que describe a representación, a transmisión, a codificación e decodificación de estruturas de datos. Prové un conxunto de regras formais para describirla estrutura de obxectos que son independentes das técnicas de codificación

dunha máquina, aportando unha notación formal que elimina ás ambigüidades.

### **51.5.2.2 ESPECIFICACIÓNS TÉCNICAS SNMP MÍNIMAS REQUIRIDAS**

Existen diversas RFCs que definen SNMP. Por elo é importante establecer uns requisitos ou especificacións mínimas. Estas especificacións mínimas son:

- Versión do protocolo SNMPv2c (Community-based SNMPv2 - RFC 1901)  
Utiliza o mesmo modelo que a primeira versión do protocolo SNMP, e como tal non inclúe mecanismos de seguridade. As únicas melloras introducidas nesta versión consisten nunha maior flexibilidade dos mecanismos de control de acceso, xa que se permite a definición de políticas de acceso consistentes en asociar un nome de comunidade con un perfil de comunidade formado por unha vista MIB e uns dereitos de acceso a dita vista (so lectura ou lectura e escritura).
- A MIB deberá ser compatible co formato ASN.1. As implementacións doutros estándares da MIB son opcionais. ASN.1 está deseñado para definir información estruturada (mensaxes) de tal forma que sexa independente da máquina utilizada. Para facer isto ASN.1 define tipos de datos básicos, como enteiros e cadeas de texto, e permite construír novos tipos de datos a partir dos xa definidos. Tamén utiliza palabras especiais (keywords) para definir os seus procedementos, definir novos tipos, asignar valores, definir macros e módulos.
- O acceso múltiple deberá ser permitido, existindo 3 niveis de acceso cos seus correspondentes “login” e “password”.
- O requirimento mínimo respecto á seguridade, é a xeración de “Traps” no caso dunha autenticación fallida. A información relevante do infractor que deberá ser enviada no TRAP, será a dirección IP.

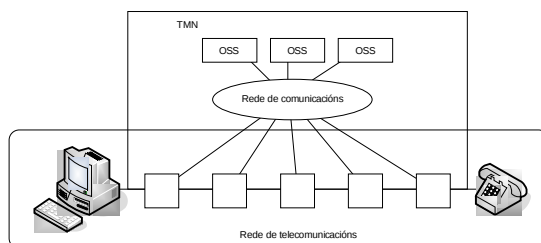
### **51.5.3 TMN**

TMN (Telecommunications Management Network) define un marco de traballo para alcanzala interoperabilidade e comunicación entre redes de comunicacións e sistemas operativos heteroxéneos. TMN foi desenvolvido por



ITU coma unha infraestrutura para soportar a xestión e despregue de servizos dinámicos de telecomunicacións.

TMN provee un framework flexible, escalable, confiable, barato e fácil de mellorar. TMN permite crear redes mas capaces e eficientes definindo unha forma estándar de realizalas tarefas de xestión da rede e comunicacións. O procesamento en TMN pode ser distribuído para melloralas escalabilidade. Unha rede de telecomunicacións está composta de elementos de conmutación, circuítos, terminais, etc. En terminoloxía TMN todos estes elementos son Elementos da Rede (NE Network Elements). TMN permite a comunicación entre os NEs e OSS (Operations Support Systems).



TMN usa principios de orientación a obxectos e interfaces estándar para definir as comunicacións entre diferentes entidades na rede. O interface de xestión estándar chámase Q3. TMN basease en estándares OSI como CMIP (Common Management Information Protocol), GDMO (Guideline for definition of management objects), ASN.1 e o modelo de referencia OSI. As funcións de xestión realízanse a través de operacións compostas de primitivas CMIS (Common Management Information Service).

A información de xestión da rede, así como as regras polas que a información se presenta e xestiona, chámanse MIB (Management Informaion Database). Os procesos que xestionan a informa chámanse entidades que poden ser de dous tipos: xestor ou axente.

TMN describe as redes de telecomunicacións dente distintos puntos de vista:

- Modelo funcional: representado por bloques que aportan unha visión xeral das funcións e características de TMN.

- o OS (Operation System): realiza funcións de operación do sistema incluíndo monitorización e control das funcións de xestión de telecomunicacións.
  - o MD (Mediation Device): Realiza funcións de mediación entre os interfaces locais TMN e o modelo de información dos OS.
  - o QA (Q-Adapters): Permite a TMN xestionar NEs que non teñen interfaces TMN.
  - o NE (Network Entity): Contén información xestionable que é monitorizada e controlada polo OS.
  - o WS (Workstations): Traducen a información entre formato TMN e un formato comprensible polo usuario.
  - o DCN (Data Communication Network): Representa a rede de comunicacións cubrindo os niveis 1 a 3 de OSI.
- Conxunto de interfaces:
  - o Q: Os interfaces Q existen entre dous bloques funcionais TMN que pertencen o mesmo dominio.
    - Qx: existe entre os NE e os MD, QA e MD e entre os MD e outro MD.
    - Q3: é a interface do OS e existe entre os NEs e OS, QA e OS, MD e OS e entre OS e outro OS.
  - o F: As interfaces F existen entre os WS e OS e entre os WS e MD.
  - o X: Estas interfaces existen entre dous OS TMN de diferentes dominios ou entre un OS TMN e outro OS nunha rede non TMN.
- Modelo lóxico ou de negocio: Este modelo está baseado en capas de distintos niveis xerárquicos:
  - o BML (Business Management Layer): Planificación de alto nivel, presupostos, BLAs (Business Level Agreements), etc.
  - o SML (Service Management Layer): Usa a información presentada pola capa NML para xestionar os servizos contratados por clientes actuais ou potenciais. Tamén é o punto

clave de contacto con provedores de servizo e outras entidades administrativas.

- o NML (Network Management Layer): A NML ten visibilidade de toda a rede baseada na información dos OSs da capa EML. NML permite xestionar os NEs de forma individual ou coma un grupo.
- o EML (Element Management Layer): Xestiona cada elemento da rede contendo OSs, cada un dos cales xestiona certos NEs. Tamén contén a os MDs.
- o NEL (Network Element Layer): Representa a información xestionable por TMN nun NE. OS QA e os NE están localizados nesta capa.

## **51.6 SISTEMAS DE CABLEADO**

O cableado dunha determinada organización ou edificio organizase seguindo os principios do cableado estruturado. Os sistemas de cableado estruturado son as infraestruturas de cable (xa sexa par de cobre, coaxial, fibra óptica, etc. Ou unha combinación deles) que transportan ós sinais de datos dende un emisor ata un receptor dentro de un edificio, nun campus, ...

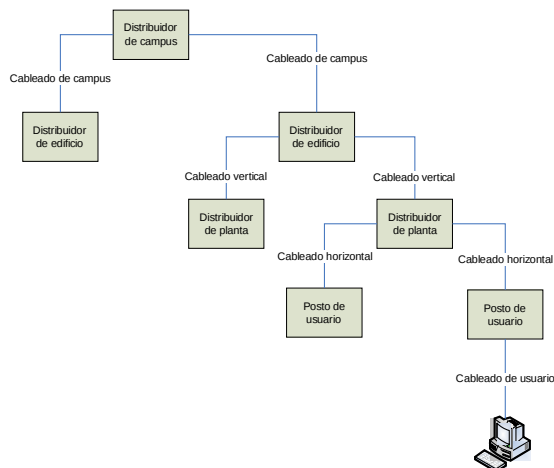
O cableado estruturado facilita enormemente os cambios de ubicacións en persoas e equipos ó permitir cambiar as conexións dun punto a outro sen necesidade de instalar novos cables.

Tamén facilita os cambios no equipamento de telecomunicacións xa que está pensado para ser independente duns equipos (teléfonos, concentradores, ...) concretos.

Existen varias normas que establecen como debe ser o cableado, as máis importantes son a CENELEC EN 50173 (que define o cableado estruturado) e a lexislación vixente en materia das Instalacións Comúns de Telecomunicacións.

### **51.6.1 ESTRUCTURA DO CABLEADO ESTRUCTURADO**

O cableado estruturado establece de forma xerárquica con cada elemento de orde inferior interconectado cun elemento de nivel superior.



Os principais compoñentes do cableado son:

- **Cableado de campus:** Cableado dende tódolos distribuidores de edificios ó distribuidor de campus. Soe realizarse usando fibra óptica e / ou liñas punto a punto (posiblemente sobre unha rede pública) polas distancias implicadas. Pode incluír repetidores e outros elementos de conexión.
- **Cableado Vertical:** Cableado dende os distribuidores de planta ó distribuidor do edificio. Soe comporse de varios cables UTP ou fibra óptica que conectan cada distribuidor de planta co distribuidor do edificio.
- **Cableado Horizontal:** Cableado dende o distribuidor de planta (chegando a uns paneis patch -un conxunto de conectores RJ45 instalados nun bastidor de 19 polgadas- instalados en devandito distribuidor) aos postos de usuario. Soe ser un so cable UTP no que non se permiten pontes, derivacións e empalmes ó longo de todo o traxecto. A máxima lonxitude permitida, independentemente do tipo de medio utilizado, é de 90 m (+ 3 m usuario + 7 m cable de conexión ao patch panel = 100m).



- **Cableado de Usuario:** Cableado dende o posto de usuario aos equipos. Soe consistir nun latiguillo que conecta a toma da parede co equipo (xa sexa un PC, un teléfono, ...).

Os principais puntos da rede de cableado estruturado son:

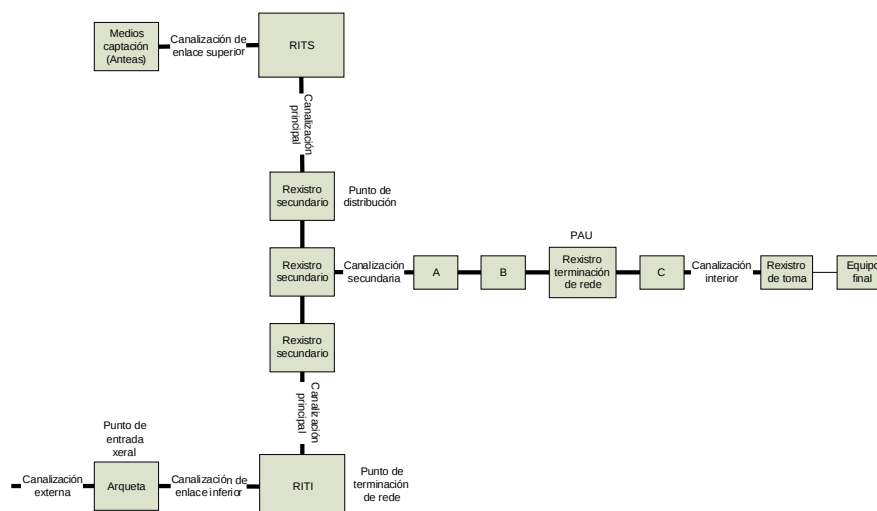
- **Distribuidor de campus:** Punto central onde chega todo o cableado de campus.
- **Distribuidores de edificio:** Punto onde se conecta o cableado de campus e onde chega todo o cableado vertical do edificio.
- **Distribuidores de planta:** Punto onde se conecta o cableado vertical e chega todo o cableado horizontal da planta.
- **Postos de usuario:** Punto onde se conecta o cableado horizontal co cableado de usuario.

### **51.6.2 INSTALACIÓNS COMÚNS DE TELECOMUNICACIÓNS**

Un proxecto de ICT describe as instalacións necesarias para poder dotar a un edificio (normalmente un edificio de vivendas) dunha infraestrutura común de telecomunicacións. Este proxecto se debe xustificar tecnicamente mediante os cálculos e especificacións correspondentes, co fin de cumprir minimamente as seguintes funcións:

- Captación, adaptación e distribución dos sinais de radiodifusión sonora e televisión terrestres.
- Captación, adaptación e distribución dos sinais de radiodifusión sonora e televisión por satélite.
- Acceso ó servizo telefónico dispoñible ó público (RTB).

O proxecto tamén incorpora a infraestrutura necesaria que permite ó acceso ós servizos de telecomunicacións de banda ancha que poidan ofrecer os diferentes provedores.



### Canalizacións nunha ICT:

- Canalización de enlace superior: conexión entre os elementos de captación do sinal do TDT e satélite (antenas) ata o RITS.
- Canalización de enlace inferior: conexión entre a arqueta onde se accede ás redes de telefonía (RTB) e datos ata o RITI.
- Canalización principal: distribución do cableado dende o RITI e o RITS ata os rexistros secundarios en cada planta.
- Canalización secundaria: dispersión do cableado dende o rexistro secundario da planta ata os distintos rexistros de terminación da rede / PAU dos usuarios.
- Canalización interior: cableado interior da vivenda dende o PAU ata as tomas.

### Puntos principais dunha ICT:

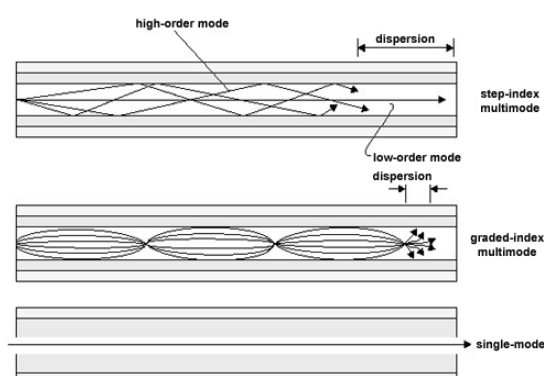
- Recinto de instalacións de telecomunicacións superior (RITS): recinto dedicado ás telecomunicacións en exclusiva e situado na parte superior do edificio, contendo normalmente o equipamento necesario para a recepción / amplificación do sinal da TDT ou de satélite.
- Recinto de instalacións de telecomunicacións inferior (RITI): recinto dedicado ás telecomunicacións en exclusiva e situado na parte inferior do edificio, contendo normalmente a distribución do cableado para voz e datos cara ás vivendas.

- Rexistros principais: Rexistros ós que chegan as distintas canalizacións de enlace.
- Rexistros secundarios: Rexistros existentes en cada planta, a onde chega a canalización principal, e de onde se distribúe a canalización secundaria
- Rexistro de terminación de rede: Rexistro onde acaba a rede de distribución e dispersión do edificio e comeza a do usuario.
- Punto de acceso o usuario (PAU): Punto a onde se conecta a rede do usuario.
- Rexistro de toma: Toma a onde se conectan os equipos finais.

### 51.6.3 MEDIOS DE TRANSMISIÓN

#### 51.6.3.1 FIBRA ÓPTICA

En xeral, distínguense dous tipos de fibras ópticas, multimodo e monomodo, esta clasificación define como a luz viaxa no interior da fibra:



- Multimodo: En fibras multimodo o núcleo é máis grosso (entre 50 e 100 micrómetros) que nas fibras monomodo, facendo posible que a luz viaxe usando varios modos de propagación (varios camiños). Á súa vez as fibras multimodo poden clasificarse en índice escalonado (índice de refracción constante con velocidades de transmisión baixas da orde de 50 Mbps) e índice gradual (índice de refracción non constante con velocidades de transmisión elevadas da orde dos 1 Gbps). As fibras multimodo usanse para distancias curtas.
- Monomodo: Neste tipo de fibras a luz só ten un camiño posible usándose para longas distancias e requirindo conectores de mellor precisión e dispositivos máis caros. O diámetro do núcleo está entre os 7 e os 10 micrómetros. Existen 3 tipos de fibras monomodo: NDSF (Non

Dispersion-Shifted Fiber), DSF (Dispersion-Shifted Fiber) e NZ-DSF (Non Zero-Dispersion-Shifted Fiber).

Algúns dos tipos de fibra óptica son:

- ITU G.651: multimodo índice gradual de 50 micrómetros de núcleo e 125 micrómetros de revestimento.
- ITU G.652: NDSF cunha lonxitude de onda de 1.130 nm cun alcance de 1000km a 2,5Gbps, 60 Km a 10Gbps e 3 km a 40 Gbps.
- ITU G.653: DSF
- ITU G.655: NZ-DSF. Soportando 2,5Gbps a 6000Km, 10Gbps a 400Km e 40 Gbps a 25Km.

#### **51.6.3.2 PAR TRENZADO**

O tipo de cable máis usado para comunicacións é sen dubida o cable de par trenzado, en concreto os cables de 4 pares trenzados con diferentes illamentos e categorías. Atendendo ó seu illamento estes cables divídense en:

- UTP: Unshielded Twisted Pair ou par trenzado non blindado. Consiste en 4 pares de fíos nos que cada par esta trenzado seguindo un patrón.
- FTP: Foil/Folded Twisted Pair ou par trenzado recuberto. Consiste nun cable UTP que é recuberto cunha lamina de aluminio / cobre para mellorar o seu illamento.
- STP: Shielded Twisted Pair ou par trenzado blindado. Consiste en 4 pares de fíos nos que cada par a parte de estar trenzado está envolto nunha lámina de cobre ou aluminio para mellorar o seu illamento contra interferencias.

Atendendo ás súas características de transmisión os cables de par trenzado clasifícanse en categorías:

Categoría	Frecuencia	Aplicacións
Cat 1	0,4 MHz	Telefonía
Cat 2	4 MHz	Redes en desuso
Cat 3	16 MHz	Ethernet 10BASE-T e 100BASE-T4
Cat 4	20 MHz	Token Ring 16 Mbit/s

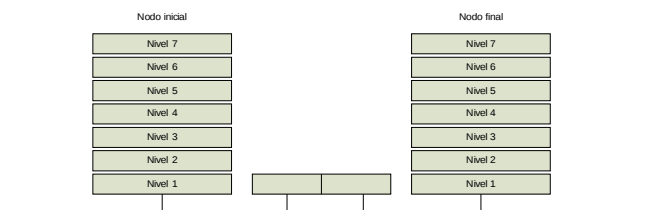


Cat 5	100 MHz	Ethernet 100BASE-TX e 1000BASE-T (non recomendable)
Cat 5e	100 MHz	Ethernet 100BASE-TX e 1000BASE-T
Cat 6	250 MHz	Ethernet 1000BASE-T
Cat 6e	250 MHz	Non é un estándar
Cat 6a	500 MHz	Ethernet 10GBASE-T
Cat 7	600 MHz	Ethernet 10GBASE-T (estándar aínda por aprobar)
Cat 7a	1000 MHz	Ethernet 10GBASE-T (estándar aínda por aprobar)

## 51.7 ELECTRÓNICA DE REDE

### 51.7.1 REPETIDORES

O repetidor é un elemento que permite a conexión de dous tramos de rede e que ten como función principal rexenerar o sinal para permitir alcanzar distancias maiores. Tipicamente o repetidor recibe o sinal dende un dos segmentos, amplifícao e emíteo no outro segmento.

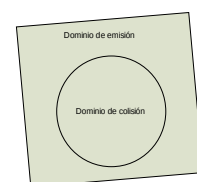


As súas características principais son:

- É a forma mais simple e barata de conectar segmentos de rede.
- Utilízanse para superar limitacións de distancia.
- Só valen para conectar topoloxías de rede compatibles.
- Non illan tráfico nin segmentan a rede.

### 51.7.2 CONCENTRADORES

Un concentrador é un dispositivo que funciona como centro de cableado para unha rede con topoloxía en estrela. A súa función consiste en que o tráfico que chega a calquera dos portos propáguese a través dos demais portos. Isto crea un medio de rede compartido e reúne ás computadoras conectadas á rede nun único dominio de colisión e de difusión, da mesma forma que se estiveran conectadas a un único cable. Como implicación



seus  
crea

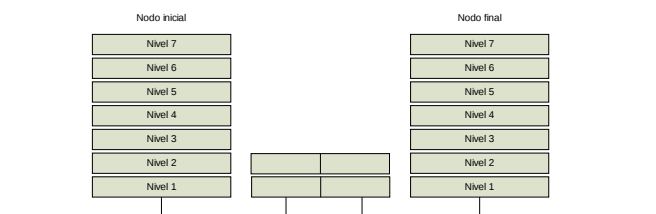
directa deste último temos que a velocidade de transmisión entre todos os nodos conectados a un concentrador é a mesma que entre dúas máquinas conectadas por un cable.

Os concentradores pódense apilar ou interconectar entre eles, funcionando coma un único concentrador con máis portos, coas mesmas vantaxes e limitacións.

### 51.7.3 PONTES

Unha ponte é un dispositivo utilizado para conectar segmentos de redes. Opera no nivel de enlace de datos e é selectivo respecto aos paquetes que pasan a través del. Fronte ós repetidores que traballan so con sinais, as pontes traballan con tramas.

Unha ponte non transmite datos ós segmentos conectados ata que chega toda a trama. Por este motivo, dous sistemas que se encontran en segmentos separados por unha ponte poden transmitir á vez sen que se produza unha colisión. Unha ponte conecta segmentos de rede de tal forma que mantén no mesmo dominio de difusión pero en distintos dominios de colisión.



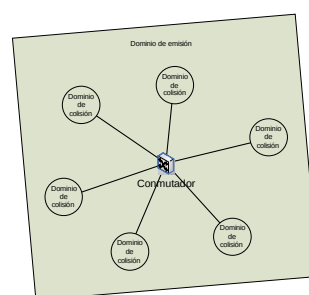
As súas características principais son:

- Poden illar o tráfico baseándose na dirección MAC.
- O igual que os repetidores, as pontes non son direccionables na rede (transparentes para niveis superiores).
- Só operan no nivel MAC de enlace (conectan segmentos da mesma rede).
- Estenden a topoloxía da rede (i.e. Anel-bus)
- Illan erros MAC (i.e. Tramas demasiado longas)
- Existen dous tipos:

- o Transparentes: Conectan topoloxías de rede compatibles (i.e. 10BaseT-10Base2) e non modifican ningunha parte de la trama.
- o De traslación: Conectan diferentes topoloxías de rede (i.e. 10BaseT-Token Ring) adaptando a trama ó protocolo MAC destino.

#### **51.7.4 CONMUTADORES**

Un conmutador opera no nivel de enlace de e é en esencia unha ponte multiporto no que un dos portos é un segmento de rede independente. Un conmutador recibe tráfico seus portos e ó contrario que un concentrador, o cal reenvía o tráfico a través tódolos demais portos, só o reenvía polo porto necesario para alcanzar o seu destino.



datos  
cada  
polos  
de

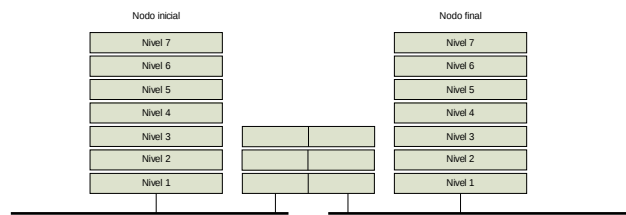
Un sistema conectado a un conmutador posúe o equivalente a unha conexión dedicada con cada un dos sistemas restantes conectados o conmutador e con todo o ancho de banda.

As súas principais características son:

- Diseñados para solucionar problemas de rendemento de LAN (escaseo de ancho de banda, colos de botella na rede).
- Alto rendemento no envío de paquetes e baixa latencia.
- Segmentan un dominio de colisión en outros mais pequenos.
- Reduce ou case elimina a contenda polo acceso ó medio.

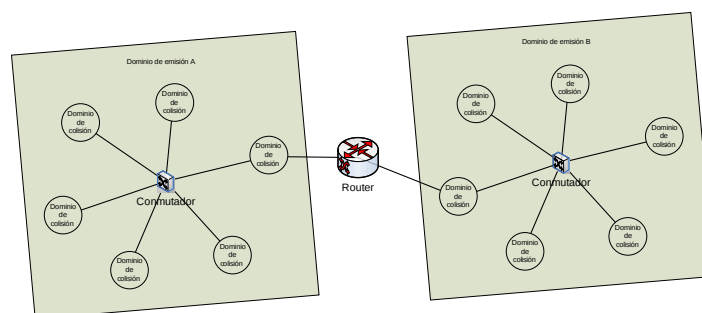
#### **51.7.5 ENCAMIÑADORES**

A labor dun encamiñador é a de conectar dúas redes completamente independentes no nivel de rede. Os encamiñadores son máis selectivos que as pontes no tráfico que pasa entre as redes e son capaces de seleccionar de forma intelixente a ruta máis eficiente cara un destino específico.



As funcións básicas dun encamiñador son:

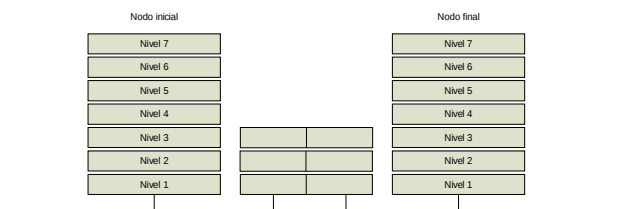
- Segmenta a rede en dominios individuais de envío (redes illadas a nivel MAC)
- Proporcionan envío intelixente de paquetes: analizan o tráfico e para cada paquete seleccionan a rede que proporciona a mellor ruta cara o destino. Un paquete pode pasar por varios encamiñadores no seu camiño cara o destino, cada un deles coñécese como salto. O obxectivo soe ser que chegue co menor número de saltos. Para elo utilizan as chamadas táboas de encamiñamento.
- Proporcionan acceso a las WAN de maneira eficiente.
- Soportan camiños redundantes (tolerancia a fallos).
- Proporcionan seguridade / firewall: analizan todo paquete que chega de unha das redes á que está conectado. Se a dirección de orixe e de destino pertencen á mesma rede descártano, se non reenvíanolo ó seu destino a través de outra rede.



### 51.7.6 PASARELAS

Unha pasarela conecta dúas redes distintas que usan protocolos e arquitecturas distintos a todos os niveis. A súa función é traducir o protocolo dunha rede ao protocolo da outra, pero tamén poden conectar redes que usen o mesmo protocolo. Neste último caso entran as que traducen IP a IP, por exemplo facendo NAT (Network Address Translation, que converte unha

dirección IP dunha rede –normalmente unha IP privada dunha LAN- noutra dirección IP –normalmente nunha IP pública- sendo capaz de inverter o 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-lei 1/1998, de 27 de febreiro
- A Lei 8/1999, de 6 de abril, de reforma da Lei 49/1960, de 21 de xullo, de Propiedade Horizontal
- O Real Decreto 401/2003, de 4 de abril, que aproba o Regulamento regulador das Infraestruturas Comúns de Telecomunicacións
- A Lei 10/2005, de 14 de xuño, de Medidas Urxentes para o Impulso da Televisión Dixital Terrestre, de Liberalización da Televisión por Cable e de Fomento do Pluralismo

**Autor:** Matías Villanueva Sampayo

Director de Informática Asociación Provincial de Pensionistas y Jubilados de A Coruña

Colegiado del CPEIG



## **52. EQUIPAMENTO HARDWARE. SERVIDORES. POSTO DE TRABALLO. DISPOSITIVOS PERSOAIS.**

## **Tema 52 Equipamento Hardware. Servidores. Posto de Trabalho. Dispositivos Persoais**

---

### **ÍNDICE**

<b>52.1.- Equipamento Hardware.....</b>	<b>2</b>
52.1.1 <i>Arquitecturas hardware.....</i>	<i>2</i>
52.1.2 <i>Compoñentes básicos hardware dun equipo.....</i>	<i>3</i>
52.1.3 <i>Clases de ordenadores.....</i>	<i>4</i>
<b>52.2.- Servidores.....</b>	<b>4</b>
52.2.1 <i>Características dun servidor.....</i>	<i>5</i>
52.2.2 <i>Clúster.....</i>	<i>6</i>
52.2.2.1 <i>Clases de clústeres.....</i>	<i>6</i>
52.2.2.2 <i>Compoñentes dun clúster.....</i>	<i>7</i>
52.2.3 <i>Servidores Blade.....</i>	<i>8</i>
<b>52.3.- Posto de traballo.....</b>	<b>9</b>
<b>52.4.- Dispositivos persoais.....</b>	<b>10</b>
52.4.1 <i>PDA .....</i>	<i>10</i>
52.4.2 <i>TABLET .....</i>	<i>11</i>
52.4.3 <i>Smartphones.....</i>	<i>11</i>
<b>52.5.- Bibliografía.....</b>	<b>13</b>

## **52.1.- EQUIPAMENTO HARDWARE**

### **52.1.1 Arquitecturas hardware**

O ordenador pódese ver como un dispositivo electrónico destinado ao tratamento automatizado da información. Para que un ordenador trate a información é necesario un sistema de información que, ante unha entrada, execute unha serie de instrucións e devolva un resultado.

Unha arquitectura de ordenador consiste no deseño, estudo da estrutura e funcionamento dun ordenador. Especifica as interrelacións que deben existir entre os compoñentes e elementos físicos e lóxicos.

#### **Modelos de arquitecturas de ordenadores:**

##### **Arquitectura Von Newman:**

Consiste nunha unidade central de proceso que se comunica a través dun só bus cun banco de memoria onde se almacenan tanto as instrucións do programa como os datos que serán procesados por este. Esta arquitectura é a máis empregada na actualidade.

Na memoria almacénanse tanto os datos como as instrucións que forman o programa, de tal maneira que o cambio dun programa a outro só implica un cambio no valor de posicións de memoria.

Na arquitectura de Von Newman prodúcese na CPU unha certa ralentización debido a que tanto as instrucións como os datos deben pasar da memoria á CPU por unha canle (bus). Este efecto coñécese como "o atasco de Von Newmann". Isto limita o grao de paralelismo (accións que se poden realizar ao mesmo tempo) e, xa que logo, o desempeño da computadora.

Nesta arquitectura asígnaselle un código numérico a cada instrución. Estes códigos almacénanse na mesma unidade de memoria que os datos que se van procesar para seren executados na orde en que se atopan



almacenados en memoria. Isto permite cambiar rapidamente a aplicación da computadora e deu orixe ás computadoras de propósito xeral.

### **Arquitectura Harvard**

Esta arquitectura xurdiu na universidade do mesmo nome, pouco despois que a arquitectura Von Newman. Do mesmo xeito que na arquitectura Von Newman, o programa almacénase como un código numérico na memoria, pero non no mesmo espazo de memoria nin no mesmo formato que os datos. Por exemplo, pódense almacenar as instrucións en doce bits na memoria de programa, namentres os datos se almacenan en 8 bits nunha memoria á parte.

O feito de ter un bus separado para o programa e outro para os datos permite que se lea o código de operación dunha instrución, ao mesmo tempo que se len da memoria de datos os operandos da instrución previa. Así evítase o problema do atasco de Von Newman e obtense máis rendemento.

A complexidade desta arquitectura só compensa cando o fluxo de instrucións e de datos é máis ou menos o mesmo. Por iso **non** é demasiado utilizada en ordenadores de propósito xeral. Non obstante, si se utiliza nalgúns casos para construír procesadores de sinal (DSP).

### **Arquitecturas segmentadas**

Buscan mellorar o rendemento realizando paralelamente varias etapas do ciclo de instrución ao mesmo tempo. O procesador divídese en varias unidades funcionais independentes e repártense entre elas o procesamento das instrucións.

Se un procesador ten un ciclo de instrución sinxelo, consistente soamente nunha etapa de busca do código de instrución e noutra etapa de execución da instrución, nun procesador sen segmentación as dúas etapas realizaríanse de maneira secuencial para cada unha das instrucións; pola contra, nun procesador con segmentación, cada unha destas etapas se asigna a unha unidade funcional diferente, a busca á unidade de busca e a

execución á unidade de execución. Estas unidades poden traballar de forma paralela en instrucións diferentes. Estas unidades comunícanse por medio dunha cola de instrucións na que a unidade de busca coloca os códigos de instrución que leu para que a unidade de execución os tome da cola e os execute.

A mellora no rendemento non é proporcional ao número de segmentos debido a que cada etapa non emprega o mesmo tempo en realizarse, ademais de que se pode presentar competencia polo uso dalgúns recursos como a memoria principal. Outra razón pola que as vantaxes deste esquema se perden é cando se encontra un salto no programa e todas as instrucións que xa se buscaron e se atopan na cola deben descartarse e hai que empezar a buscar as instrucións desde cero a partir da dirección á que se saltou. Isto reduce o desempeño do procesador e aínda se investigan maneiras de predicir os saltos para evitar este problema.

### **Arquitectura multiprocesamento**

Cando se desexa incrementar o rendemento é necesario utilizar máis dun procesador para a execución do programa.

Para facer unha clasificación deste tipo de arquitecturas utilízase a taxonomía de Flynn, que se basea no número de instrucións concorrentes e nos fluxos de datos sobre os que operar:

- *SISD (Simple Instruction Simple Data)*. Ordenador secuencial que non explota o paralelismo nin nas instrucións nin nos fluxos de datos; por exemplo, as máquinas con monoprocesador.
- *MISD (Multiple Instruction Simple Data)*. Pouco común debido a que a efectividade dos múltiples fluxos de instrucións adoita precisar de múltiples fluxos de datos. Utilízanse en situacións de paralelismo redundante; por exemplo, en navegación aérea.
- *SIMD (Simple Instruction Multiple Data)*. Un ordenador que explota varios fluxos de datos dentro dun único fluxo de instrucións para

realizar operacións que poden ser paralelizadas de forma natural. Nesta clasificación entrarían os Procesadores matriciais e os Procesadores vectoriais (aplican un mesmo algoritmo numérico a unha serie de datos matriciais).

- MIMD (Multiple Instruction Multiple Data). Téñense múltiples procesadores que, de forma sincronizada, executan instrucións sobre diferentes datos. O tipo de memoria que estes sistemas utilizan é distribuída. Nesta arquitectura engópanse os sistemas distribuídos, distinguindo aqueles que explotan un único espazo compartido de memoria (Procesadores superescalares, Multiprocesador simétrico [SMP] e Acceso non uniforme a memoria [NUMA]) daqueles que traballan con espazos de memoria distribuída, como os Clústers.
  - o Nos sistemas SMP (*Simetric Multiprocessors*), varios procesadores comparten a mesma memoria principal e periféricos de E/S, normalmente conectados por un bus común. Coñécense como simétricos, xa que ningún procesador toma o papel de mestre e os demais de escravos, senón que todos teñen dereitos similares en canto ao acceso á memoria e periféricos e ambos son administrados polo sistema operativo.
  - o Os Clústers son conxuntos de computadoras independentes conectadas nunha rede de área local ou por un bus de interconexión e que traballan cooperativamente para resolver un problema. É clave no seu funcionamento contar cun sistema operativo e programas de aplicación capaces de distribuír o traballo entre as computadoras da rede.

### **52.1.2 Compoñentes básicos hardware dun equipo**

As partes físicas (hardware) que compoñen un ordenador pódense esquematizar nas seguintes:

1. **PROCESADOR** tamén coñecido como **CPU** (*Central Process Unit*). Encárgase de interpretar e executar as instrucións dos programas, realizando cálculos aritméticos e lóxicos cos datos. Tamén é o encargado de comunicarse coas demais partes do sistema.

Internamente está constituído por unha colección complexa de circuítos electrónicos. Cando se incorporan todos estes circuítos nun chip de silicio, a este chip denomínaselle microprocesador.

A CPU está composta pola unidade aritmética lóxica, a unidade de control e os rexistros do sistema:

- a. Unidade de Control (UC): A función da unidade de control consiste en ler as instrucións que residen na memoria principal, interpretalas e executalas dándolle as oportunas ordes á unidade aritmético-lóxica e aos restantes elementos do sistema.
- b. Unidade Aritmético-Lóxica (ALU): Executa as operacións aritméticas lóxicas que lle sinala a instrución residente na unidade de control.
- c. Rexistros do sistema: Son circuítos que serven como área interna de traballo. Almacenan unha palabra de bits. Estes circuítos son moi rápidos e forman parte do propio procesador.

Hai que facer mención especial dos **microprocesadores multinúcleo**, que combinan dous ou máis procesadores independentes nun só circuítro integrado. Un dispositivo de dobre núcleo contén soamente dous microprocesadores independentes. En xeral, os microprocesadores multinúcleo permiten que un dispositivo computacional exhiba unha certa forma do paralelismo a nivel de subproceso, tamén chamado fío ou *thread* (*thread-level parallelism* - TLP) sen incluír múltiples microprocesadores en paquetes físicos separados. Esta forma de TLP coñécese a miúdo como multiprocesamento a nivel de chip (*chip-level multiprocessing*) ou CMP.

2. **MEMORIA PRINCIPAL.** Lugar onde se almacenan os datos e as instrucións dos programas en execución; pódense recuperar e gravar nela datos a través das dúas operacións básicas definidas sobre ela: lectura ou escritura.

Está constituída por celas ou elementos capaces de almacenar 1 bit de información. A memoria organízase en conxuntos de elementos dun tamaño determinado chamados *palabras de memoria*. A cada palabra correspóndelle un enderezo único.

Cada palabra é unha unidade direccionable na memoria. O mapa de memoria correspóndese co espazo de memoria direccionable. Este espazo vén determinado polo tamaño dos enderezos.

3. **BUSES.** Para funcionar o hardware necesita unhas conexións que lles permitan aos compoñentes comunicárense entre si e interaccionar. Estas conexións denomínanse buses ou canles. Un bus constitúe un sistema común interconectado que coordina e transporta información entre as partes do ordenador.

Un bus caracterízase por dúas propiedades:

- A cantidade de información que pode manipular simultaneamente, chamada “ancho de bus”.
- A rapidez con que pode transferir os devanditos datos.

Existen tres tipos de buses nun ordenador, en función do tipo de datos que transporten:

- *Bus de Control:* Encárgase de transmitir datos que serán utilizados como ordes de control.
- *Bus de Enderezos:* Encárgase de transmitir datos que serán utilizados como enderezos de memoria.
- *Bus de Datos:* Encárgase de transportar datos coma tales.

O conxunto destes tres buses forma o **Bus do Sistema**.

4. **PERIFÉRICOS.** Unha das funcións básicas do ordenador é enviar e recibir datos desde dispositivos externos á CPU. Estes dispositivos coñécense co nome xenérico de periféricos, podendo ser de lectura, de escritura e de lectura e escritura.

Os periféricos teñen como *handicap* a diferenza entre as súas velocidades de transmisión e a velocidade de operación do ordenador. Os periféricos clasifícanse segundo a súa función en:

- *Dispositivos periféricos de entrada.* Introducen datos e instrucións na CPU; por exemplo: un rato, un teclado.
- *Dispositivos periféricos de saída.* Permiten ver os resultados; por exemplo: un monitor, unha impresora.
- *Dispositivos periféricos de ENTRADA/SAÍDA (E/S).* Teñen comunicación bidireccional coa CPU; por exemplo, un dispositivo de almacenamento.

### **52.1.3 Clases de ordenadores**

A raíz da evolución da tecnoloxía, pódese facer unha clasificación non rixida dos diferentes tipos de ordenadores existentes:

- *Superordenadores:* deseñados especialmente para cálculos que precisen unha gran velocidade de proceso. Normalmente están constituídos por un gran número de procesadores que traballan en paralelo, conseguindo realizar así billóns de operacións por segundo.
- *Mainframe:* están deseñados principalmente para darlles servizo a grandes organizacións. A súa potencia de cálculo é inferior aos anteriores, cifrándose a execución en millóns de operacións por segundo. Caracterízanse por soportar a conexión dun gran número de terminais. Poden intervir en procesos distribuídos nos que se conectan dous ou máis ordenadores en paralelo.

- *Miniordenadores*: son máquinas de tipo medio, é dicir, a súa capacidade de proceso é inferior ás anteriores e, daquela, poden controlar un número menor de terminais.
- *Microordenadores*: o seu funcionamento baséase no uso dun microprocesador. Proporcionan unha serie de prestacións que, en potencia, manexabilidade, portabilidade, prezo, etc., abarcan unha gama inferior de necesidades informáticas, tanto no ámbito profesional coma no privado. Podemos identificar dous grupos importantes: os ordenadores persoais (*Persoal Computer PC*) e as estacións de traballo (*Workstation*).

## **52.2.- SERVIDORES**

Como se observa no apartado anterior, na clasificación dos ordenadores non aparece o termo 'servidor'. Este termo nace orixinalmente no mundo software debido á arquitectura cliente/servidor, na que uns programas denominados *clientes* realizan peticións a outros programas denominados *servidores*, os cales atenden as tales peticións realizando as accións necesarias.

- Un **servidor** defínese entón como un programa que acepta conexións con obxecto de atender peticións mediante o envío de respostas.
- Un **cliente** defínese como un programa que establece conexións co propósito de realizar peticións.

Este uso dual pode levar a confusión. Por exemplo, no caso dun servidor web, este termo poderíase referir á máquina que almacena e manexa os sitios web, e neste sentido é utilizada polas compañías que ofrecen *hosting* ou hospedaxe. Alternativamente, o servidor web poderíase referir ao software, como o servidor de http de Apache, que funciona na máquina e

manexa a entrega das páxinas web como resposta a peticións dos navegadores dos clientes.

Debido á especialización e criticidade de moitos tipos de servidores, o termo ‘servidor’ utilízase para se referir ao ordenador (hardware) onde está instalado o programa que atende as peticións.

Así, un servidor, no ámbito profesional, é un ordenador especificamente deseñado para optimizar a execución dun determinado programa servidor ou dun conxunto deles.

Loxicamente este hardware específico precisa dun sistema operativo (SO) personalizado para executar programas servidores, sendo habitual que as compañías proporcionen SO para usuario final (Windows 7, Ubuntu Desktop ) e SO para servidores (Windows 2008 Server R2, Ubuntu Server...).

### **52.2.1 Características dun servidor**

Existen factores como a fiabilidade, o rendemento ou o custo que determinan o tipo de servidor (hardware) que se require para albergar un software servidor. Así, pódese ter nun mesmo servidor hardware varios programas servidores, ou ben pódese ter un servidor hardware por cada programa servidor.

Desde este punto de vista, calquera ordenador que albergue un determinado software servidor podería ser considerado un servidor. Non obstante, as máquinas que se deseñan co propósito de albergaren programas servidores teñen unha serie de características particulares que fan necesario empregar hardware especializado, orientado a unha alta fiabilidade e rendemento.

- Teñen que procesar numerosas peticións de clientes nun tempo curto, por iso necesitan CPU con velocidades altas de procesamento. Se, por características da aplicación, se require unha gran cantidade de procesamento, é máis recomendable engadir máis CPU para traballar



en paralelo que aumentar a velocidade dunha única CPU, por cuestións de redundancia e fiabilidade.

- Se o servidor recibe peticións concorrentemente é necesario que conte cunha cantidade de memoria principal ou RAM elevada que lle permita abrir *threads* e atender de forma adecuada os clientes.
- Os buses polos que circula a información dentro do servidor teñen que ser de alto rendemento para non provocar atascos.
- Algúns tipos de servidores (ficheiros e bases de datos sobre todo) necesitan unha tecnoloxía de almacenamento altamente eficiente, e é normal encontrar dous tipos de tecnoloxías distintas:
  - o SAN (*Storage Area Network*). É unha rede especializada que permite un acceso rápido e fiable entre servidores e recursos de almacenamento independentes ou externos. Desta forma un dispositivo de almacenamento non é propiedade exclusiva dun servidor, senón que os dispositivos de almacenamento son compartidos entre todos os servidores da rede como recursos individuais. Esta arquitectura esixe dispoñer dunha infraestrutura de rede de alta velocidade dedicada só para Almacenamento e Backup, optimizada para mover grandes cantidades de datos e consistente en múltiples recursos de almacenamento xeograficamente distribuídos.
  - o NAS (*Network Attached Storage*). Os dispositivos NAS son dispositivos de almacenamento aos que se accede a través de protocolos de rede.

Os dispositivos NAS utilizan usualmente máis dun dispositivo de almacenamento, na maioría dos casos están compostos por RAID (*Redundant Arrays of Independent Disks*) de discos, o que aumenta a capacidade de almacenamento, a seguridade e a velocidade de acceso á información.

- Os servidores están preparados para ofrecer servizos cun grao de dispoñibilidade de máis do 99%. Isto implica:
  - o Que está acendido as 24 horas do día, polo que é necesario un sistema de refrixeración adecuado. Por esta razón sitúanse en Centros de Procesos de Datos onde existe a temperatura e humidade óptimas de funcionamento.
  - o Que teñen que contar con Sistemas de Alimentación Ininterrompida para evitar que un corte eléctrico os deixe indispoñibles.
  - o Que é necesario utilizar compoñentes **hot swap**, que son compoñentes que se poden substituír “en quente sen parar o servidor”. Isto ten especial importancia con servidores críticos que non poden estar parados por unha acción planificada. Os compoñentes **hot swap** máis comúns son:
    - Os discos duros configurados en RAID.
    - As fontes de alimentación.
- Os servidores poden estar situados en armarios RACK ou non. A configuración de servidores en RACK é modular, permitindo agregar ou quitar compoñentes con máis facilidade (engadir unha cabina de fitas de backup, unha nova fonte de alimentación ou un novo servidor ).

### **52.2.2 Clúster**

Un clúster é un tipo de ordenador distribuído ou paralelo que consiste nun grupo de ordenadoras interconectadas que traballan conxuntamente na solución dun problema. Estes sistemas constitúen unha solución flexible, de baixo custo e de gran escalabilidade para aplicacións que requiren unha elevada capacidade de cómputo e memoria.

A tecnoloxía de clústeres evolucionou en apoio de actividades que van desde aplicacións de supercómputo e software de misións críticas, servidores Web e comercio electrónico, ata bases de datos de alto rendemento, entre outros usos.

Os clústeres ofrecen as seguintes características:

- *Alto rendemento*: deseñados para dar altas prestacións en canto a capacidade de cálculo e velocidade de proceso.
- *Alta dispoñibilidade*: deseñados para garantir a total e absoluta dispoñibilidade do servizo no tempo ofrecendo un funcionamento ininterrompido. Todas as máquinas deste clúster están sincronizadas e monitorizadas entre si. Se se produce un fallo nalguna das máquinas do clúster, detéctase devandito fallo automaticamente y as outras máquinas asumen as funcións e seguen funcionando mantendo así a dispoñibilidade do sistema o software. Son tolerantes a fallos.
- *Abalo de carga*: Un clúster estará composto por un ou máis nodos que actúan como *frontend* do clúster, e que se ocupan de repartir as peticións de servizo que reciba o clúster a outros ordenadores do clúster que forman o *backend* de éste, evitando así os atascos.
- *Escalabilidade*: É relativamente alcanzable aumentar un nodo nun sistema cluster.

Un clúster de servidores ten principalmente dúas vantaxes considerables sobre as solucións de servidores estándar:

- Garanten a alta dispoñibilidade de servizos e datos.
- Permite aproveitar ao 100% a capacidade dos nodos introducidos (non hai nodos en caseta-by).

#### 52.2.2.1 Clases de clústeres

A forma en que operará o clúster está determinada pola función que éste deberá desempeñar:

- Clúster de Alto Rendemento: diseñado para dar altas prestacións en canto a capacidade de cálculo. Existen distintas aplicacións que se lles pode dar a este tipo de clúster, entre as cales atopamos: cálculos matemáticos, renderizacións de gráficos, compilación de programas, descifrado de códigos.
- Clúster de Alta Dispoñibilidade: están diseñados para garantir o funcionamento ininterrompido de certas aplicacións. A idea principal deste tipo de clúster é proporcionar un servizo ininterrompido as 24 horas do día, os 7 días da semana.

Están formados por un conxunto de dous ou máis máquinas que comparten os discos de almacenamento de datos, e se monitorizan mutuamente. Se se produce un fallo do hardware ou das aplicacións dalgunha das máquinas do clúster, o software de Alta Dispoñibilidade é capaz de rearrancar automaticamente os servizos que fallaron en calquera das outras máquinas del clúster. E cando a máquina que fallou recupérase, os servizos son novamente migrados á máquina orixinal.

- Clúster de Alta Eficiencia: Son clústeres cuxo obxectivo de deseño é o executar a maior cantidade de tarefas no menor tempo posible. Existe independencia de datos entre as tarefas individuais.

Os clúster de alta eficiencia e alta dispoñibilidade adoitan utilizarse para contornas empresariais e esta funcionalidade soamente pode ser efectuada por hardware especializado, mentres que os clúster de alto rendemento son propios de universidades e centros de cálculo.

#### 52.2.2.2 Compoñentes dun clúster

Para que un clúster funcione como tal, non basta sóo con conectar entre si os ordenadores, senón que é necesario proveelos dun sistema de manexo do

clúster, o cal encárguese de interactuar co usuario e os procesos que corren en él para optimizar o funcionamento. É dicir que, para poder funcionar, require tantos compoñentes hardware como software.

- **Nodos.** Son os ordenadores en sí mesmos, existindo ordenadores persoais, sistemas multi-procesador ou estacións de traballo (workstations). Poden ser:
  - o *Dedicados:* o seu uso está exclusivamente dedicado a realizar tarefas relacionadas co clúster.
  - o *Non dedicados:* o seu uso non está exclusivamente dedicado a realizar tarefas relacionadas co clúster, utilizándose os ciclos de reloxo do ordenador cando éste non se utiliza.
- **Almacenamento.** Pode consistir nunha NAS, unha SAN, ou almacenamento interno no servidor. O protocolo máis comúnmente utilizado é NFS (Network File System), sistema de ficheiros compartido entre servidor e os nodos. Con todo existen sistemas de ficheiros específicos para clústeres como Lustre (CFS) e PVFS2.
- **Rede de interconexión.** Utilízanse Redes de Alta Velocidade como solución de alto rendemento para que as comunicacións non sexan o atasco do rendemento do sistema.

As redes de interconexión son un compoñente fundamental dos clústeres que proporcionan: alto ancho de banda, baixa latencia, fiabilidade e escalabilidade.

As redes de interconexión comúns en clúster son:

- o Ethernet: Estándar de redes de ordenadoras de área local con acceso ao medio por contenda CSMA/CD.
- o Fast Ethernet: Serie de estándares de IEEE de redes Ethernet de 100 Mbps (megabits por segundo).

- o Gigabit Ethernet: Ampliación do estándar Ethernet que consegue unha capacidade de transmisión de 1 gigabit por segundo.
  - o SCI (Scalable Coherent Interface): Estándar de interconexión de redes de alta velocidade utilizado para multi-procesamiento con memoria compartida e paso de mensaxes.
  - o ATM (Asynchronous Transfer Mode): Tecnología de telecomunicación desenvolvida para facer fronte á gran demanda de capacidade de transmisión para servizos e aplicacións.
  - o Myrinet: Rede de interconexión de clústeres de altas prestacións. O procesamiento das comunicacións de rede faise a través de chips integrados nos cartóns de rede de Myrinet (Lanai chips), descargando á CPU de gran parte do procesamiento das comunicacións.
  - o HIPPI (High Performance Parallel Interface): Bus para conexións de alta velocidade para dispositivos de almacenamento en superordenadores. foi substituído progresivamente por outras tecnoloxías máis rápidas.
  - o FiberChannel: Tecnología de rede utilizada principalmente para redes de almacenamento, dispoñible primeiro á velocidade de 1 Gbps e posteriormente a 2, 4 e 8 Gbps.
  - o Infiniband: É unha rede xurdida dun estándar desenvolvido especificamente para realizar a comunicación en clústeres. A conexión básica é de 2Gbps efectivos e se poderían alcanzar os 96Gbps.
- **Sistema Operativo.** Ten que ser multiproceso e multiusuario.
  - **Middleware.** Actúa entre o sistema operativo e as aplicacións, recibindo os traballos entrantes ao clúster e redistribuíndolos de

maneira que o proceso se execute máis rápido e o sistema non sufra sobrecargas nun servidor determinado. Está composto de dous subniveles de software:

- o *SSI (Single System Image)*: ofrece aos usuarios un acceso unificado a todos os recursos do sistema.
- o *Dispoñibilidade do sistema*: que permite servizos como puntos de recoñecemento, recuperación de fallos, soporte para tolerancia a fallos.

### **52.2.3 Servidores Blade**

Blade Server é unha arquitectura que conseguiu integrar en cartóns todos os elementos típicos dun servidor. Cada servidor blade é un cartón (chamada *blades*) que contén a memoria RAM, o disco duro e a CPU. Os servidores blade en cartóns insérense nun chasis que se coloca nun rack estándar ocupando entre 4Ou e 6Ou dentro do rack, permitindo albergar un máximo de 16 servidores blade nun chasis. Este chasis, á súa vez integra e permite compartir os elementos comúns como son:

- A ventilación e a refrigeración.
- Os switches de rede redundante co cableado.
- As fonte de alimentación e o SAI tipo hot swap.
- Interfaces de almacenamento.

Ao estar todo integrado no chasis conséguese reducir o consumo eléctrico, cableado, sistemas de arrefriado e o espazo dentro do rack.

As empresas que requiren da actualización dos seus sistemas enfróntanse ao problema de consumo eléctrico, espazo, control de temperatura e ubicación dos novos equipos. Tradicionalmente, ata a chegada dos servidores Blade, o método para incrementar novos requirimentos era agregar máis servidores en rack, o que ocupa máis espazo, complica o

cableado, fai más complexa a gestión de administración dos sistemas, consome máis recursos, etc.

A tecnoloxía blade supón un deseño máis eficiente en canto a custo e espazo. Para iso reduciuse o chasis, baixouse o consumo, simplificado o cableado e o mantemento, mentres se incrementan as funcionalidades.

Estes son os principios básicos nos que se fundamenta a arquitectura blade e que ao final proporciona unha redución do custo total.

### **Diferenzas entre un sistema de servidores montados en rack e blade server**

A principal diferenza é que nun sistema montado en rack, o servidor é unha unidade completa en si mesmo. Isto significa que contén a CPU, memoria, fonte de alimentación, ventiladores e disipadeores. Estes servidores son atornillados no rack, e cada un é conectado á rede corporativa usando un cable separado.

Os blade servers son unha versión compacta de sistemas montados en rack. O blade inclúe unha CPU, memoria e dispositivos para almacenar datos. Pero non ten fonte de alimentación eléctrica nin ventiladores. Os blades son inseridos en slots e enlazados entre si grazas a un bus de alta velocidade dentro do chasis.

### **Vantaxes**

- Reduce a gestión grazas á súa infraestrutura simplificada.
- Comparte fontes de alimentación e ventiladores e unha gestión do sistema centralizada diminuindo custos porque requiren menos electrónica e consomen menos enerxía.
- O chasis elimina a maioría de o cableado que se atopa nos sistemas montados en rack.



- Intercambio en quente (Hot-Swap): se un blade falla pode ser substituído sen ningún impacto nos outros blades.
- Facilitan a gestión e reducen tempo e custo administrativo ao estar todos os servidores nun só equipo.
- Redúcese o espazo ao integrar nun só chasis moitos servidores, sen reducir poder de cómputo.
- Escalabilidade horizontal: porque nos ofrece ampliar o número de servidores facilmente a medida que vai crescendo a demanda.
- Alta dispoñibilidade, pois a maioría de os equipos posúen elementos redundantes que garanten o funcionamento continuado dos servidores sen interrupcións.

### **52.3.- POSTO DE TRABAJO**

Omá s habitual en calquera empresa é que no posto de traballo exista un microordenador, é dicir, ou ben un PC ou unha estación de traballo (en inglés workstation). O concepto de PC ou ordenador persoal é amplamente aceptado.

Unha Workstation é un microordenador de altas prestacións especialmente deseñado para niveis de alto rendemento en certas tarefas, como poden ser, deseño gráfico, edición de vídeo, gestión de redes de Internet, aplicacións de alto consumo, etc. Estes potentes ordenadores atoparon o seu sitio na ingeniería e desenvolvemento de software entre outras cousas, debido á súa habilidade multitarea.

Na actualidade os PCs son bastantes potentes en canto a memoria e capacidade de procesamento. Con todo, o hardware das estacións de traballo está optimizado para situacións que requiren un alto rendemento e fiabilidade, moita cantidade de memoria, computación de multitarea, etc.

onde xeralmente se manteñen operativas en situacións nas cales calquera ordenadora persoal tradicional dejaría rápidamente de responder.

Os profesionais cando escoitan a palabra estación de traballo, pensan que é unha máquina que non necesitan e que ten un custo moi superior ás expectativas. A realidade é que iso cambiou, especialmente en todo o relativo ao factor prezo, e agora, cunha inversión mínima, un profesional pode, grazas a unha estación de traballo, obter ata un 50 por cento máis de rendemento nas súas tarefas diarias.

Existen profesionais que compran un PC potente, con máis de 2 GB de memoria, cun cartón gráfica de alto nivel, con alta capacidade de memoria interna, etc. porque necesitan traballar con aplicacións de software. Fano porque non coñecen a existencia das estacións de traballo pero, sobre todo, porque non saben as diferenzas que teñen cun PC e as funcionalidades e vantaxes que poden ofrecerlle. Un PC, por exemplo, no apartado de memoria, chega ata onde chega e aí xorden os problemas. Existen estacións de traballo que pode alcanzar os 128 GB de memoria, cinco discos duros, biprocesadores, etc.

As principais aplicacións dunha Workstation son:

- CAD (Computer Aided Design, Diseñou Asistido por Ordenador): destinadas ao deseño e análise de sistemas de ingeniería e arquitectura.
- AEC (Architecture Engineering Construction): aplicables á edición de planos de construción e arquitectura, elaboración de orzamentos e seguimentos de obras.
- CAM (Computer Aided Manufacturing): aplicables no deseño, análise e proba de circuitos integrados, cartóns e outros sistemas electrónicos.

- CASE (Computer Aided Software Engineering): axuda á gestión completa de os ciclos de vida dos desenvolvementos de aplicacións lógicas.
- GIS (Geographic Information System): para edición, captura e análise de información sobre determinadas zonas geográficas, con base en referencias de mapas dixitalizados.
- Sistemas expertos: basados en técnicas de programación de intelixencia artificial, para aplicacións talles como detección electrónica de erros, funcións de diagnóstico ou configuración de ordenadores.
- Aplicacións empresariais: investigación cuantitativa, seguridade, simulación de análise reais...
- Edición electrónica: creación para o seu posterior publicación de periódicos, revistas, presentacións e documentación en xeral.
- Telecomunicacións: gestión de redes, desenvolvemento de aplicacións de telecomunicacións baseadas en intelixencia artificial, aplicacións de apoio á investigación e desenvolvemento (I+D), edición electrónica e procesado de imáxenes.
- As estacións de traballo tamén poden ser utilizadas como pasarelas (gateways), para acceder a grandes ordenadores, e para executar remotamente utilizando protocolos de comunicacións.

## **52.4.- DISPOSITIVOS PERSOAIS**

### **52.4.1 PDA**

Unha PDA (Persoal Dixital Assistant) é un ordenador de peto deseñado como unha axenda electrónica, pero que actualmente posúen unha potencia razoable e son capaces de realizar numerosas funcións máis alá das de

mera axenda electrónica constituyéndose como unha extensión mesma do ordenador persoal, que poderemos sincronizar con éste.

Outros términos asociados son palmtop e handhelds. Un palmtop é un ordenador pequeno que literalmente colle na palma da man. Un handheld é un ordenador sumamente pequeno que se pode soste coa man.

Os términos PDA, palmtop e handhelds xurdiron para cubrir necesidades diferentes. Actualmente a división entre ambas é moi difusa; ambos os términos utilízanse indistintamente.

As tecnoloxías de comunicacións inalámbricas (Bluetooth, Wi-Fi, IrDA (infravermellos), GPS...) permiten que cunha PDA pódase consultar o correo electrónico, usalos como navegador GPS ou para temas relativos á domótica.

Pero máis alá das funcións e software coas que vén equipado a PDA, o que o fai verdadeiramente potente é a posibilidade de personalización case ilimitada ao permitir cargar as aplicacións “baixo demandá”.

### **Características:**

- Teñen un tamaño físico moi reducido para que caiba na man.
- Son bastantes lixeiros para que sexa fácil o seu transporte nun peto.
- A pantalla é táctil ocupando gran parte do dispositivo e deixando pouco espazo para situar botón hardware. Non adoitan dispor dun teclado con botóns (salvo algúns dispositivos) polo que para agregar texto utilízase un teclado virtual ou se lle añade un teclado externo por USB.
- Teñen capacidade multimedia, xa que integran altofalante, micrófono e grabadora de voz.
- Dispón de conexión de periféricos: para dispositivos de almacenamento externo e para módulos de expansión.

- Amplo soporte de conexións inalámbricas: Bluetooth, infravermellos, Wi-fi.
- Funcionamento con baterías de Litio-ion.
- Capacidade de almacenamento por encima dos 64 MB que se pode ampliar mediante o uso de cartóns de memoria Flash.
- A sincronización cos ordenadores persoais permite a actualización do directorio, facendo que a información do ordenador e da PDA sexa a mesma. A sincronización tamén evita a perda da información almacenada no caso de que o accesorio pérdase, sexa roubado ou destruído.
- Utilizan sistemas operativos específicos como son Windows Mobile, HP webOS, Linux.

#### **Limitacións:**

- Potencia de computación reducida, debido a que os microprocesadores teñen que ter en conta a duración das baterías, o sobrecalentamento, etc.
- Capacidade de almacenamento, aínda que hoxe en día con cartóns de memoria de varios GB é unha limitación menor.
- Baixa duración das baterías.
- Comunicacións.
- Software específico.

#### **52.4.2 TABLET**

O Tablet é un ordenador portátil de tamaño reducido, con pantalla sobre a cal o usuario pode escribir usando un lápiz especial (o stylus). O texto manuscrito é dixitalizado mediante recoñecemento de escritura. O lápiz

también utilízase para moverse dentro do sistema e utilizar as ferramentas e funcións das Tablet

O Tablet combina a potencia dun ordenador portátil coa comodidade dun PDA.

En función de se dispoñen ou non de teclado distínguense:

- Tablet “Slate”: non dispón de teclado e é necesario utilizar un lápiz ou os dedos para manipulalo.
- Tablet “Convertible”: posúe un teclado. Pode ser deslizable para poder deslizarse debaixo da pantalla ou de modo que a pantalla poida virar.

### **Características:**

- Os microprocesadores empregados nestes dispositivos están baseados en solucións para móbil.
- Para o almacenamento adóitanse utilizar discos EIDE convencionais pero de 2,5” (máis finos).
- A memoria que adoitan utilizar é SODIMM (small online DIMM), especiais para laptop e impresoras.
- Pantalla táctil.
- Novas formas de control mediante voz e escritura manual.

### **52.4.3 Smartphones**

Estes dispositivos fan as funcións dun teléfono móbil convencional, pero están dotados dunha maior versatilidade, xa que tamén inclúen algunhas das funcións dun ordenador persoal. Na actualidade todos eles teñen en común un conxunto amplo de características, como unha pantalla táctil de gran formato, conectividade WiFi, Bluetooth, 3G... No entanto, existen outros importantes parámetros que convén ter en consideración:

### **Pantalla**

É un compoñente de extrema importancia debido a que as pantallas táctiles dos smartphones son a interfaz directa de comunicación entre o usuario e o propio dispositivo.

Existen dous tecnoloxías aplicables a estas superficies táctiles:

- As capacitivas: é a máis adecuada para facilitar a interacción directa co dedo en lugar dos habituais stylus, xa que para que respondan ao instanbástache con deslízalo, polo que o usuario non necesita exercer ningún tipo de presión sobre a superficie. Además, poden detectar varias pulsacións de xeito simultánea, polo que a experiencia para o usuario é máis atractiva que no caso das resistivas.
- As resistivas: están formadas por varias capas, polo que cando as presionamos entran en contacto. Isto produce un cambio de corrente, facilitando, deste xeito, a detección da pulsación. Por esta razón, a experiencia de usuario neste caso parece ser menos atractiva que no anterior, xa que a resposta do dispositivo é algomá s lenta, ou polo menos é a sensación que pode brindarnos.

### **Sistema operativo**

O funcionamento dun S.O. afecta directamente ao rendemento do dispositivo, a usabilidade da súa interfaz e as funcionalidades que pon a disposición dos usuarios.

Actualmente o S.O. que se implanta nun Smartphone adoptou tanta transcendencia como o equipo mesmo. A tal punto que se fala, de **“Smartphones Android”**, para referirse a teefinosfonos que funcionan a través deste desenvolvemento de Google . Polo tanto, a elección do sistema é case tan importante como a dun smartphone en si. Hai que ter en conta que además estes S.O. tamén utilízanse nos tablets, por exemplo o iOS de Apple atópase no seu smartphone iPhone e no seu tablet iPad, o HP webOS implantar nos smartphones Palmpre e no seu tablet TouchPad, etc. A continuación expónse os S.O. máis relevantes no mercado:

- **HP webOS** é un sistema operativo multitarea baseado en Linux, desenvolvido por Palm, Inc., agora propiedade de Hewlett-Packard Company. Cabe destacar que usa tecnoloxías web como HTML5, JavaScript e CSS e soporta Flash.

webOS inclúe unha característica chamada "Synergy" que permite conectar o sistema con numerosos servizos de redes sociais e integrar información de varias fontes.

webOS fai uso do cloud computing para a sincronización de datos

- **Android.** é un sistema operativo multitarea baseado en Linux non sóo no seu núcleo, senón tamén no seu concepto: de código aberto e gratuíto. Isto significa que calquera fabricante que desexe poderá instalar Android nos seus equipos posibilitando que o sistema estea dispoñible nunha ampla gama de smartphones. Foi deseñado originalmente para dispositivos móbiles, talles como teefonos intelixentes, tablets, pero que actualmente se atopa en desenvolvemento para usarse en netbooks e PC.

O *Android Market* é un catálogo de aplicacións que poden ser descargadas e instaladas en dispositivos Androidsen a necesidade dun PC

- **BlackBerry ÉVOS un sistema operativo móbil desenvolvido por Research In Motion para os seus dispositivos BlackBerry. Ao comezo da súa andaina os BlackBerry estiveron orientados ao público corporativo, pero tras a aparición do iPhone abriuse ao uso persoal (do mesmo xeito que moitos smartphones). A interfaz máis cómoda para usar un BlackBerry é o teclado físico, que non é sóo un accesorio como noutros smartphones senón que é a chave para acceder a todas as funcionalidadees.**
- **Windows Phone** é un sistema operativo móbil desenvolvido por Microsoft, como sucesor da plataforma Windows Mobile. Está pensado



para o mercado de consumo xeneralista en lugar do mercado empresarial polo que carece de moitas funcionalidades que proporciona a versión anterior

O Hub Marketplace é o lugar no que se poden comprar e descargar todo tipo de contido como aplicacións, música, películas, programas de TV, podcast.

- **ios** é o sistema operativo móbil de Apple desenvolvido originalmente para o iPhone, sendo después usado no iPod Touch e iPad. Dise que é un XO que marca tendencias. Na última versión do XO (iOS 4) sopórtase a multitarea. Un dos aspectos máis criticados na súa falta de soporte para Flash.

A interfaz de usuario de iOS baséase en con o concepto de manipulación mediante xestos multitáctil. Os elementos da interfaz componse por deslizadores, interruptores e botóns. A resposta é inmediata e provece dunha interfaz fluída. A interacción con o sistema operativo realízase mediante xestos como deslizar, tocar e pellizca

O App Store de Apple é onde se poden comprar e descargar contidos. Foi pioneira nese aspecto.

A carga das aplicacións realízase case instantáneamente, brindando fluidez ao desempeñou xeneral do teeifono.

- Outros 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, Zvonkou Vranesic and Safwat Zaky. Organización de Ordenadores, 5ª edición. Ed. Mc Graw Hill, 2002.
- PCWORD Marzo 2010.

- <http://é.wikipedia.com>

**Autor:** Francisco Javier Rodríguez Martínez

Subdirector de Sistemas Escola Superior Enxeñaría Informática Ourense

Colexiado do CPEIG



# **53. CONCEPTO, EVOLUCIÓN E TENDENCIAS DOS SISTEMAS OPERATIVOS. SISTEMA OPERATIVO UNIX-LINUX. SISTEMA OPERATIVO WINDOWS.**

Tema 53. Concepto, evolución e tendencias dos sistemas operativos.  
Sistema operativo UNIX-LINUX. Sistema operativo Windows

---

## **ÍNDICE**

### **53.1.- Sistema Operativo**

- 53.1.1 Concepto*
- 53.1.2 Evolución dos Sistemas Operativos*
- 53.1.3 Clasificacións dos Sistemas Operativos*
- 53.1.4 Estrutura dos Sistemas Operativos*
- 53.1.5 Funcións dun Sistema Operativo*
- 53.1.6 Tendencias*

### **53.2.- Sistema Operativo UNIX-LINUX**

- 53.2.1 Características*
- 53.2.2 Arquitectura de Unix-Linux*
- 53.2.3 Xestión de procesos*
- 53.2.4 Xestión de memoria*
- 53.2.5 Xestión de E/S*
- 53.2.6 Xestión de arquivos*

### **53.3.- Sistema Operativo Windows**

- 53.3.1 Características*
- 53.3.2 Arquitectura de Windows*
- 53.3.3 Xestión de procesos*
- 53.3.4 Xestión de memoria*
- 53.3.5 Xestión de E/S*
- 53.3.6 Xestión de arquivos*
- 53.3.7 Seguridade*

### **53.4.- Bibliografía**

## **53.1.- SISTEMA OPERATIVO**

### **53.1.1 Concepto**

Pódese definir un sistema operativo (S.O.) como un conxunto de programas que controlan directamente os recursos hardware (HW) ou físicos dun ordenador (CPU, memoria principal e periféricos), proporcionando unha máquina virtual que oculta os detalles físicos da máquina e lles ofrece ás persoas un contorno máis amigable. O sistema operativo é a capa de software máis baixa dun computador. Cada capa ocúltalles ás capas superiores certos detalles das capas inferiores. Desta forma constrúese o software, baseándonos no que xa existe.

O sistema operativo ten unha serie de funcións, que se poden agrupar en 3:

1. Inicializar a máquina. Prepara a máquina para o funcionamento. Hai 2 formas de inicialización:

- a) TOTAL: Inicialización de todas as funcións e servizos que a máquina pode ofrecer. Por exemplo, MS-DOS ten inicialización total.
- b) PARCIALMENTE: Vaise ser selectivo cos tipos de servizos que se inician. Por exemplo, Linux e Windows.

A principal vantaxe/utilidade da inicialización parcial é a recuperación da máquina ante fallos: consiste en que se falla un servizo da máquina non fai falla apagar toda a máquina, só hai que lanzar de novo o servizo.

2. Servir de máquina virtual. Ocúltanse detalles de hardware proporcionando un contorno máis amigable. Isto ten 2 obxectivos:

- a) A SEGURIDADE: En lugar de que o usuario acceda directamente a un recurso HW, faino o S.O. para que non se produzan operacións non

desexadas, tamén chamadas operacións perigosas: operacións de entrada/saída (ES), operacións de acceso á memoria.

O HW ten dúas formas de actuar: modo supervisor e modo usuario.

Todos os programas actuarán en modo usuario ata o momento en que haxa que acceder ao HW; será daquela cando cambie a modo supervisor para evitar as operacións que poidan causar problemas. Xérase unha interrupción ao realizarse unha destas operacións susceptibles de fallo. Esa interrupción cóllea o sistema operativo e actúa en consecuencia. O sistema operativo tomará o control do hardware e realizará a operación que se lle indica.

Unha interrupción é un sinal físico que xeran os dispositivos do sistema e que a trata o sistema operativo.

Ao conxunto de interrupcións chámase **interface interna** do sistema operativo.

- b) **ABSTRACCIÓN**: Abstráense as características físicas e reais da máquina ofrecendo unha serie de servizos incluso maiores dos que pode ofrecer a propia máquina. Por exemplo, para traballar con ficheiros utilízanse nomes, pero o ordenador non utiliza eses nomes para se referir a eles; emprega un enderezo.

A E/S: cando tecleamos un dato vémosto en pantalla tal como o imaxinamos, aínda que realmente para a máquina son uns e ceros.

Isto constitúe a **interface externa** do S.O., a linguaxe coa que nos imos a comunicar con el. Denomínase SHELL.

Xa que logo, temos 2 tipos de interface:

- A externa: forma de comunicación entre nós e o ordenador; a través de comandos/ordes (abstracción).

- A interna: forma de comunicación do sistema operativo co hardware (modo supervisor).

3. Administrar os recursos para o seu funcionamento. Esta administración ten que cumprir 3 características:

- ten que ser CORRECTA: se hai 2 procesos que queren acceder a un recurso, haille que dar acceso primeiro a un e logo a outro, pero non mesturalos.
- ten que ser XUSTA: se temos 2 procesos hailles que dar saída aos dous; un proceso non pode monopolizalo todo.
- ten que ser EFICIENTE: para mellorar o rendemento do sistema.

Por último dicir que un S.O. ten que ter estas 2 características:

- DETERMINISMO: se se repite a mesma operación cos mesmos datos de entrada debemos obter os mesmos resultados.
- INDETERMINISMO: no sentido de que ten que responder oportunamente ás interrupcións, é dicir, non sabe qué interrupción vai chegar primeiro, non coñece a orde, pero debe saber tratalas.

### **53.1.2 Evolución dos Sistemas Operativos**

Os sistemas operativos evolucionaron en paralelo ao desenvolvemento do HW. Conforme o HW ía incorporando novas capacidades, os S.O. debían adaptarse para permitir xestionar eficientemente esas novas capacidades.

A evolución do S.O. pódese organizar en xeracións con algunhas características comúns:

#### **Primeira Xeración**

Vai desde 1945 a 1955. Caracterízase porque non existía un sistema operativo. Eran os propios deseñadores das máquinas os que as programaban a través de cableado e os que as manexaban.

#### **Segunda Xeración**

Desde 1955 a 1965. No campo do hardware aparece o transistor. Empézanse a utilizar as tarxetas perforadas. Distínguense 2 tipos de sistema operativo:

- Monitor Residente: o S.O. limitábase a cargar os programas na memoria, léndoos de tarxetas perforadas, e a executalos. O problema era atopar unha forma de optimizar o tempo entre a retirada dun traballo e a montaxe do seguinte.
- Traballo por lotes: utilízanse as fitas magnéticas. Como solución para optimizar o tempo de montaxe xurdiu a idea de agrupar os traballos en lotes, nunha mesma fita ou conxunto de tarxetas, de forma que se executasen un a continuación doutro sen perder a penas tempo na transición. Na memoria do computador existen dous ítems: a) o monitor de lotes: indicando que traballo se está executando e b) o traballo actual.

Estes dous tipos de sistema operativo caracterízanse por:

- Non existe ningún planificador (o que decide qué traballo se vai realizar): a razón da súa inexistencia é que non é necesario, xa que só hai un traballo na memoria principal.
- Tampouco existe un reloxo (mide o tempo que lle ocupa un traballo á CPU): non é necesario porque só hai un proceso en memoria executándose.

### **Terceira Xeración**

Abarca desde a 1965 a 1980. No campo do hardware temos os circuítos integrados con tecnoloxía LSI e VLSI. Antes de vermos os distintos S.O., paga a pena deixar claros dous conceptos: Programa: código (algo estático) e Proceso: programa en execución (algo dinámico).

- S.O. Multiprogramación. Na memoria principal vai haber máis dun programa. A CPU executa instrucións dun programa; cando o que se





atopa en execución realiza unha operación de E/S, en lugar de esperar a que remate a operación de E/S, pásase a executar outro programa. Deste xeito é posible, tendo almacenado un conxunto adecuado de tarefas en cada momento, utilizar de maneira óptima os recursos dispoñibles.

Vaise definir o grao de multiprogramación como o número de programas que hai actualmente en memoria.

OverHead é un parámetro que mide a diferenza de tempo entre aquel en que o sistema operativo está dedicado a facer as súas tarefas e o tempo dedicado ao cambio de contexto entre procesos.

- S.O. Multiproceso. Ten varios procesos na memoria principal. Hai que distinguir que:
  - o *Multiprogramación IMPLICA Multiproceso.* Multiprogramación: varios programas na memoria principal. Ao estaren na memoria principal estanse executando. Programas en execución = procesos.
  - o *Multiproceso NON IMPLICA Multiprogramación.* Agora ben, podemos ter unicamente un programa en memoria e este programa quere lanzar varios procesos. Un programa pode querer imprimir, ler algo polo teclado... lanzar procesos. Varios procesos = multiproceso.
- S.O. Multiprocesador. Utilízanse onde hai 2 CPU ou máis.
- S.O. Interactivos. Sistemas que dalgunha forma manteñen un diálogo co usuario mediante o SHELL (linguaxe de comandos).

É moi importante o tempo de resposta: tempo que transcorre entre que o usuario lle manda facer algo ao sistema ata que obtén a resposta. Sempre se intenta minimizar o tempo de resposta.
- S.O. Multiusuario. Aqueles sistemas operativos nos cales varios usuarios poden acceder ao mesmo ordenador simultaneamente.

Por exemplo: calquera sistema UNIX ou LINUX. Pódese ter unha máquina e xerar usuarios que acceden a esa máquina (a través de rede local, Internet...).

- S.O. de Tempo Compartido. Pretenden dotar a cada persoa dunha parte da CPU. O usuario ve o computador como de seu, aínda que non o é.
- S.O. de Tempo real. Estes sistemas úsanse en contornos onde se deben aceptar e procesar en tempos moi definidos un gran número de sucesos, na súa maioría externos ao ordenador. Se o sistema non respecta as restricións de tempo nas que se deben entregar as operacións, dise que fallou o seu resultado.

### **Cuarta Xeración**

Abarca desde 1980 ata os nosos días e está marcada polos ordenadores persoais.

Sistema Operativo de Rede. O usuario é consciente de que existen outras máquinas. O usuario xa non quere traballar só; quere traballar con outros usuarios. Ten que acceder de forma explícita a esas máquinas.

Sistema Operativo Distribuído. O parámetro clave é a transparencia: o usuario non é consciente de que existen outras máquinas; non sabe en que máquina está.

### **53.1.3 Clasificacións dos Sistemas Operativos**

- Segundo o número de usuarios:
  - o S.O. monousuarios: só aceptan un usuario nun momento determinado.
  - o S.O. multiusuarios: aceptan simultaneamente máis dun usuario.
- Segundo o hardware:
  - o Segundo o número de CPU:

- S.O. monoprocesador: só controla unha CPU.
- S.O. multiprocesador: varios procesadores (máis complicado de deseñar).
- o Segundo a organización da memoria principal:
  - S.O. centralizados: unha memoria principal; os procesadores van estar intentando acceder a esta memoria principal. Os procesos comunícanse a través da memoria.
  - S.O. distribuídos: cada procesador ten a súa propia memoria principal. Os procesos teñen outros mecanismos de comunicación.
- Segundo o modo de traballo cos sistemas operativos:
  - o Interactivo (on-line): o usuario dialoga coa máquina.
  - o Batch (off-line): non hai comunicación coa máquina cando está a realizar o traballo.
- Segundo o obxectivo para o que foron deseñados:
  - o S.O. de propósito xeral: capaces de realizar calquera tarefa.
  - o S.O. de propósito específico: só poden realizar unha tarefa específica; instálanse en microprocesadores que controlan o funcionamento de electrodomésticos, vehículos, equipos de electrónica, consumo, etc.
  - o S.O. de Tempo Real: ofrecen unha resposta nun intervalo de tempo ben definido.
  - o S.O. Virtuais: operan no HW dun ordenador ofrecéndolles aos niveis superiores copias exactas da máquina real, de forma que en cada copia se pode executar un sistema operativo distinto.
  - o S.O. de dispositivos móbiles: débense adaptar ás limitacións que estes dispositivos presentan: procesadores lentos, memoria limitada, pantallas pequenas e consumo de enerxía limitado. Exemplos típicos

para estes dispositivos son iOS de Apple, Windows Mobile, Android, etc.

### **53.1.4 Estrutura dos Sistemas Operativos**

#### Sistemas operativos monolíticos

Estes S.O. non teñen unha estrutura definida. O S.O. escríbese como unha colección de procedementos entrelazados de tal xeito que cada un pode chamar a calquera outro. As características deste tipo de estrutura son:

- Construción do S.O. baseado en procedementos compilados separadamente que se unen nun só ficheiro obxecto a través do enlazador (*linker*).
- Boa definición de parámetros de enlace entre os distintos procedementos existentes, o que xera axuste.
- Carece de protección ao entrar a procedementos que xestionan diferentes aspectos dos recursos do computador, como almacenamento, E/S, etc.
- Son feitos a medida, o que ten como vantaxe que son eficientes e rápidos, e como desvantaxe que carecen de flexibilidade para crecer.

#### Sistemas operativos con capas

O SO organízase nunha xerarquía de estratos, estando construído cada un deles sobre o outro, que ten menor xerarquía ca el. Exemplos: THE, MULTICS.

#### Sistemas operativos Cliente-Servidor.

Minimizar o *kernel* (núcleo) do S.O., desprazando o código de todos os seus servizos a estratos o máis superiores posibles. Para iso, a maioría das súas funcións impleméntanse como procesos de usuario —denominados procesos servidores— de forma que cando un proceso de usuario, chamado proceso cliente, necesita un servizo do S.O., o que fai é enviarlle unha

mensaxe ao proceso servidor correspondente, que realiza o traballo e devolve a resposta.

### **53.1.5 Funcións dun Sistema Operativo**

As principais funcións que teñen os S.O. son a xestión de procesos, a xestión da memoria principal, a xestión do almacenamento secundario e a xestión dos dispositivos de entrada/saída.

#### **Xestión de procesos**

A CPU é o recurso principal do computador de modo que é necesaria unha xestión eficiente da mesma para garantir o seu aproveitamento.

O S.O. ten que cargar os distintos procesos, inicialos, supervisar a súa execución, levando a cabo os cambios de contexto necesarios, e detectar a súa terminación normal ou anormal. Nos contornos multiusuario é fundamental a activación de mecanismos de protección que limiten as posibilidades de acceso de cada proceso a unha serie de recursos para os que conte coa debida autorización.

#### **Xestión de memoria principal**

Nun sistema multiproceso os procesos teñen que compartir a CPU, atopándose na memoria principal para poder pasar a executarse inmediatamente; así, varios procesos teñen que compartir a memoria principal sen que uns poidan acceder aos recursos doutros.

Para isto hai que dividir a memoria en bloques e estes asignánselles a distintos procesos. Para facer a división utilízase a segmentación, a paxinación ou a segmentación paxinada.

#### **Xestión dos sistemas de arquivos**

Nun sistema de arquivos, o S.O. tense que facer cargo de: a xestión do espazo libre/ocupado; dos cachés de lectura e escritura; do vínculo entre nomes e arquivos; das asociacións entre os bloques físicos dos dispositivos

e os bloques lóxicos, e dos permisos para o acceso e modificación dos distintos elementos.

### **Xestión de entrada/saída (E/S)**

A velocidade con que se comunican o procesador e a memoria principal contrasta coa velocidade cando os programas deben interactuar con algún tipo de dispositivo de E/S; durante este proceso, a execución do programa vese interrompida, xa que a comunicación cos devanditos dispositivos é significativamente máis lenta que coa memoria.

Conxuntamente coa multiprogramación xorden dous conceptos: o acceso directo á memoria (DMA) e as interrupcións. O procesador cede o control da E/S a un módulo que se encarga de executar este tipo de operacións (o controlador de DMA) e de agardar ata que estas se completen; cando isto sucede avisa ao procesador (que se atopa mentres tanto executando outras instrucións —ben sexa do mesmo proceso ou dalgún outro—) que pode continuar coas operacións subseguintes que quedaron pendentes cando se realizou a petición de E/S mediante unha interrupción.

#### ***53.1.6 Tendencias***

Actualmente, a mobilidade é o primordial na nosa sociedade, e asociada a esta mobilidade está a seguridade. Empézase a falar de sistemas operativos na nube (*cloud computing*) e consolídanse os sistemas operativos dos dispositivos móbiles.

Outro aspecto destacable, derivado do momento económico, é o aforro de custos. Froito disto pódese ver unha tendencia máis que clara á virtualización.

### **S.O. en dispositivos móbiles**

Se existe unha carreira hoxe en día no desenvolvemento de S.O., está nos S.O. para dispositivos móbiles. Os novos sistemas operativos converten o teléfono nun completo aparato multimedia. Ata hai ben pouco tempo a elección dun móbil viña determinada polas súas características físicas:

recepción do sinal, cámara... pero coa chegada dos smartphone, a elección do S.O. converteuse en algo moi importante.

Contrariamente ao mundo do ordenador persoal, e debido quizais á súa xuventude no mercado, non existe un dominador claro de S.O. móbiles. Hai fabricantes de hardware que son os fabricantes dos seus propios sistemas operativos; por exemplo, Apple, que só distribúe o S.O. iOS para iphones e iPad, o mesmo que RIM, que distribúe o seu S.O. BlackBerry OS en dispositivos BlackBerry, etc. No outro extremo están os fabricantes que utilizan S.O. doutras compañías, coma Android, Symbian, Windows Mobile...

As compañías que fabrican e distribúen o seu propio S.O. teñen a favor que as actualizacións dos dispositivos son moi controladas.

Outra tendencia virá da man do crecemento dos dispositivos *tablets* (tabletas), tendo en conta os anuncios de lanzamentos de tabletas: Apple (iPad 2), RIM (PlayBook), Samsung (Galaxy Tab 2), etc. Isto lles dará aínda máis pulo aos S.O. móbiles.

### **S.O. na nube ou en rede**

Estes S.O. xorden do concepto de Computación na Nube (*Cloud Computing*), que é un novo paradigma que, basicamente, permite ter servizos computacionais a través de internet.

Unha das grandes vantaxes que se lle poden encontrar a este novo paradigma é o baixo investimento que hai que realizar en HW, xa que toda a infraestrutura da computación na nube se atopa nos grandes provedores de servizos de internet. Bastaría con un hardware mínimo, un navegador e unha boa conexión a internet.

Outra das vantaxes sería que as aplicacións non se instalan no PC; son aplicacións Web, o que fai que sexan compatibles cos máis dos formatos coñecidos.

Ademais, permite ter unha única copia dun ficheiro dispoñible en calquera lugar e momento.

Os seus puntos débiles son a seguridade e a necesidade dunha conexión a internet.

Estes S.O. son unha boa opción para os *notebook* que teñen pouco hardware, e mesmo poderían facer que os fabricantes apostasen por modelos máis baratos que permitirían difundir moito máis a informática.

Entre os S.O. máis importantes destacan: eyeOS, ChromeOS de Google, oOS, iCloud, etc.

### **53.2.- SISTEMA OPERATIVO UNIX-LINUX**

UNIX é un sistema operativo creado en 1969 por un grupo de investigadores dos laboratorios Bell de AT&T —entre eles Ken Thompson, Dennis Ritchie e Douglas McIlroy— como unha versión reducida do proxecto MULTICS; primeiro foi escrito en ensamblador, pero iso impedía a portabilidade a diferentes computadores. Despois de que Dennis Ritchie en 1973 crease a linguaxe C, reescríbese UNIX totalmente nesta linguaxe de alto nivel, facendo deste xeito o código case totalmente independente do tipo de máquina e permitindo a instalación de UNIX en diferentes plataformas.

Inicialmente, os laboratorios AT&T Bell, consideraron que UNIX era máis ben un proxecto de investigación e chegarono a distribuír de forma gratuíta entre departamentos informáticos das universidades, os cales podían modificalo e adaptalo ás súas necesidades. Pero, a gran demanda do sistema operativo fixo que os laboratorios Bell iniciasen a súa venda a través de distribucións oficiais, concedéndolles aos usuarios que o requirían licenzas de uso.

Debido ás múltiples versións no mercado de UNIX, o IEEE especificou unha familia de estándares para definir unha interface de programación de aplicacións (API) para que todas as versións fosen 'compatibles'. Esta familia coñécese como POSIX (*Portable Operating System Interface*; o X vén de UNIX como sinal de identidade da API )



Linux creouse en 1991 por Linus Torvalds baseándose noutros dous sistemas operativos:

- O sistema aberto UNIX.
- O sistema educativo Minix, creado en 1987 por Andrew S. Tanenbaum.

Torvalds crea só o Kernel, o núcleo do sistema sen a capa de servizos, xestores, aplicacións gráficas, etc., que serán creadas posteriormente por outros autores. O código do núcleo podémolo atopar no enderezo ([www.kernel.org](http://www.kernel.org)).

Na comunidade de programadores créase o proxecto GNU (*Gnu's Not Unix*), proxecto para xerar software libre, onde se xeran editores, compiladores, etc., baixo a licenza pública xeral GPL (*General Public License*): usar, copiar, distribuír e modificar sempre que se conserve a sinatura do autor, podendo cobrar por iso.

Linux créase con esta filosofía de libre distribución, e o sistema operativo completo que se constrúe con este núcleo tamén. A todo o sistema dáselle o nome de GNU/Linux (distribución completa do sistema operativo con Linux), que contén o núcleo máis as outras capas do sistema operativo e utilidades. Aínda que moitas veces denomínase todo o sistema simplemente LINUX.

### **53.2.1 Características**

As características máis salientables do sistema UNIX son:

- UNIX foi deseñado como un sistema multiusuario en tempo compartido; ofrece; protección dos datos privados sobre ficheiros e protección do contorno de execución.
- Portabilidade: UNIX foi escrito na linguaxe C, unha linguaxe de alto nivel, o cal fai que sexa relativamente fácil de ler, entender,

modificar e transportar a outras máquinas cunha arquitectura física diferente.

- Código e funcionamento escrito baixo a familia de estándares POSIX (*Portable Operating System Interface*).
- Interface de usuario simple e interactiva: o intérprete de ordes (*shell*) é un programa independente que o usuario pode substituír. A sintaxe de utilización é idéntica para todas as ordes.
- Modularidade: Proporciona primitivas que permiten construír grandes programas a partir doutros máis sinxelos, así como librerías para *linkaxe*.
- Posúe bibliotecas compartidas para facilitar o enlace dinámico.
- Protección de memoria.
- Soporta diferentes sistemas de arquivos, incluídos os de Microsoft Windows.
- Sistema de arquivos con estrutura de árbore invertida (de múltiples niveis que permite un fácil mantemento) e xerárquico (permite a unión de diversos sistemas de ficheiros co sistema principal, e unha separación de directorios).
- Todos os arquivos de usuario son simples secuencias de bytes (8 bits ); non teñen ningún formato predeterminado.
- Independencia de dispositivos: Os discos e os dispositivos de entrada e saída (E/S) trátanse todos do mesmo xeito: como meros arquivos. As peculiaridades dos dispositivos mantéñense no núcleo (kernel).
- A arquitectura da máquina é completamente transparente para o usuario, o que permite que os programas sexan fáciles de escribir e transportables a outras máquinas con hardware diferente.

- UNIX non incorpora deseños sofisticados; de feito, a maioría dos algoritmos foron seleccionados pola súa sinxeleza e non pola súa rapidez ou complexidade.
- Incorpora todos os servizos de rede, TCPIP, DNS, sendmail, etc.
- Proporciona un completo contorno de programación: os filtros son utilidades simples que se concentran en realizar ben unha soa función. Pódense combinar de forma moi flexible utilizando as *pipes* (tubos) e os reenderezos de E/S segundo as necesidades e preferencias de cada usuario.
- Mantemento fácil: consecuencia directa da modularidade. O sistema segue a evolucionar e perfecciónase e enriquecese con novas funcionalidades.
- Carácter aberto: permite ampliar facilmente a funcionalidade con novos compoñentes sen ter que depender dun único fabricante.

### **53.2.2 Arquitectura de Unix-Linux**

A arquitectura está baseada en capas ou niveis, de forma que cada capa unicamente pode comunicarse coas capas que se atopan nos niveis inmediatamente inferior e superior.

Na capa inferior temos toda a parte do hardware que o sistema operativo debe xestionar. Por riba deste sitúase o kernel de Unix, que é o encargado da administración de procesos, xestión do sistema de arquivos, entradas/saídas, etc. Aos procesos que traballan a ese nivel chámaselles procesos en modo kernel.

A biblioteca estándar sitúase por encima do kernel; encárgase, por exemplo, das operacións de apertura, peche, etc. A este nivel trabállase en modo usuario. A interface entre as dúas capas, ou o acceso da capa de

biblioteca estándar á do kernel, realízase a través da interface de chamadas ao sistema.

A un nivel superior temos os programas e utilidades, coma o *shell*, compiladores, etc., que lles serven de axuda a desenvolvedores e usuarios que interactúan co sistema operativo. A interface entre esta capa e a inmediatamente inferior é a través da interface de biblioteca.

Por último, situaríanse os usuarios que, por medio da interface de usuario, se comunican co *shell*, ou outras utilidades do sistema Unix.

O núcleo de UNIX (kernel) é de tipo monolítico, diferenciándose dúas partes principais: o núcleo dependente da máquina e o núcleo independente. O núcleo dependente encárgase das interrupcións, dos dispositivos de baixo nivel e de parte da administración da memoria. O núcleo independente é igual en todas as plataformas e inclúe a xestión de chamadas do sistema, a planificación de procesos, a paxinación e intercambio, a xestión de discos e do sistema de arquivos.

### **53.2.3 Xestión de procesos**

A xestión de procesos en UNIX é por prioridade e *round robin*. Nalgunhas versións xestiónase tamén un axuste dinámico da prioridade de acordo co tempo que os procesos esperaron e co tempo que xa usaron a CPU. O sistema proporciona facilidades para contabilizar o uso de CPU por proceso e unha pila común para todos os procesos cando necesitan estarse executando en modo privilexiado (cando fixeron unha chamada ao sistema ).

Os procesos traballan en modo usuario e en modo kernel. O paso de modo usuario a kernel ou viceversa realízase a través de *traps* que crean unha interrupción para acceder á interface de chamadas ao sistema e ao resto dos compoñentes de nivel kernel. O paso do modo kernel a usuario é un retorno tras a realización da petición que motivou o paso ao modo kernel.

UNIX permite que un proceso faga unha copia de si mesmo por medio da chamada «fork», o cal é moi útil cando se realizan traballos paralelos ou concorrentes; tamén se dispón de facilidades para o envío de mensaxes entre procesos (*pipes, signals*).

Os procesos non interactivos denomínanse *daemons* ou procesos *background*. Cando se inicia un proceso, asígnaselle un identificador PID, gárdase o proceso que o lanzou PPID, o propietario que o lanzou UID e o grupo de pertenza GID, o que definirá o perfil de permisos de acceso aos que terá dereito. Existe a posibilidade de alterar o usuario ou grupo efectivo de permisos durante a execución do proceso mediante a chamada a **setuid** ou **setgid**, sempre que se dispoña dos permisos apropiados. Tamén existe unha bandeira de permisos **setuid** asociada ao arquivo do programa que permite executar este, cos permisos do propietario do arquivo en lugar dos do usuario que o executa.

LINUX combina multiprogramación e tempo compartido.

O xestor de procesos no kernel do sistema UNIX encárgase da asignación de CPU, a programación de procesos e as solicitudes dos procesos. Para realizar estas tarefas, o kernel mantén varias táboas importantes para coordinar a execución de estes procesos e a asignación dos dispositivos.

Utilizando unha política predefinida, o programador de procesos selecciona un proceso da cola de procesos listos e comeza a súa execución durante un período de tempo xa dado.

O algoritmo de programación de procesos selecciona o proceso coa maior prioridade para ser executado primeiro. Se varios procesos teñen a mesma prioridade, aplícase o algoritmo *round-robin*.

#### **53.2.4 Xestión de memoria**

Os sistemas UNIX utilizan o manexo de memoria virtual; o esquema máis usado é a paxinación por demanda e combinación de segmentos paxinados, en ambos os casos con páxinas de tamaño fixo.

En todos os sistemas UNIX úsase unha partición de disco duro para a área de intercambio (*swap*). Esa área resérvase durante a instalación do sistema operativo.

Unha regra moi difundida entre administradores de sistemas é asignar unha partición de disco duro que sexa polo menos o dobre da cantidade de memoria real do ordenador. Con esta regra permítese que se poidan intercambiar flexiblemente todos os procesos que estean na memoria RAM nun momento dado por outros que estean no disco.

Se non caben todos os programas na memoria principal faise uso da partición de intercambio (*swapping*).

- *Swap out*. Cando non caben en memoria procesos activos, “expúlsase” un proceso de memoria principal, copiando a súa imaxe a *swap*, aínda que non é necesario copiar todo o mapa. Existen diversos criterios de selección do proceso que se vai intercambiar: dependendo da prioridade do proceso; preferencia aos procesos bloqueados; non intercambiar se está activo DMA sobre mapa do proceso.
- *Swap in*. Cando haxa espazo na memoria principal, intercámbiase o proceso á memoria copiando a imaxe desde *swap*.

Todos os procesos que forman parte do kernel non poden ser intercambiados a disco.

Cada proceso dispón do seu propio espazo de enderezos, organizado en segmentos segundo:

- *Text Segment*: que almacena o código.
- *Data Segment*: que almacena os datos ou variables que utilizan os procesos; este ten dúas partes: *Initialized Data* (datos iniciados) e *Uninitialized Data* (datos non iniciados).
- *Stack Segment*: que almacena a información referente a chamadas a outras funcións.

É posible compartir código entre procesos mediante o emprego de *Shared Text Segments*. Dous procesos nunca comparten os segmentos de datos e de pila (salvo os *thread*); a forma de compartir información lévase a cabo mediante o emprego de segmentos especiais de memoria compartida *Shared Segments*.

Linux comparte moitas características dos esquemas de xestión de memoria doutras implementacións UNIX, pero ten as súas propias.

No que respecta á memoria virtual, o direccionamento de memoria virtual de Linux fai uso dunha estrutura de táboa de páxinas con tres niveis, formada polos seguintes tipos de táboas (cada táboa individual é do tamaño dunha páxina): Directorio de páxinas: un proceso activo ten un só directorio de páxinas, que é do tamaño dunha páxina. Cada entrada no directorio de páxinas apunta a unha páxina do directorio intermedio de páxinas. Para un proceso activo, o directorio de páxinas ten que estar na memoria principal. Directorio intermedio de páxinas: este directorio pode ocupar varias páxinas e cada entrada deste directorio apunta a unha páxina da táboa de páxinas. Táboa de páxinas: esta táboa de páxinas tamén pode ocupar varias páxinas, e cada entrada da táboa de páxina fai referencia a unha táboa virtual do proceso.

Para utilizar esta estrutura da táboa de páxinas a tres niveis, un enderezo virtual en Linux vese como un conxunto de catro campos. O campo máis á esquerda (máis significativo) utilízase como índice no directorio de páxinas. O seguinte campo serve como índice no directorio intermedio de páxinas. O terceiro campo serve como índice na táboa de páxinas. E o cuarto e último campo indica o desprazamento dentro da páxina seleccionada da memoria.

### **53.2.5 Xestión de E/S**

Os dispositivos de entrada e saída son considerados ficheiros especiais: toda entrada/saída está baseada no principio de que todos os dispositivos se poden tratar como ficheiros simples aos que se accede mediante

descriptores de arquivos cuxos nomes se atopan normalmente no directorio «/dev».

Cada proceso en UNIX mantén unha táboa de arquivos abertos (onde o arquivo pode ser calquera dispositivo de entrada/saída). Esa táboa ten entradas que corresponden aos descriptores, os cales son números enteiros obtidos por medio da chamada do sistema.

As chamadas ao xestor de entrada/saída fanse de dúas formas: síncrona e asíncrona. O modo síncrono é o modo normal de traballo e consiste en facer peticións de lectura ou escritura, e o proceso espera a que o sistema lle responda.

O xestor de entrada/saída utiliza como elementos principais o buffer de cache; o código xeral de xestión de dispositivos, e drivers de dispositivos de hardware. Existen dous tipos de dispositivos:

Dispositivos de bloques:

- Usan secuencias de bytes (bloques).
- Utilizan buffer-cache.
- Están estruturados en bloques de tamaño fixo (512 bytes).
- Permiten optimizar o rendemento.

Dispositivos de carácter:

- Son dispositivos sen estrutura (terminais, impresoras, etc.).
- Non usan buffer.
- As operacións realízanse carácter a carácter.

## **Interrupcións e excepcións**

UNIX permite interromper a CPU asincronamente. Ao recibir a interrupción, o kernel almacena o contexto actual, determina a causa e responde á



interrupción. Tras responder a esta, devolve o contexto interrompido e segue executando. O HW asígnalles as prioridades aos dispositivos de acordo coa orde de actuación nas interrupcións.

Así como as interrupcións están causadas por factores externos a un proceso, as excepcións son sucesos inesperados producidos por procesos, tales coma a execución de instrucións reservadas, de forma que o sistema, ao se atopar cunha, tende a reiniciar a instrución en lugar de pasar á seguinte.

Non obstante, o kernel debe ter a posibilidade de impedir a aparición de interrupcións en momentos críticos para evitar a degradación dos datos. O sistema que se utiliza é o de dispoñer dun conxunto de instrucións restrinxidas que colocan o nivel de execución do procesador no estado de palabra (*status word*). Ao asignar un nivel de execución do procesado, todas as interrupcións dese nivel e inferiores quedan suprimidas, permitindo só as superiores.

### **53.2.6 Xestión de arquivos**

Un sistema de arquivos permite realizar unha abstracción dos dispositivos físicos de almacenamento da información para que sexan tratados a nivel lóxico, como unha estrutura de máis alto nivel e máis sinxela que a estrutura da súa arquitectura hardware particular.

O sistema de arquivos UNIX caracterízase porque posúe unha estrutura xerárquica, realiza un tratamento consistente dos datos dos arquivos, protexe os datos dos arquivos e trata os dispositivos e periféricos (terminais, unidades de disco, fita, etc.) coma se fosen arquivos.

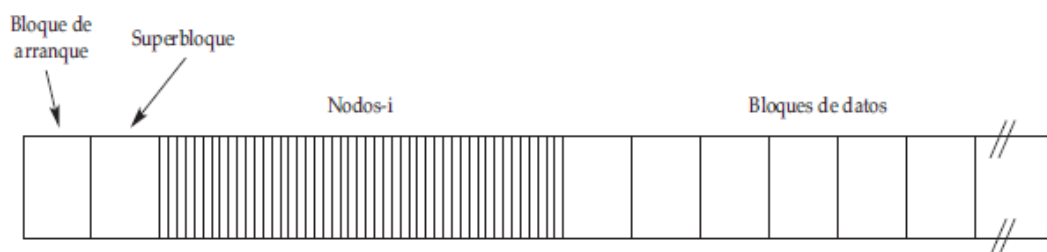
O sistema de arquivos está organizado, a nivel lóxico, en forma de árbore invertida, cun nodo principal coñecido como nodo raíz ("/"). Cada nodo dentro da árbore é un directorio e pode conter pola súa vez outros nodos (subdirectorios), arquivos normais ou arquivos de dispositivo.

Os nomes dos arquivos (*pathname*) especificáanse mediante a ruta (*path*), que describe como localizar un arquivo dentro da xerarquía do sistema. A ruta dun arquivo pode ser absoluta (referida ao nodo raíz) ou relativa (referida ao directorio de traballo actual).

Todos os sistemas UNIX poden manexar múltiples particións de disco, cada unha cun sistema de arquivos distinto.

Unha partición de disco clásica en UNIX contén unha estrutura como a da figura.

- Bloque de arranque: contén o código para arrancar o computador con esa partición.
- Superbloque: contén información crucial acerca da organización do sistema de arquivos, incluído o número de nodos-i (i-nodes), o número de bloques de disco e o principio da lista de bloques de disco libres. A destrución do superbloque fai que o sistema de arquivos xa non se poida ler.
- Nodos-i: contén a representación interna dun ficheiro que permite, entre outras cousas, localizar todos os bloques de disco que conteñen os datos do arquivo.
- Bloques de Datos: almacenan a información. O normal é que un arquivo ocupe máis dun bloque de datos, sen que sexa necesario que estean contiguos.



Dentro da estrutura de directorios de UNIX - Linux existen unha serie de directorios comúns a todas as instalacións que é preciso coñecer:

- /: Directorio raíz, inicio do sistema de arquivos.
- /tmp: Directorio de arquivos temporais.
- /dev : Directorio de dispositivos. Nel atópanse todos os dispositivos de E/S, que se tratan como arquivos especiais.
- /etc: Directorio para arquivos de sistema diversos.
- /bin: Directorio para programas binarios (executables).
- /lib: Directorio de bibliotecas do sistema.
- /usr: Directorio de usuarios.
- /home: Directorio base a partir do cal se sitúan os directorios por defecto das contas de usuario.

LINUX comezou empregando o sistema de arquivos de MINIX, pero estaba limitado a nomes de 14 caracteres e a arquivos de 64 MB de tamaño. A primeira mellora veu da man dun sistema de arquivos denominado Ext, que permitía nomes de arquivo de 255 caracteres e 2 GB de tamaño por arquivo, pero era moi lento. A evolución partiu do sistema de arquivos Ext2, con nomes de arquivo longos, arquivos grandes e mellor rendemento. Ext2 evolucionou a Ext3, que trouxo principalmente as transaccións (*journaling*) a Ext2. En Ext3 almacénase a información necesaria para restablecer os datos afectados pola transacción no caso de que esta falle. A evolución de Ext3 é **Ext4**, que soporta un tamaño máximo de sistema de arquivos de 1 ExaByte (1 ExaByte = 1024 PetaBytes = 1048576 TeraBytes) e un tamaño máximo por arquivo de 16 TB para os arquivos e, doutra banda, modifica estruturas de datos importantes, como a destinada a almacenar os datos do arquivo utilizando **“extent”**, que é un conxunto de bloques físicos contiguos, mellorando o rendemento ao traballar con ficheiros de gran tamaño e reducindo a fragmentación.

### **53.3.- SISTEMA OPERATIVO WINDOWS**

#### **53.3.1 Características**

A familia de S.O. Windows é propiedade de Microsoft. Poderíase dicir que, basicamente, existen dúas versións distintas de S.O. Windows: aquelas enfocados ao mundo empresarial e aquelas enfocados ao consumidor final ou usuario doméstico.

Dentro desta simple clasificación poderíamos facer outras máis. Orientado ao usuario doméstico existen S.O. para equipos de sobremesa, portátiles, tablets, e dispositivos móbiles. E orientado ao mundo empresarial podemos distinguir S.O. para servidores e S.O. para estacións de traballo. Aínda poderíamos dividir máis os S.O. para servidores (Standard, Enterprise, Datacenter, Web, Storage, Small Business Server...)

Os últimos S.O. que viron a luz son Windows 7 coas versións Starter (só para 32 bits), Home Basic, Home Premium, Professional, Ultimate, Enterprise. E a nivel de S.O. para servidores está Windows Server 2008 R2.

É destacable o interese de mellora adquirido por Microsoft cos S.O. de servidor, comprometéndose a un cambio cada 5 anos (antes do 2008 estaba o 2003) e a unha revisión cada 2 anos aprox. (por iso existe Windows Server 2008 R2).

Windows Server 2008 é o último S.O. de servidor que inclúe estas melloras:

- Novo proceso de reparación de sistemas NTFS: proceso en segundo plano que repara os arquivos danados.
- Creación de sesións de usuario en paralelo: reduce tempos de espera nos Terminal Services e na creación de sesións de usuario a grande escala.
- Peché limpo de Servizos.
- Sistema de arquivos SMB2: de 30 a 40 veces máis rápido o acceso aos servidores multimedia.

- *Address Space Load Randomization* (ASLR): protección contra *malware* na carga de controladores en memoria.
- *Windows Hardware Error Architecture* (WHEA): protocolo mellorado e estandarizado de informe de erros.
- Virtualización de Windows Server: melloras no rendemento da virtualización.
- PowerShell: inclusión dunha consola mellorada con soporte GUI para administración.
- Server Core: o núcleo do sistema renovouse con moitas e novas melloras.

Nos seguintes apartados imos ver características de Windows e, aínda que a maioría son comúns para todas as versións, as explicacións estarán máis centradas en Windows 2008 Server R2.

### **53.3.2 Arquitectura de Windows**

A estrutura modular de Windows 2008 proporciona unha gran flexibilidade. O seu deseño permítelle executarse nunha gran variedade de plataformas hardware. Nesta estrutura modular distínguense dúas capas principais:

- **Modo usuario**: Os seus programas e subsistemas están limitados aos recursos do sistema aos que teñen acceso. Está formado por subsistemas que lles poden pasar peticións de E/S aos controladores apropiados do modo núcleo a través do xestor de E/S.
- **Modo núcleo ou kernel**: Ten acceso total ao hardware da máquina, impedíndolles aos servizos do modo usuario e ás aplicacións accederen á o hardware, que queda totalmente protexido polo sistema operativo. A arquitectura dentro do modo núcleo componse do seguinte:

- o O micrónúcleo: situado entre a capa de abstracción de hardware e o Executive, proporciona a xestión *multiprocesador*: xestión de procesos, fíos e tratamento de interrupcións e de excepcións.
- o Unha capa de abstracción de hardware (en inglés *Hardware Abstraction Layer* ou HAL), encárgase de ocultar as diferenzas de hardware e, xa que logo, proporciona unha plataforma única onde poida executarse o S.O. independentemente do HW.
- o Controladores ou tamén chamados drivers: utilizados para interactuar cos dispositivos hardware.
- o Executive: sobre o cal son implementados todos os servizos de alto nivel. Relaciónase con todos os subsistemas do modo usuario. Ocúpase da entrada/saída, a xestión de memoria, Plug&Play, a seguridade e a xestión de procesos.

Dado que o enlace estático dos programas de usuario coas bibliotecas da API Win32 implicaría un tamaño enorme dos programas e un desperdicio de memoria, pois cada programa en execución había ter a súa copia destas bibliotecas, todas as versións de Windows manexan bibliotecas compartidas, chamadas bibliotecas de vínculos dinámicos (DLL; Dinamic Link Libraries).

### **53.3.3 Xestión de procesos**

Os procesos créanse como obxectos, e un proceso pode ter varios fíos. Dado que o proceso é un obxecto, a súa composición será un conxunto de datos só accesibles a través dun conxunto de funcións que os ocultan do resto de aplicacións ou funcións. Estas funcións ou servizos actívanse por medio de mensaxes. O proceso terá polo menos un fío que, pola súa banda, pode executar outros fíos, podendo facelo en paralelo nun sistema multiprocesador.

Windows mantén dúas listas diferentes coa información de todos os procesos e fíos. Cada proceso ten asociado un bloque ou estrutura de datos EPROCESS, que apunta ao EPROCESS seguinte e ao anterior (dobre lista enlazada); a outra estrutura é ETHREAD, para recoller a información dos fíos.

O algoritmo de planificación está baseado en colas de retroalimentación de múltiples niveis con prioridades. Cada cola xestiónase cunha política *round robin*.

A planificación aplícase sobre os fíos, non aos procesos (sen ter en conta a que proceso pertencen os distintos fíos que se executan), e está baseada en prioridades; é dicir, sempre se executará o fío de maior prioridade da cola de fíos preparados.

Cando se selecciona un fío para a súa execución, concédeselle un *quantum*, ou intervalo de tempo durante o cal se lle permite ao fío executarse antes de que o faga outro fío do mesmo nivel de prioridade. Os valores do *quantum* poden variar.

Aínda que se lle conceda un *quantum* a un fío, este podería non consumilo completamente se aparece no sistema un novo proceso de maior prioridade, que obrigaría ao que se está executando a abandonar o procesador.

O sistema trata igual a todos os fíos que teñan a mesma prioridade, asignándolle a cada fío de maior prioridade un intervalo de tempo de procesador cun *round robin*. Se ningún destes fíos estivese preparado para executarse, pasarían a executarse, coa mesma política, os da prioridade inmediatamente inferior.

En cada un destes casos, Windows debe determinar que fío debe executarse a continuación, e esta decisión é o que se coñece como *dispatcher*.

Cada proceso recibe unha prioridade base para todos os seus fíos. O sistema baséase en 32 prioridades, do 0 (menor prioridade) ao 31 (maior prioridade):

- A prioridade 0 está reservada para o fío de sistema responsable de poñer a cero as páxinas libres cando non as necesiten ningún fío.
- As prioridades 1 a 15 son as reservadas para os procesos de usuario (prioridades variables).
- As prioridades 16 a 31 están reservadas para o sistema operativo (prioridades en tempo real).

O planificador funciona accedendo á táboa polo proceso de prioridade 31 e vendo se ten fíos listos para executar. Se os hai, colle o primeiro da lista e execútao durante un *quantum*. Namentres existan procesos preparados dunha prioridade superior, o sistema ha concederlles todo o tempo que precisen. Este comportamento repítese para cada unha das entradas da táboa de prioridades.

En certas condicións, un subprocesso pode ver incrementada a súa prioridade base, pero nunca por riba da prioridade 15, e nunca para subprocessos de prioridade maior de 15. Se unha operación de E/S libera un subprocesso, este ve incrementada a súa prioridade base de modo que se poida executar pronto.

Tamén se produce aumento de prioridade se o subprocesso estaba a agardar por un semáforo, mutex ou outro suceso. Estas elevacións de prioridade van diminuindo a medida que un subprocesso beneficiado vai consumindo por completo o seu *quantum*, ata volver situarse na súa prioridade base.

#### **53.3.4 Xestión de memoria**

A xestión de memoria en Windows é de memoria virtual con paxinación. As aplicacións de 32 bits teñen un espazo de enderezo do proceso de 4 GB de memoria. Os sistemas operativos de Microsoft Windows proporciónalles



ás aplicacións acceso a 2 GB de espazo de enderezo do proceso, especificamente coñecido como espazo de enderezos virtuais do modo de usuario. Todos os subprocesos pertencentes a unha aplicación comparten o mesmo espazo de enderezos virtuais do modo de usuario. Os 2 GB restantes resérvanse para o sistema operativo (tamén coñecido como espazo de enderezo do modo de kernel).

O espazo de enderezos virtuais paxínase por demanda con tamaño fixo de páxinas (mínimo 4KB para arquitecturas x86 e x64bits e 8KB para arquitecturas IA64 e máximo de 4MB para arquitectura x86, 2MB para x64 e 16MB para IA64).

Windows utiliza un algoritmo de **paxinación por demanda anticipada**, é dicir, cada vez que se produce un fallo de páxina, o sistema copiará en memoria a páxina correspondente á referencia a memoria que causou o fallo de páxina, e ademais un conxunto de páxinas próximas a ela, tanto anteriores coma posteriores, ao supoñer que, debido á localidade das referencias, é case seguro que nun futuro próximo tamén se fará referencia a estas páxinas, que cando se queiran utilizar xa estarán en memoria e, polo tanto, non producirán fallos de páxinas adicionais.

O mecanismo de paxinación apóiase moito no concepto de **Conxunto de Traballo (Working Set)** que asegura unha certa cantidade de memoria física para cada proceso.

Windows préstalle especial atención ao momento de arranque dos procesos, xa que, como non teñen ningunha páxina cargada na memoria, ata que carguen todas as páxinas necesarias hanse producir moitos fallos de páxina. Para optimizar a carga dos procesos, Windows conta co que se coñece como “*Prefetcher*” que ten como misión acelerar o proceso de carga.

Se se produce un fallo de páxina e é necesario substituír algún marco de páxina que está en memoria, Windows emprega o algoritmo LRU (aínda que algunhas versións utilizan tamén FIFO).

Permite compartir páxinas, ao poder protexelas contra lectura ou escritura. Igualmente admite que se poida bloquear unha páxina en memoria que sexa crítica, impedindo que se poida substituír ante unha falta de páxina, facilitando así a implementación de aplicacións en tempo real.

### **53.3.5 Xestión de E/S**

O sistema de entrada/saída (E/S) de Windows é o que permite utilizar os dispositivos facilitando o acceso aos mesmos e independizando os programas dos dispositivos, ofrecendo ademais seguridade no seu uso e a escalabilidade do sistema.

As entradas e saídas en Windows poden ser síncronas (o proceso esperará ata que se complete a operación no dispositivo hardware) ou asíncronas (o proceso lanza a operación e segue coa súa execución, e cando a operación E/S finaliza o S.O. avísao).

En Windows cárganse e descargan os drivers en calquera momento, evitando que consuman recursos se non se van utilizar.

Isto faise grazas ao *Plug and Play* (PnP), que permite detectar calquera dispositivo que se conecte ao sistema e cargar o driver correspondente.

O sistema de E/S componse dos seguintes módulos:

- O xestor de E/S: define a infraestrutura que soporta os drivers de dispositivos. Forma parte do sistema operativo.
- O driver de dispositivo: proporciona un interface de E/S para un determinado tipo de dispositivo. Os drivers reciben peticións canalizadas a través do xestor de E/S, diríxenas ao dispositivo concreto e informan o xestor de que se completou a operación de E/S. Estes módulos desenvólvenos os fabricantes.

- O xestor de PnP: detecta os dispositivos hardware ao conectarse ou desconectarse.
- O xestor de enerxía: facilítalle ao sistema, así como aos drivers de dispositivo, os cambios de estado de consumo de enerxía eléctrica de acordo coa actividade do dispositivo.

### **53.3.6 Xestión de arquivos**

En Windows, a asignación do espazo realízase o subsistema de ficheiros en unidades “clúster” cuxo tamaño depende da capacidade do disco; normalmente, oscila desde 512 bytes ata 4 Kbytes. Utiliza 64 bits para direccionar os clúster e permite definir ficheiros de 264TB (16.384 petabytes), aínda que, lóxicamente, o tamaño máximo dos ficheiros está limitado pola capacidade dos discos.

Windows xestiona os discos e a información que conteñen baseándose en particións e volumes.

- **Particións.** Cada disco pódese dividir en particións primarias e estendidas. As particións primarias serán aquelas que poidan conter un S.O. e, polo tanto, permitan o arranque do S.O. desde elas. De aquí podemos deducir que o sistema require como mínimo unha partición primaria nalgún disco.

Unha partición nunca poderá exceder dun disco. Só pode haber unha partición estendida por disco e, como máximo, só poderá conter 4 particións en total.

Unha vez creada a partición, é necesario darlle formato para que poida conter datos. Un volume é sinónimo de partición formateada.

En Windows, as particións xestiónanse o xestor de particións. Este xestor utiliza o xestor de E/S para identificar as particións e crear os dispositivos que as representen, é dicir, as unidades lóxicas correspondentes.

Este xestor envíalle un comando ao xestor de volumes (descrito máis adiante) para saber se a partición ten un volume asociado e, se é así, a partir dese momento calquera acción sobre a partición ha notificarlla ao xestor de volumes.

- **Volume.** Desde o punto de vista do usuario, un volume é unha partición formateada. As particións primarias só poderán conter un volume, namentres que as estendidas poderán albergar varios, tendo en conta que un sistema só poderá ter como máximo 24 volumes, xa que se identifican por medio das letras do abecedario, e en inglés hai 24 letras.

En Windows Server podemos traballar con dous tipos de discos:

- Discos básicos. Son os que se basean exclusivamente en táboas de particións MBR (*Master Boot Record*) ou táboas GPT (*GUID Partition Table*).
- Discos dinámicos. Baséanse en *volumes dinámicos*, que permiten a creación de volumes de particións múltiples tales coma simples, distribuídos, espellos, *stripes* e RAID-5. Os discos dinámicos particiónanse co Administrador de discos lóxicos (LDM – *Logical Disk Manager*).

Windows traballa cos seguintes tipos de volumes dinámicos:

- Volumes distribuídos (*spanned*). É un único volume lóxico composto por un máximo de 32 particións libres nun ou máis discos. É unha forma de xuntar o espazo non asignado nun sistema con varios discos nunha única unidade lóxica.
- Volumes Espello. Neste tipo de volume, o contido da partición dúplícase nunha partición idéntica noutro disco, aínda que se ven como un único volume e non como dous. Os volumes espello coñécense como RAID de nivel 1 (RAID1) e son tolerantes a fallos.
- Volumes divididos (*Striped*). Similar ao volume distribuído, utiliza o espazo de varios discos e convérteos nunha única unidade lóxica.

Utiliza un tipo especial de formato para escribir no disco e ten máis rendemento que o volume distribuído. Os fallos de escritura adoitan ser maiores que no caso do volume distribuído. Coñécense como RAID de nivel 0 (volumes RAID-0).

- Volumes RAID-5. Como os volumes *stripped*, pero con tolerancia a fallos, xa que distribúen a información de paridade entre todos os discos membros do volume.

### **Sistemas de ficheiros**

Windows soporta os seguintes formatos de sistemas de ficheiros:

A) CDFS (sistema de ficheiros de CD-ROM): só permite a lectura e soporta os formatos de disco ISO-9660 e Joliet.

B) UDF: é un subconxunto do formato ISO-13346 con extensións para formatos como CD-R e DVD-R/RW. UDF está incluído na especificación DVD e é máis flexible que o CDFS.

C) FAT12, FAT16, e FAT32: Windows é compatible co sistema de ficheiros FAT por compatibilidade con MS-DOS e outras versións de Microsoft Windows. O formato FAT (*File Allocation Table*) inclúe un mapa de bits que se utilizan para identificar clústers ou bloques no disco.

FAT32 ten unha capacidade teórica para direccionar volumes de 8 terabytes (TB); non obstante limita os volumes a un máximo de 32 GB.

D) NTFS (*New Technology File System*): é o formato nativo de Windows Server para os sistemas de ficheiros. NTFS utiliza enderezos de disco de 64 bits, co que podería xestionar volumes de ata 16 exabytes; así e todo, Windows limita o tamaño dun volume NTFS ao que se poida direccionar con 32 bits, que é un pouco menos de 256 TB (con clústeres de 64 KB). NTFS admite ficheiros de máximo 16 TB.

NTFS engade características de seguridade de ficheiros e directorios, cotas de disco, compresión de ficheiros, enlaces simbólicos baseados en directorios e cifrado. Unha das súas características máis significativas é a

recuperabilidade: rexistra os cambios que se realizan nos metadatos coma se fosen transaccións coa finalidade de que se poidan recuperar no caso da perda de ficheiros ou dos seus datos.

A estrutura central de NTFS é a táboa mestra de arquivos MFT (*Master File Table*), que é unha sucesión lineal de rexistros de tamaño fixo (1 KB). Cada rexistro de MFT describe un arquivo ou un directorio, contén os atributos do arquivo, como o seu nome e marcas de tempo, e a lista de enderezos de disco onde están os seus bloques. Se un arquivo é demasiado grande pode ser necesario empregar máis dun rexistro MFT para conter a lista de todos os bloques. Neste caso, o primeiro rexistro denomínase rexistro base, e apunta aos demais rexistros MFT.

### **53.3.7 Seguridade**

O administrador de seguridade, compoñente do Executive, fai que se respecte o complexo mecanismo de seguridade de Windows 2008, que satisfai os requisitos C-2 do Libro Laranxa do Departamento de Defensa de Estados Unidos.

Cada usuario e grupo de Windows 2008 identifícase cun SID (*Security ID*) único no mundo. Cada proceso leva asociado unha ficha de acceso que especifica o seu SID e outras propiedades.

Cada obxecto ten asociado un descriptor de seguridade que indica quen pode realizar que operacións con el. Un descriptor de seguridade está formado por un encabezado, seguido dunha DACL (*discretionary Access Control List*) cun ou máis elementos de control de acceso (ACE). Os máis importantes son *Allow* e *Deny*. Ademais do DACL, o descriptor ten unha SACL (*System Access Control List*) que non especifica quen pode usar o obxecto, senón que operacións co obxecto se asentán no rexistro de sucesos de seguridade do sistema (función de auditoría).

Nun sistema autónomo a validación corre por conta do proceso *winlogon* e a configuración de seguridade almacenada na propia máquina nas claves do rexistro: SECURITY e SAM. A primeira establece as políticas globais de seguridade e a segunda a seguridade específica de cada usuario.

Nun sistema en rede, a autenticación dos usuarios está centralizada en certos servidores denominados controladores do dominio. Os equipos organízanse dentro de dominios, podendo estes estar xestionados mediante o emprego do *Active Directory*.

Windows 2008 dispón de administración centralizada de certificados. Nas versións anteriores confiábase en que cada aplicación mantiña a súa propia lista de claves ou CA fiables.

O protocolo KERBEROS (RFC 1510), que é un estándar de internet para autenticación, é o método nativo que empregan os sistemas Windows 2008. Calquera servidor do Directorio Activo, automaticamente, ten o servizo do 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*, 5<sup>th</sup> Edition. Mark E. Russinovich, David A. Solomon, Alex Ionescu. Microsoft Press, 2009.

**Autor:** Francisco Javier Rodríguez Martínez

Subdirector de Sistemas Escola Superior Enxeñaría Informática Ourense  
Colexiado do CPEIG

## **54. SERVIDORES DE MENSAXERÍA. SISTEMAS DE CORREO.**



## Tema 54.- Servidores de Mensaxería. Servidores de Correo

---

### **ÍNDICE**

#### **Tema 54.- Servidores de Mensaxería. Servidores de Correo**

##### **54.1 Servidores de Mensaxería**

##### **54.2 Servidores de Correo**

##### **54.3 Bibliografía**

### **54.1 SERVIDORES DE MENSAXERÍA**

Un servidor de mensaxería é unha aplicación que posúe a capacidade de manexar mensaxes entre dúas ou máis entidades, xa sexan aplicacións de usuario ou outros sistemas de xestión de mensaxes. As mensaxes dun servidor de mensaxería son enviadas a través dun *middleware*, o cal facilita a comunicación entre os distintos elementos do sistema utilizando normalmente un conxunto de regras e especificacións que posibilitan a comunicación entre as distintas partes. Outra das características dos servidores de mensaxería é a capacidade de almacenaxe das mensaxes; este almacenamento prodúcese polo xeral nunha cola, ata que é posible o seu envío cara ao seu destinatario que, normalmente, resulta ser outra aplicación.

É moi habitual atopar nunha empresa ou organización un sistema de mensaxería funcionando nun servidor e esperando o envío de mensaxes á súa cola de entrada. Desde alí, o *middleware* analiza mensaxe a mensaxe e determina o destino de cada unha. Unha vez no servidor, unha mensaxe só ten dúas posibilidades de entrega: ou ser enviada de maneira local, ou que teña que ser redirixida a outro servidor de mensaxería para que sexa el o que realice a entrega. Se a mensaxe vai ser entregada a un destino local, entón é enviada inmediatamente á caixa do correo local. Pola contra, se a mensaxe se determina como remota, o servidor de mensaxería debe enviarlla a outro servidor de mensaxería dentro do seu contorno para que sexa este o que realice a entrega da mensaxe.

Polo xeral, se existen problemas de conexión entre os servidores, ou non é posible determinar a localización do servidor de mensaxería remoto, o usuario que realizou o envío da mensaxe é informado da situación a través

doutra enviada polo servidor de mensaxería. Este tipo de mensaxes adoitan ser só de notificación de que se está a ter problemas co envío da mensaxe, posto que o servidor de mensaxería continuará tentando enviar a mensaxe ata que se esgoten o número máximo de intentos de envío, ou ata que a mensaxe caduque, é dicir, exceda un límite de tempo de estancia no servidor.

Normalmente, os modelos dos servidores de mensaxería adáptanse a unha arquitectura centralizada ou seguen unha solución distribuída.

#### **54.1.1      *Sistema de mensaxería centralizada***

Un sistema de mensaxería centralizada fundaméntase nun núcleo de datos, o cal aloxa todos os recursos e servizos dos servidores que conforman o sistema. Este núcleo de datos permite que calquera usuario do sistema de mensaxería se conecte aos servizos de mensaxería, ben sexa de forma local ou remota.

As características dun sistema de mensaxería centralizado son:

- **Datos:** Todos os datos e a información se atopan albergados e se xestionan desde o núcleo, incluso cando os usuarios establecen unha conexión remota para a súa utilización. Esta centralización facilita en gran medida a administración dos servizos, xa que a fai máis sinxela.
- **Actualizacións:** As actualizacións débense realizar unicamente no núcleo central, onde se atopa todo o sistema.
- **Localización:** O centro de datos engádelle ao sistema dispositivos de illamento da alimentación ou sistemas de alimentación ininterrompida (SAI). Proporciona ademais a posibilidade de ofrecer servizos mesmo cando se produce algunha modo eficaz.

### **54.1.2      *Sistema de mensaxería distribuído***

Un sistema de mensaxería distribuído está formado por unha serie de sucursais repartidas en distintas localizacións conectadas entre si. Cada sucursal posúe un servidor ou servidores de mensaxería con todos os seus servizos de maneira independente do resto de sucursais. Cada un dos servidores de mensaxería realiza o envío das súas mensaxes locais e redirixe aos outros servidores aquelas mensaxes que non son de dominio local e que si son capaces de resolver algún dos outros servidores.

- **Datos:** A información atópase tamén distribuída entre cada unha das sucursais e cada unha delas xestiona e administra esta información e os seus servizos, o que provoca un aumento na complexidade destas tarefas.
- **Actualizacións:** Cada vez que se leva a cabo unha tarefa de actualización esta tense que realizar en cada unha das sucursais para que teña efecto en todo o sistema.
- **Localización:** Cada sucursal posúe o seu propio centro de datos, os cales poden ofrecer os mesmos servizos que nunha arquitectura centralizada.

## **54.2    *SERVIDORES DE CORREO***

Un servidor de correo é unha aplicación que nos permite enviar mensaxes (correos) duns usuarios a outros, con independencia da rede que os devanditos os usuarios estean a utilizar.

Para logralo defínense unha serie de protocolos, cada un cunha finalidade concreta:

- *SMTP, Simple Mail Transfer Protocol*: É o protocolo que se utiliza para que dous servidores de correo intercambien mensaxes.
- *POP, Post Office Protocol*: Utilízase para obter as mensaxes gardadas no servidor e pasarllas ao usuario.
- *IMAP, Internet Message Access Protocol*: A súa finalidade é a mesma que a de POP, pero o funcionamento e as funcionalidades que ofrecen son diferentes.

Así pois, un servidor de correo consta en realidade de dous servidores: un servidor SMTP, que será o encargado de enviar e recibir mensaxes, e un servidor POP/IMAP, que será o que lles permita aos usuarios obter as súas mensaxes.

Para obter as mensaxes do servidor, os usuarios sérvense de clientes, é dicir, programas que implementan un protocolo POP/IMAP. Nalgunhas ocasións o cliente execútase na máquina do usuario, mais existe outra posibilidade: que o cliente de correo non se execute na máquina do usuario; é o caso dos clientes vía web.

O correo electrónico é unha das aplicacións TCP/IP máis utilizadas nestes días. Na súa forma máis sinxela, o correo electrónico é unha maneira de enviar mensaxes ou cartas electrónicas dun computador a outro.

O correo electrónico de internet implementouse orixinalmente como unha función do protocolo FTP. En 1980 Suzanne Sluizer e Jon Postel realizaron traballos cun protocolo que posteriormente se denominaría SMTP (*Simple Mail Transfer Protocol*). Hoxe en día séguese a utilizar este protocolo, cos avances lóxicos que require o tipo de transferencia actual.

O protocolo SMTP foi desenvolvido pensando en que os sistemas que intercambiarían mensaxes serían grandes computadores, de tempo compartido e multiusuario, conectadas permanentemente á rede internet.

Mais, coa aparición dos ordenadores persoais, que teñen unha conectividade ocasional, fíxose necesaria unha solución para que o correo chegase a estes equipos. Para resolver esta limitación, nacen os protocolos POP e IMAP.

Xa que logo, podemos discriminar dous tipos de axentes que están implicados na transferencia de correo, MUA e MTA:

- Axente de usuario (MUA), interface para ler e escribir as mensaxes; son os clientes finais.
- Axente de transporte (MTA ou estafeta), encargado do transporte das mensaxes (SMTP). O primeira MTA ao que o cliente lle entrega o seu correo, chámase MSA (S de *sending*), e o última, que o recibe e llo entrega ao cliente destinatario chámase MDA (D de *delivering*)
- Cando un MTA non é o destinatario dun correo, débello entregar a outro, e así ata chegar ao seu destino. Este comportamento é coñecido como **Relay**.

É moi importante configurar ben a función Relay dun MTA, porque se se configura de forma aberta, pode terminar sendo unha fonte de SPAM.

#### **54.2.1      *Sistemas de correo electrónico: arquitectura***

Os sistemas de correo electrónico configúranse para que traballen de forma asíncrona na comunicación, de forma que o cliente envía unha mensaxe e non ten que agardar resposta. Deste xeito, as caixas do correo e as funcións de transmisión e recepción de mensaxes sitúanse nun servidor de correo.

O servidor de correo permanece “á escoita” de conexións doutros servidores de correo para a recepción de mensaxes con destino aos seus usuarios; almacena as mensaxes de correo recibidas nas caixas do correo e realiza a transmisión de mensaxes dos usuarios a outros servidores remotos, é dicir, o servidor de correo actúa como un MTA.

Os usuarios dun servidor interactuarán con el a través dun cliente de correo. Para a recuperación de mensaxes utilízase POP3 ou IMAP4. O envío de mensaxes non se realizará directamente aos servidores remotos, senón que, en primeiro lugar, se lle envía a mensaxe ao servidor de correo que lle dá servizo mediante SMTP, e será este servidor o que realice a transmisión definitiva da mensaxe ao servidor de correo remoto que albergue a caixa do correo destino.

Tendo en conta isto, a arquitectura dun sistema de correo inclúe:

- Servidores de correo para o envío, recepción e almacenamento da información dos usuarios. Deberán estar correctamente configurados para poder ser alcanzables no DNS.
- Clientes de correo utilizados polos usuarios para, esencialmente, compoñer e ler os correos electrónicos.
- Soporte para plataformas de acceso: hoxe en día pódese acceder desde o posto de traballo na intranet da empresa, desde un equipo portátil na extranet, o desde smartphones e PDA.
- Sistema de almacenamento das mensaxes nas respectivas caixas do correo.
- Sistema de Directorio (*Active Directory* ou LDAP) útiles para acceder á información dos usuarios da empresa (nome, cargo, etc.).

### **Clientes de correo**

Os clientes de correo permítenlles aos usuarios interaccionar co sistema para enviar e recibir mensaxes. Desde os inicios do correo electrónico ata hoxe en día, podemos clasificar os clientes en:

- Clientes en modo texto: é o cliente accesible desde a interface de comandos Shell mediante unha conta na máquina que alberga o servidor de correo.
- Clientes pesados: software que se instala no PC do usuario e xestiona todo o ciclo de vida da creación, envío e recepción de mensaxes, así como a posibilidade de almacenamento local; por exemplo, Microsoft Outlook, Lotus Notes Thunderbird, etc.
- Clientes lixeiros: non fai falta instalar ningún software no PC, senón que o usuario accede ao sistema de correo a través dunha interface web cun navegador. A seguridade na comunicación pódese implementar mediante SSL.
- Clientes en smartphones ou PDA: Permiten acceder ás mensaxes en calquera lugar e a calquera hora. Normalmente configúranse con IMAP4 como protocolo de recuperación para permitir que, posteriormente, as mensaxes procesadas sexan visibles tamén desde o PC.

### **Servidores de correo**

Ata hai poucos anos a un servidor de correo pedíase que xestionase correctamente o servizo do correo. Actualmente, téndese a proporcionar unha solución unificada de mensaxería para unha organización que integre mensaxería móbil, mensaxería instantánea, *groupware*, etc., de tal xeito que a fronteira entre servidores puros de correo electrónico e servidores xerais de mensaxería ou contorno colaborativo está pouco clara.



Para escoller un servidor ou outro cumpriría ter en conta as seguintes consideracións:

- O cliente que se asocia ao servidor, xa que algúns servidores esixen un tipo determinado de cliente, como Lotus Notes.
- Estreitamente relacionado co anterior punto está a integración de servidor e cliente e, polo xeral, obtense unha mellor integración cando o servidor e o cliente son do mesmo fabricante, como sucede con Microsoft Outlook e Microsoft Exchange Server, ou Lotus Notes e Lotus Domino.
- O nivel de xestión requirido, a solución de almacenamento e a dispoñibilidade. Para unha organización pode resultar insuficiente tocante a rendemento, flexibilidade e escalabilidade utilizar os discos dunha máquina para almacenar as caixas do correo, así que é máis habitual contar con dispositivos de almacenamento dedicados como solucións NAS ou SAN, con conexións rápidas de fibra óptica e que, ademais, facilitan o uso de clústeres activo/activo ao permitiren que un servidor asuma as caixas do correo xestionadas por outro en caso de caída.
- É importante utilizar técnicas de *benchmarking* para avaliar as seguintes características:
  - o A capacidade de tratar correo concorrentemente.
  - o A velocidade de entrega.
  - o A extensibilidade e funcións implementadas.
  - o A estabilidade.
- Ao tratarse dunha aplicación vital para unha organización, o correo electrónico debe ser configurado como unha solución de alta

dispoñibilidade, o cal require o establecemento de políticas de redundancia adecuadas para garantir o servizo.

Actualmente, os programas servidor de correo máis estendidos son:

- Microsoft Exchange Server.
- Lotus Domino/Notes.
- Sendmail.

#### **54.2.2 SMTP (Simple Mail Transfer Protocol)**

O significado das siglas de SMTP é “Protocolo Simple de Transmisión de Correo”. Este protocolo é o estándar de internet para o intercambio de correo electrónico. SMTP necesita que o sistema de transmisión poña á súa disposición unha canle de comunicación fiable e con entrega ordenada de paquetes, para o cal o uso do protocolo TCP (porto 25) na capa de transporte é o adecuado. Para que dous sistemas intercambien correo mediante o protocolo SMTP non é preciso que exista unha conexión interactiva, xa que este protocolo usa métodos de almacenamento e reenvío de mensaxes.

Realmente son tres os estándares que se aplican a un envío de correo desta clase. O termo SMTP é frecuente e erroneamente usado para se referir á combinación do grupo dos tres estándares involucrados no envío de correo electrónico. Isto débese a que os tres están estreitamente relacionados, pero falando estritamente, SMTP é un dos tres estándares. Os tres estándares son:

- Un estándar para o intercambio de correo entre dous computadores que especifica o protocolo usado para enviar correo entre "host" TCP/IP. Este estándar é SMTP e está definido orixinalmente no RFC 821; foi actualizado nos RFC 2821 e RFC 5321 (outubro 2008).

- Un estándar do formato da mensaxe de correo, contido en dous RFC:
  - o RFC 822 describe a sintaxe das cabeceiras do correo electrónico e describe a interpretación do grupo de campos da cabeceira. Este protocolo foi actualizado nos RFC 2821 e 5322.
  - o RFC 1049 describe cómo un conxunto de documentos de tipos diferentes do texto ASCII plano se poden usar no corpo do correo. Os estándares son PostScript, Scribe, SGML, TEX, TROFF e DVI. O nome do protocolo oficial para este estándar é MAIL.
- Un estándar para o encamiñamento de correo usando o DNS (sistema de nomes de dominio), descrito en RFC 974. O nome oficial do protocolo para este estándar é DNS-MX.

## **Funcionamento**

O protocolo SMTP é un protocolo cliente/servidor, polo que sempre é o usuario SMTP o que inicia a sesión e o servidor de correo o que responde.

O protocolo SMTP baséase na entrega de mensaxes extremo a extremo. Cando un servidor de SMTP require transmitir unha mensaxe a outro servidor SMTP, o emisor (servidor que inicia a sesión SMTP) establece unha conexión co receptor (servidor que recibe petición de establecer sesión SMTP). Esta conexión é unidireccional; é dicir, o emisor pódelle enviar correo ao receptor, pero durante esa conexión o receptor non lle pode enviar correo ao emisor. Se o receptor ten que lle enviar correo ao emisor, ten que agardar a que finalice a conexión establecida e establecer outra en sentido contrario, cambiando os papeis de emisor e receptor. Unha vez establecida a conexión, o emisor envía comandos e mensaxes.

O protocolo SMTP funciona con comandos e respostas de texto escritas en ASCII-NVT (estándar USA - 7 bits).

Cada comando envíase ao servidor SMTP, ao porto 25, de maneira predeterminada. A cada comando enviado polo cliente séguelle unha resposta do servidor SMTP composta por un código numérico de tres díxitos, seguido dunha mensaxe descritiva. O número está pensado para un procesado automático da resposta, namentres que o texto permite que un humano interprete a resposta.

No protocolo SMTP todas as ordes, respostas e datos son liñas de texto, delimitadas polo carácter CRLF. Todas as respostas teñen un código numérico ao comezo da liña.

### **Fluxo**

Os pasos fundamentais para traballar co correo electrónico utilizando este protocolo son os seguintes:

- O cliente SMTP conéctase ao servidor SMTP, realizando un telnet polo porto 25 e agarda resposta.
- O servidor SMTP pode responder.
  - o “220 Service Ready”, xunto co nome de dominio do servidor, se o servizo de correo está dispoñible.
  - o “421 Service not available”, se o destinatario é temporalmente incapaz de responder.
- Se o servizo está dispoñible, o cliente tense que identificar. Para iso envía o comando HELO seguido polo nome de dominio do seu equipo. Desde abril de 2001, as especificacións para o protocolo SMTP, definidas en RFC 2821, indican que o comando HELO sexa substituído polo comando EHLO.
  - o Un receptor SMTP que non soporte o RFC 2821 responderá cunha mensaxe “*500 Syntax error, command unrecognized*”. O

emisor SMTP debería intentalo de novo con HELO ou, se non pode retransmitir a mensaxe, enviar unha mensaxe QUIT.

- o Se un receptor SMTP soporta as extensións de servizo, responde cunha mensaxe "250 OK" que inclúe unha lista das extensións de servizo que soporta.
- O emisor inicia agora unha transacción enviándolle o comando MAIL FROM: ao servidor. Este comando contén a ruta de volta ao emisor que se pode empregar para informar de erros. Se se acepta o comando, o receptor responderá cunha mensaxe "250 OK". Calquera outro código indica erro.
- O segundo paso do intercambio de correo consiste en darlle ao servidor SMTP o destinatario da mensaxe (pode haber máis dun receptor). Isto faise enviando un ou máis comandos "RCPT TO: <destinatarios>" (se hai máis dun destinatario estes irán separados por comas. Cada un deles recibirá unha resposta "250 Recipient OK", se o servidor coñece o destino, ou un "550 Non such user here" se non.
- O seguinte paso é informar o servidor de que se vai empezar a introducir o corpo da mensaxe; para iso utilízase a orde DATA.
- O servidor contesta con "354 Start mail input, end with <CRLF>.<CRLF>", onde se indica que o final da mensaxe se debe finalizar cun punto nunha única liña, seguido dun retorno de carro.
- O cliente envía os datos liña a liña, acabando coa liña <CRLF>. <CRLF> que o servidor recoñece con "250 OK" ou a mensaxe de erro apropiada se calquera cousa foi mal.
- Unha vez que o servidor recibe a mensaxe finalizada cun punto pode almacenala se é para un destinatario que pertence ao seu dominio,

ou ben retransmitirla a outro servidor para que finalmente chegue a un servidor do dominio do receptor.

- Agora hai varias accións posibles:
  - o O emisor non ten máis mensaxes que enviar; pechará a conexión cun comando QUIT, que será respondido con "221 Service closing transmission channel".
  - o O emisor non ten máis mensaxes que enviar, pero está preparado para recibir mensaxes (se os hai) do outro extremo. Mandará o comando TURN. Os dous SMTP intercambian os seus papeis e o emisor que era antes receptor pode enviar agora mensaxes.

Se se require autenticación TLS/SSL a conexión realízase aos portos 465 ou 587, en vez do porto 25.

### **54.2.3 POP (Post Office Protocol)**

O protocolo de oficina de correo, POP, é un protocolo que ten como misión a entrega final do correo ao destinatario; non serve para enviar correos nin para envialos. O seu obxectivo principal é poder xestionar os correos sen ter que estar conectado a internet, é dicir, permítelles aos usuarios con conexións intermitentes ou moi lentas (p. ex., módem), descargar o correo electrónico namentres teñen conexión e revisalo posteriormente ata estando desconectados.

#### **Modelo de comunicacións POP**

A descrición do protocolo POP podémola atopar no RFC 1939. A última versión do POP é a 3, por iso é habitual referirse a este protocolo como POP3.

O protocolo POP3 é un protocolo cliente/servidor, polo que sempre é o usuario POP3 o que inicia a sesión e o servidor de correo o que responde.

O protocolo POP3 funciona con comandos e respostas de texto escritas en ASCII.

O cliente POP conéctase co servidor a través do porto TCP, 110. Para conectarse ao servidor, é necesario unha conta de identificación nesta máquina (o que lle permite ter un espazo reservado para os seus correos). Deseguido cómpre verificar que é dono da conta a través dunha clave. Unha vez conectado ao sistema, o cliente POP pode dialogar co servidor para saber, entre outras cousas, se existen mensaxes na caixa, cantos mensaxes son, ou para solicitar a descarga dalgunha delas.

Cando a conexión TCP está establecida, POP3 continúa con tres fases:

- **Autorización:** Envíase o login e password para identificar o usuario que quere ler o correo. Cando se verifica que o nome e a clave son correctos, o servidor pasa a un estado de transacción. Antes de pasar a este estado, o servidor POP bloquea a caixa do correo para impedir que os usuarios modifiquen ou borren o correo antes de pasar ao estado seguinte.
- **Transacción:** Prodúcese a manipulación do contido da caixa do correo do usuario.
- **Actualización:** Todas as modificacións se realizan cando o cliente finaliza o servizo (co comando QUIT).

Polo tanto, o protocolo POP3 administra a autenticación utilizando o nome de usuario e o contrasinal. Non obstante, isto non é seguro, xa que os contrasinais, do mesmo xeito que os correos electrónicos, circulan pola rede como texto plano, sen cifrar. En realidade, segundo RFC 1939, é posible cifrar o contrasinal utilizando un algoritmo MD5 e beneficiarse

dunha autenticación segura. Aínda así, debido a que este comando é opcional, hai poucos servidores que o implementen. Ademais, o protocolo POP3 bloquea as bandexas de entrada durante o acceso, o que significa que é imposible que dous usuarios accedan de maneira simultánea á mesma bandexa de entrada.

## **Fluxo**

Os pasos fundamentais para traballar co correo electrónico utilizando este protocolo son os seguintes:

- O cliente establece unha conexión TCP no porto 110 do servidor POP.
- O servidor POP responderá cun indicador de estado e unha palabra clave. Se o servizo está dispoñible responderá co indicador de estado +OK; en caso contrario responderá con -ERR.
- Se o servizo está dispoñible pásase á fase de autorización e o cliente identifícase cos comandos USER e PASS.
- Se a información é correcta, o servidor responderá con +OK e dá acceso exclusivo á caixa do correo.
- O cliente pode interactuar coa caixa do correo; para iso utiliza os seguintes comandos
  - o LIST mostra os correos que hai na caixa e o seu tamaño.
  - o STAT dá o número de correos non borrados na caixa e a súa lonxitude total.
  - o TOP <nº\_mens> <num\_liñas> mostra n liñas do correo; o seu número dáse no argumento. No caso dunha resposta positiva do servidor, este enviará de volta os encabezados do correo, despois unha liña en branco e finalmente as primeiras n liñas do correo.



- o RETR <nº\_mens> recolle un correo especificado polo seu número.
  - o DELE <nº\_mens> borra un correo especificado polo seu número.
  - o RSET recupera os correos borrados (na conexión actual).
  - o UIDL obtén a listaxe con todos os identificadores únicos de mensaxes. O servidor asígnalle un identificador único a cada mensaxe, de modo que non cambie o seu identificador entre sesións. Este identificador é o UID.
- Para rematar a sesión POP utilízase o comando QUIT. Elimínanse aquelas mensaxes que foron marcadas co comando DELE. Ata que non se invoca a orde QUIT, as mensaxes marcadas non son borradas da caixa do correo.

Se se require autenticación TLSSSL a conexión realízase ao porto 995, non ao porto 110.

#### **54.2.4 IMAP - Internet Message Access Protocol**

O protocolo IMAP (Protocolo de acceso a mensaxes de internet) é un método utilizado polas aplicacións cliente de correo electrónico para obter acceso ás mensaxes almacenadas remotamente. Neste caso, as mensaxes non son recuperadas polo xestor de correo, senón que se traballa con elas directamente sobre o servidor.

É un protocolo máis complexo que POP3. Algunhas vantaxes sobre o anterior son:

- As transaccións IMAP poden durar moito máis tempo.
- O servidor garda información do estado dos mails (se foron lidos ou non, se foron gardados nunha carpeta, etc.).

- Pódense definir distintas carpetas para acceder a distintas caixas do correo.
- Pódenselle devolver partes da mensaxe ao cliente, aforrando ancho de banda.
- Pódese conectar máis dun cliente á mesma caixa do correo.
- Posúe buscadores que se executan no servidor.
- A diferenza de POP (onde o Cliente debe estar conectado ao Servidor para que se realicen os cambios), IMAP permítelles aos Clientes realizaren cambios tanto estando estes conectados como desconectados.
- É totalmente compatible con diferentes estándares de mensaxes de Internet, como MIME.

Con todo, posúe certas desvantaxes:

- É máis complexo de implementar que POP3.
- O servidor debe ser máis potente para atender a todos os usuarios. Consome máis recursos de CPU, memoria, etc.

O protocolo IMAP é un protocolo cliente/servidor, polo que sempre é o usuario IMAP o que inicia a sesión e o servidor de correo o que responde.

Os clientes IMAP poden acceder seguindo un destes tres modos de conexión:

- **Modo offline.** Periodicamente conéctase ao servidor para descargar mensaxes novas e sincronizar calquera cambio que se poida producir nas diferentes carpetas. Existe a posibilidade de borrar as mensaxes

a medida que as descargamos, seguindo un funcionamento moi semellante a POP3.

- **Modo online.** Accédese directamente á copia das mensaxes do servidor exactamente cando fai falta, sincronizando os cambios practicamente ao instante.
- **Modo desconectado.** Neste caso o cliente traballa cunha copia local namentres que non ten acceso a internet, creando/borrando/lendo os seus emails. A próxima vez que se conecte a Internet estes cambios han sincronizarse coa copia mestra do servidor.

O protocolo IMAP funciona con comandos e respostas de texto escritas en ASCII. Actualmente a versión operativa é a 4 por iso este protocolo tamén se coñece como IMAP4.

Dado que se parte dun modelo no que as mensaxes se gardan normalmente no servidor despois de ser lidas, IMAP define unha maneira sinxela de administralas: con caixas do correo, é dicir, con carpetas. Estas seguen unha xerarquía de tipo árbore. Seguindo o estándar, sempre existirá unha caixa do correo de entrada que será a principal, pero poderemos crear outras carpetas con diferentes atributos. Por exemplo, existen atributos para especificar que unha carpeta contén só correos (*\NoInferiors*) ou só carpetas (*\NoSelect*), pero tamén poden ter outros atributos que indiquen se existen ou non mensaxes novas desde a última vez que a abrimos (*\Marked* e *\Unmarked*).

Unha clase parecida de etiquetas poden ter os correos que se reciban e/ou envíen. Unha das máis usadas será a que indica se está lido ou non (*\Seen*), pero tamén existen outras que indican que a mensaxe foi contestada (*\Answered*), que a mensaxe foi destacada (*\Flagged*), que é un borrador (*\Draft*), etc... Toda esta información se garda directamente no servidor e

non no cliente, o que permite sincronizar perfectamente estes metadatos entre varios clientes.

Na RFC 2060 (actualmente, a RFC 3501) defínense as instrucións para poder interactuar co servidor de correo e as súas caixas do correo.

Fases dunha Sesión IMAP. Do mesmo xeito que no POP3, nunha sesión IMAP existen as seguintes fases:

- *Non-authenticated state*: Neste estado o Cliente aínda non se autenticou co Servidor.
- *Authenticated state*: O Cliente foi autenticado polo Servidor e debe seleccionar unha caixa do correo para interactuar.
- *Selected state*: O cliente seleccionou unha caixa do correo e pódense realizar accións sobre os correos contidos nela.
- *Logout state*: A conexión foi finalizada.

## **Fluxo**

Os pasos fundamentais para traballar co correo electrónico utilizando este protocolo son os seguintes:

- O cliente establece unha comunicación TCP co servidor IMAP polo porto 143.
- O servidor responde con OK se o servizo está dispoñible; en caso contrario o servidor responderá con BAD.
- Deseguido, o cliente tense que identificar mediante o comando LOGIN <usuario> <password>, para poder acceder ás caixas do correo. Esta é unha forma non segura, porque a password non vai cifrada. Pódese utilizar o comando AUTHENTICATE para autenticar o usuario de forma segura.

- Se os datos son correctos o servidor responde OK. Se se produce un fallo de autenticación devolverá un NON. Se os argumentos non son válidos devolverá un BAD.
- Agora o cliente pode interactuar coas súas mensaxes. Para iso usa os comandos:
  - o LIST para ver as caixas do correo existentes.
  - o SELECT <nome\_caixa do correo> para ver o contido dunha caixa do correo determinada.
  - o CREATE <nom\_caixa do correo\_nova> para crear caixas do correo.
  - o DELETE <nome\_caixa do correo> para borrar caixas do correo.
  - o RENAME <nome\_caixa do correo\_old> <nome\_caixa do correo\_new> para renomear caixas do correo.
  - o FETCH <num\_mens> <parte\_mens> para ver as diferentes partes das mensaxes da caixa do correo que se seleccionou.
  - o CLOSE pecha a caixa do correo e borra as mensaxes marcadas para borrar.
  - o EXPUNGE borra todas as mensaxes marcadas para borrar.
  - o SEARCH busca mensaxes segundo algún criterio de busca.
  - o COPY copia as mensaxes dunha carpeta a outra.
- Co comando LOGOUT remata a sesión.

Se se require autenticación TLS/SSL a conexión realízase ao porto 993, non ao porto 143.

#### **54.2.5      *Formato de mensaxes en internet***

A RFC 2822 define o estándar do formato de mensaxe de Internet. O correo electrónico divídese en dúas partes separadas por unha liña en branco.

- A cabeceira da mensaxe.
- O corpo da mensaxe.

**Corpo da mensaxe.** Contén a información que se intercambian o emisor e o receptor. A forma en que está codificada vén determinada polo RFC 2231.

**Encabezados da mensaxe.** É a metainformación colocada antes do corpo da mensaxe. En xeral, o software de transporte de correo non revisa nin altera os encabezados do correo, a excepción da cabeceira *Received*. Están formadas pola tupla Palabra\_clave: valor. As cabeceiras máis importantes son:

- From: Enderezo do emisor da mensaxe.
- Reply-to: Conta de correo a onde se dirixirán as respostas ao correo. En ausencia deste campo as respostas diríxense a o/s enderezo/s indicados no campo From.
- To: Este campo contén o/s enderezos do/s principal/is destinatario/s da mensaxe.
- Cc: Copia a destinatarios. Campo que indica o/s enderezo/s aos que se lles fará chegar unha copia do correo, aínda que o contido da mensaxe poida que non vaia dirixido expresamente a eles.
- Bcc: Copia oculta. Mándaselles unha copia aos destinatarios aquí indicados sen que o resto de destinatarios teñan coñecemento diso.

- Message-IDE: É un identificador único de cada mensaxe. Este código é asignado polo servidor de onde sae a mensaxe. Este identificador non se pode cambiar nin modificar.
- Reference: Contén todos os Message-IDE das mensaxes ás que este fai referencia. Este campo é xerado pola aplicación cliente.
- KeyWords: Palabras crave que identifican o contido da mensaxe.
- Return-Path: Contén a traxectoria de regreso ao remitente.
- Received: É a información que se utiliza para comprobar os problemas que puidesen ter aparecido na repartición dunha mensaxe. Nela móstranse os enderezos das máquinas polas que pasou a mensaxe en dirección ao seu destino, xunto coa data e hora en que o fixo.
- Date: Data e hora na que a mensaxe é entregada á cola do servidor SMTP para o seu envío. Este campo establéceo o servidor orixe.
- Subject: Este campo contén un pequeno texto coa descrición do asunto da mensaxe.
- X- : Son campos definidos polo usuario. Sempre teñen que empezar por X-, seguidos do nome que se lle queira asignar ao campo. Por exemplo, X-mailer: “O meu xestor de correo”. Estase utilizando unha cabeceira X-SPAM para marcar correos como presuntos correos lixo.

Só as cabezas subliñadas son obrigatorias segundo o estándar.

#### **54.2.6      *Extensións de SMTP***

##### **54.2.6.1      ESMTP**

O protocolo ESMTP é unha extensión do protocolo SMTP, definido na RFC 4954.

Trátase dun mecanismo para autenticar a identidade do cliente que se conecta ao servidor, e ademais permite a negociación dunha capa de seguridade para facer máis segura a comunicación. O protocolo SMTP permanece inalterado; o que se fai é agregar os seguintes comandos:

- EHLO dominio: Fai que o servidor realice unha consulta ao DNS do reverso do dominio indicado para verificar que este exista.
- ETRN dominio (*Extended Turn*). Este comando permite que o cliente lle pida ao servidor que lle envíe todas as mensaxes que posúe destinadas ao cliente. Se hai mensaxes para a máquina cliente, o servidor debe iniciar unha nova sesión SMTP para enviarlle as mensaxes.
- AUTH: Comando que serve para negociar un protocolo de seguridade para o intercambio de datos. Os posibles protocolos, para a capa de seguridade, que se poden negociar dáos como resposta o servidor ao comando EHLO.

#### 54.2.6.2 MIME

O protocolo SMTP impón determinadas restricións sobre o contido das mensaxes:

- O contido só debe estar composto de caracteres ASCII; non se pode enviar ficheiros binarios como audio, vídeo, documentos, etc.
- As liñas non poden exceder os 100 caracteres.
- O tamaño total do contido non pode exceder unha determinada dimensión.
- Ademais, tamén existen problemas á hora de enviar mensaxes en linguaxes distintas do inglés:
  - o Linguaxes sen alfabetos “occidentais” (chinés, xaponés)



- o Linguaxes con alfabetos non latinos (ruso, árabe)
- o Linguaxes con acentos (alemán, castelán)

Para resolver estas limitacións definíronse as especificacións MIME (*Multipurpose Internet Mail Extensions*) que son unhas extensións do correo electrónico, utilizadas tamén noutros protocolos coma o HTTP, que permiten a transmisión de datos non ASCII, a través de e-mail, no corpo da mensaxe.

MIME non cambia a SMTP nin o substitúe, polo que as mensaxes que se envíen con MIME tamén cumprirán este protocolo. Dado que SMTP utiliza para comandos e respostas o ASCII de 7 bits, o camiño seguido para transmitir calquera ficheiro é transformar (codificar) o ficheiro non ASCII en ASCII de 7 bits (facéndoo compatible con SMTP), transmitilo neste formato e reconvertelo en destino ao formato orixinal (descodificalo).

MIME incorpora as seguintes características ao servizo de correo electrónico:

- Capacidade de enviar múltiples adxuntos nunha soa mensaxe.
- Lonxitude ilimitada da mensaxe.
- Uso de conxuntos de caracteres non pertencentes ao código ASCII.
- Uso de texto enriquecido (deseños, fontes, cores, etc.).
- Adxuntos binarios (executables, imaxes, arquivos de audio ou vídeo, etc.), que se poden dividir de ser necesario.

As cabeceiras descritas na RFC 2822 son suficientes para enviar correo codificado en texto ASCII, pero non son adecuadas para mensaxes multimedia. Para iso MIME engade unhas cabeceiras que describen o tipo de contido da mensaxe e o tipo de código. Estas son:

- **MIME-Version:** Contén a versión das extensións MIME empregadas na mensaxe.
- **Content-Transfer-Encoding:** Sinala como foi codificada a mensaxe para a súa transmisión por e-mail, de forma que poida viaxar sen problemas de que se corrompa desde o destinatario ao receptor a través dos axentes de correo (MUA). Para transferir datos binarios, MIME ofrece cinco formatos de codificación:

- o 7bit: Significa que o ficheiro é SÓ texto ASCII (caracteres non acentuados). As liñas deben ser "curtas", de 100 caracteres ou menos, terminando con CRLF.
- o *Quoted-Printable*: Utilizado por texto que é maioritariamente US-ASCII (7 bit) pero cunha pequena porcentaxe de caracteres "estrañas" (8 bit). Este é o caso do castelán.

Nesta codificación, cada carácter de 8-bits é codificado en tres caracteres de 7 bits; o primeiro o signo igual (=) e o valor hexadecimal do carácter. Por exemplo, o "ñ", "F1" en hexadecimal, codifícase como "=F1".

- o base64: usado para codificar secuencias arbitrarias de octetos de forma que satisfaga as regras de 7bit. Utilízase para enviar binarios.
  - o 8bit: formato de texto de 8 bits.
  - o binary: envío de binarios.
- **Content-Type:** indica que tipos de datos contén a mensaxe. Un tipo de MIME está composto da seguinte forma: tipo\_mime\_principal/subtipo\_mime. Pódense atopar os seguintes tipos:



- o text: texto con ou sen formato.
- o image: imaxes estáticas.
- o vídeo: imaxes dinámicas; pode incluír audio.
- o audio: son.
- o message: significa que o contido está configurado segundo o estándar RFC 822; isto pode ser usado para reexpedir mensaxes.
- o application: emprégase para sinalar que o contido é para serlle enviado a un programa externo; por exemplo, texto para unha impresora PostScript.
- o multipart: unha mensaxe tamén pode ter varias partes con varios contidos separados, mesmo de tipos diferentes (texto, audio e imaxes). Incluso cada parte pode ter subpartes (ser, pola súa vez, multiparte), posto que o formato MIME pode ser recursivo.

Á parte do tipo, tamén se pode especificar un subtipo, ambos os dous separados por unha barra inclinada /. Por exemplo image/gif é unha imaxe en formato GIF; o tipo é imaxe e o subtipo gif; text/html, text/plain, etc.

Se o tipo é *multipart*, os subtipos admitidos son:

- o *mixed*: permite que unha soa mensaxe conteña varias submensaxes independentes, cada unha co seu tipo e codificación. Desta forma pódense incluír nunha mensaxe imaxes, audio, vídeo....

- o *parallel*: permite incluír nunha mensaxe subpartes que se poden ver simultaneamente; por exemplo, reproducir audio e vídeo.
- o *digest*: permite incluír nunha mensaxe varias mensaxes.
- o *alternative*: permite que nunha mesma mensaxe se poida incluír unha única información pero en diversos formatos. Isto é útil cando os destinatarios teñen distinto hardware e/ou sistema operativo.

Finalmente, pode ter parámetros opcionais empezando por un punto e coma ;. Por exemplo, o parámetro `charset=` en `Content-type: text/plain; charset=iso-8859-1`, indica que o corpo da mensaxe utiliza o xogo de caracteres ISO-8859-1.

### **54.3 BIBLIOGRAFÍA**

- *Internet y Correo electrónico*. Silva Salinas, Sonia; López Sanjurjo, Catherin, (aut.) Ideeaspropias Editorial, 2007.
- *Correo electrónico*. Romero Dueñas, Carlos González Hermoso, Alfredo. Edelsa, 2001.

**Autor:** Francisco Javier Rodríguez Martínez

Subdirector de Sistemas Escola Superior Enxeñaría Informática Ourense

Colexiado do CPEIG





# **55. SERVIDORES DE APLICACIÓNS E SERVIDORES WEB.**

## Tema 55.- Servidores Web e Servidores de Aplicacións

---

<b>55.1 Servidores Web.....</b>	<b>2</b>
55.1.1 <i>Introdución Cliente/Servidor.....</i>	2
55.1.2 <i>Servidores Web.....</i>	3
55.1.3 <i>Características dos servidores web.....</i>	4
55.1.4 <i>Arquitectura.....</i>	5
55.1.4.1 <i>Funcionamento do servidor web.....</i>	6
55.1.5 <i>Apache.....</i>	7
55.1.5.1 <i>httpd.conf.....</i>	8
55.1.5.1.1 <i>Directivas de contorno global.....</i>	8
55.1.5.1.2 <i>Directivas de configuración do servidor principal.....</i>	9
55.1.5.2 <i>Módulos de Apache.....</i>	10
55.1.6 <i>Microsoft IIS.....</i>	10
55.1.6.1 <i>Administración de IIS.....</i>	11
55.1.7 <i>Lighttpd.....</i>	12
<b>55.2 Servidores de Aplicacións.....</b>	<b>13</b>
55.2.1 <i>Servizos proporcionados por un servidor de aplicacións.....</i>	15
55.2.2 <i>Estándar J2EE.....</i>	16
55.2.3 <i>Estrutura dun servidor de aplicacións.....</i>	17
55.2.4 <i>Oracle Weblogic (antes BEA WebLogic).....</i>	18
<b>55.3 Servidores de Aplicacións e Servidores Web.....</b>	<b>21</b>
<b>55.4 Bibliografía.....</b>	<b>23</b>

## **55.1 Servidores Web**

### **55.1.1 Introducción Cliente/Servidor**

A tecnoloxía Cliente/Servidor consiste no procesamento cooperativo da información mediante un conxunto de procesadores, no cal múltiples clientes, xeograficamente dispersos, poden realizar peticións a un ou máis servidores centrais.

Desde unha perspectiva funcional, podemos definir cliente-servidor como unha arquitectura distribuída que lles permite aos usuarios obter acceso de forma transparente á información. Este tipo de arquitectura é a máis estendida nos sistemas distribuídos.

Un sistema cliente servidor baséase nas seguintes características:

- *Servizo*: o servidor proporciónaos e o cliente utilízalos.
- *Recursos compartidos*: son moitos os clientes que empregan os mesmos servidores mediante os cales comparten recursos non só lóxicos senón tamén físicos.
- *Protocolos asimétricos*: os clientes son os encargados de iniciar a comunicación co servidor, os cales agardan o establecemento da conexión de forma pasiva.
- *Transparencia de localización*: os clientes non saben onde se localizan fisicamente os recursos que desexan utilizar.
- *Independencia da plataforma*.
- *Sistemas debilmente axustados*: interacción baseada en envío de mensaxes.



- *Encapsulación de servizos*: a implantación que os servidores realizan dos servizos son transparentes para os clientes.
- *Escalabilidade horizontal*: incorporar novos clientes.
- *Escalabilidade vertical*: aumentar a potencia dos servidores.
- *Integridade*: tanto os datos como os programas están centralizados en servidores que facilitan a súa integridade e mantemento.

### **55.1.2 Servidores Web**

Un servidor http ou servidor web é un programa que permite procesar as peticións dos distintos navegadores, servindo os recursos que estes soliciten mediante os protocolos HTTP ou HTTPS. De forma xeral, un servidor web funciona de xeito moi simple, executando constantemente as seguintes accións:

1. Agardar peticións no porto TCP indicado.
  - a. Por defecto empregarase o porto 80.
2. Recibir unha petición.
3. Procesar a solicitude.
4. Enviarlle ao cliente a resposta obtida, empregando a mesma conexión pola que se recibiu a petición.
5. Volver agardar novas peticións.

Se un servidor web se cingue ao patrón anterior, cumprirá todos os requisitos básicos dos servidores HTTP, inda que se verá limitado a servir ficheiros estáticos. Os servidores web existentes na actualidade deseñáronse e configuráronse a partir do patrón anterior, onde a variación

entre eles só radica no tipo de peticións que van atender, se son ou non multiproceso, etc.

### **55.1.3 Características dos servidores web**

- *Servir ficheiros estáticos:* un servidor web debe ser capaz de servir ficheiros estáticos que se localicen nalgún lugar do disco (requisito imprescindible).
  - Debe ser posible especificar que parte do disco se vai servir.
  - Inda que un servidor poida especificar un directorio por defecto, non debe obrigalo a empregar un concreto.
  - En moitos servidores é posible especificar outros subdirectorios ou directorios, indicando en que punto do sistema de ficheiros virtual do servidor irán localizados os recursos.
- *Seguridade:* un servidor web debe poder especificar directivas de seguridade, isto é, establecer quen pode acceder a que recursos.
  - Algúns servidores permiten especificar os ficheiros que se considerarán como índice do directorio.
- *Contido dinámico:* é unha das características fundamentais. Indica a capacidade do servidor para ofrecer contido dinámico.
  - A gran maioría do contido web que se serve é dinámico.
  - Punto fundamental á hora de elixir un servidor.
- *Soporte para distintas linguaxes:* a maior parte dos servidores ofrece soporte para algunhas linguaxes de programación como:
  - PHP
  - JSP: para que un servidor atenda peticións JSP requirirá algún tipo de software para funcionar, como un contedor de Servlets.
  - ASP

- o CGI (sistema máis antigo e sinxelo para xerar contido dinámico)

Antes de seleccionar unha linguaxe de programación de servidor, cómpre considerar se se desexa unha linguaxe máis estándar que poida ser atendida por calquera servidor xenérico, ou ben se se prefire unha arquitectura concreta, etc.

#### **55.1.4      *Arquitectura***

A arquitectura dun servidor web divídese en:

1. Capa servidor
2. Capa soporte

**Capa servidor:** contén 5 subsistemas, cuxa función é a de executar as funcionalidades do servidor.

- *Subsistema de recepción:* é o encargado de agardar polas peticións do cliente a través da rede.
  - o Ten a capacidade de manexar peticións simultáneas, podendo analízalas para determinar se son ou non compatibles co navegador.
- *Analizador de peticións:* asocia ao recurso de rede un arquivo local.
- *Control de acceso:* encárgase de validar e permitir o acceso.
- *Controlador de recursos:* fixa o tipo de recurso que se solicitou, execútao e obtén a resposta.
- *Rexistro de transacción:* a súa función é rexistrar as peticións xunto coas súas respostas.

**Capa soporte:** conforma a interface entre o servidor web e o sistema operativo, e manexa os seguintes subsistemas.

- *Útil:* contén as funcións que empregan os outros subsistemas.

- *Capa abstracta do sistema operativo*: encapsula o funcionamento do sistema operativo para facilitar a portabilidade do servidor entre as diferentes plataformas.

#### 55.1.4.1 Funcionamento do servidor web

Un servidor web execútase agardando peticións por parte dun navegador web (cliente) e atendendo as devanditas peticións de forma axeitada, respondendo mediante unha mensaxe de erro ou unha páxina web coa resposta á petición formulada.

Por exemplo, se tecleamos [www.xunta.es](http://www.xunta.es) nun navegador, o proceso que se desencadea é o seguinte:

- O navegador realiza unha petición HTTP ao servidor do enderezo solicitado.
- O servidor responde enviando o código HTML da páxina solicitada.
- O cliente recibe o código da páxina, interprétao e móstrao en pantalla.

É o cliente o encargado de interpretar o código HTML, mostrar os textos e obxectos da páxina, as súas cores, fontes, etc. O servidor, pola súa banda, limítase a transmitir o código da páxina sen realizar ningún tipo de interpretación da devandita páxina.

Un servidor web, ademais de transmitir código HTML, tamén pode entregar aplicacións web, que son segmentos de código que se executan cando se producen certas peticións ou respostas HTTP.

Cómpre distinguir entre:

1. *Aplicacións no lado do cliente*: é o navegador web o encargado de executar estas aplicacións no equipo do usuario (scripts). Nesta

categoría atopamos aplicacións como Applets de Java ou Javascript.

- O servidor proporciónalle o código destas aplicacións ao cliente e é o navegador deste quen as executa.
- É necesario que o navegador do cliente dispoña da capacidade para executar estas aplicacións.
- Por defecto, a maioría dos navegadores permite executar scripts de java e javascript, inda que mediante plugins se poden engadir máis linguaxes.

2. *Aplicacións no lado do servidor*: é o servidor o encargado de executar a aplicación, a cal, unha vez executada, xera un código HTML que o servidor toma e envía ao navegador do cliente mediante HTTP.

En xeral, a opción que se escolle é a das aplicacións no lado do servidor, xa que, ao executarse no servidor e non no equipo do cliente, este non require ningún tipo de software ou funcionalidade engadida, mentres que no caso das aplicacións no lado do cliente, si que é necesario.

### **55.1.5 Apache**

O servidor Apache é un servidor web de código aberto, que se desenvolve dentro do proxecto HTTP Server da Apache Software Foundation, e que pode ser instalado en plataformas Windows, Unix, Mac e outras. Este servidor vén instalado na maioría das distribucións de Linux e en Mac OS X; Apache vén integrado como parte do seu propio servidor web.

Trátase do servidor web máis empregado, e malia que presenta algunhas vulnerabilidades de seguridade, a gran maioría delas só poderían ser explotadas de forma local e non remotamente.

#### 55.1.5.1 httpd.conf

Apache pode ser configurado mediante o ficheiro *httpd.conf*. Cada vez que se introduza unha modificación neste ficheiro, será necesario reiniciar o servizo Apache. Trátase dun servidor altamente configurable, inda que a súa interface gráfica non é demasiado intuitiva.

O ficheiro de configuración *httpd.conf* pódese dividir en varias seccións:

- *Sección 1*: Contorno global. Sección do ficheiro onde se localizan as rutas a outros ficheiros de configuración e se describe o funcionamento xeral do servidor.
- *Sección 2*: Contorno servidor principal. Sección do ficheiro onde se describe a configuración que non atende as peticións dos servidores virtuais. Trátase do comportamento predeterminado do servidor.
- *Sección 3*: Contorno de servidores virtuais. Sección do ficheiro onde se poden configurar servidores virtuais para traballar co mesmo programa.

##### 55.1.5.1.1 **Directivas de contorno global**

A configuración realízase mediante directivas, variables almacenadas nun arquivo de texto, que permiten alterar e controlar o funcionamento de Apache en función dos valores que estas tomen.

- *ServerType*: permite indicar como será a resposta do servidor.
  - o *Inetd*: execútase cando hai unha petición.
  - o *Standalone*: sempre existe un proceso *httpd* en execución e este crea novos fillos para as conexións cos diferentes clientes.

- *ServerRoot*: permite detallar o directorio que actuará como raíz do servidor.
- *Timeout*: permite especificar o número de segundos que se mantén á espera un servidor, desde que se recibe a petición ata que se entende a conexión como inactiva.
- *MaxClients*: limita o número máximo de clientes que se poden conectar de forma simultánea. Se se supera este número, os clientes son bloqueados.
- *Listen*: permítelle a Apache atender peticións noutra dirección e/ou portos ademais dos establecidos por defecto.
- *BinAddress*: emprégase para especificar que direccións ou IP se deben atender no servidor. Permite dar soporte a servidores virtuais.
- *LoadModule*: permite cargar un novo módulo para proporcionarlle maior funcionalidade ao servidor.

#### **55.1.5.1.2 Directivas de configuración do servidor principal**

- *Port*: permite especificar o porto en que escoitará o servidor. Só pode existir unha directiva *Port*, mentres que se poden especificar varias *Listen*.
- *User e Group*: permite indicar o usuario ou grupo que pode iniciar a execución de httpd.
- *ServerAdmin*: establece o enderezo de correo electrónico onde enviar os problemas que poidan xurdir. Este enderezo mostrarase nas páxinas de erro que xera o servidor.
- *ServerName*: permite asignar o nome do servidor, que lles será mostrado aos clientes. Non é aconsellable empregar o nome real da máquina.
- *ServerSignature on/off/email*: emprégase para que, en caso de acceso

a unha páxina inexistente, o servidor devolva unha páxina de erro indicando a versión de Apache e o nome da máquina.

- *DocumentRoot*: especifica o directorio onde se localizan os documentos web que o servidor poñerá a disposición dos clientes.

#### *55.1.5.2 Módulos de Apache*

Apache é un servidor estruturado en módulos cuxa configuración se realiza mediante a modificación das directivas presentes en cada módulo.

Os módulos de Apache poden ser clasificados nos seguintes grupos:

- Módulos base: módulos que engloban as funcións básicas de Apache.
- Módulos multiproceso: módulos que se encargan da interconexión cos portos do ordenador, aceptando as peticións e enviando as peticións aos distintos fíos para seren atendidas. Módulos adicionais: calquera módulo que incorpore unha funcionalidade ao servidor.

#### **55.1.6 Microsoft IIS**

IIS (Internet Information Services) é un servidor web específico para o sistema operativo Microsoft Windows. IIS converte un ordenador nun servidor web, que permite publicar páxinas web e facelas accesibles localmente, cara a unha intranet ou cara a Internet; ademais, proporciona



as funcións e ferramentas necesarias para realizar de forma sinxela a administración dun servidor web seguro.

IIS baséase en diversos módulos que lle proporcionan a capacidade de servir varios tipos de páxinas, como ASP (Active Server Pages), ASP.NET, PHP ou Perl.

#### 55.1.6.1 Administración de IIS

A última versión de IIS é a 7, aplicable a Windows 7, Windows Server 2008, Windows Server 2008 R2 e Windows Vista.

En IIS7 hai varias ferramentas para realizar a súa administración e configuración, entre as cales se inclúen:

- Administrador de IIS.
- Ferramenta de liña de comandos denominada Appcmd.exe.
- Almacén de configuración de IIS que consta de arquivos ApplicationHost.config e Web.config.
- Espazo de nomes de Instrumental de Administración de Windows (WMI).

### **55.1.7      *Lighttpd***

Lighttpd é un servidor web libre, distribuído baixo a licenza BSD, deseñado para ser rápido, seguro, flexible, e respectuoso cos estándares. Está deseñado para contornos onde a velocidade é moi importante e se requiren respostas rápidas e de alta escalabilidade. Consome menos memoria e procesador que outros servidores.

Algunhas características de lighttpd son:

- Permite a comunicación con programas externos mediante SCGI ou FastCGI.
- Ten un módulo de reescritura e de redirección de URL.
- Fixéronse melloras específicas para a súa integración con PHP e Ruby on Rails.
- Permite módulos externos.
- Permite VirtualHosting.
- Pode servir tanto HTTP como HTTPS.
- Autenticación con LDAP, htpasswd ou MySQL.
- Acepta Webdav.

Lighttpd pódese usar só ou combinado con outros; de feito, é habitual empregalo para liberar de carga a outros servidores máis lentos, especialmente cando hai que realizar o envío de ficheiros grandes, que adoita ser moito máis rápido ca no resto de servidores. É común atopar lighttpd en combinación con instalacións de Apache, para facelo máis escalable e rápido en situacións de carga.

## **55.2 Servidores de Aplicacións**

Por servidor de aplicacións entendemos aquel que permite a execución dunha serie de aplicacións. Habitualmente trátase dun programa software que xestiona case por completo as funcións de lóxica de negocio e de acceso aos datos da aplicación. O seu propósito é xestionar de xeito centralizado a forma en que os clientes se conectan á base de datos ou aos servizos cos que estes deben interactuar.

Os servidores de aplicacións comezan a xurdir cando se fai patente que as aplicacións cliente/servidor ían presentar problemas de escalabilidade cando se tratase de servir a un gran número de usuarios. Ademais, era necesario trasladar as regras de negocio a un lugar intermedio entre os clientes e a base de datos.

O concepto de servidor de aplicacións está moi ligado ao de sistema distribuído, os cales permiten mellorar 3 aspectos fundamentais nunha aplicación:

- *A alta dispoñibilidade:* refírese á necesidade de que un sistema funcione 24 horas ao día, todos os días. Para poder cumprir con esta característica son necesarias técnicas de equilibrio de carga e de recuperación ante fallos.
- *A escalabilidade:* consiste na capacidade de facer crecer un sistema cando aumenta o número de peticións. Cada sistema pode atender un número limitado de peticións, xa que os seus recursos son finitos; ao engadir novos equipos, a cantidade de recursos multiplícase e, con iso, o número de peticións que poden ser atendidas.

- *O mantemento:* ten que ver coa facilidade para realizar actualizacións, depurar fallos e manter o sistema.

### **55.2.1      *Servizos proporcionados por un servidor de aplicacións***

- *Xestión da sesión:* o servidor debe conservar a información entre peticións dun usuario mentres dure a antedita sesión.
  - o Esta é unha característica fundamental para as aplicacións de comercio electrónico, que requiren establecer o usuario a través da súa navegación polo sitio web; con todo, o protocolo http é un protocolo sen sesión, polo que non permite manter unha conexión aberta entre cliente e servidor máis aló do que dura a transferencia de información. Por iso son os servidores de aplicacións os que se encargan de todo o relacionado coa xestión da sesión.
- *Equilibrio de carga:* un servidor de aplicacións debe proporcionar técnicas para equilibrar a súa propia carga, é dicir, debe ser capaz de repartir o procesamento entre diversos servidores, o cal é fundamental para a súa escalabilidade.
  - o As peticións que realizan os clientes transmítense á máquina que estea menos ocupada en cada momento, o que mellorará o rendemento global da aplicación.
  - o Cun bo equilibrio de carga, ademais de conseguir un sistema máis escalable, conséguese unha maior tolerancia a fallos.
- *Acceso aos datos:* un servidor de aplicacións proporciona un acceso sinxelo para realizar a administración das conexións a bases de datos relacionais.
  - o É habitual que tamén permitan o acceso a outros tipos de fontes de datos como:
    - ERP
    - Repositorios XML

- **Sistemas herdados**
  - *Pooling de conexións*: é habitual que os servidores de aplicacións manteñan de forma permanente conexións coas bases de datos. Estas conexións distribúense entre os procesos de forma transparente, xa que sería moi custoso, ademais de influír negativamente no rendemento da aplicación, abrir unha conexión por cada consulta que se queira realizar.
  - *Xestión de transaccións*: as transaccións son fundamentais en calquera software e máis aínda nos de tipo comercial, xa que evitan a aparición de información inconsistente.
    - o Os servidores de aplicacións adoitan contar con esta característica, de maneira que, con indicar en que momento se inicia unha transacción e en que momento se finaliza, o propio sistema se encargaría de desfacer os pasos intermedios no caso de que se produza un erro na aplicación.

### **55.2.2 Estándar J2EE**

As plataformas máis comúns en que se asentan os servidores de aplicacións son J2EE e .NET. J2EE está máis estendida e, ata hai relativamente pouco, era impensable poñer en funcionamento un servidor de aplicacións que non seguisse este modelo.

O estándar J2EE permite desenvolver aplicacións empresariais de forma eficiente e sinxela. O feito de desenvolver unha aplicación con tecnoloxías J2EE permite que esta sexa despregada en calquera servidor de aplicacións que cumpra co devandito estándar. Un servidor de aplicacións é unha implementación da especificación J2EE que se compón de:

1. Cliente Web ou contedor de applets: é un navegador web que interactúa co contedor web mediante HTTP.
  - a. Pode executar applets e código javascript.
  - b. Recibe páxinas HTML ou XML.
2. Aplicación Cliente: trátase de clientes que non se executan dentro dun navegador.
  - a. Poden utilizar distintas tecnoloxías para comunicárense co contedor web.
  - b. Poden comunicarse directamente coa base de datos.
3. Contedor Web ou servidor web: correspóndese coa parte visible dun servidor de aplicacións.
  - a. Emprega os protocolos HTTP e SSL.
4. Servidor de aplicacións: proporciona servizos que dan soporte á execución e dispoñibilidade das aplicacións despregadas.

Existen distintas implementacións partindo deste estándar, cada unha cunhas peculiaridades de seu que as poden facer máis adecuadas para un determinado sistema. Algunhas das máis destacadas son:

- Oracle Weblogic (BEA WebLogic)
- IBM WebSphere
- Sun-Netscape IPlanet
- Sun One
- Oracle IAS
- Borland AppServer
- HP Bluestone

### **55.2.3 Estrutura dun servidor de aplicacións**

Un servidor de aplicacións aséntase nunha estrutura en 3 capas que permite realizar unha estruturación máis eficiente do sistema.

- *Capa cliente:* contén os programas que executan os usuarios, como navegadores Web. Estes programas poden estar escritos en calquera linguaxe de programación.
- *Capa media:* contén o servidor de aplicacións e outros que poden ser direccionados polos clientes, como servidores proxy ou servidores web existentes.
- *Capa datos:* contén os recursos, como sistemas de bases de datos, ERP, etc.

#### **55.2.4 Oracle Weblogic (antes BEA WebLogic)**

OracleWebLogic Server é un servidor de aplicacións completo e baseado en estándares, que proporciona o fundamento sobre o cal unha empresa pode construír as súas aplicacións. Presenta un completo conxunto de características, como son o cumprimento dos estándares abertos, a arquitectura de varios niveis, e o apoio para desenvolvemento baseado en compoñentes, etc.

Oracle WebLogic Server proporciona todas as funcións básicas esenciais



dun servidor de aplicacións e servizos, tales como:

- Equilibrio de carga
- Tolerancia a fallos
- Servizos Web
- Transparencia na rede
- Integración de sistemas herdados
- Xestión de transaccións
- Seguridade
- Multi-threading
- Persistencia
- Conectividade con bases de datos
- Agrupación de recursos

Estas funcionalidades axilizan o desenvolvemento de aplicacións e alivian os esforzos dos desenvolvedores.

Ademais de J2EE, Oracle WebLogic Server implementa todos os estándares importantes de programación, integración e traballo en rede que son a base para a construción dunha infraestrutura de aplicacións, incluíndo:

- XML: Oracle WebLogic Server implementa a última versión da API de Java para o procesamento de XML (JAXP), e inclúe un analizador integrado Apache Xerces e un analizador XML de alto rendemento deseñado especificamente para pequenas e medianas empresas.
- SOAP: SOAP é o novo estándar para o intercambio de información nun contorno distribuído. É o protocolo de comunicación para definir o

formato dos datos para os servizos Web que se entregan a través de HTTP.

- WSDL: WSDL é unha linguaxe baseada en XML utilizada para describir un servizo web publicado. BEA WebLogic Server ten soporte incorporado para WSDL e xera un guión WSDL de forma automática cando un servizo Web se implementa no servidor WebLogic.
- UDDI: un rexistro UDDI é un directorio de servizos web, distribuído e baseado en Web, moi semellante a un caderno de teléfonos. Oracle WebLogic Server inclúe incrustado un rexistro UDDI e unha API para a procura e a actualización deste ou calquera outro rexistro UDDI.
- JMX e SNMP: a infraestrutura do servidor WebLogic baséase no estándar aberto e extensible JMX. Ademais, o axente SNMP está dispoñible para a compatibilidade con sistemas que se baseen en SNMP.
- Os administradores de sistemas poden configurar as súas políticas de seguridade baseadas en roles de acceso.

### **55.3 Servidores de Aplicacións e Servidores Web**

A diferenza básica entre o servidor web e un servidor de aplicacións é que o servidor web serve para ver as páxinas nun navegador web, mentres que un servidor de aplicacións proporciona os métodos necesarios, que poden ser chamados polas aplicacións cliente. Noutras palabras, as peticións HTTP son manexadas polos servidores web e a lóxica de negocio sérvese aos programas de aplicación, a través dunha serie de protocolos no servidor de aplicacións. Nun servidor de aplicacións, un cliente pode utilizar a GUI e os servidores web, mentres que nos servidores web o cliente pode usar HTML e HTTP.

	<b><i>Servidor Web</i></b>	<b><i>Servidor de Aplicacións</i></b>
<i>Que é?</i>	Un servidor que xestiona conexións HTTP.	Un servidor que lle expón a lóxica do negocio ao cliente mediante unha serie de protocolos, pero non exclusivamente HTTP.

<i>Engade funcionalidade?</i>	Un servidor web non engade funcionalidade; simplemente recibe unha petición e envíalle a resposta ao cliente.	Engade funcionalidade, posto que implementa unha lóxica de negocio intermedia.
<i>Que tipo de aplicacións serve?</i>	Só baseadas en web.	Aplicacións baseadas en web, mais tamén outras que non o son, o cal é posible porque un servidor de aplicacións inclúe internamente un servidor web.
<i>Que tipo de clientes permite?</i>	Navegadores.	Navegadores e interfaces pesadas.
<i>Cales son as súas funcións?</i>	Almacenar ficheiros escritos en HTML, PHP, etc., de xeito que sexan accesibles para os navegadores web cando os sitios web necesiten acceder a eles.	Ofrecer aplicacións a outro sistema.

## **55.4 Bibliografía**

- *Apache: The Definitive Guide*, Third Edition. Ben Laurie, Peter Laurie.
- *Apache. Soluciones y ejemplos para administradores de Apache*. Ken Coar e 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 e Bobby Martya.

**Autor:** Francisco Javier Rodríguez Martínez

Subdirector de Sistemas da Escola Superior de Enxeñaría Informática de Ourense

Colexiado do CPEIG

**56. DESEÑO DE CENTRO DE  
PROCESOS DE DATOS.  
INSTALACIÓNS  
(ELECTRICIDADE, CONTROL DE  
ACCESO, CONTROL DE  
PRESENZA, SISTEMA ANTI-  
INCENDIOS, CLIMATIZACIÓN,  
SISTEMAS DE ALIMENTACIÓN  
ININTERROMPIDA).**

Tema 56: Deseño dun centro de procesamento de datos. Instalacións (electricidade, control de acceso, control de presenza, sistema anti-incendios, climatización, sistemas de alimentación ininterrompida).

---

<b>56.1 Centro de procesamento de datos.....</b>	<b>1</b>
<b>56.2 Deseño dUN centro de procesamento de datos.....</b>	<b>1</b>
<b>56.3 Instalacións.....</b>	<b>19</b>
<b>56.4 Clasificación dos CPD.....</b>	<b>29</b>
<b>56.5 Bibliografía.....</b>	<b>31</b>

### **56.1CENTRO DE PROCESAMIENTO DE DATOS**

Un centro de procesamento de datos é o conxunto de recursos físicos, lóxicos e humanos necesarios para a organización e control das actividades informáticas dunha empresa ou organización. Considerarase que é aquel lugar onde se atopan os equipos informáticos principais que dan soporte ao conxunto de información dunha organización. Pódese dicir que os Centros de Procesamento de Datos (CPD) son os depositarios, os "gardiáns" da información utilizada por todas as áreas dunha organización.

### **56.2DESEÑO DUN CENTRO DE PROCESAMIENTO DE DATOS**

Un CPD pode ocupar un cuarto dun edificio, un ou varios andares, ou un edificio enteiro. A maioría do equipamento adoita presentarse en forma de servidores montados en armarios rack (tamén chamados bastidores, cabinets ou armarios) de 50 cm de ancho. Poden aloxar distintos dispositivos:

- Servidores cunha carcasa deseñada para se adaptar ao bastidor. Existen servidores de 1U, 2U e 4U e, recentemente, popularizáronse

os servidores blade que permiten compactar máis compartindo fontes de alimentación e instalación de cables.

- Conmutadores e encamiñadores de comunicacións.
- Paneis de parcheo, que centralizan toda a instalación de cables da planta.
- Devasa.
- Sistemas de audio e vídeo.

Os armarios rack adoitan estar dispostos en filas formando corredores entre eles. Isto permítelles ás persoas accederen ao frontal e á parte posterior de cada armario. Certos equipamentos do CDP como os mainframes e os dispositivos de almacenamento poden chegar a ser tan grandes como os propios racks e sitúanse ao longo destes.

Para levar a cabo o deseño dun CPD débense ter en conta moitas consideracións que van desde a localización xeográfica, a análise de riscos, as infraestruturas interiores... ata as medidas de seguridade, tanto físicas como lóxicas.

#### **56.2.1 *Requisitos que ten que cumprir o centro de procesamento de datos***

En primeiro lugar débense establecer os requisitos que ten que intentar cumprir o CPD:

- Instalación de alto risco. Considérase un CPD como unha instalación de alto risco. Unha instalación de alto risco é aquela que ten as seguintes características:
- Datos ou programas que conteñen información confidencial de interese nacional ou que posúen un valor competitivo alto no mercado.



- Perda potencial considerable para a institución e, en consecuencia, unha ameaza potencial alta para a súa subsistencia.
- Disponibilidade e monitorización “24x7x365”. Un centro de datos deseñado apropiadamente proporcionará dispoñibilidade, accesibilidade e confianza 24 horas ao día, 7 días á semana, 365 días ao ano.
- Fiabilidade infalible (5 ‘noves’). É dicir, cun 99,999% de dispoñibilidade, o que se traduce nunha única hora de non dispoñibilidade ao ano. Os centros de datos deben ter redes e equipos altamente robustos e comprobados.
- Seguridade, redundancia e diversificación. Almacenaxe exterior de datos, tomas de alimentación eléctrica totalmente independentes e de servizos de telecomunicacións para a mesma configuración, equilibrio de cargas, SAI ou Sistemas de Alimentación Ininterrompida ), control de acceso, etc.
- Control ambiental / Prevención de incendios. O control do ambiente trata da calidade do aire, a temperatura, a humidade, a electricidade, o control do lume e, por suposto, o acceso físico.
- Acceso Internet e conectividade WAN. Os centros de datos deben ser capaces de facer fronte ás melloras e avances nos equipos, estándares e anchos de banda requiridos, pero sen deixar de seren manexables e fiables. As comunicacións dentro e fóra do centro de datos provense por enlaces WAN, CAN/MAN e LAN nunha variedade de configuracións dependendo das necesidades particulares de cada centro.
- Rápido despregamento e reconfiguración. Outros aspectos tratan das previsións para facer fronte a situacións críticas, co obxectivo de superalas e volver rapidamente á normalidade en caso de catástrofe.

- Xestión continua do negocio. O funcionamento de moitas compañías que constantemente realizan miles de transaccións por minuto xira arredor da información almacenada. Para garantir a fiabilidade existen os sistemas intelixentes de control de asignacións e monitorización.
- Instalación de cables flexible, robusta e de altas prestacións. A infraestrutura física dos centros debe soportar sistemas de comunicación de alta velocidade, altas prestacións capaces de atender o tráfico de SAN (Storage Area Networks), NAS (Network Attached Storage), granxas de servidores de arquivos/aplicación/web, servidores blade e outros dispositivos de almacenaxe (Fibre channel, SCSI ou NAS) así como sistemas de automatización do edificio, sistemas de voz, vídeo e CCTV.

#### **56.2.2 *Análise de riscos e plans de continxencia***

Para realizar un bo deseño tamén debemos establecer un compromiso entre a necesaria operatividade do sistema fronte aos diversos riscos potenciais, os mecanismos e técnicas que permiten minimizar os seus efectos e custos directos e indirectos do emprego das devanditas técnicas.

Do estudo pormenorizado dos riscos e da criticidade determínase o nivel aceptable de seguridade e elíxense as medidas que cómpre adoptar. Estas medidas tradúcense na seguridade preventiva e o plan de continxencia.

##### **56.2.2.1 *Análise de riscos***

Deberemos determinar cuantitativa e cualitativamente os riscos a que estea sometida a organización. Unha vez tipificados procederemos a estimar a probabilidade de ocorrencia de cada un. Esta probabilidade non depende tanto do risco en si como das características concretas de cada CPD. Para iso pódese confeccionar unha escala cuns niveis subxectivos ou ben se pode recorrer ás estatísticas propias da instalación (no caso de existiren) ou ás editadas por empresas de consultoría ou seguros.

Débese establecer unha listaxe priorizada de elementos críticos (aplicacións, bases de datos, software de base, equipos centrais, periféricos, comunicacións) segundo o impacto que a súa carencia ou mal funcionamento causaría na operatividade do sistema.

Para iso podemos utilizar unha escala que marque o tempo que se podería tolerar un fallo de funcionamento de cada elemento: 24 horas, 2-3 días, 1 semana, 15 días, máis dun mes. Tamén podemos ter en conta a diferente criticidade segundo a época do ano, do mes ou da semana.

#### 56.2.2.2 Elección de medidas que cómpre adoptar

Consiste en seleccionar as medidas de seguridade que permitan previr os danos no posible e corrixilos ou minimizalos unha vez acaecidos, determinando os recursos necesarios para a súa implantación.

#### 56.2.2.3 Plan de continxencia

As medidas de corrección plásmanse nun plan cuns obxectivos concretos:

- Minimizar as interrupcións na operación normal.
- Limitar a extensión das interrupcións e dos danos.
- Posibilitar unha volta rápida e sinxela ao servizo.
- Ofrecerlles aos empregados unhas normas de actuación fronte a continxencias.
- Prover os medios alternativos de procesamento en caso de catástrofe.

Para garantir a súa validez e que non quede obsoleto co tempo, deberá estar en continua revisión. Ademais, o persoal debe estar adestrado mediante probas simuladas periódicas. Na elaboración do plan debe intervir a dirección, os técnicos de explotación, os técnicos de desenvolvemento, o persoal de mantemento, os usuarios e os provedores.

O plan debe recoller, en forma de plans unitarios, as respostas aos diferentes problemas que poidan xurdir, e divídese en:

- **Plan de urxencia:** Guía de actuación "paso a paso" en cada fallo ou dano. Determina unha serie de accións inmediatas (parada de equipos, aviso a responsables, activar ou desactivar alarmas, uso de extintores ou outros elementos auxiliares, chamada a mantemento, lanzar salvagardas ou listaxes, etc.), unha serie de accións posteriores como salvamento, valoración de danos, elaboración de informes, relanzar procesos, relanzar o sistema operativo, recuperar copias de seguridade, saltar procesos, etc., así como unha asignación de responsabilidades, tanto para as accións inmediatas como para as posteriores.
- **Plan de recuperación:** Desenvolve as normas de actuación para reiniciar todas as actividades normais da organización, ben no mesmo CPD, ben noutro centro de apoio. Se se recupera no propio centro, deberanse activar os equipos duplicados ou auxiliares (se non é automático), utilizaranse os soportes de procesamento alternativos, iniciaranse as actuacións de mantemento ou substitución de equipos danados e utilizaranse, se é preciso, as copias de seguridade. Se se utiliza un centro de apoio, débense definir os procedementos que cómpre empregar segundo a causa que orixinou o problema, débese realizar unha política de traslados (e volta posterior ao centro orixinal), débese recuperar o sistema operativo, o software de base e as aplicacións, débense relanzar as operacións (recuperando desde a última salvagarda en caso de necesidade) e débese revisar a operación mediante a introdución de probas que aseguren o correcto funcionamento.
- **Plan de apoio:** Especifica todos os elementos e procedementos necesarios para operar no centro de apoio (se existe) e manter nel información sobre a configuración do equipo e das comunicacións, do

sistema operativo, do software de base, das aplicacións, do soporte humano e técnico, subministracións de documentación e formularios, modo de rexenerar o software para o seu funcionamento normal, regras de explotación e operación, política de accesos e confidencialidade, identificación de usuarios, terminais, etc.

### **56.2.3 *Localización xeográfica***

Os edificios ou instalacións dos CPD requiren unhas características adicionais de protección física que deben ser consideradas antes de seleccionar a súa situación, tendo en conta aspectos tales como a posibilidade de danos por lume, inundación, explosión, disturbios civís, proximidade de instalacións perigosas (depósitos de combustible, aeroportos, acuartelamentos, etc.) ou calquera outra forma de desastre natural ou provocado.

Deberanse analizar de forma integral as características dominantes das distintas contornas, avaliando as vantaxes e os riscos potenciais que puidesen afectar ao bo funcionamento do CPD e suscitando as respostas adecuadas en relación coa contorna natural, artificial e urbanística.

#### **56.2.3.1 Contorna natural**

Teremos en conta:

- Climatoloxía: tormentas, precipitacións de auga e neve, temperaturas extremas, furacáns, xistra e ventos dominantes.
- Xeotecnia: mecánica dos solos (correimentos de terra, afundimentos, estrutura fisicoquímica, humidade, existencia de minerais magnéticos, sismicidade, etc.).
- Hidroloxía: proximidade de ríos, proximidade do mar, encoros próximos e posibles avenidas, etc.

#### **56.2.3.2 Contorna artificial**

Podemos considerar:

- Acceso a medios de urxencia: bombeiros, policía, servizos sanitarios, etc.
- Centrais de gas ou depósitos de gas, centrais nucleares.
- Redes de telecomunicacións.
- Subministración eléctrica, redes de subministración accesibles.
- Plantas petroquímicas, fábricas de cemento, betumes, derivados do vidro, etc.
- Conducións ou depósitos de líquidos (auga potable, augas residuais, combustibles, etc.).
- Contaminación atmosférica: po, vapores corrosivos ou tóxicos, etc.
- Perturbacións locais: ruídos, vibracións, radiacións parasitas (radares, balizas de navegación, emisoras de radio e televisión, torres de telecomunicacións, liñas de alta tensión próximas, grandes transformadores ou motores, centrais eléctricas, repetidores, centrais nucleares, aeroportos).

#### 56.2.3.3 Contorna urbanística

Temos, entre outras:

- Dotacións urbanas: metro, autobuses, intercambiadores ferroviarios, autoestradas, aeroportos, portos marítimos, hospitais, universidades, supermercados, etc.
- Zonas urbanas: parcelas abertas, edificacións contiguas, zonas de oficinas e negocios, parques empresariais, recintos feirais.
- Ambiente de traballo e saúde laboral (microclima de traballo, contaminación ambiental, sobrecargas físicas e psíquicas influentes, etc.).

Actualmente acuñouse o termo "AMENITIES" para abarcar todos os servizos complementarios que non son estritamente necesarios para o desempeño da actividade de procesamento de datos, pero que se poden ofrecer no conxunto da oferta inmobiliario, sobre todo nos parques empresariais ou zonas singulares.

Entre eles, están:

- Áreas de descanso, lecer e servizos terciarios.
- Gardería.
- Aparcadoiro.
- Clubs, ximnasios e instalacións deportivas.
- Caixeiros automáticos.
- Restaurantes e cafeterías.
- Hoteis.
- Centros comerciais.

#### **56.2.4      *Infraestruturas interiores***

Unha vez seleccionada a localización física do edificio que albergará o CPD, haberá que analizar as características específicas das instalacións, facendo fincapé nalgúns aspectos:

- Deben estar deseñadas de xeito que non se faciliten indicacións do seu propósito nin se poida identificar a localización dos recursos informáticos.
- Incluír zonas destinadas a carga e descarga de subministracións e a súa inspección de seguridade.

- Cumprir, nos elementos construtivos internos (portas, paredes, chans, etc.), o máximo nivel de protección esixido pola Norma Básica de Edificación (NBE/CPI-91).
- Dispoñer de canalizacións protexidas de cables de comunicacións e de electricidade, para evitar ataques (sabotaxes, lume, roedores, insectos), interceptación ou perturbacións por fontes de emisión próximas (radio, electricidade, magnetismo, calor).

#### 56.2.4.1 Habitabilidade

A maioría de construcións de edificios públicos, de oficinas ou de negocios non empezaron a cubrir as necesidades de preinstalacións e instalacións informáticas ata ben entrados os anos oitenta.

Actualmente, o deseño arquitectónico dun CPD debe estar o máis próximo posible á arquitectura intelixente. Este feito deu cabida á domótica.

A domótica comprende todos aqueles desenvolvementos tecnolóxicos enfocados ao deseño de solucións rendibles que poida ter o inmovible no marco da propia xénese do proxecto arquitectónico. É a automatización do edificio mais a dispoñibilidade dos recursos das telecomunicacións e da ofimática.

Os requirimentos de habitabilidade teñen en conta a arquitectura informática do momento. Preven non só o crecemento do equipamento informático, senón tamén o cambio total a outro contorno informático e manteñen rendibles as infraestruturas e as dotacións intelixentes ou servizos avanzados do inmovible:

- Habitabilidade en horizontal: é o edificio informático óptimo, o de poucos andares.
- Habitabilidade en torre: as torres perden en diafanidade, dificultan a extensión horizontal da sala de ordenadores e complican a evacuación de urxencia, etc.



#### 56.2.4.2 Requirimentos das edificacións e instalacións

Aplicaranse as normas xerais de obrigado cumprimento:

- Norma Básica da Edificación.
- Normas tecnolóxicas da Edificación.
- Ordenanzas Municipais.
- Regulamentos electrotécnicos.
- Verificación dos Produtos e Subministracións Industriais no marco da construción.
- Normas de Preinstalación das Firmas Informáticas.

Ademais da aplicación das normas xerais, o estudo para a elección do edificio deberá comprender todo o que compete á arquitectura tradicional, e moi especialmente a:

- A estrutura e sobrecargas de uso.
- As fachadas do inmovible.
- Accesos aos almacéns.
- Instalacións para as salas de informática.
- Peiraos de carga e descarga, elevadores, montacargas, etc.
- Acceso ao edificio de mercadorías pesadas (montacargas industrial).
- Acceso á Sala de Informática (sempre portas dobre folla).
- Existencia de saídas de Seguridade ao CPD.
- Falso chan e teito tecnolóxicos.
- Protección contra as infiltracións de auga e humidade.

- Subministracións de enerxía eléctrica e auga.
- Iluminación de día e de urxencia.
- Resistencia ao lume en minutos da estrutura, forxados e muros de carga.
- Muros devasa.
- Portas contra incendios.
- Situación das portas de acceso e evacuación.
- Túneles de seguridade e escaleiras de urxencia.
- Particións interiores ou tabiques dobres.
- Que non crucen as salas de informática conducións de augas tanto pluviais como de desaugadoiros agás as propias da climatización.
- Tratamentos referentes a resistencias eléctricas, acústicas e mecánicas.
- Protección contra a enerxía eléctrica de reacción: toma de terra do edificio, pararraios.

### **56.2.5      *Seguridade física***

A seguridade física consiste no conxunto de mecanismos e normas encamiñados a protexeren as persoas, instalacións, equipos centrais e periféricos e os elementos de comunicacións contra posibles danos. Está relacionada cos controis que protexen dos desastres naturais como incendios, inundacións ou terremotos, dos intrusos ou vándalos, dos perigos ambientais e dos accidentes.

Os controis de seguridade física regulan, ademais da sala onde se alberga o equipo do ordenador, a entrada de datos, a contorna (bibliotecas, rexistros cronolóxicos, medios magnéticos, áreas de almacenamento de copias de

seguridade e salas de instalacións de servizos) e todos os detalles ou requirimentos tanto arquitectónicos como de preinstalación e mantemento de todos os servizos e infraestruturas, mesmo a previsión de dispoñer dunha seguridade física integral da contorna, de conformidade co artigo 9 da LOPD (Lei orgánica de protección de datos de carácter persoal).

Deberase contemplar e analizar a seguridade física independentemente dos sistemas de xestión e control implantados no CPD.

Instalarase un sistema informatizado para a xestión e o control integral de todas as alarmas procedentes do equipamento informático, das infraestruturas e das instalacións específicas de seguridade do CPD.

Este sistema recibirá os sinais de alarma, dispoñerá da xestión destes e da posibilidade de realizar desde o mesmo a modificación de certos parámetros ou operacións de parada, arranque ou manobra do equipamento das salas de informática ou do recinto do CPD:

- Rede de incendios (sala do CPD, áreas de servizos e despachos, zonas do SAI e do grupo electrógeno).
- Alarmas en xeral.
- Arranque, parada ou manobra da contorna industrial do CPD.
- Control de accesos e movementos.
- Control de aforro de enerxía.
- Control no bloque de multicompartimentos de reparto.
- Control da expedición da produción.
- Control dos *stocks* de almacéns.
- Estado das baterías dos SAI e control dos grupos electrógenos.

- Control de climatización, sobrepresión e renovación ambiental.
- Rede de sondas ambientais en falso chan, teito e sala de ordenador.
- Rede de detección de humidade.

O obxectivo das áreas controladas é permitir un coñecemento inmediato e preciso do feito e da súa localización, polo que a súa actuación debe ser absolutamente fiable dentro duns parámetros previamente establecidos. Iso esixe unhas revisións de funcionamento e un rigoroso mantemento preventivo cuxa periodicidade dependerá do sistema de detección e do tipo de área controlada a que se aplique.

A detección dun feito anómalo require a información necesaria para unha reacción proporcionada. Dependendo da información fornecida polo medio de detección e os parámetros previamente establecidos, antes de chegar a un estado de alarma pódese pasar por un estado de alerta.

Así, os medios de reacción vanse organizando en previsión da súa posible actuación. Todos os medios de detección deben integrarse no Sistema de Xestión da Seguridade para que os xestione e:

- Avise da anomalía e a súa gravidade.
- Inicie accións de corrección automáticas ou propoña accións manuais que ten que realizar o persoal adestrado para iso.
- Controle as actuacións (que, quen, como, onde e cando).

Este sistema debe estar baixo vixilancia permanente e combinado cos servizos de mantemento para os casos de mal funcionamento de calquera medio de detección. Cómpre subliñar que os sistemas de detección deben funcionar ata coa subministración eléctrica de urxencia.

#### 56.2.5.1 Control de acceso e movementos

Refírese ás medidas que podemos establecer para evitar un acceso indebido ao conxunto do CPD. Foron xa mencionadas na seguridade física. O establecer un área segura é importante para o bo funcionamento do centro, posto que a información almacenada e os procedementos que se realizan no CPD son vitais para a organización.

Por iso se deben adoptar todas as medidas cuxo custo estea xustificado. Entre elas:

- Servizo de seguridade: que non só controle os accesos ao recinto, senón que tamén realice inspeccións periódicas das dependencias, sobre todo das que non teñan persoal en cada momento. A súa importancia faise evidente en horas nocturnas ou días festivos.
- Barreiras, portas de seguridade, ausencia de fiestras. Son medidas que tenden a dificultar o acceso de persoal non autorizado.
- Vídeo vixilancia e alarmas volumétricas: controladas por unha centraliña na cabina de seguridade.

##### **56.2.5.1.1 Planificación do acceso**

Os responsables das áreas controladas deben manter uns controis de acceso efectivos e proporcionais ao valor dos activos que cómpre protexer para que poidan cumprir cuns requisitos de auditabilidade mínimos. Os obxectivos son:

- Permitir o acceso unicamente ás persoas autorizadas polo responsable da área.
- Rexistrar as entradas e/ou saídas (quen, por onde e cando).

Para facilitar o control dos accesos a estas áreas, é recomendable a existencia dun único punto ou porta de acceso habitual para entrada e

saída, sen prexuízo de que existan outras saídas para urxencias que se poidan abrir desde o interior empurrando unha barra.

A entrada nas Áreas de Acceso Limitado (AAL) tense que efectuar desde unha área interna, nunca desde unha área pública. Cada área de acceso limitado debe ter identificado formalmente un responsable ou propietario cuxas responsabilidades son:

- Aprobar e manter actualizada a relación de persoas con autorización de acceso permanente. As persoas que teñan a súa autorización cancelada, por petición da súa dirección ou por causar baixa na empresa, deben ser eliminadas da relación de acceso nun tempo razoable.
- Aprobar accesos temporais a estas áreas. Neste caso a persoa autorizada debe saber que a autorización é para unha soa vez.

As Áreas de Acceso Restringido (AAR) non deben ter fiestras ao exterior e a entrada a estas tense que efectuar desde unha área interna ou unha área de acceso limitado, nunca desde un área pública. Teñen que ter barreiras de illamento de chan e teito, incluíndo o falso chan e o falso teito, ou ben detectores volumétricos de intrusos.

Cada área de acceso restringido debe ter identificado formalmente un responsable ou propietario cuxas responsabilidades son:

- Aprobar e manter actualizada a relación das persoas con autorización de acceso permanente, xeralmente, porque o traballo que van realizar require a súa presenza dentro da área. A lista de acceso debe ser actualizada, sempre que haxa cambios que así o aconsellen, e revisada formalmente polo menos cada seis meses. As persoas que teñan a súa autorización cancelada por petición da súa dirección ou por causar baixa na empresa teñen que ser eliminadas da lista de acceso de contado.

- Aprobar os accesos temporais a estas áreas, incluíndo os accesos do persoal que, estando destinado na área, accede fóra da súa xornada laboral. Neste caso, a persoa autorizada debe saber que a autorización é para unha soa vez. As autorizacións temporais deben conter:
  - o Nome de quen autoriza se non é o propietario.
  - o O nome da persoa autorizada.
  - o Razón social (se corresponde) ou motivo.
  - o Data e hora de acceso e a sinatura.
  - o Data e hora de saída e a sinatura.

#### **56.2.6      *Seguridade lóxica***

Este tipo de seguridade debe estar completamente coordinada coa seguridade física, xa que as dúas están estreitamente relacionadas e comparten obxectivos e orzamentos.

A seguridade lóxica consiste no conxunto de operacións e técnicas orientadas á protección da información contra a destrución, modificación indebida, divulgación non autorizada ou atraso na súa xestión.

É conveniente que o provedor ofrezca diferentes niveis de acceso segundo a función desexada: desde a combinación de usuario e clave, que pode ser abondo para a publicación de páxinas HTML con datos non críticos, pasando pola transferencia de datos mediante conexións HTTPS, (por exemplo, para as aplicacións de control a disposición do usuario ou para a consulta das súas estatísticas), ata chegar ás conexións completamente cifradas, ben empregando HTTPS ou tecnoloxía VPN, complementadas con autenticación de cliente mediante certificación dixital.

Ademais, é necesario un servizo de log, reporting e detección de intrusos. Nun provedor de servizos é normal que haxa centos de intentos de acceso

non autorizado á semana, desde os típicos varridos de portos, os intentos de exploits do “bug do día”, ata algúns intentos máis elaborados e perigosos. Unha cuestión adecuada neste punto é saber cantos intentos de acceso se detectan regularmente. Se a resposta é poucos ou ningún, debémonos preocupar, xa que se pon en dúbida a capacidade de detección das ferramentas e técnicas que se empregan, ou peor aínda, os procedementos de seguimento e resolución dos devanditos incidentes.

Para realizar o seguimento de calquera incidente é necesario dispoñer dos ficheiros de rexistro das diferentes aplicacións, ben sexan estándar ou programadas a medida para os distintos servizos. Sempre é conveniente que o provedor proporcione informes de acceso ás diferentes aplicacións, incluíndo aqueles que reflicten os enderezos IP desde os que se producen os accesos e os fallos de autenticación.

A combinación de todo o comentado anteriormente debería cubrir as necesidades que se buscan en canto á seguridade lóxica, sempre que se realice de xeito coherente e con coñecemento dos aspectos críticos para o cliente.

A infraestrutura do CPD debe incluír medidas de seguridade que protexan fronte a ataques a través das redes ás que este estea conectado. Como o núcleo da electrónica de rede adoita —e debe— estar situado no CPD, é necesario contemplar estas necesidades á hora de implantar un novo CPD.

É común que o acceso a internet sexa un recurso crítico para a organización, polo que se recomenda contratar dous provedores de acceso distintos e establecer unha configuración con alta dispoñibilidade de todos os elementos de rede que se atopen na ruta cara a Internet (devasas, routers, switches, etc.). Isto é especialmente crítico se a organización proporciona servizos en liña, tales como comercio electrónico ou hosting web.



Se é necesario adoptar medidas adicionais de seguridade do perímetro como IDS/IPS, filtrado de contidos ou antivirus de correo electrónico e/ou navegación web, así como mecanismos de acceso remoto (VPN), a devasa corporativa —ou mesmo o proxy, se se dispón del— é o lugar idóneo para iso. Deste xeito centralízase a administración destas medidas e redúcense os posibles puntos de fallo. Actualmente existe gran cantidade de dispositivos que dispoñen de todas estas funcionalidades nun único equipo.

Ademais dos evidentes mecanismos de control que é necesario establecer desde e cara a Internet, é moi conveniente realizar unha segregación de redes. É dicir, convén realizar unha división da rede interna da organización en distintas subredes, interconectadas entre elas por devasas que establezan os fluxos de información permitidos entre cada unha. Cada servidor, en función das necesidades de control de acceso das aplicacións que execute, conectarase finalmente a unha destas subredes.

## **56.3 INSTALACIÓNS**

### **56.3.1.1 Instalacións eléctricas**

Os cadros de mandos instalaranse en lugares facilmente accesibles, con espazo folgado (previndo as posibles ampliacións), correcta e claramente etiquetados e, por suposto, co máis estrito rigor en materia de calidade de aparatos e montaxe (deberán cumprir coas normas habituais de protección e seccionamento).

Evitaranse as perturbacións electromagnéticas, illando adecuadamente aquelas máquinas xeradoras de campos indutivos e harmónicos.

Evitarase a electricidade estática empregando os revestimentos máis adecuados, instalando tomas de terra convenientes e mantendo a humidade no rango adecuado (polo menos do 55%).

Os recursos informáticos son sensibles ás variacións de tensión e de frecuencia da corrente eléctrica. Os requirimentos básicos para a subministración de enerxía eléctrica son dous: Calidade e Continuidade.

Relacionado coa Calidade pódese destacar que:

- As variacións de frecuencia débense corrixir con equipos estabilizadores que a manteñan dentro dos rangos establecidos polos fabricantes dos recursos informáticos que hai que alimentar, aínda que algúns recursos informáticos de nova tecnoloxía lévanos incluídos.
- As variacións de tensión deben ser manexadas por un Sistema de Alimentación Ininterrompida (SAI, en inglés UPS), de xeito que se poidan previr os efectos de posibles microcortes.

En relación coa continuidade da subministración eléctrica, débese ter en conta que as caídas de tensión poden ser manexadas por un SAI (UPS), pero só por tempo limitado, xa que o desgaste dos seus acumuladores é moi rápido e a súa recarga moi lenta para utilizalo en cortes sucesivos e nunca como única alternativa.

As solucións habituais baséanse nunha das seguintes ou na combinación de varias delas:

- Conexión conmutada a dúas compañías subministradoras.
- Conexión conmutada a dúas estacións transformadoras da mesma compañía pero situadas en rutas de subministración diferentes.
- Capacidade de transformación de corrente asegurada mediante equipos redundantes.
- Equipos electróxicos de combustión.

Sempre que o volume das instalacións informáticas así o aconselle, a subministración eléctrica e as tomas de terra deben ser independentes das xerais do edificio e estar a unha distancia suficiente delas, correctamente instaladas e rigorosamente mantidas.

#### *56.3.1.2 Control de acceso*

Este control baséase en medidas de identificación unívoca das persoas que acceden ao CPD. O servizo de seguridade debe levar un rexistro das entradas e saídas ao centro. As visitas autorizadas deben levar obrigatoriamente unha tarxeta identificadora ou etiqueta nun lugar visible que indique claramente que é unha visita, as áreas ás que pode acceder e o tempo de validez (adoita ser diaria).

O persoal propio debe portar unha tarxeta identificadora con fotografía. Pódense utilizar cores para identificar as áreas ás que pode acceder.

En centros de alta seguridade pódense requirir medidas auxiliares de identificación:

- Pegadas dactilares.
- Fondo de ollo (retina).
- Introducción de códigos de acceso para abrir as portas.

#### **56.3.1.2.1 Niveis de seguridade de acceso**

As instalacións da empresa deben clasificarse en varias áreas ou zonas que, dependendo da súa utilización e os bens contidos, estarán sometidas a uns ou outros controis de acceso. As instalacións pódense clasificar de acordo cos criterios e denominacións seguintes:

- Áreas Públicas: espazos nos que non hai ningún tipo de restrición de acceso a empregados ou persoas alleas á empresa.

- Áreas Privadas: espazos reservados habitualmente aos empregados e persoas alleas á empresa con autorización por motivos de negocio. Nelas pode haber recursos informáticos cun valor baixo.
- Áreas de Acceso Limitado (AAL): espazos con acceso reservado a un grupo reducido de empregados e persoas alleas á empresa autorizadas por un acordo escrito. Pódense concentrar nelas recursos informáticos que, no seu conxunto, teñen un valor medio.
- Áreas de Acceso Restringido (AAR): espazos con acceso reservado a un grupo moi reducido de empregados e persoas alleas á empresa autorizadas por un acordo escrito, que teñan necesidade de acceder por razóns de negocio. Nelas atópanse recursos informáticos que, en conxunto, teñen un valor alto ou conteñen activos de información críticos para as actividades do negocio.

As dúas últimas denomínanse Áreas Controladas. Teñen que permanecer pechadas, mesmo cando estean atendidas, e os seus accesos controlados. Nas áreas controladas, todos os empregados e as persoas alleas á empresa con autorización para acceder por razóns de negocio teñen que levar permanentemente e en lugar visible un identificador:

- Os empregados, polo menos, con fotografía e nome.
- As demais persoas, polo menos o nome (lexible) e distintivo da función que cumpren (ex.: visita, contratado, subministrador, etc.).
- Os identificadores dos empregados con acceso a áreas controladas poden ter a posibilidade de lectura por banda magnética ou por calquera outro medio, para facilitar o control de accesos e o seu rexistro.

Todo identificador, especialmente os que permiten o acceso a áreas controladas, é persoal e debe ser considerado como un contrasinal de

acceso físico e non se pode compartir con ninguén, para evitar verse envolto nalgún incidente de seguridade non desexado.

Nas áreas controladas ten que estar prohibido comer, fumar, consumir bebidas alcohólicas e calquera tipo de drogas. As dúas últimas están consideradas de alto risco potencial para a instalación, polo que adicionalmente se lles debe impedir a entrada a calquera área controlada ás persoas de quen se sospeite que as consumen.

Os equipos informáticos que sexan perigosos ou combustibles teñen que ser almacenados a unha distancia prudencial e non seren trasladados á área onde se atopan o resto de recursos informáticos ata o momento da súa utilización. De igual forma, hai que retiralos da zona inmediatamente despois de finalizar o seu uso.

#### *56.3.1.3    Sistemas anti-incendios*

O lume causa o maior número de accidentes nos CPD. Por iso é imprescindible controlar puntos zonais e ademais realizar un estudo en función dos axentes extintores (ter en conta a prohibición do uso do halón, Protocolo de Montreal sobre CFC).

Procederáse a estudar como medidas:

- O acceso dos bombeiros a calquera zona do edificio previndo as tomas de auga a presión convenientes.
- A resistencia ao lume dos materiais de construción, carpintería, revestimento, etc. Evitaranse aqueles materiais que xeren produtos tóxicos ou gran cantidade de fume ao seren sometidos ao lume (NBE-CPI-91). Tamén hai que evitar que se acumulen listaxes de control e outros papeis no CPD.
- O mecanismo máis adecuado para cortar a alimentación eléctrica en caso de incendio.

- Os mecanismos idóneos para evitar que os condutos de refrixeración e ventilación actúen como chemineas e contribúan a propagar o incendio, parándose automaticamente o aire acondicionado en caso de incendio.
- A división do edificio, illando aquelas zonas que conteñan materiais facilmente combustibles, que se limitarán ao máximo.
- Tabiques de formigón con pranchas e portas ignífugas.
- A instalación de portas contra lumes dotadas dos mecanismos que aseguren o seu peche de forma automática.
- A prohibición de fumar, colocando carteis claramente visibles, nas zonas de maior risco.
- O mobiliario, fabricado con materiais resistentes ao lume.
- Os contedores de papel, materiais plásticos, etc., deberán ter unha tapa metálica, que permanecerá pechada de forma automática.
- A construción de recintos de protección combinada ou a disposición de armarios ignífugos.
- A instalación dun sistema de alarmas cruzadas e centralizadas no Sistema Integral de Xestión da Seguridade, para a detección ou extinción de incendios no CPD.

A maioría dos armarios que se utilizan nas salas de informática non son ignífugos, senón refractarios ou simples caixas fortes. Non corresponden ao grao de vulnerabilidade esixido na CEE.

En caso de incendio, a súa extinción pódese realizar con medios manuais ou automáticos. Os medios manuais baséanse en extintores portátiles, mangueras, etc. É importante resaltar que:

- Existen diferentes tipos de lume (de sólidos, líquidos, gases eléctricos ) e hai extintores axeitados para cada tipo.
- O elemento extintor localizado nunha área debe ser o apropiado para o que previsiblemente se pode declarar nela. Calquera medio de extinción pode ser excelente se é empregado nunha área, ou máis daniño que o mesmo lume se se usa noutra.
- Nunca se debe empregar un medio de extinción manual baseado en auga onde poida haber lume eléctrico por perigo de electrocución.
- Non é aconsellable a intervención de persoal non adestrado para iso.
- Sempre que se dispoña de tempo, hai que avisar á brigada interior de incendios (se a houbese) ou ao servizo de bombeiros.

Os medios automáticos baséanse na inundación da área mediante auga, CO<sub>2</sub> ou outros axentes extintores. O máis recomendable é o baseado en auga, polo seu baixo custo e o seu nulo impacto na contorna. Os sistemas automáticos baseados na auga deben ter un mecanismo de preacción que, en caso de chegar a un estado de alerta ou alarma, substitúe o aire da condución por auga.

A actuación destes sistemas de extinción debe ser combinada coa previa desconexión da subministración de enerxía eléctrica da área afectada.

O axente extintor máis usado actualmente é o HFC 227ea, que é un hidrofluorocarburo (ou heptafluoropropano). Desde o punto de vista ambiental, o axente extintor HFC 227ea foi aceptado pola EPA (Axencia de protección ambiental americana) no marco do programa de novas alternativas significativas (Significant New Alternative Program ou SNAP). Este gas pode intervir nas maiores clases de incendio e é seguro, limpo e non é condutor eléctrico.

#### 56.3.1.4 Climatización

Coa evolución tecnolóxica xa existen no mercado recursos informáticos que reducen (practicamente eliminan) os tradicionais requirimentos de aire acondicionado. Con todo, debido ao parque existente en España e á súa antigüidade media, débense ter en conta as seguintes consideracións:

- Para manter o ambiente coa temperatura e a humidade adecuadas, especialmente os das grandes instalacións, hai que disipar a calor que xeran a través do aire acondicionado.
- A suficiente potencia e redundancia destes equipos permitirá que traballen desafoadamente e que as operacións de mantemento sexan sinxelas e frecuentes.
- Un elemento fundamental do sistema acondicionador de aire é o mecanismo de corte automático logo de se producir a detección dun incendio.

Recoméndanse equipos de climatización específicos para salas informáticas con control microprocesador de temperatura e humidade. Estes equipos deben ser do tipo servizos total e capaces de produciren frío, calor e humectar ou deshumidificar de forma automática, dentro dunhas marxes de  $\pm 1^{\circ}\text{C}$  e  $\pm 2\%\text{HR}$  para valores de funcionamento previstos de  $21^{\circ}\text{C}$  e  $60\%\text{HR}$ .

As unidades de climatización deberanse calcular para un funcionamento continuo 24h/día e os 365 días do ano. A potencia frigorífica para unha temperatura de bulbo seco interior de  $24^{\circ}\text{C}$  debería bastar para manter as características das salas para as variacións de temperatura ambiente medias actuais e para o 120% da carga total dos locais (carga eléctrica + contribución dos locais + iluminación + presenza non continua de persoas en sala).



#### 56.3.1.5 Sistemas de alimentación ininterrompida

Tamén denominados SAI (UPS, *Uninterruptible Power Supply*), é un dispositivo que, grazas ás súas baterías, pódelle proporcionar enerxía eléctrica tras un corte da mesma a todos os dispositivos que teña conectados. Outra das funcións dos SAI é a de mellorar a calidade da enerxía eléctrica que chega ás cargas, filtrando subidas e baixadas de tensión e eliminando harmónicos da rede no caso de usar corrente alterna.

Existen dous tipos de SAI:

- SAI de corrente continua (activo). As cargas conectadas aos SAI requiren unha alimentación de corrente continua, polo tanto estes transformarán a corrente alterna da rede comercial a corrente continua e usarana para alimentar a carga e almacenala nas súas baterías. Xa que logo, non necesitan convertedores entre as baterías e as cargas.
- SAI de corrente alterna (pasivo). Estes SAI xeran como saída un sinal alterno, polo que necesitan un inversor para transformar o sinal continuo obtido das baterías nun sinal alterno.

#### 56.3.1.6 Outras características que cómpre ter en conta

##### **56.3.1.6.1 Recinto de protección combinada**

Son recintos de protección combinada aqueles compartimentos dentro dos CPD capaces de garantir unha custodia segura dos soportes magnéticos de apoio ante os axentes máis perigosos que os poidan atacar. Estarán dotados polo menos con:

- Apantallamento electromagnético e gaiolas de Faraday.
- Protección contra reaccións químicas que produzan HCL e gases de combustión corrosivos dentro da cámara.
- Protección contra a intrusión e o roubo (porta de seguridade).

- Protección contra o vandalismo e explosións.
- Protección contra incendios e os seus efectos derivados (fumes e vapores).
- Protección contra as inundacións interiores do CPD.
- Protección contra o impulso electromagnético nuclear (NEMP).
- Selado das instalacións e da cámara contra altas frecuencias e incendios.

#### **56.3.1.6.2 Instalacións de auga**

Evitaranse no posible as canalizacións de auga na sala de ordenadores (sobre todo por falso teito, falso chan ou visibles). En todo caso, preveranse os mecanismos de detección de fugas e a instalación de válvulas que poidan pechar as conducións afectadas. Os detectores de auga basearanse en sensores puntuais ou de banda que cubran áreas completas.

Os cables deben estar impermeabilizados cando discorran por zonas con risco de humidade ou inundación. Se non é posible separar os condutos de auga do resto de instalacións, preverase dotar o teito ou soleira do forxado, por onde discorran as tubaxes, da inclinación oportuna para evacuar a auga cara aos puntos de drenaxe establecidos, evitando a súa acumulación.

Se existen no edificio, ou pegados a el, depósitos de auga ou outro tipo de líquido, asegurase a súa estanquidade e instalaranse de xeito que a súa rotura non afecte aos servizos esenciais nin, por suposto, ás persoas.

No caso de salas de informática situadas en sotos, reforzase a estanquidade de paredes, pisos, teitos, portas e fiestras. Preverase a instalación de bombas automáticas para evacuar posibles inundacións, que se deben alimentar cun sistema eléctrico illado do resto da sala para permitir o seu funcionamento independente.

Se as CPU precisan auga fría para a refrixeración, preverase unha rede de tubaxes coas súas válvulas de corte e retención, sondas detectoras e sistema auxiliar de urxencia desde o contador da canle con filtrado do líquido.

#### **56.4 CLASIFICACIÓN DOS CPD**

O estándar TIA-942 describe os requisitos que debe cumprir a infraestrutura dun centro de procesamento de datos. Establécense catro niveis de dispoñibilidade:

- **Tier I:** Centro de procesamento de datos (CPD) básico. A taxa de dispoñibilidade máxima do CPD é do 99,671% do tempo, é dicir, o nivel Tier I do estándar TIA-942 consegue reducir o tempo de parada do CPD ao longo dun ano a 29 horas como máximo.

Un CPD Tier I pode admitir interrupcións tanto planeadas como non planeadas. Conta con sistemas de aire acondicionado e distribución de enerxía, pero pode non ter chan técnico, SAI ou xerador eléctrico. Se os posúe, poden ter varios puntos únicos de fallo. A carga máxima dos sistemas en situacións críticas é do 100%. A infraestrutura do CPD deberá estar fóra de servizo polo menos unha vez ao ano por razóns de mantemento e/ou reparacións. Os erros de operación ou fallas nos compoñentes da súa infraestrutura causarán a interrupción do CPD.

- **Tier II:** Compoñentes Redundantes. A taxa de dispoñibilidade máxima do CPD é do 99,749% do tempo, é dicir, o nivel Tier II do estándar TIA-942 consegue reducir o tempo de parada do CPD ao longo dun ano a 22 horas como máximo. Un CPD con compoñentes redundantes é lixeiramente menos susceptible a interrupcións, tanto planeadas como non planeadas. Estes CPD contan con chan técnico, SAI e xeradores eléctricos, pero está conectado a unha soa liña de distribución eléctrica. O seu deseño é N+1, o que significa que existe

polo menos un duplicado de cada compoñente da infraestrutura. A carga máxima dos sistemas en situacións críticas é do 100%. O mantemento na liña de distribución eléctrica ou noutros compoñentes da infraestrutura pode causar unha interrupción do servizo.

- **Tier III:** Mantemento Concorrente. A taxa de dispoñibilidade máxima do CPD é do 99,982% do tempo, é dicir, o nivel Tier III do estándar TIA-942 consegue reducir o tempo de parada do CPD ao longo dun ano a 1,5 horas como máximo. As capacidades dun CPD deste nivel permítenlle realizar calquera actividade planeada sobre calquera compoñente da infraestrutura sen interrupcións na operación. As actividades planeadas inclúen mantemento preventivo, reparacións ou substitución de compoñentes, agregar ou eliminar compoñentes, realizar probas de sistemas ou subsistemas, entre outras. Para infraestruturas que utilizan sistemas de arrefriamento por auga, significa dobre conxunto de tubaxes. Debe existir suficiente capacidade e dobre liña de distribución dos compoñentes, de xeito que sexa posible realizar mantemento ou probas nunha liña namentres que a outra atende a totalidade da carga. Neste nivel, actividades non planeadas como erros de operación ou fallos espontáneos na infraestrutura poden aínda causar unha interrupción do CPD. A carga máxima nos sistemas en situacións críticas é do 90%.

Moitos CPD Tier III son deseñados para actualizarse a Tier IV, cando os requirimentos do negocio xustifiquen o custo.

- **Tier IV:** Tolerante a Fallos. A taxa de dispoñibilidade máxima do CPD é do 99,995% do tempo, é dicir, o nivel Tier IV do estándar TIA-942 consegue reducir o tempo de parada do CPD ao longo dun ano a 26 minutos como máximo.

Un CPD deste nivel dispón de capacidade para realizar calquera actividade planeada sen interrupcións no servizo, pero, ademais, a funcionalidade tolerante a fallos permítelle á infraestrutura continuar operando mesmo ante un evento crítico non planeado. Isto require dúas liñas de distribución simultaneamente activas, típico nunha configuración System+System. Dende o punto de vista eléctrico, isto significa dous sistemas de SAI independentes, cada sistema cun nivel de redundancia N+1. A carga máxima dos sistemas en situacións críticas é do 90%. Persiste un nivel de exposición a fallos, polo inicio dunha alarma de incendio ou porque unha persoa inicie un procedemento de apagado de urxencia (EPO), os cales deben existir para cumprir cos códigos de seguridade contra incendios ou eléctricos.

### **56.5 BIBLIOGRAFÍA**

Centro de procesamento de datos en Wikipedia:

[http://es.wikipedia.org/wiki/Centro\\_de\\_procesamiento\\_de\\_datos](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 Rodríguez Martínez

Subdirector de Sistemas da Escola Superior de Enxeñaría Informática de Ourense

Colexiado do CPEIG

**57. VIRTUALIZACIÓN DE  
SERVIDORES. VIRTUALIZACIÓN  
DO ALMACENAMENTO.  
VIRTUALIZACIÓN DO POSTO  
CLIENTE. COMPUTACIÓN  
BASEADA EN SERVIDOR (SBC).  
GRID COMPUTING. CLOUD  
COMPUTING. GREEN IT E  
EFICIENCIA ENERXÉTICA.**

Tema 57: Virtualización de servidores. Virtualización do almacenamento. Virtualización do posto cliente. Computación baseada en servidor (SBC). Grid Computing. Cloud computing. Green IT e eficiencia enerxética.

---

<b>57.1 Virtualización de servidores.....</b>	<b>1</b>
<b>57.2 Virtualización do almacenamento.....</b>	<b>5</b>
<b>57.3 Virtualización do posto cliente.....</b>	<b>10</b>
<b>57.4 Computación baseada en servidor.....</b>	<b>12</b>
<b>57.5 Grid Computing.....</b>	<b>14</b>
<b>57.6 Cloud computing.....</b>	<b>18</b>
<b>57.7 Green IT e eficiencia enerXética.....</b>	<b>21</b>
<b>57.8 Bibliografía.....</b>	<b>29</b>

### **57.1 VIRTUALIZACIÓN DE SERVIDORES**

Podemos definir virtualización como a técnica que consiste basicamente en agrupar diferentes aplicacións e servizos de sistemas heteroxéneos dentro dun mesmo hardware, de xeito que os usuarios e o propio sistema os vexan como máquinas independentes dedicadas. Para iso, o sistema operativo virtualizado debe ver o hardware da máquina real como un conxunto normalizado de recursos con independencia dos compoñentes reais que o formen.

Desta forma, para virtualizar un sistema de servidores, os administradores deben, basicamente, optimizar os recursos dispoñibles, incluíndo o número e a identidade dos servidores físicos individuais, procesadores e sistemas operativos, co obxectivo de producir unha mellora tanto na xestión coma no manexo de sistemas informáticos complexos. O administrador do sistema virtual utilizará un software para a división do servidor físico en

contornos virtuais illados. Estes contornos son o que se coñece tecnicamente como servidores privados virtuais, mais tamén se poden atopar referencias a eles como particións, instancias, contedores ou emulacións de sistemas.

En concreto, podemos dicir que un servidor privado virtual é un termo de mercadotecnia empregado polos servizos de hosting para se referiren a unha máquina virtual para o uso exclusivo dun cliente individual do servizo. O termo utilízase para salientar que a máquina virtual, malia executarse no mesmo equipo físico que as máquinas virtuais doutros clientes, é funcionalmente equivalente a un equipo físico independente, está dedicado ás necesidades individuais do cliente e pode ser configurado para executarse como un servidor de internet (é dicir, para executar software de servidor). O termo VDS ou Virtual Dedicated Server (Servidor Virtual Dedicado) para o mesmo concepto.

Cada servidor virtual pode executar o seu propio sistema operativo e ser reiniciado de modo independente.

### **57.1.1 Funcionamento**

O servidor físico realiza unha abstracción dos recursos que se denomina Hypervisor ou VMM (Virtual Machine Monitor), elemento software que se instala na máquina onde se vai levar a cabo a virtualización e sobre a que se configuran as máquinas virtuais, que é onde van residir as aplicacións. É o encargado de xestionar os recursos dos sistemas operativos “aloxados” (guest) ou máquinas virtuais.

Desde un punto de vista lóxico, o usuario percibe que son máquinas independentes e illadas entre si, pero desde unha perspectiva física, todas as máquinas virtuais residen nun único servidor. A estas máquinas virtuais asígnaselles unha porcentaxe dos recursos do servidor físico, que serán os únicos que o cliente coñeza.



Pódense atopar tres modelos de virtualización: o modelo de máquina virtual ou virtualización completa, o modelo paravirtual ou virtualización parcial, e a virtualización a nivel de sistema operativo.

#### *57.1.1.1 Virtualización completa*

O modelo de máquina virtual está baseado na arquitectura cliente/servidor, onde cada cliente funciona como unha imaxe virtual da capa hardware. Este modelo permite que o sistema operativo cliente funcione sen modificacións. Ademais, permítelle ao administrador crear diferentes sistemas cliente con sistemas operativos independentes entre eles. A vantaxe principal deste modelo radica no descoñecemento por parte dos sistemas hóspede do sistema hardware real sobre o que está instalado. Con todo, realmente todos os sistemas virtuais fan uso de recursos hardware físicos. Estes recursos son administrados polo hypervisor, que coordina as instrucións CPU, convertendo as peticións do sistema convidado nas solicitudes de recursos apropiados no host, o que implica unha sobrecarga considerable. Case todos os sistemas poden ser virtualizados utilizando este método, xa que non require ningunha modificación do sistema operativo. Malia isto, é necesaria unha virtualización da CPU como apoio para a maioría dos hypervisores que levan a cabo a virtualización completa.

Exemplos típicos de sistemas de servidores virtuais son VMware Workstation, VMware Server, VirtualBox, Parallels Desktop, Virtual Iron, Adeos, Mac-on-Linux, Win4BSD, Win4Lin Pro, e z/VM, openvz, Oracle VM, XenServer, Microsoft Virtual, PC 2007 e Hyper-V.

#### *57.1.1.2 Paravirtualización*

O modelo de máquina paravirtual (PVM) ou virtualización parcial baséase, como o modelo anterior, na arquitectura cliente/servidor, incluíndo tamén a necesidade de contar cun sistema monitor. Con todo, neste caso, o VMM accede e modifica o código do sistema operativo do sistema hóspede. Esta modificación coñécese como porting. O porting serve de soporte ao VMM

para que poida realizar chamadas ao sistema directamente. Do mesmo xeito que as máquinas virtuais, os sistemas paravirtuais son capaces de soportar diferentes sistemas operativos instalados no hardware real. Esta técnica utilízase con intención de reducir a porción de tempo de execución empregada polo hóspede encargado de realizar as operacións, que son moito máis difíciles de executar nun contorno virtual en comparación cun contorno non virtualizado. Así, permítese que o(s) convidado(s) e o hóspede soliciten e recoñezan estas tarefas, que doutro xeito serían executadas no dominio virtual (onde o rendemento de execución é peor). Unha plataforma paravirtualizada exitosamente pode permitir que o VMM sexa menos complexo (pola recolocación da execución das tarefas críticas do dominio virtual no dominio do servidor), e/ou reducir a degradación do rendemento global da máquina virtual durante a execución de convidado.

UML, XEN, Xen, Virtuozzo , Vserver e OpenVZ (que é o código aberto e a versión de desenvolvemento de Parallels Virtuozzo Containers) son modelos de máquinas paravirtuais.

#### 57.1.1.3 Virtualización por S.O.

A virtualización a nivel de sistema operativo diferénciase das anteriores en que, neste caso, non existe un sistema cliente/servidor propiamente dito. Neste modelo o sistema principal exporta a funcionalidade do sistema operativo desde o seu propio núcleo. Por esta razón, os sistemas virtuais usan o mesmo sistema operativo que o nativo (inda que na maioría dos casos poden instalar distintas distribucións). Esta arquitectura elimina as chamadas do sistema entre capas, o que favorece unha redución importante no uso de CPU. Ademais, ao compartir os ficheiros binarios e librerías comúns do sistema na mesma máquina, a posibilidade de escalado é moito maior, permitindo que un mesmo servidor virtual sexa capaz de dar servizo a un gran número de clientes ao mesmo tempo.

A virtualización de SO mellora o rendemento, xestión e eficiencia. Podemos entendelo como un sistema en capas. Na base reside un sistema operativo

hóspede estándar. A seguir atopamos a capa de virtualización, cun sistema de arquivos propietario e unha capa de abstracción de servizo de kernel que garante o illamento e seguridade dos recursos entre distintos contedores. A capa de virtualización fai que cada un dos contedores apareza como servidor autónomo. Finalmente, o contedor aloxa a aplicación ou carga de traballo.

Exemplos de sistemas que usan virtualización a nivel de sistema operativo son Virtuozzo e Solaris.

## **57.2 VIRTUALIZACIÓN DO ALMACENAMENTO**

Este tipo de virtualización permite unha maior funcionalidade e características avanzadas no sistema de almacenamento. Consiste en abstraer o almacenamento lóxico do almacenamento físico e adoita usarse en SAN (Storage Area Network, Rede de área de almacenamento).

Este sistema de almacenamento tamén se coñece como “storage pool”, matriz de almacenamento, matriz de disco ou servidor de arquivos. Estes sistemas adoitan usar hardware e software especializado, xunto con unidades de disco co fin de proporcionar un almacenamento moi rápido e fiable para o acceso a datos. Son sistemas complexos, e poden ser considerados como un ordenador de propósito especial deseñado para proporcionar capacidade de almacenamento xunto con funcións avanzadas de protección de datos. As unidades de disco son só un elemento dentro do sistema de almacenamento, xunto co hardware e o software de propósito especial incorporado no sistema.

Os sistemas de almacenamento poden ser de acceso a nivel de bloque, ou acceso a nivel de ficheiros. O acceso por bloques adoita levarse a cabo por medio de Fibre Channel , iSCSI , SAS , FICON ou outros protocolos. Para o acceso a nivel de arquivo úsanse os protocolos NFS ou CIFS.

Dentro deste contexto podémonos atopar con dous tipos principais de virtualización: a virtualización por bloques e a virtualización por arquivos.

### **57.2.1      *Virtualización por bloques***

Este tipo de virtualización baséase na abstracción (diferenciación) entre o almacenamento lóxico e o almacenamento físico, conseguindo que o acceso non teña en conta o almacenamento físico ou estrutura heteroxénea.

Existen tres tipos de virtualización por bloques: baseada en host, baseada en dispositivos de almacenamento e baseada en rede.

#### *57.2.1.1      Virtualización baseada en host*

Esta virtualización require software adicional que se executa no host. Nalgúns casos a administración de volumes está integrada no sistema operativo, e noutros casos ofrécese como un produto separado. Os volumes (LUN) dispoñibles no sistema son manexados por un controlador de dispositivos físicos tradicional. Por enriba deste controlador atópase unha capa software (o xestor de volumes) que intercepta as peticións de E/S, e proporciona a procura de meta-datos e mapeamentos de E/S.

Os sistemas operativos máis modernos teñen algún tipo de xestor de volumes lóxicos integrado (MVI en UNIX/Linux, ou Administrador de discos lóxicos ou LDM en Windows), que realiza tarefas de virtualización.

Existen varias tecnoloxías que efectúan este tipo de virtualización, como poden ser a xestión de volumes lóxicos (Logical Volume Management, LVM), os sistemas de arquivos (CIFS, NFS) ou a montaxe automática (autofs).

#### *57.2.1.2      Virtualización baseada en dispositivos de almacenamento*

Pódese levar a cabo a virtualización baseada en medios de almacenamento masivo utilizando un controlador de almacenamento primario que proporcione os servizos de virtualización e permita conexión directa dos controladores de almacenamento. En función da implementación é posible usar modelos de distintos fabricantes.

O controlador primario proporcionará a posta en común e os meta-datos de servizo de xestión. Tamén pode ofrecer servizos de replicación e migración a través dos controladores que se virtualizan.

Unha nova xeración de controladores de serie do disco permite a inserción posterior dos dispositivos de almacenamento.

Os sistemas RAID poden ser un exemplo desta técnica. Estes sistemas combinan varios discos nunha soa matriz.

As matrices avanzadas de disco contan a miúdo con clonación, instantáneas e replicación remota. En xeral, estes dispositivos non ofrecen os beneficios da migración de datos ou de replicación a través de almacenamento heteroxéneo, xa que cada fabricante tende a utilizar os seus propios protocolos propietarios.

#### *57.2.1.3 Virtualización baseada en rede*

Esta é unha virtualización de almacenamento que opera nun dispositivo baseado en rede (polo xeral un servidor estándar ou un smart switch) e o uso de redes iSCSI ou FC de Fibre Channel para conectar como SAN (Storage Area Network). Este é o tipo de virtualización de almacenamento máis común.

O dispositivo de virtualización atópase na SAN e proporciona a capa de abstracción entre os host, que permiten a entrada/saída, e os controladores de almacenamento, que proporcionan capacidade de almacenamento.

Hoxe en día existen dúas implementacións distintas, a baseada no **dispositivo** e a baseada en **conmutación**. Ambos os modelos proporcionan os mesmos servizos: xestión de discos, procura de meta-datos, migración e replicación de datos. Igualmente, ambos os modelos precisan dun hardware específico que permita ofrecer os devanditos servizos.

A baseada en dispositivos consiste en establecer o hardware especializado entre os hosts e a parte de almacenamento. As solicitudes de entrada/saída rediríxense ao dispositivo, que realiza a asignación de meta-datos, mediante o envío das súas propias ordes de E/S á solicitude de almacenamento subxacente. O hardware usado tamén pode proporcionar almacenamento de datos en caché, e a maioría das implementacións proporcionan algún tipo de agrupación de cada un dos dispositivos para manter un punto de vista atómico tanto de meta-datos como dos datos da caché.

Este tipo de almacenamento tamén se pode clasificar en in-band (simétrica ) ou out-of-band (asimétrica).

#### **57.2.1.3.1 In-band (simétrica)**

Neste caso os dispositivos de virtualización aséntanse entre o host e o almacenamento. Todas as peticións de E/S e datos pasan a través do dispositivo. Os host nunca interactúan co dispositivo de almacenamento senón co dispositivo de virtualización.

#### **57.2.1.3.2 Out-of-band (asimétrica)**

Os dispositivos usados neste tipo de virtualización tamén son chamados servidores de meta-datos. A única finalidade destes dispositivos é proporcionar a asignación de meta-datos. Isto implica o uso de software adicional no host, que é coñecedor da localización real dos datos. Deste xeito, intercéptase a petición antes de que saia do host, solicítase unha procura de meta-datos no servidor (pode ser a través dunha interface que non sexa SAN) e devólvese a localización real dos datos solicitados polo host. Finalmente recupérase a información a través dunha solicitude de E/S común ao dispositivo de almacenamento. Non se pode dar un almacenamento en caché, xa que os datos nunca pasan a través do dispositivo de virtualización.

### **57.2.2 Virtualización a nivel de arquivo**

Con este tipo de virtualización preténdese eliminar as dependencias entre o acceso a datos a nivel de arquivo e a localización física destes. Esta técnica, coñecida como NAS (Network-Attached Storage) ou almacenamento conectado a rede, adoita ser un equipo especializado pensado exclusivamente para almacenar e servir ficheiros. Os equipos que funcionan como dispositivo NAS adoitan incluír un sistema operativo específico para ese fin, como pode ser FreeNAS ou FreeBSD.

Estes sistemas poden conter un ou máis discos duros, dispostos a miúdo en contedores lóxicos redundantes ou arrays RAID.

NAS utiliza protocolos baseados en arquivos como NFS (sistemas UNIX), SMB/CIFS (Server Message Block/Common Internet File System) (sistemas MS Windows), ou AFP (Apple Filing Protocol, sistemas Apple Macintosh). As unidades NAS non adoitan limitar os clientes a un único protocolo. FTP, SFTP, HTTP, UPnP, rsync e AFS (Andrew File System) tamén o soportan.

Deste xeito conséguese optimizar a utilización do almacenamento e as migracións de arquivos sen interrupcións.

### **57.2.3 Diferenzas entre NAS e SAN**

NAS proporciona almacenamento e un sistema de arquivos, o que adoita contrastar con SAN, que só proporciona almacenamento baseado en bloques e deixa do lado do cliente a xestión do sistema de arquivos.

NAS aparece no sistema cliente como un servidor de arquivos (pódense asignar unidades de rede ás accións do servidor), mentres que un disco a través dunha SAN se presenta ao cliente como un disco máis do sistema operativo, que podemos montar, desmontar, formatar...

	<b>NAS</b>	<b>SAN</b>
<b>Tipo de datos</b>	Arquivos compartidos	Datos a nivel de bloque, por exemplo, bases de datos.
<b>Cable</b>	Ethernet LAN	Fibre Channel dedicado

<b>utilizado</b>		
<b>Cientes principais</b>	Usuarios finais	Servidores de aplicacións
<b>Acceso a disco</b>	A través do dispositivo NAS (IP propia)	Acceso directo

### **57.3 VIRTUALIZACIÓN DO POSTO CLIENTE**

Esta técnica consiste na separación do contorno de usuario dun ordenador persoal da máquina física co modelo cliente-servidor. O modelo que segue un servidor para implementar esta característica denomínase VDI (Virtual Desktop Infrastructure, Infraestrutura de Escritorio Virtual), tamén chamada Interface de Escritorio Virtual.

A maioría das implementacións comerciais desta tecnoloxía usan un servidor central remoto para levar a cabo a “virtualización” do escritorio do cliente, en lugar de usar o almacenamento local do cliente remoto. Isto implica que todas as aplicacións, procesos, configuracións e datos do cliente están almacenadas no servidor e se executan de forma centralizada.

O sistema cliente pode utilizar unha arquitectura de hardware completamente diferente da utilizada polo contorno de escritorio proxectado, e tamén pode estar baseada nun sistema operativo completamente diferente.

O modelo de virtualización do posto cliente permite o uso de máquinas virtuais para que múltiples subscritores de rede poidan manter escritorios individuais nun só ordenador, o servidor central. Este servidor central pode operar nunha residencia, negocio ou centro de datos. Os usuarios poden estar xeograficamente dispersos, pero todos están conectados á máquina central por unha rede de área local, unha rede de área ampla, ou Internet.



### 57.3.1 **Modos de operación de VDI**

Basicamente existen catro modelos de operación VDI:

- Aloxado (como servizo). Adoita contratarse a provedores comerciais e normalmente proporciona unha configuración do sistema operativo do posto cliente administrado. Os principais subministradores son CITRIX, VMware e Microsoft.
- Centralizado. Neste caso todas as instancias VDI están aloxadas nun ou máis servidores centralizados, os datos están en sistemas de almacenamento conectados a estes. Este modelo, pola súa vez, pode distinguir dous tipos:
  - o VDI estático ou persistente. Existe unha única imaxe de escritorio asignado por cliente e estes deben ser xestionados e mantidos.
  - o VDI dinámico ou non persistente. Existe unha imaxe mestra común para todos os clientes que se clona e personaliza no momento da petición cos datos e aplicacións particulares de cada cliente.
- Remoto (ou sen ataduras). Ten como base o concepto de VDI centralizado pero permite traballar sen a conexión a un servidor central ou a Internet. Cópiase unha imaxe ao sistema local e execútase sen necesidade de máis conexión. As imaxes teñen un certo período de vida e actualízanse de forma periódica. Esta imaxe execútase no sistema local que necesita un sistema operativo e un hipervisor (que executa a instancia VDI). Isto implica que o dispositivo cliente teña maiores necesidades de memoria, espazo en disco, CPU... A vantaxe é a menor dependencia de conexión.

Os modelos aloxado e centralizado necesitan unha rede que conecte co servidor onde se executa a instancia VDI. O concepto base deste modelo é

similar ao de clientes lixeiros, debido a que o cliente só ten que mostrar o escritorio virtual.

No caso do modelo remoto, permíteselles aos usuarios copiar a instancia VDI no sistema e logo executarase o escritorio virtual sen necesidade de ningún tipo de conexión.

#### **57.4 COMPUTACIÓN BASEADA EN SERVIDOR**

Tamén coñecida como SBC, do inglés Server Based Computing, consiste na separación do procesamento de certas tarefas como a xestión de datos, que será realizada nun servidor central, e outras tarefas de procesamento, como a presentación de aplicacións de usuario e impresión de datos no cliente. O único transmitido entre servidor e cliente son as pantallas de información. Esta arquitectura pode dar solución aos principais problemas que aparecen cando se executan aplicacións nos clientes. Ademais simplifica procesos como poden ser os contornos hardware, actualizacións de software, despregamento de aplicacións, soporte técnico, almacenamento e copia de seguridade de datos. Centralízase a xestión de todos estes procesos nun único servidor.

Os clientes que actúan nesta arquitectura adoitan chamarse “thin clients”, ou clientes lixeiros; este é un termo xeral para dispositivos que se basean nun servidor para operar. O thin client proporciona pantalla, teclado, rato e un procesador básico que interactúa co servidor. Os thin client non almacenan ningún dato localmente e require poucos recursos de procesamento. A característica máis destacada destes terminais é a redución de custos asociados co mantemento, administración, soporte, seguridade e instalación de aplicacións, en comparación cun PC tradicional.

Esta tecnoloxía está composta por tres compoñentes principais:

- Sistemas operativos multi-usuario que permiten o acceso e execución de modo concorrente, usando aplicacións diferentes e con sesións de

usuario protexidas. Exemplos dalgunhas terminais de servizo 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.

- O thin client pódese executar cunha cantidade mínima de software, pero necesita polo menos un programa de conexión a servizos de terminal. O thin client e o programa de servizos de terminal poden ser executados en sistemas operativos completamente diferentes.
- Un protocolo que lles permita ao programa de servizos de terminal e ao thin client comunicárense e enviar as pulsacións de teclado, de rato e as actualizacións de pantalla a través da rede. Os protocolos máis populares son RDP3 (Remote Desktop Protocol), ICA e NX.

Entre as vantaxes da computación baseada en servidor pódense nomear:

- Redución dos custos de administración. A xestión de clientes lixeiros está case na súa totalidade centralizada no servidor.
- Redución de custos de hardware. O hardware nos clientes lixeiros é en xeral máis barato, porque non é necesario ter memoria para as aplicacións ou un procesador de grande alcance.
- Seguridade. Pode ser controlada centralmente.
- Menor consumo de enerxía. O hardware especializado no cliente lixeiro ten un consumo moito menor de enerxía que os tradicionais.
- Redución da carga de rede. O tráfico de rede que xeran os terminais lixeiros só é o dos movementos do rato, teclado e información de pantalla desde / cara ao usuario. No caso de que un cliente pesado abra e gardase un documento, xa implicaría o paso deste dúas

veces pola rede. Usando protocolos eficientes de rede tales como ICA e NX xa é posible usar esta tecnoloxía nun ancho de banda de 28,8 Kbps.

- Actualización de hardware simple. Se o uso está por riba dun límite predefinido, é relativamente sinxelo solucionar o problema; bastaría cun disco novo nun rack de servidores, aumentando así o número de recursos, exactamente a cantidade necesaria. Se ocorre isto con clientes pesados, habería que substituír un PC completo, o que carrexaría tanto custos económicos como de recursos humanos.

Malia o anterior, esta tecnoloxía tamén presenta certos inconvenientes:

- Altos requirimentos de servidor. Ao centrarse a carga de traballo no servidor, o sistema de clientes lixeiros implica maior consumo de recursos nos servidores; mesmo é habitual que se use un gran número de servidores, o que se denomina “granxa de servidores”.
- Pobre rendemento multimedia. O envío de datos de son e vídeo requiren moito ancho de banda, polo que estes sistemas son menos útiles para aplicacións multimedia.
- Menos flexibilidade. Non todos os produtos software do mercado poden funcionar correctamente nun cliente lixeiro.

### **57.5 GRID COMPUTING**

Arquitectura distribuída e paralela, de ámbito extenso xeograficamente, na que se premia a distribución, e a continuación a paralelización. Os seus creadores foron Ian Foster e Carl Kesselman. O seu nome provén do paradigma da rede eléctrica (power grid).

Baséase no compartimento, selección e agregación de forma dinámica e en tempo de execución de recursos autónomos, distribuídos xeograficamente, dependendo de criterios como a dispoñibilidade do hardware, a capacidade

transaccional, o rendemento que se lle poida dar á solución final, o custo e os criterios de calidade do servizo que o demandante poida proporcionar e esixir.

A rede está formada por un conxunto de ordenadores independentes e interconectados que poñen a disposición do grid os excedentes do seu procesamento individual, é dicir, os ciclos de reloxo dos seus CPU non aproveitados por eles mesmos, sen poder superar unha determinada porcentaxe de dedicación configurada individualmente en cada nodo. A partir da porcentaxe proporcionada por cada nodo, virtualízase un recurso computacional único.

Os sistemas baseados en grid computing están indicados para atender produtividades sostidas e sostibles, sen poder nunca superar un determinado limiar. Nestes sistemas garántese a escalabilidade como un criterio parametrizable. É posible definir con que criterio engadimos cada novo nodo á solución final.

Actualmente, o único criterio que se ten en conta é a capacidade de procesamento (transaccionalidade), pero no futuro será posible ter en conta criterios máis finos, referidos á calidade do servizo.

Ademais, estes sistemas están dotados dun comportamento dinámico, segundo o cal un determinado programa en execución no sistema pode modificar en tempo real o dimensionamento da grid para adaptalo ás súas necesidades.

#### **57.5.1 Características**

- Podemos conseguir un máximo aproveitamento dos nodos (100% de utilización da CPU).
- Os nodos non teñen que estar dedicados. Ademais, ao contrario que no caso do clúster, asegurámonos que a contribución ao Grid non vai exceder unha determinada porcentaxe de tempo de procesamento en cada nodo.

- Son sistemas heteroxéneos, nos que podemos atopar diversos HW e SW.
- A escalabilidade parametrizable é a característica máis potente desta arquitectura.

### **57.5.2      *Funcionalidades***

- Localización dinámica de recursos (máquinas con excedente).
- Optimización do acceso a datos, mapeando as estruturas de datos en cachés temporais locais (directorios).
- Autenticación do usuario (usr/pwd, certificados...).
- Monitorización de tarefas e procesos desde calquera nodo da rede, sempre que o usuario teña permisos.
- As máquinas atópanse en situación paritaria.
- Se é posible, paralelízase. O fundamental é a distribución de procesos debilmente axustados.

### **57.5.3      *Arquitectura Grid***

Habitualmente descríbese a arquitectura do Grid en termos de “capas”, executando cada unha delas unha determinada función. Como é habitual neste tipo de enfoque, as capas máis altas están máis cerca do usuario, en tanto que as capas inferiores están máis preto das redes de comunicación.

Empezando polos cimentos, atopámonos coa capa de rede, responsable de asegurar a conexión entre os recursos que forman o Grid.

Na parte máis alta está a capa de recursos, constituída polos dispositivos que forman parte do Grid: ordenadores, sistemas de almacenamento, catálogos electrónicos de datos e mesmo sensores que se conectan directamente á rede.

Na zona intermedia está a capa "middleware", encargada de proporcionar as ferramentas que permiten que os distintos elementos (servidores, almacéns de datos, redes, etc.) participen de forma coordinada nun contorno Grid unificado. Esta capa é a encargada das seguintes funcións:

Atopar o lugar conveniente para executar a tarefa solicitada polo usuario.

- Optimiza o uso de recursos, que poden estar moi dispersos.
- Organiza o acceso eficiente aos datos.
- Encárgase da autenticación dos diferentes elementos.
- Ocúpase das políticas de asignación de recursos.
- Executa as tarefas.
- Monitoriza o progreso dos traballos en execución.
- Xestiona a recuperación fronte a fallos.
- Avisa cando se terminou a tarefa e devolve os resultados.

O ingrediente fundamental do middleware son os metadatos (datos sobre os datos), que conteñen, entre outras cousas, toda a información sobre o formato dos datos e onde se almacenan (ás veces en varios sitios distintos).

O middleware está formado por moitos programas software. Algúns deses programas actúan como axentes e outros como intermediarios, negociando entre eles, de forma automática, en representación dos usuarios do Grid e dos provedores de recursos. Os axentes individuais presentan os metadatos referidos aos usuarios, datos e recursos. Os intermediarios encárganse das negociacións entre máquinas (M2M) para a autenticación e autorización dos usuarios e encárganse de definir os acordos de acceso aos datos e recursos e, no seu caso, o pagamento polos mesmos. Cando queda

establecido o acordo, un intermediario planifica as tarefas de cómputo e supervisa as transferencias de datos necesarias para acometer cada traballo concreto. Ao mesmo tempo, unha serie de axentes supervisores especiais optimizan as rutas a través da rede e monitorizan a calidade do servizo.

Na capa superior deste esquema está a capa de aplicación onde se inclúen todas as aplicacións dos usuarios, portais e ferramentas de desenvolvemento que soportan esas aplicacións. Esta é a capa que ve o usuario.

Ademais, nas arquitecturas máis comúns do Grid, a capa de aplicación proporciona o chamado "serviceware", que recolle as funcións xerais de xestión tales como a contabilidade do uso do Grid que fai cada usuario.

Para poder facer todo o anterior, as aplicacións que se desenvolvan para seren executadas nun PC concreto teranse que adaptar para poder invocar os servizos adecuados e utilizar os protocolos correctos. Igual que as aplicacións que inicialmente se crearon para funcionar illadamente se adaptan para poder ser executadas nun navegador web, o Grid requirirá que os usuarios dediquen certo esforzo a "GRIDizar" as súas aplicacións.

Con todo, unha vez adaptadas ao Grid, milleiros de usuarios poderán usar estas aplicacións, utilizando as capas de middleware para adaptárense aos posibles cambios no tecido do Grid.

## **57.6 CLOUD COMPUTING**

Modelo que permite o acceso a un conxunto compartido de recursos informáticos configurables a través da rede (por exemplo, redes, servidores, almacenamento, aplicacións e servizos) que poden ser desenvolvidos e despregados rapidamente cun mínimo esforzo de xestión ou interacción co provedor de servizos.



Este termo refírese á utilización e o acceso de múltiples recursos baseados en servidores a través dunha rede. Os usuarios da “nube” poden acceder aos recursos do servidor empregando un ordenador, netbook, pad computer, smart phone ou outro dispositivo. No cloud computing, o servidor presenta e xestiona as aplicacións; os datos tamén se almacenan de forma remota na configuración da nube. Os usuarios non descargan nin instalan aplicacións no seu sistema, todo o procesamento e almacenamento se mantén polo servidor. Os servizos en liña poden ser ofrecidos a partir dun “provedor da nube” ou dunha organización privada.

### **57.6.1      *Arquitectura***

Normalmente a arquitectura dos sistemas software implicados no desenvolvemento de cloud computing inclúen múltiples compoñentes denominados “compoñentes cloud” que se comunican mediante mecanismos de baixo acoplamento, tales como as colas de mensaxes.

Os dous compoñentes máis significativos da arquitectura cloud computing coñécense como o front-end e o back-end. O front-end é a parte vista polo cliente, é dicir, o usuario do PC. Isto inclúe a rede do cliente e as aplicacións utilizadas para acceder á nube a través dunha interface de usuario, como un navegador web. O back-end da arquitectura é a propia nube, que comprende varios ordenadores, servidores e dispositivos de almacenamento de datos.

Dentro desta arquitectura pódense distinguir as seguintes capas:

- Proveedor: Empresa responsable de proporcionar o servizo na “nube”.
- Cliente: Serán o hardware e software deseñados para cloud computing, que permiten interactuar cos servizos remotos.
- Aplicación: Son os servizos na “nube” ou “Software as a Service” (SaaS), o software proporciónase a través de internet coma se dun servizo se tratase. Deste xeito evítase a necesidade de instalar e

executar no equipo do cliente a aplicación. Redúcense así o mantemento e o apoio.

- **Plataforma:** Son os servizos de plataforma na “nube”, tamén coñecidos como “Platform as Service” (PaaS); proporcionan unha plataforma de procesamento e unha pía de solucións como un servizo, constitúen a base e infraestrutura das aplicacións da nube. Facilita o desenvolvemento de aplicacións evitando o custo e a complexidade de mercar e manter o hardware e as capas de software de base.
- **Infraestrutura.** Servizos de infraestrutura, tamén coñecidos como “Infrastructure as a Service” (IaaS); proporciona a infraestrutura como un servizo, adoita ser unha plataforma virtualizada. En lugar de mercar servidores, software, centro de datos especiais ou equipos de rede, os clientes adquiren estes recursos de servizos externos. A IaaS evolucionou a partir das ofertas de servidores virtuais privados.

### **57.6.2 Modelos de implementación**

- **Nube pública ou external cloud:** É o concepto tradicional onde os recursos se presentan a través de internet en función da demanda, a través de aplicacións ou servizos web.
- **Nube da comunidade:** Dáse cando varias organizacións coas mesmas necesidades comparten recursos. Neste caso existen menos usuarios que na nube pública e ofrécese maior privacidade e seguridade. Un exemplo pode ser o “Gov Cloud” de Google.
- **Nube híbrida:** É común que unha empresa use tanto a nube pública como desenvolvementos privados para satisfacer as súas necesidades con respecto ás TI. Existen varias empresas como HP, IBM, Oracle e VMware que ofrecen tecnoloxías para manexar a complexidade de mantemento, seguridade e privacidade consecuencia do uso do conxunto destes servizos.

- Nube combinada: Denomínase ao conxunto formado por varios servizos cloud de distintos provedores.
- Nube privada: É trasladar o concepto de nube pública a unha rede de uso privado. É dicir, o uso da nube única e exclusivamente dentro da rede dunha empresa.

### **57.7 GREEN IT E EFICIENCIA ENERXÉTICA**

O termo Green Computing acuñouse posiblemente por vez primeira tralo inicio do programa Energy Star en 1992, promovido polo Goberno estadounidense.

Tiña por obxectivo etiquetar monitores e equipamento electrónico caracterizados pola súa eficiencia enerxética. O termo quedou rexistrado xa en 1992 nun grupo de noticias. Hoxe en día o programa Energy Star é o motor da eficiencia enerxética nos sistemas electrónicos (non só de procesamento da información, senón tamén do equipamento electrónico doméstico).

A adopción de produtos e aproximacións máis eficientes poden permitir máis equipamento dentro do mesmo gasto enerxético, o que se denomina pegada enerxética, ou energy footprint. As regulacións estanse multiplicando e poderían limitar seriamente as empresas á hora de construíren centros de procesamento de datos, xa que o efecto das redes de abastecemento eléctrico, as emisións de carbono polo incremento de uso e outros impactos ambientais están a ser investigados. Xa que logo, as organizacións deben considerar as regulacións e ter plans alternativos para o crecemento dos seus centros de procesamento de datos e da súa capacidade.

Co paso dos anos, o número de servidores existentes en todo o mundo crece de forma case exponencial. Consecuencia disto é o crecente gasto enerxético para a refrixeración e xestión dos equipos. Hoxe en día xa se

están empezando a propoñer solucións que optimicen este gasto enerxético.

Este consumo enerxético non é o único problema ambiental relacionado coas TI. A etapa de fabricación de equipos presenta serios problemas relacionados co ambiente: materiais de refugallo tóxicos, produción de gases contaminantes, etc. A tendencia actual é a de minimizar o impacto contaminante (carbon footprint) presente nas tecnoloxías de fabricación dos sistemas electrónicos.

Finalmente, tamén ten un impacto inmediato a eliminación de equipos para as TI, caracterizados por un tempo de vida incrivelmente breve duns dous ou tres anos. Se non se reciclan de forma eficiente acaban tirados en vertedoiros e, debido á presenza de compoñentes tóxicos, son unha fonte de contaminación terrestre e das augas. Todos estes aspectos deben ser considerados de xeito global polos fabricantes e usuarios de equipos TI. A concienciación da existencia deste problema levou á elaboración de numerosas e ríxidas normativas a todos os niveis, o que empeza a obter algúns resultados.

GreenPeace Internacional realiza unha clasificación cos 18 principais fabricantes do sector electrónico (ordenadores persoais, teléfonos móbiles, etc.) de acordo coas súas políticas de redución de emisións tóxicas, reciclaxe ou minimización de impacto no cambio climático, e publícao na súa “Guía para a Electrónica Verde” (*Guide to Greener Electronics*), de publicación trimestral. Como se pode ver nos resultados de decembro de 2010, as empresas do sector obteñen unhas cualificacións realmente baixas, sendo a mellor Nokia, cun 7,5 sobre 10.

A metade destas 18 empresas suspenden un estudo que busca que as empresas analizadas:

- Limpen os seus produtos ao eliminar substancias perigosas. Os produtos químicos perigosos con risco impiden a posterior reciclaxe dos equipos.
- Reciclen equipos/productos baixo a súa responsabilidade unha vez quedan obsoletos.
- Reduzan o impacto climático debido ás súas operacións e produtos.

Por todo o exposto, a resolución efectiva do impacto ambiental das tecnoloxías TI require un enfoque holístico do problema que englobe as catro vías:

- Utilización ecolóxica: principalmente a través da redución do consumo enerxético. A produción de enerxía eléctrica é a principal fonte de xeración de gases de efecto invernadoiro.
- Deseño ecolóxico ou eco-deseño: inclúe deseño de equipos máis eficientes enerxeticamente e respectuosos co ambiente.
- Fabricación ecolóxica: eliminando completamente ou minimizando o impacto do proceso de fabricación no ambiente (emisións, materiais de refugallo, etc.).
- Eliminación ecolóxica: unha vez finalizado o período de utilización dun equipo, débense poñer en marcha as estratexias denominadas tres R: reutilización e renovación de equipos e, se non son aproveitables, reciclaxe.

A idea principal do enfoque holístico é que se peche o ciclo de vida dos equipos TI de xeito que non se prexudique o ambiente, o que permitiría conseguir unha mellora substancial cara ao desenvolvemento sostible.

#### **57.7.1      *Tecnoloxías verdes***

Hoxe en día existen distintos enfoques tecnolóxicos que se achegan a un desenvolvemento sostible das TI.

- **Monitores LCD.** Co paso dos anos os monitores pasaron de ser CRT a LCD; este cambio non é só estético ou de tamaño, senón que os niveis de consumo diminuíron notablemente. Un monitor CRT medio require 85W se está activo, fronte aos 15W dun LCD, 5W en modo baixo consumo para un CRT mentres que un LCD consumiría 1,5W. Apagados os dous consumirían 0,5W. Nos últimos anos revolucionouse o mercado das pantallas de ordenador coa aparición da tecnoloxía OLED (Organic Light Emitting Diode), baseada na utilización de díodos LED cuxa capa electro-luminescente se fai cun composto orgánico (un polímero que se ilumina ao aplicarlle unha voltaxe). A vantaxe principal deste tipo de pantallas fronte ás tradicionais de cristal líquido (LCD) é que os díodos OLED non necesitan retro-iluminación, polo que o consumo de enerxía que requiren é moi inferior.
- **Discos duros.** O consumo dos discos duros non é para nada desprezable, sobre todo no arranque do sistema. Por exemplo, o disco Seagate Barracuda 7200.8 require ata 2,5 A da liña de alimentación de 12 V. Se a isto lle sumamos 3W que extrae desde a liña de +5 V pódese chegar a un consumo de pico no arranque de 33 W. Se en lugar de só un disco duro falamos dun equipo con dous ou máis empezamos a falar de cifras moi comprometidas. Isto fixo que os fabricantes de discos duros comezasen a ter en conta o consumo nos seus produtos, creando case todos unha nova gama denominada “verde” ou “ecolóxica”. Por exemplo, Western Digital con “Caviar Green”, Samsung con Eco Green, ou Hitachi con eco-friendly Deskstar e Travelstar. Como alternativa aos discos tradicionais aparecen os discos en estado sólido (SSD), que presentan menores consumos de enerxía e é a tecnoloxía á que se espera evolucionen os sistemas de almacenamento.

- CPD. Aquí é onde se aloxa toda a infraestrutura de soporte aos diversos servizos computacionais, e unha estrutura adecuada permitirá bos aforros de enerxía, de espazo e de custos a medio e/ou longo prazo. Buscando a redución de enerxía pódese empezar pola acción máis simple, que é apagar o equipo que non se estea utilizando, a redución do hardware estudando necesidades reais, ou actuacións específicas en función da actividade da empresa.
- Virtualización. A virtualización de servidores permite o funcionamento de múltiples servidores nun único servidor físico. Isto axuda a reducir a pegada de carbono do centro de datos ao diminuír o número de servidores físicos e consolidar múltiples aplicacións nun único servidor, co cal se consome menos enerxía e se require menos arrefriamento. Ademais lógrase un maior índice de utilización de recursos e aforro de espazo.
- Cliente/Servidor. Estes sistemas manteñen o software, as aplicacións e os datos no servidor. Pódese ter acceso á información desde calquera lugar e o cliente non require moita memoria ou almacenamento. Este ambiente consome menos enerxía e arrefriamento.
- Cloud computing. Isto proporciónalles aos seus usuarios a posibilidade de utilizar unha ampla gama de recursos en rede para completar o seu traballo. Ao utilizar computación en nube, as empresas vólvense máis ecolóxicas porque diminúen o seu consumo de enerxía ao incrementar a súa capacidade sen necesidade de investir en máis infraestrutura.
- Tele traballo. Definido por *Merrian-Webster* como o traballo en casa co uso dun enlace electrónico coa oficina central. Ao non se desprazar o empregado, a contaminación é menor.

### **57.7.2      Actividades relacionadas con Green IT**

Existen varias actividades que promoven e intentan liquidar as cuestións expostas anteriormente. Estas actividades están patrocinadas ben desde administracións públicas, ben desde empresas, que están entendendo que Green IT, ademais dunha necesidade, pode ser un negocio, desde o punto de vista de asesoría e servizos, ou ben por consorcios de empresas.

The Green Grid (<http://www.thegreengrid.org>) é un consorcio global dedicado a avanzar na eficiencia enerxética dos centros de procesamento de datos e en ecosistemas de computación de negocio. En cumprimento da súa misión, The Green Grid céntrase en:

- Definir métricas e modelos significativos e centrados no usuario.
- Desenvolver estándares, métodos de medida, procesos e novas tecnoloxías para mellorar o rendemento dos centros de procesamento de datos fronte ás métricas definidas.
- Fomentar a adopción de estándares, procesos, medidas e tecnoloxías enerxeticamente eficientes.

O comité de directores de The Green Grid está composto polas seguintes compañías membros: AMD, APC, Dell, HP, IBM, Intel, Microsoft, Rackable Systems, Sun Microsystems e VMware.

Climate Savers. Iniciada por Google e Intel en 2007, Climate Savers Computing Initiative ([www.climatesaverscomputing.org](http://www.climatesaverscomputing.org)) é un grupo sen ánimo de lucro de consumidores e negocios con conciencia ecolóxica e organizacións conservacionistas. A iniciativa comezou baixo o espírito do programa Climate Savers de WWF (<http://www.worldwildlife.org/climate/projects/climateSavers.cfm>), que mobilizou a unha ducia de compañías desde 1999 para que recortasen as emisións de dióxido de carbono, demostrando que reducir as emisións é bo para o negocio. O seu obxectivo é promover o desenvolvemento,



despregamento e adopción de tecnoloxías intelixentes que poidan mellorar a eficiencia de uso da enerxía do computador e reducir o seu consumo cando o computador se atopa inactivo.

SNIA (Storage Networking Industry Association, <http://www.snia.org>) é unha organización global sen ánimo de lucro composta por unhas compañías da industria do almacenamento. SNIA Green Storage Initiative (<http://www.snia.org/green>) está levando a cabo unha iniciativa para avanzar no desenvolvemento de solucións enerxeticamente eficientes para o almacenamento en rede, incluíndo a promoción de métricas estándares, a formación e o desenvolvemento de boas prácticas enerxéticas ou o establecemento de alianzas con organizacións como The Green Grid.

Energy Star. En 1992 a Axencia de Protección Medioambiental de EE.UU. (U.S. Environmental Protection Agency) lanzou o programa Energy Star, que se planificou para promover e recoñecer a eficiencia enerxética en monitores, equipos de climatización e outras tecnoloxías. Aínda que de carácter voluntario inicialmente, resultou pronto de ampla aceptación, pasando a ser un feito a presenza dun modo de descanso (sleep mode) na electrónica de consumo.

Directiva Europea de Eco-Deseño. Seguindo a mesma liña que a iniciativa Energy Star de EE.UU., a Unión Europea aprobou a Directiva 2005/32/EC para o eco-deseño, novo concepto creado para reducir o consumo de enerxía de produtos que a requiren, tales como os dispositivos eléctricos e electrónicos ou electrodomésticos. A información relacionada coas prestacións ambientais dun produto debe ser visible, de xeito que o consumidor poida comparar antes de comprar, o cal está regulado pola Directiva de Etiquetaxe da Enerxía (Energy Labelling Directive). Os produtos aos que se lles conceda a eco-etiqueta serán considerados como cumpridores das medidas, de forma moi similar á etiqueta de Energy Star.

O Código de Conduta da Unión Europea para Centros de Datos está sendo creado como resposta ao crecente consumo de enerxía en centros de datos

e á necesidade de reducir o impacto ambiental, económico e de seguridade de abastecemento enerxético relacionado. O obxectivo é informar e estimular aos operadores ou propietarios dos centros de datos a que reduzan o consumo de enerxía dunha forma rendible sen dificultar o seu funcionamento. Este código de conduta quere conseguir isto mediante a mellora da comprensión da demanda de enerxía dentro do centro de datos, aumentando a concienciación, e mediante a recomendación de prácticas e obxectivos enerxeticamente eficientes.

Grupo de traballo sobre Green IT da plataforma INES (Iniciativa Española de Software e Servizos, <http://www.ines.org.é>) é a Plataforma Tecnolóxica Española na área dos Sistemas e Servizos Software e constitúe unha rede de cooperación científico-tecnolóxica integrada polos axentes tecnolóxicos relevantes deste ámbito (empresas, universidades, centros tecnolóxicos, etc.).

Segundo a Axenda Estratéxica de Investigación de INES, o plan de dinamización para o Grupo de Traballo de Green IT consiste nas seguintes accións:

- Análise da influencia e importancia das solucións de Green IT.
- Difusión das informacións, noticias e existencia deste grupo de traballo por Internet.
- Fomentar o interese e apoiar o desenvolvemento baixo Green IT.

Big Green Innovations (<http://www.ibm.com/technology/greeninnovations/>), programa de IBM. Dentro deste programa, e con fins educativos, IBM presentou un centro de datos virtual ecolóxico denominado Virtual Green Data Center.

A lista Green500 (<http://www.green500.org>) proporciona unha clasificación dos supercomputadores máis eficientes enerxeticamente do mundo,

servindo como unha visión complementaria á lista Top500 (<http://www.top500.org>).

Outras empresas, como Google, Dell ou Symantec, están desenvolvendo programas de eficiencia enerxética, tanto para os seus propios procesos de TI como para os dos seus 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. Berlín: Springer, cop. 2007.
- Virtualización na Wikipedia: <http://é.wikipedia.org/wiki/Virtualizaci%C3%B3n>
- *Green IT: Tecnologías para la Eficiencia Energética en Sistemas TI.* Marisa López-Vallejo, Eduardo Huedo Cuesta e 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 Rodríguez Martínez

Subdirector de Sistemas da Escola Superior de Enxeñaría Informática de Ourense

Colexiado do CPEIG



**58. REDES SAN E ELEMENTOS  
DUN SAN. REDES DE  
ALMACENAMENTO:  
TOPOLOXÍAS, PROTOCOLOS,  
ELEMENTOS DE CONEXIÓN.  
SISTEMAS DE  
ALMACENAMENTO:  
ARQUITECTURAS E  
COMPOÑENTES. SERVIDORES:  
HBA E SOFTWARE MULTIPATH.**

**Tema 58: Redes SAN e elementos dun SAN. Redes de almacenamento: topoloxías, protocolos, elementos de conexión. Sistemas de almacenamento: arquitecturas e compoñentes. Servidores: HBA e Software MultiPath.**

---

## **ÍNDICE**

58.1.1 Estructura das SAN.....	5
58.1.2 Protocolos.....	5
58.1.3 Topoloxías.....	8
58.1.3.1 Topoloxías en AoE.....	8
58.1.3.2 Topoloxías en Fibre Channel.....	9
58.1.3.3 Topoloxías en iSCSI.....	11
58.2.1 Arrays de discos.....	11
58.2.2.1 Estratexias (Niveis) de RAID.....	12
2.2 Copias de seguridade.....	19
58.3.1 Protocolos de SAN e HBAs.....	22
58.3.2 Software multipath.....	23

### **58.1. REDES DE ALMACENAMIENTO: TOPOLOXÍAS, PROTOCOLOS, ELEMENTOS DE CONEXIÓN.**

Como resumo unha SAN é unha rede donde se realiza o almacenamento e se xestiona a seguridade dos datos. As SAN ( *Storate Area Network*, Redes de Almacenamento) son redes nas que se conectan servidores de almacenamento (especialmente arrays de discos). Tamén hai que considerar como parte das SAN as librerías necesarias para o uso dos arrais e os accesos ás redes. De forma contraria ás redes tradicionais, nas SAN empréganse protocolos orientados á recuperación da información dos arrays de disco e inspirados nos propios estándares de comunicación con discos tradicionais (SCSI e SATA).

Normalmente o equipamento deseñado para participar nestas redes soe ser especialmente caro aínda que o seu prezo depende, nunha grande medida, ás tecnoloxías e protocolos empregados para a transmisión dos datos. Entre as tecnoloxías disponibles na actualidade atópanse: iSCSI (Internet Small Computer Storage Interconnect), Fibre Channel e AOE (ATA Over Ethernet, Advanced Technology Attachment Over Ethernet).

Entre as vantaxes da interconexión de redes de almacenamento resáltanse as seguintes:

- Elimina os límites de distancia de discos introducidos por SCSI ou ATA
- Consigue maior caudal de datos xa que os protocolos están especificamente deseñados para a transferencia de datos de dispositivos de almacenamento.
- Permite un aproveitamento maior dos discos permitindo que máis dun servidor acceda ao mesmo disco.
- Capacidade para o uso de múltiples discos de forma transparente dende un ou varios servidores.

- Adquisición de discos diferida debido ao maior aproveitamento
- Capacidades de recuperación ante desastres. Os arrays de discos empregados nas SAN soen dispor de discos de reserva (para fallos doutros discos) e permitir distintos esquemas de RAID.
- Recuperación en quente ante desastres
- Mellor capacidade de administrador. A administración é máis sinxela e está máis centralizada.
- Reducción dos custos de administración e de almacenamento de datos
- Mellora de dispoñibilidade global xa que as SAN teñen menos fallos ca os discos internos dos equipos.
- Reducción de servidores eliminando servidores de arquitos antigos (NFS, SMB, etc).
- Reducción do caudal das redes convencionais pois as copias de seguridade podense facer dende as SAN
- Incremento da rapidez das operacións de Entrada/Saída
- Reducción dos custos de administración de backups
- Protección de datos críticos
- Incremento da capacidade de forma transparente
- Desenvolvemento e proba de aplicacións de forma máis eficiente mediante o uso de copias dos datos de produción realizadas na SAN.
- Facilita o emprego de clusters de servidores que teñen que dispor dun almacenamento común.
- Permiten o almacenamento baixo demanda de forma que calqueira servidor pode solicitar espacio de almacenamento segundo as súas necesidades.

Dentro dunha organización, deberíase incluír nunha SAN a seguinte información:

- A información almacenada por SGBDs (Sistemas Xestores de Bases de Datos). De feito, algúns sistemas xestores como Oracle, Sybase, SQLServer, DB2, Informix ou Adabase recomendan esta alternativa

- A información almacenada por servidores de arquivos. Os servidores de arquivos funcionarán mellor e con menos recursos se os arquivos están almacenados nunha SAN.
- Servidores de backup. Se os servidores de backup están conectados a unha SAN conseguírase reducir os tempos de copia de seguridade con respecto a facelos nunha LAN (Local Area Network, Rede de Área Local) e reducir o tráfico da LAN.
- Arquivos de servidores de voz e video para streaming. Debido a que este tipo de servizos require grandes cantidades de disco, unha SAN pode reducir os custes asociados ao almacenamento desprazar o máximo posible o custo (incluir novos discos nos arrays cando sexan necesarios).
- Buzóns de usuario (mailboxes) de servidores de correo permitindo que os servidores de correo funcionen mais rápido e que se poida realizar unha restauración rápida en caso de que algún arquivo se corrompa.
- Servidores de aplicacións de alto rendemento. As SAN poden mellorar o rendemento de calquera aplicación incluíndo xestores documentales, aplicacións científicas, aplicacións de datawarehouse e cadros de mando integrais, aplicacións para xestionar as relacións cos clientes (CRM), etc.
- Solucións de Virtualización.

Asimesmo non é convinte usar unha SAN para:

- Servidores web que non requiran grandes necesidades de almacenamento (a maioría)
- Servidores con servizos de rede básicos como DNS, DHCP, WINS (Windows Internet Name Servers) e controladores de dominio de Windows (DC). Este tipo de servidores non requiren das capacidades de almacenamento permitidas polas SAN.
- PCs de escritorio
- Servidores que necesitan menos de 10Gb de almacenamento
- Servidores que non necesitan un acceso rápido á información



- Servidores que non comparten arquivos

### **58.1.1 Estructura das SAN**

Habitualmente as SAN concíbense e estruturanse en tres capas:

1. A capa de hosts: Constituída na súa maioría polos servidores, os drivers e software necesarios para a conexión á rede e os HBAs (Host Bus Adapters) que son dispositivos (tarxetas) que se conectan a cada servidor para acceder ao almacenamento (nalgúns solucións concretas son adaptadores Ethernet simples e no caso Fibre Channel levan un conector GBIC-Gigabit Interface Connector).
2. A capa de estrutura (fabric layer): Constituída por HUBs, Switches, Gateways e Routers se fose necesario. Se se emprega a tecnoloxía Fibre Channel, todos estes dispositivos empreñan GBICs (Gigabit Interface Connectors) para a interconexión dos dispositivos das capas superiores e inferiores.
3. A capa de almacenamento (storage layer): Constituída por todo tipo de dispositivos de almacenamento.

Un conxunto de discos situados no mesmo sitio e sen funcionalidades adicionais coñécese como JBOD (Just a Bunch Of Disks). Dentro da capa de almacenamento, os arrays non son simplemente JBODs, senón que inclúen certas funcionalidades interesantes implementadas no firmware da controladora como o RAID.

### **58.1.2 Protocolos**

Na actualidade existen distintos protocolos que permiten as comunicacións na capa de infraestrutura entre os distintos equipos que participan nunha 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) e (viii) iSER (iSCSI Extensions for RDMA).

AoE permite facer dispoñíble discos SATA a través dunha rede Ethernet interconectada con fíos de par trenzado (Gigabit Ethernet) ou fibra óptica (10 Gigabit Ethernet). Este tipo de solucións é moi popular polo seu baixo custe e alto rendemento. Coraid Inc. fabrica este tipo de solucións.

FCP é a solución máis destacada e permite mapear o protocolo SCSI sobre Fibre Channel. Fibre Channel é unha tecnoloxía Gigabit e deseñado especificamente para redes SAN. Fibre Channel é un protocolo inspirado no modelo OSI e deseñado en 5 capas (FC0, FC1, FC2, FC3 e FC4) e, a pesar do seu nome, pode ser empregado sobre cables de fibra ou pares trenzados.

FcoE é unha encapsulación do protocolo Fibre Channel sobre redes Ethernet. Deste xeito as capas FC0 e FC1 son reemplazadas polas capas física e de Enlace empregadas no protocolo Ethernet. Empregando esta tecnoloxía pódense combinar na SAN tecnoloxías baseadas no uso do protocolo IP con Fibre Channel ou empregar o mesmo hardware para a rede LAN e a SAN reducindo o custo do hardware.

ESCON (Enterprise System Connection) sobre Fibre Channel (FICON) é un protocolo empregado para interconectar mainframes de IBM con dispositivos de almacenamento ESCON (tamén deseñados por IBM).

HyperSCSI permite o mapeo de SCSI sobre redes Ethernet. Non chegou a ser comercializado porque xa que FCP estaba totalmente establecido. É unha solución de baixo custo semellante a AoE que usa directamente o protocolo Ethernet para transmitir comandos SCSI (CDBs, Command Descriptor Blocks).

iFCP ou SANoIP: Son solucións para mapear FCP sobre o protocolo IP.

iSCSI (Internet Small Computer Interface) é un protocolo da capa de aplicación de TCP/IP para o almacenamento de datos que se usa para transmitir comandos SCSI (CDBs). Funciona habitualmente nos portos 860 e 3260 TCP. Este tipo de solucións pode ser empregada para almacenamento empregando redes de área extensa (incluso Internet). Os clientes de almacenamento chámanse iniciadores (initiators) e poden realizar operacións de almacenamento sen necesidade de empregar cables de propósito específico como no caso de FCP.

iSCSI Extensions for RDMA (Remote Direct Memory Access) (iSER). É unha tecnoloxía que permite extender o protocolo iSCSI implementando o Acceso Directo a Memoria. Este acceso directo a memoria é típicamente implementado sobre TCP mediante o protocolo iWARP (Internet Wide Area RDMA Protocol) ou sobre a tecnoloxía InfiniBand que é un estándar que proporciona conectividade de alta velocidade e baixa latencia para o almacenamento de datos.

Debido a que os protocolos máis empregados para desenvolvemento de SAN son FCP, iSCSI e AoE, o documento centrarase en maior medida neles. A figura 1 amosa unha comparativa entre as capas que componen os protocolos máis empregados para o desenvolvemento de SAN.

	SCSI	SCSI	
	iSCSI	FC4 – Capa	
		de mapeo	
ATA	Capa de transporte	-FC3 – Capa	
	TCP	de servizos	
		comúns	
AoE	Capa de rede – IP	FC2 – Capa de	FC-PH
		Red	
Capa de Enlace –	Capa de enlace –	FC1 – Capa de	
Ethernet	Ethernet	Enlace	
Capa física	Capa física	FC0 – Capa física	
AOE	iSCSI	Fibre	
		Channel	

*Figura 1: Estrutura dos protocolos de SAN máis extendidos*

Como se pode ver na *Figura 1*, a Tecnoloxía AOE é moito máis sinxela que as tecnoloxías iSCSI ou FibreChannel. De aí deriva o seu baixo custo e a súa rapidez.

### **58.1.3 Topoloxías**

As topoloxías dispoñibles para o desenvolvemento de SAN dependen de forma importante das tecnoloxías empregadas. Polo tanto, este subapartado dividírase en distintas seccións para estudar as topoloxías posibles segundo cada un dos protocolos estudados.

#### **58.1.3.1 Topoloxías en AoE**

AoE depende exclusivamente do protocolo Ethernet (capa física e de enlace do modelo TCP-IP) obviando a estrutura e funcionamento das capas superiores (IP, TCP, UDP). AoE non permite o routing (por funcionar sobre a capa de enlace) e representa unha alternativa de baixo custo para iSCSI y Fibre Channel. Ademais de existir hardware específico (Coraid Inc.), existen distribucións de Linux que implementan o protocolo do lado do servidor

permitindo compartir discos segundo este paradigma (Lanart Bussiness Server).

Dado a súa particular concepción, as topoloxías típicas de AoE son equivalentes ás distintas posibilidades de interconexión que ofrece Ethernet a nivel de capa 2. Polo tanto, AOE permite dúas topoloxías básicas:

- Punto a punto na que o equipo host interconéctase directamente co dispositivo de almacenamento mediante un cable par trenzado.
- Infraestrutura conmutada. Todos os dispositivos interconéctanse cun switch Ethernet. Segundo as interfaces de rede dos arrays (Gigabit / 10 Gigabit) haberá que empregar un switch adecuado e un dispositivo adecuado para o computador (con fíos de par trenzado ou fibra).

#### 58.1.3.2 Topoloxías en Fibre Channel

Un enlace Fibre Chanel está constituído por dúas fibras ópticas empregadas para transmitir TX e recibir RX. Para a comunicación empregando as fibras ópticas emprégase un protocolo específico deseñado especificamente para a comunicación con dispositivos de almacenamento.

Con esta tecnoloxía pódense despregar tres tipos de topoloxías:

1. Punto a punto (FC-P2P, Point to Point): implica que sólo existen dous dispositivos participando na SAN que son o servidor e o array de disco. Estos dispositivos interconectanse directamente.
2. Anel arbitrado (FC-AL, Arbitrated loop): implica que os dispositivos están nunha disposición en forma de anel (Token Ring). No anel participan tanto servidores como arrays de disco. O principal problema desta topoloxía consiste en que cando falla unha conexión interrompese o funcionamento do anillo enteiro. Este é o método máis barato para crear unha SAN.
3. Infraestrutura conmutada (FC-SF, Switched Fabric). Todos os dispositivos se conectan a conmutadores (switches) de FC. A forma

de funcionar é moi similar ao funcionamento de Ethernet no sentido en que cando un servidor quere realizar unha operación de almacenamento nun array, realízase unha interconexión das bocas do switch donde está o servidor e o array.

No caso de contar con aneis arbitrados, soense usar hubs (concentradores) que realizan internamente as conexións que implementan o anel. Na Figura 2 amósase esquemáticamente o funcionamento dun hub.

#### *Figura 2: Esquema de funcionamento dun hub*

Dado o funcionamento interno dun hub, o despregue de topoloxías en anel resulta moi sinxelo. Ademais, este tipo de topoloxías admite infinidade de arquitecturas de rede entre as que se inclúen a colocación de hubs en cascada (Figura 3) ou en bucle.

#### *Figura 3: Topoloxía en anel usando hubs en cascada*

No caso das topoloxías de anel unindo os hubs en forma de bucle obtense unha mellor redundancia para as conexións. Aínda que pareza estrano, este tipo de configuracións pode tolerar fallos nun determinado hub así como a posibilidade de usar distintas rutas para as conexións que poden ser empregadas para mellorar a velocidade de transferencia de datos como se verá no apartado 3.

#### *Figura 4: Topoloxía en anel usando hubs en forma de bucle*

De forma semellante a cómo se pode refinar a topoloxía en anel, a topoloxía en de infraestrutura conmutada pode implementar bucles de switches ou outras combinacións que permiten eliminar a posibilidade de fallos e multiplicar as rutas dispoñibles para o acceso aos equipos participantes na SAN para aumentar a velocidade de acceso e implementar a tolerancia a fallos.

### 58.1.3.3 Topoloxías en iSCSI

iSCSI é unha arquitectura de SAN considerablemente distinta á ofrecida por Fibber Channel. En vez de deseñar por completo un protocolo, iSCSI é un protocolo que na capa de aplicación de TCP/IP aproveitando por completo toda a arquitectura de capas de TCP/IP e permitindo o salto entre distintas redes (routing). Na práctica, non ter unha conectividade cunha velocidade superior a 1 Gbps non permite alcanzar velocidades adecuadas no almacenamento.

Dado que iSCSI e FCP son protocolos moi extendidos, é posible mercar arrays que teñen soportan conexións iSCSI de forma nativa e implementan ao mesmo tempo un gateway para FCP. De feito, unha das maiores vantaxes introducidas por iSCSI é a posibilidade de administrar este tipo de equipos sen un coñecemento profundo de FCP aínda que con coñecementos avanzados de TCP/IP.

Debida a toda esta casuística, a topoloxía en iSCSI pode ser calqueira empregada nunha rede TCP/IP convencional despregada sobre unha capa de enlace calqueira (Ethernet, 802.11x, Token Ring, etc).

## **58.2. SISTEMAS DE ALMACENAMENTO: ARQUITECTURAS E COMPOÑENTES**

Os sistemas de almacenamento que se poden conectar a unha SAN son arrays de discos e sistemas de backup. Nos seguintes subapartados farase unha descripción detallada de estas tecnoloxías.

### **58.2.1 Arrays de discos**

Un array de discos é un sistema de almacenamento que contén múltiples discos. A principal diferenza con un JBOD é que dispón de memoria caché e funcionalidades avanzadas como o RAID e a virtualización. Un array de discos componse de:

- Unha controladora de disco
- Memoria cache
- Carcasa dos discos
- Fonte de alimentación

Normalmente os arrays de discos soen contar con maior dispoñibilidade, resistencia e facilidade de mantemento. Para implementar estas características emplean redundancia de hardware. Ademais normalmente, os discos poden ser intercambiados sen realizar un apagado do equipo.

Dentro dos arrays de discos é común empregar distintos esquemas de RAID (Redundant Array of Independent Disks) para xestionar o espazo nos discos. A nivel lóxico, a tecnoloxía RAID permite combinar varios discos físicos nunha soa unidade de disco lóxica á que se lle asigna un identificador único chamado LUN (Logical Unit Number).

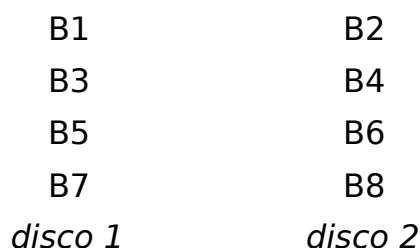
Outra característica habitual dos arrays de disco é a existencia de discos de reserva (spare disks) que serven para o reemplazo automático de discos que fallan nun volume RAID (so ten sentido nalgúns tipos de RAID). O seguinte apartado presenta as estratexias de RAID e as súas características. Os discos de reserva poden ser hot spare (en quente) ou (standby spare) en frío. A diferenza dos standby, os hot están físicamente conectados á SAN e inicializados de forma que o proceso de uso é máis eficiente.

#### 58.2.2.1 Estratexias (Niveis) de RAID

Existen distintos niveis de RAID que teñen que ver cos esquemas de seguridade e redundancia implementados. Os esquemas de RAID máis empregados son o 0, 1 e o 5. Non obstante, existen multitude de esquemas algúns dos cales son propietarios.



Un RAID 0 (ou volumen dividido) distribúe os datos equitativamente entre dous ou máis discos sen información de paridade nin redundancia algunha. RAID 0 permite aumentar o rendemento e crear grandes volúmenes virtuais mediante a combinación de discos de pequena capacidade. Un RAID 0 creado a partir de discos de distinto tamaño terá unha capacidade igual ao número de discos multiplicado polo tamaño do disco con menor capacidade. A fiabilidade dunha unidade lóxica RAID 0 será igual á fiabilidade media dos discos que o compoñen. Non é posible a utilización de discos de reserva cando se produce un fallo dun disco. A Figura 5 amosa unha configuración RAID 0.



*Figura 5: Esquema de uso dos discos en RAID 0*

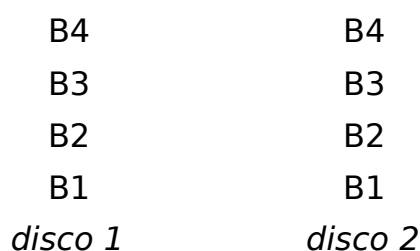
Un RAID L distribúe os datos en dous ou máis discos de forma non equitativa e sen paridade nin redundancia algunha. Os discos funcionan como extensións permitindo aumentar o espazo dispoñible pero sen sacar proveito do feito de existir varios discos. Cando existen discos de distintos tamaños, unha unidade lóxica RAID L permite que a capacidade global sexa igual á suma das capacidades dos discos que o conforman. A figura 6 amosa un esquema do funcionamento de RAID L.

B6  
B5  
B4  
B3



*Figura 6: Esquema de uso dos discos en RAID L*

Un RAID 1 (ou espello) crea unha copia exacta dos datos almacenados en dous ou máis discos segundo se pode apreciar na figura 7. Un volume lóxico RAID 1 terá tanto espazo como o máis pequeno dos discos que o conforman. A fiabilidade de empregar un RAID 1 é igual ao produto das probabilidades de fallo dos discos que conforman o RAID 1. Ademáis, pese ao que parece máis probable, o tempo de acceso ao disco pode reducirse xa que é posible emplear as distintas copias para ler máis rápido. No caso de escritura os discos escríbense ao mesmo tempo sen empeorar nin mellorar o rendemento. Cando un disco falla neste esquema de RAID, é posible a súa substitución automática por un disco de reserva (spare disk).



*Figura 7: Esquema de uso dos discos en RAID 1*

Un RAID 2 divide os datos a nivel de bits (en lugar de a nivel de bloques como se fai nos anteriores esquemas) e usa un código de Hamming para a corrección de erros. Ademáis, os discos sincronízanse coa controladora para funcionar cunha alta taxa de transferencia. A pesares de esto, actualmente non se emprega este tipo de RAID xa que teóricamente serían necesarios 39 discos nun sistema informático moderno dos que 32 se empregarían para almacenar os bits individuais e 7 para a corrección de erros. A figura 8

amosa un esquema do almacenamento dos bits nos distintos discos en RAID 2.

d1	d2	d3	d4	d <sub>p1</sub>	d <sub>p2</sub>	d <sub>p3</sub>
c1	c2	c3	c4	c <sub>p1</sub>	c <sub>p2</sub>	c <sub>p3</sub>
b1	b2	b3	b4	b <sub>p1</sub>	b <sub>p2</sub>	b <sub>p3</sub>
a1	a2	a3	a4	a <sub>p1</sub>	a <sub>p2</sub>	a <sub>p3</sub>
<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 dos discos en RAID 2*

Un RAID 3 usa unha división a nivel de bytes cun disco de paridade dedicado. Non se sóe usar na práctica xa que non é posible atender varias peticións simultáneas xa que cada bloque de disco (habitualmente de 512bytes) estará dividido en varios discos na mesma dirección en cada ún deles. A figura 9 amosa o funcionamento dun RAID 3.

b10	b11	b12	b <sub>p(10-12)</sub>
b7	b8	b9	b <sub>p(7-9)</sub>
b4	b5	b6	b <sub>p(4-6)</sub>
b1	b2	b3	b <sub>p(1-3)</sub>
<i>disco 1</i>	<i>disco 2</i>	<i>disco 3</i>	<i>disco 4</i>

*Figura 9: Esquema de uso dos discos en RAID 3*

Un RAID 4 (IDA, Independent Data Access) dispón de acceso independente aos discos e discos de paridade. Usa unha división a nivel de bloques con un disco de paridade adicado. Necesita un mínimo de 3 discos físicos permitindo que funcionen de forma independente cando se pide un único bloque. Ademáis, este esquema permite resolver peticións de escritura e lectura de forma simultanea sendo o único cuello de botella o disco que

almacena as paridades. A figura 10 amosa un esquema do funcionamento deste 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 dos discos en RAID 4*

Un RAID 5 usa unha división dos datos a nivel de bloques distribuíndo a información de paridade entre todos os membros do conxunto. Este esquema de RAID é moi popular gracias ao seu baixo custo na implementación da redundancia. Na práctica o calculo da paridade soe ser implementado por hardware. Funciona dun modo parecido á RAID 4 pero evitando que o disco de paridade sexa un cuello de botella mediante a distribución de toda a información de paridade por todos os discos. Ademáis permite a lectura e escritura de datos de forma simultánea sempre e cando os bloques que hai que ler simultaneamente estén en distintos discos. Este esquema permite o uso de discos de reserva de forma automática sempre e cando o fallo non se produza en máis dun disco aínda que, neste caso, ás veces faise uso da referencia RAID 5E. O número de discos que admite RAID 5 é teóricamente ilimitado permitindo reducir a probabilidade de fallos e aumentar o rendemento con cada disco adicional. A figura 11 amosa un esquema do funcionamento deste 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 dos discos en RAID 5*

Unha unidade lóxica RAID 6 amplia as funcionalidades dun volume RAID 5 engadindo un bloque de paridade adicional calculado a partir doutro polinomio diferente. Ao engadir códigos adicionais é posible alcanzar calqueira número de discos e recuperarse ante un fallo que se produza en 1 bloque por cada un dos discos. O RAID 6 é ineficiente cando se emprega un número reducido de discos pero aumenta a eficiencia a medida que se incrementa o número de discos. Neste sentido, as operacións de lectura non se ven penalizadas en exceso mentres que as operacións de escritura requiren dun maior tempo para o almacenamento dos dous códigos de paridade. A capacidade total de almacenamento dun volume RAID 6 é igual ao produto da capacidade dos discos multiplicado polo número de discos menos 2 [*capacidade* \* (*n*-2)]. De forma paralela a RAID 5, permítese o uso automático de discos de reserva aínda que esta variante é coñecida ás veces como RAID 6E. A figura 12 amosa un esquema do funcionamento deste 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 dos discos en RAID 6*

RAID 5E e 6E fai referencia, como ben se ten mencionado anteriormente ao uso de discos de reserva cos esquemas de RAID correspondentes. Hai que ter en conta non obstante, que os discos de reserva non pertencen nas solucións SAN a unha unidade lóxica concreta senón que están dispoñibles para os posibles fallos que poidan producirse en todas as unidades lóxicas do array de discos.

Unha unidade lóxica RAID 0+1 (ou RAID 01) é un RAID usado para compartir datos entre varios discos facendo un espello de cada copia segundo amosa a figura 13.

*Figura 13: Esquema de uso dos discos en RAID 0+1*

O esquema RAID 1+0 (as veces denominado RAID 10) é semellante ao RAID 0+1 coa excepción de que invirte os niveles de RAID que o forman segundo o esquema que se mostra na figura 14. Este esquema é moito máis robusto ca o raid 0+1 e está a empezar a ser adoptado en moitos entornos empresariais debido ao incremento da probabilidade de fallos nos novos discos.

*Figura 14: Esquema de uso dos discos en RAID 1+0*

De forma paralela a como se crearon or RAID 1+0 e 0+1 créáronse respectivamente os raid 3+0 e 0+3. Destos dous é popular o RAID 30 que está deseñado para obter unha tasa de transferencia alta con gran fiabilidade. O principal problema que plantexa é o seu custo de implantación debido á necesidade de empregar gran cantidade de discos.

Un RAID 100 (ou tamén chamado RAID 10 + 0) é unha división de conxuntos RAID 10. A principal vantaxe deste esquema é o maior rendemento mantendo un nivel de seguridade moi alto. Esta elección soe ser habitual para o almacenamento de bases de datos extremadamente grandes. A figura 15 amosa o funcionamento deste esquema de RAID.

*Figura 14: Esquema de uso dos discos en RAID 100*

Un RAID 50 (RAID 5+0) combina a división en bloques dun RAID 0 coa paridade distribuída dun RAID 5 tal como se amosa na figura 15.

*Figura 15: Esquema de uso dos discos en RAID 50*

Existen outras combinacións de RAID como o RAID 5+3, o RAID 0+5, o RAID 5+1 ou o RAID 6+0 que son factibles de ser implementados nas SAN. Sen embargo, a combinación de RAIDs non é unha estratexia comunmente empregada.

Tamén se destaca a existencia de distintos esquemas de RAID propietarios como son: RAID de Paridade Doble, RAID 1.5 (RAID 15 é incorrecto), RAID 7, RAID S (ou RAID de paridade), MATRIX RAID, IBM SERVER RAID 1E e RAID Z.

## **2.2 Copias de seguridade**

As copias de seguridade poden facerse sobre a rede LAN ou sobre a SAN. Sen embargo, o principal obxectivo das SAN é eliminar tráfico de almacenamento das redes LAN. Neste sentido resulta máis adecuado facer o backup dentro da propia SAN.

Existen dúas opcións para facer copias de seguridade sobre unha LAN: (i) Usar unha unidade de cinta en cada computador ou (ii) usar software de backup nun servidor para volcar a información sobre a LAN e facer o backup no servidor. A primeira das opcións é unha opción cara porque hai

que mercar unha unidade de cinta e as cintas correspondentes para cada servidor, mentres que a segunda opción resulta máis lenta e ocupa a meirande parte do ancho de banda da rede LAN. A opción de facer o backup na SAN resulta máis atractiva porque combina a vantaxe de realizar o backup na LAN coa posibilidade de eliminar o tráfico na rede LAN.

Cando se fala de backup é habitual manexar o termo de xanela de backup. A xanela de backup é simplemente un espazo de tempo no que se pode realizar a copia de seguridade e no cal, normalmente, as aplicacións non se están executando ou están en modo de offline. Este último concepto é habitual nos servidores de bases de datos (por exemplo o quiescent mode dos servidores IDS2K de Informix ou o offline mode das bases de datos de Oracle). A ventana de backup é cada vez máis pequena por necesidades propias das empresas (como a necesidade de globalizarse e internacionalizarse) e por iso cada vez é máis importante reducir o tempo de backup. Por iso é necesario conta cunha solución que sea realmente rápida sendo capaz de mover os datos dun xeito realmente eficiente. O backup na SAN resulta moito máis rápido reducindo asía xanela de backup necesaria.

Para realizar o backup pódense usar unidades de cinta colocadas nos propios servidores aínda que realizando as comunicacións unicamente sobre a SAN. Existen distintos tipos de unidades de backup con distintos tipos de medios de almacenamento incluíndo os seguintes: (i) DAT cunha capacidade dende 1.3 ata 80GB e unha velocidade entre 0,5 e 6 MBps., (ii) DLT cunha capacidade de 40 ata 80GB e unha velocidade de entre 6 e 60 MBps, (iii) SDLT cunha capacidade de 100 a 300GB e unha velocidade de entre 11 e 36 MBps, (iv) AIT cunha capacidade de 50 a 400GB e unha velocidade de entre 6 e 24 MBps, (v) LTO1-5 cunha capacidade entre 100GB e 1,6 TB e unha velocidade de entre 15 e 180 MBps. Segundo o dispositivo concreto será posible determinar o tempo necesario para almacenar os datos así como as unidades de cinta necesarias.



Outra posibilidade para realizar o backup nunha SAN consiste en empregar bibliotecas de cintas (a menudo coñecidos informalmente como robots de backup). As bibliotecas de cintas son conxuntos de cintas colocados en determinadas disposicións xunto cun brazo robotizado que permite o intercambio de forma automática da cinta que se está a grabar. Existen distintos tamaños de librerías de cintas logrando con algúns esquemas conseguir capacidades de backup importantes.

Ademáis dos backups sobre cintas, resulta interesante mencionar a posibilidade de facer imaxes e instantáneas (snapshots) dos contidos dos discos. Mentres que as imaxes son copias bit a bit dos discos, as instantáneas son soamente copias dos metadatos dos discos (punteiros que apuntan a onde está almacenada a información nos discos físicos). Este tipo de funcionalidades soe estar directamente implementada nos arrays de disco conectados ás redes SAN.

### **58.3. SERVIDORES: HBA E SOFTWARE MULTIPATH**

Para que os servidores da capa Host se poidan conectar á SAN necesitan empregar un HBA (Host Bus Adapter). Trátase dun dispositivo (tarxeta) que permite o acceso á SAN. Este mesmo término tamén se usa para dispositivos que permiten a conexión dentro do PC de dispositivos de almacenamento SCSI, SAS ou incluso SATA. Dependendo da tecnoloxía, o HBA pode ser diferente. O subapartado 3.1 fai un estudo dos distintos HBA empregados segundo o protocolo da rede SAN.

Doutra banda, ademáis do hardware é necesario dispor dun software a modo de controlador de dispositivo que implemente o acceso aos arrays que se encontran na SAN. Este software pode implementar multitude de características interesantes:

- Target: Permite que o equipo que ten instalado o software poida funcionar como dispositivo de almacenamento na rede SAN
- Multipath: Permite que o equipo poida acceder a un dispositivo da SAN empregando distintas rutas físicas (fios). Este acceso multiruta pode ser aproveitado para incrementar o ancho de banda, facer balanceos de carga sobre os paths ou ben para implementar redundancia de conexións ante fallos. Este apartado será especificamente tratado no apartado 3.2.
- iSCSI initiator: Combina unha rede SAN iSCSI co soporte nativo SCSI de forma que os discos remotos dos arrays actúan como discos locais SCSI.

### **58.3.1 Protocolos de SAN e HBAs**

Debido á existencia de gran variedade de protocolos para implementar ás SAN, existe unha ampla variedade de HBAs. Deste xeito, segundo o protocolo e tecnoloxía empregados, será necesario coñecer algunhas características básicas dos HBA necesarios.

Para conectar os hosts coas SAN que empreguen Fibre Channel é necesario contar con una tarxeta adaptadora. No caso deste protocolo, os HBA dispoñen de conectores GBICs (GigaBit Interface Connectors) para interconectar todos os elementos que conforman a SAN. Cada HBA dispón dun único WWN (World Wide Name) así como cada dispositivo Ethernet ten unha dirección MAC. Existen distintos modelos de HBA para FC con distintas velocidades: 1Gbps, 2Gbps, 4 Gbps, 8 Gbps, 10 Gbps e 20 Gbps. No caso de Fibre Channel o mesmo concepto HBA é abreviatura de High Bandwidth Adapter co mesmo sentido semántico.

Os HBA iSCSI ademáis de incluír unha interfaz 10GB Ethernet ou GB Ethernet, implementa normalmente un iniciador hardware de iSCSI. Este iniciador é hardware dedica que permite rebaixar a sobrecarga introducida

polo procesamento necesario para os protocolos TCP e iSCSI e as interrupcións Ethernet e mellorar polo tanto, o rendemento do servidor.

Coa tecnoloxía de Infiniband (iSER) HBA é abreviatura de Host Channel Adapter co mesmo sentido semántico.

Coa tecnoloxía AoE, o HBA é unha tarxeta Ethernet que permita a interconexión con fíos de par trenzado (en Gigabit Ethernet) ou fibra óptica (en 10 Gigabit Ethernet). Unha das vantaxes de AoE radica en que os HBA son excepcionalmente baratos.

### **58.3.2 Software multipath**

Unha característica importante das redes SAN son as súas capacidades multipath. Un path ou ruta é un camiño posible entre un HBA dun host ata á controladora dun array de discos. Un software multipath sería capa de aproveitar as distintas rutas para balancear a carga coa finalidade de maximizar a velocidade de acceso ou conseguir unha maior tolerancia a fallos.

Neste sentido, as veces os arrays de disco dispoñen de dúas conexións coa intención de facer dispoñibles múltiples paths entre un HBA dun host e unha unidade lóxica (LU) que poden ser aproveitados para unha maior velocidade de acceso. Esta característica é moi empregada en AoE, iSCSI e FC.

Na Wikipedia ([http://en.wikipedia.org/wiki/Multipath\\_I/O](http://en.wikipedia.org/wiki/Multipath_I/O)) podese obter un listado relativamente completo de software multipath para SAN.

#### **58.4 BIBLIOGRAFÍA**

1. Redes de área de Almacenamento na Wikipedia.  
[http://es.wikipedia.org/wiki/Red\\_de\\_área\\_de\\_almacenamiento](http://es.wikipedia.org/wiki/Red_de_área_de_almacenamiento)
2. Cristopher Poelker y Alex Nikitin. Storage Area Networks for Dummies.
3. RAID na Wikipedia. <http://es.wikipedia.org/wiki/RAID>

**Autor:** José Ramón Méndez Reboredo

Profesor Escola Superior Enxeñaría Informática Ourense

Colegiado del CPEIG

**59. SISTEMAS DE BACKUP:  
HARDWARE E SOFTWARE DE  
BACKUP. ESTRATEXIAS DE  
BACKUP A DISCO.  
DISPOÑIBILIDADE DA  
INFORMACIÓN RPO, RTO.  
REPLICACIÓN LOCAL E  
REMOTA, ESTRATEXIAS DE  
RECUPERACIÓN.**

Tema 59.- Sistemas de backup: hardware e software de backup. Estratexias de backup a disco. Disponibilidade da información RPO, RTO. Replicación local e remota, estratexias de recuperación.

---

<b>59.1 Sistemas de Backup: hardware e software de backup.....</b>	<b>3</b>
59.1.1 Hardware de Backup.....	4
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).....	6
59.1.1.1.3 Sun StorageTek T10000 (T10k).....	6
59.1.1.1.4 Características de almacenamento en cinta.....	7
59.1.1.2 Disco.....	8
59.1.1.3 Medios Virtuais.....	9
59.1.1.4 Medios Ópticos.....	9
59.1.1.4.1 CD.....	9
59.1.1.4.2 DVD.....	10
59.1.2 Software de Backup.....	11
59.1.2.1 Ferramentas de código aberto - AMANDA.....	11
59.1.2.2 Ferramentas de código aberto - BackupPC.....	12
59.1.2.3 Ferramentas de código aberto - Bacula.....	17
59.1.2.4 Software Propietario CommVault Simpana.....	19
59.1.2.5 Software Propietario Symantec NetBackup.....	21
<b>59.2 Estratexias de Backup a Disco .....</b>	<b>24</b>
<b>59.3 Disponibilidade da información RPO, RTO.....</b>	<b>28</b>
59.3.1.1 Obxectivo de Punto de Recuperación.....	29
59.3.1.2 Obxectivo Tempo de Recuperación.....	30
<b>59.4 Replicación local e remota, estratexias de recuperación.....</b>	<b>31</b>
59.4.1 Replicación Local.....	33
59.4.1.1 Tecnoloxías de replicación local.....	33
59.4.1.1.1 Baseada en replicación en host local.....	33
59.4.1.1.2 Baseada en arrays de discos.....	34
59.4.2 A replicación remota.....	35
59.4.2.1 Tecnoloxías de replicación remota.....	35
59.4.2.1.1 Replicación remota baseada en LVM.....	35

59.4.2.1.2 Baseada en transvase de rexistros.....	36
<b>59.5 Bibliografía.....</b>	<b>37</b>

### ***59.1 SISTEMAS DE BACKUP: HARDWARE E SOFTWARE DE BACKUP***

Un factor importante en todo sistema de backup é a elección dos sistemas hardware e software que o compoñen.



### **59.1.1 Hardware de Backup**

Na categoría de elementos hardware de backup temos:

#### *59.1.1.1 Cintas*

Tradicionalmente, os cartuchos de cinta magnética son os medios de comunicación máis habituais nos sistemas de backup. Como soporte de almacenamento dos respaldos de datos, a cinta magnética ten unha longa historia de uso e é o medio de copia de seguridade con maior nivel de madurez. A cinta magnética, ou dunha forma máis abreviada, a cinta, é un compoñente baseado en cartuchos que se fai tipicamente dalgún tipo de plástico ríxido. Contén un ou máis bobinas de plástico flexible que se impregnaron con un material con comportamento magnético.

Os cartuchos de cinta están fabricados en varios formatos. Cada formato ten unhas características diferentes que responden ás diferentes necesidades de almacenamento físico e de tempo de preservación de a copia de seguridade, tanto en termos da cantidade de datos almacenados, como de vida útil dos medios de almacenamento ou o seu custo. Os formatos de cinta de uso común son os seguintes:

- DLT/ SDLT
- LTO
- AIT
- STK 9840/9940/T10000

Segundo o tipo de cartucho de que se trate, varían as capacidades ou características como a velocidade de funcionamento. O mercado está renovando continuamente este tipo de dispositivos co fin de mellorar ambos aspectos. Con todo, existen tres formatos que podemos considerar

dos máis comúns e teñen características particulares que se describen aquí como exemplos de elementos arquitectónicos de deseño: *DLT, LTO, T10000 e STK*.

O resto dos formatos, aínda que sexan comúns, utilízanse normalmente para contornos especializados, coma o arquivado e almacenamento intermedio (nearline storage) empregado entre o almacenamento online e o almacenamento de backups.

#### ***59.1.1.1.1 Digital Linear Tape (DLT)***

Digital Linear Tape (DLT) é o formato de cinta máis antigo e polo tanto un dos produtos máis maduros do mercado. Orixinalmente foi deseñado e implementado por DEC en 1984, para posteriormente ser adquirida por Quantum e redistribuído en 1994.

DLT é o primeiro cartucho de cinta compacta para copias de seguridade de sistemas abertos na empresa. Mentres que outros tipos de medios se atopaban en uso (como a cinta media polgada, 4mm/8mm, e outros), DLT proporciona o mellor compromiso entre todos os factores debido ao seu tamaño, a fiabilidade do seu almacenamento, a capacidade, e dispoñibilidade relativa.

A conectividade de DLT límitase a os tradicionais de SCSI, e está limitado a 300 GB de capacidade nativa de almacenamento e 160 MB /seg velocidade de transferencia (SDLT600). Existían outras variantes dispoñibles, pero nunca chegaron a popularizarse con carácter xeral. Na actualidade DLT atópase normalmente como copia de seguridade de longa duración en contornos pequenos que non requiren maior capacidade.

#### **59.1.1.1.2 Linear Tape Open (LTO)**

Linear Tape Open (LTO) foi deseñado e concibido como unha evolución e alternativa aos formatos DLT e outros xa existentes, e estaba destinado a proporcionar unha plataforma común para os *backups* en cinta.

Seagate, HP e IBM foron os iniciadores orixinais do consorcio LTO, encargado de realizar o desenvolvemento inicial e o cal mantén a licenza da tecnoloxía e a certificación do proceso. En teoría, deberíase producir un formato estándar de cinta, co cal os fabricantes poderían seguir traballando co estándar no mercado e incorporando as súas propias características e funcións adicionais.

Con todo, entre o orixinal LTO-1 e os formatos de LTO-2 houbo problemas de compatibilidade. Estes problemas abarcaban desde bloqueos nas cintas cando se utilizan medios adquiridos a dous provedores distintos, ata a incapacidade dunha unidade LTO dun fabricante para ler os datos escritos nun cartucho doutra.

O LTO-1 inicial proporcionaba 100 GB de almacenamento nativo e 15 MB /seg; cos actuais sistemas de LTO-4 proporciónanse 400 GB de almacenamento nativo de 160 MB / seg. Pola súa banda, o LTO-5 proporciona 800 GB de capacidade de almacenamento nativo a 160 MB / seg.

#### **59.1.1.1.3 Sun StorageTek T10000 (T10k)**

O T10000 / StorageTek (T10k) de Sun representa un das tecnoloxías de almacenamento en cinta que mellor se comportou en termos de capacidade. O T10k é un formato propietario producido unicamente por StorageTek e atópase normalmente en contornos nos que se empregaban as tecnoloxías anteriores de Sun como o STK (9840/9940). Tamén se

utilizaron en sistemas abertos de servidores ou mainframe. O T10k está deseñado para 500 GB de almacenamento nativo de 120 MB / seg.

#### **59.1.1.1.4 Características de almacenamento en cinta**

Aínda que todos os datos anteriores indican un valor interesante en canto ao rendemento, todos os dispositivos de cinta con características similares de rendemento deben terse en conta á hora de deseñar contornos de backup.

A primeira e máis importante delas é o feito de que todas as unidades de cinta son contornos serie. A diferenza dos dispositivos de disco, os dispositivos de cinta escriben os bloques de datos de forma lineal, un tras outro. As unidades de cinta só teñen unha cabeza de escritura que escribe un bloque de datos de cada vez na cinta, a medida que esta se move por ela. Os dispositivos de disco teñen unha serie de dispositivos de escritura, ou cabezas, que se moven a varios puntos do disco xiratorio para situar os datos dun xeito óptimo. Isto permite que os dispositivos de disco poidan ler calquera anaco de información solicitada. Dado que os discos teñen varias cabezas para obter bloques de datos en paralelo, varios sistemas poden acceder ao disco ao mesmo tempo

A lectura dos datos dunha cinta realízase mediante o proceso inverso: A cinta debe rebobinarse ata o principio, cara a adiante ata o bloque que se necesita, e ler así o bloque de datos. Ao poder devolverse unicamente un segmento de datos con cada lectura, os dispositivos de cinta non se poden compartir de forma paralela entre sistemas sen un mecanismo para transferir o control entre os sistemas que usan dito dispositivo.

O tipo de conectividade tamén ten influencia sobre a utilización de dispositivos de cinta. As unidades de cinta dependen dunha conexión directa co host para o transporte dos datos. Unha vez máis, isto débese ao

feito de que as unidades de cinta son dispositivos de serie que só aceptan unha soa conexión á vez.

#### *59.1.1.2 Disco*

A cinta proporciona un método moi maduro, moi coñecido, e de baixo custo para almacenar copias de seguridade. Con todo, as debilidades, tales como a natureza secuencial da cinta, a complexidade mecánica, e a gran variabilidade do rendemento dos dispositivos de cinta están rapidamente relegando a cinta a medio de almacenamento secundario ou terciario en moitos ámbitos.

Con todos os problemas coa cinta, os administradores buscaban un medio que permitise un rápido acceso ás copias de seguridade e que proporcionase unha forma de ter un almacenamento rápido e fiable: o *disco*.

Os backup a disco son simples sistemas de arquivos que foron situados separadamente para que o software de backup os use. Aínda que isto parece sinxelo, a implementación e xestión das solucións baseadas en disco poden ser moi complexas.

O almacenamento en disco supera algunhas das desvantaxes propias das cintas. Pola capacidade de recibir datos de forma rápida, ten múltiples fluxos para almacenar copias de seguridade ao mesmo tempo, e ten a capacidade de presentar o almacenamento dun número de xeitos diferentes, dependendo da necesidade do sistema, por iso, o disco é moi empregado como medio de almacenamento de copia de seguridade primario.

Pero o disco tamén ten as súas debilidades: o custo dos medios de comunicación, a falta de portabilidade, e a dificultade de asegurar a plena utilización dos medios de comunicación fan que o disco non sexa tan satisfactorio como parece a priori.

### 59.1.1.3 Medios Virtuais

Os medios virtuais emulan o hardware físico de cinta co obxectivo de reducir ou eliminar os problemas de xestión asociados aos medios físicos. Mediante a eliminación do hardware cunha alta complexidade mecánica e de xestión e a eliminación dos seus sistemas asociados e substituíndoos por unidades de disco, os medios virtuais tamén teñen a vantaxe de aumentar a fiabilidade xeral do contorno de backup. Os medios virtuais ofrecen estas vantaxes sen cambiar os procedementos operativos nin esixir modificacións do software de copia de seguridade. Ademais, nalgúns casos, o rendemento pode aumentarse a través dun mellor uso do ancho de banda nos medios de comunicación utilizados para conectar os medios virtualizados cos servidores de backup.

Os Medios virtuais de copia de seguridade asóciáanse tradicionalmente de forma exclusiva con bibliotecas de cintas virtuais (VTL) pero recentemente realizáronse novas implementacións a través de protocolos que permiten a virtualización doutros tipos de sistemas de almacenamento.

### 59.1.1.4 Medios Ópticos

Os medios ópticos sitúanse entre as vantaxes das cintas e as do disco. Sobresaen nas áreas de fiabilidade, flexibilidade, ciclo de traballo e inamobilidade, mentres que os seus retos atopámoslos nas áreas de rendemento, capacidade e custo.

#### **59.1.1.4.1 CD**

CD, ou compact disk, é un soporte dixital óptico que se utiliza para o almacenamento de practicamente calquera tipo de datos. Na actualidade o uso do CD está decaendo a favor do aumento do uso dun novo medio de similares características, coma o DVD.

O CD serviu e segue servindo como medio de almacenamento de copias de seguridade grazas á súa fiabilidade e inamobilidade. Proporciona en comparación con outros medios como a cinta magnética, maior seguridade e protección dos datos, dado que o propio medio é moito máis robusto fronte a interaccións físicas externas (por exemplo os campos magnéticos).

Ademais de ser un medio habitual para o almacenamento de pistas de audio, os CDs utilízanse habitualmente para a xeración de copias de seguridade relacionadas coa recuperación dos sistemas.

Os sistemas de CD utilizan un dispositivo hardware específico para gravar información, coñecido como gravadora/regravadora de CD. Existen tamén dispositivos hardware similares que soamente permiten a lectura deste medio.

As capacidades habituais dos CD estándar abarcan desde os 650MB ata os 900MB.

#### **59.1.1.4.2 DVD**

Os DVDs veñen ser a evolución da tecnoloxía dixital óptica dos CDs.

Do mesmo xeito que os CDs, existen dous tipos de dispositivos para o uso dos DVDs que son as gravadoras e os lectores. Existen diferentes tipos de DVDs e diferentes categorizacións, sendo a máis importante a relativa ao número de capas, factor que determina a capacidade final do dispositivo.

As capacidades actuais abarcan desde os 4,3Gb ata os 17Gb. Os DVD utilizan dous tipos de sistemas de ficheiros que substitúen o antigo ISO 9660 dos CDs, e que son o UDF e o Joliet.

### **59.1.2 Software de Backup**

Na categoría de elementos software de backup temos ferramentas de código aberto ou software libre e software privativo ou comercial. As ferramentas máis comúns a nivel de software son:

#### **59.1.2.1 Ferramentas de código aberto - AMANDA**

Amanda (Advanced Maryland Automated Network Disk Archiver), é o software de código aberto de copia de seguridade máis coñecido. Amanda desenvolveuse inicialmente na Universidade de Maryland en 1991 co obxectivo de protexer os arquivos dun gran número de estacións de traballo cliente cun servidor de copia de seguridade único. James da Silva foi un dos seus desenvolvedores orixinais.

O proxecto Amanda rexistrouse en SourceForge.net en 1999. Jean-Louis Martineau, da Universidade de Montreal foi o líder do desenvolvemento de Amanda nos últimos anos. Durante anos, máis de 250 desenvolvedores contribuíron ao código fonte de Amanda, e miles de usuarios achegan probas e comentarios, o que o converte nun paquete robusto e estable. Amanda inclúese coa maior parte das distribucións Linux.

Nun principio, Amanda foi utilizado maioritariamente nas universidades, laboratorios técnicos, e departamentos de investigación. Hoxe, coa ampla adopción de Linux nos departamentos de informática, Amanda atópase en moitos outros lugares, sobre todo cando a atención se centra en aplicacións LAMP (Linux+Apache+MySQL+PHP). Cos anos, Amanda recibiu múltiples premios dos usuarios.

Amanda permite configurar un único servidor backup mestre para realizar múltiples copias de seguridade de equipos Linux, Unix, Mac VOS X, e Windows nunha ampla variedade de dispositivos: cintas, discos,



dispositivos ópticos, bibliotecas de cintas, sistemas RAID, dispositivos NAS, e moitos outros.

As principais razóns para a adopción xeneralizada de Amanda son:

- Que se pode configurar un único servidor de copia de seguridade de varios clientes en rede con calquera dispositivo de almacenamento: unha cinta, disco ou sistema de almacenamento óptico.
- Está optimizado para o backup en disco e cinta, permitindo escribir simultaneamente backup a cinta e disco.
- Non utiliza drivers propietarios, calquera dispositivo soportado por un sistema operativo tamén poderá funcionar en Amanda.
- Utiliza ferramentas estándar, como dump e tar. Posto que non son formatos propietarios, os datos pódense recuperar con esas mesmas ferramentas.
- Utilízase un planificador que optimiza niveis de seguridade para os diferentes clientes, de tal xeito que o tempo total do backup é aproximadamente o mesmo para cada execución.
- Existe unha ampla e activa comunidade de usuarios que crece día a día.
- O custo total de propiedade (TCO) dunha solución de backup baseada en Amanda é significativamente menor ca o TCO de calquera solución que utilice software privativo.

#### *59.1.2.2 Ferramentas de código aberto – BackupPC*

BackupPC é un sistema de alto rendemento que permite realizar copias de seguridade de sistemas Unix, Linux, Windows e MacOS nun disco. É, xa que logo, unha ferramenta baseada totalmente en disco.

Ofrece unha serie de vantaxes como son:

- **Soporta calquera sistema operativo cliente.** Isto débese a que se utilizan ferramentas estándar que ou veñen co SO ou se poden engadir ao SO, sen necesidade de instalar cliente. Así resulta máis fácil integrar un novo cliente.
- **Interface Web** con control de usuario para acceder a copias de seguridade. A maioría dos SO trae un navegador web, así que usar unha interface web é outro xeito de acelerar o proceso de incorporación de novos clientes con diferentes sistemas operativos. A interface web está deseñada para dar o máximo control posible ao cliente de forma segura. O usuario pode solicitar restauracións, e navegar facilmente e restaurar arquivos individuais. Con todo, o usuario non poderá ver as máquinas doutro usuario.
- **Soporte de clientes DHCP.** Mediante o uso de servizos estándar, BackupPC soporta clientes DHCP, a condición de que o cliente estea rexistrado cun servizo de nomes como DNS, Active Directory ou LDAP.

### **Funcionamento de BackupPC**

O modelo de BackupPC ten un usuario por cliente. Isto é así porque BackupPC foi especificamente deseñado para realizar copias de seguridade de PCs de varios usuarios (de aí o nome).

Normalmente, o usuario é o propietario dos datos da máquina. Se se traballa cun servidor de ficheiros, o usuario deberá ser un administrador.

BackupPC envía mensaxes de correo electrónico ao propietario se non pode realizar a copia de seguridade logo dun tempo configurable; o propietario pode xestionar as restauracións das copias a través dunha interface web.

Nos seguintes puntos descríbense algunhas das características proporcionadas por BackupPC:

- **Directo ao disco.** BackupPC almacena todas as súas copias de seguridade directamente no disco. Os arquivos idénticos en calquera directorio ou cliente gárdanse só unha vez, o que reduce drasticamente os requisitos de almacenamento do servidor. Estes arquivos almacénanse nun conxunto de discos. Ademais do conxunto de discos, as copias de seguridade están nunha árbore de directorios organizados por host.

BackupPC tamén ten un proceso (que se lanza polas noites) que recupera espazo do conxunto de discos que non está referenciado por ningún backup, o que evita un uso inadecuado do espazo en disco. Este é un proceso automático que o administrador non ten que configurar.

- **Sistema operativo do servidor** A parte do servidor de BackupPC está deseñada para executarse nun sistema tipo Unix con Perl e mod\_perl. Ofrece o mellor rendemento con Apache, pero pódese executar en calquera servidor web que soporte Perl (requírese mod\_perl ou Perl setuid.) O servidor debe ter un disco con gran capacidade ou RAID para almacenar os backups.

- **Sistema operativo do cliente.** Como se comentou anteriormente, soporta calquera SO. As versións máis modernas das variantes comerciais de Unix (Solaris, AIX, IRIX, HP-UX) traen na propia distribución as ferramentas tar, compress, gzip, rsync, e rsh e / ou ssh. Outros sistemas operativos tipo Unix (Linux, FreeBSD, OpenBSD, NetBSD, Mac VOS X) tamén contan con estas ferramentas.

Os clientes de Windows poden facer copias de seguridade de diferentes formas dependendo de se as políticas locais permiten ou non a instalación de software. Se non se permite, BackupPC utilizar parte da suite Samba (<http://www.samba.org>) para facer backup da información

compartida mediante SMB ou CFIS. Se se permite instalar software, utilízase rsync xunto co conxunto de ferramentas Cygwin (<http://www.cygwin.com>).

- **Soporte para ferramentas nativas.** BackupPC utiliza as ferramentas estándar de Unix para o seu funcionamento interno. Isto inclúe programas como Perl, tar, rsync comprime, gzip, bzip2, zip, apache e samba.

BackupPC non utiliza unha base de datos ou catálogo para almacenar a información de respaldo. No seu lugar, utiliza a árbore de directorios para almacenar esta información. Isto simplifica as actualizacións do sistema operativo do servidor de BackupPC ou da propia aplicación BackupPC.

- **Control dos backups e restauracións a través de interface web.** A Web é a interface principal de BackupPC. Trala configuración inicial, non é necesario acceder ao servidor mediante liña de comandos para administrar BackupPC. A interface web está escrita en Perl e foi deseñada para funcionar tanto con mod\_perl como con CGIs ou con Perl setuid.

A interface permite aos usuarios identificarse, acceder e controlar os respaldos e as restauracións.

O usuario pode solicitar copias de seguridade de tipo one-time, de tipo completa, ou de tipo incremental.

Pódense utilizar varias opcións para recuperar ficheiros:

- o Os arquivos individuais recupéranse mediante selección.
- o Os grupos de arquivos ou directorios pódense restaurar á súa localización orixinal.

o O usuario pode descargar os arquivos como un arquivo tar ou zip.

O usuario ten control absoluto sobre qué arquivos ou directorios se restauran e onde hai que restauralos. Un histórico mostra qué arquivos se modificaron durante cada copia de seguridade en cada directorio.

- **Soporte para clientes DHCP.** Os clientes BackupPC referéncianse por nome de host. Se a rede da copia de seguridade utiliza DHCP e se permite a resolución de nomes dinámica, non hai que facer nada máis para que o servidor BackupPC apoie aos clientes DHCP. Se este non é o caso, e os clientes son máquinas Windows, BackupPC pódese configurar para buscar un conxunto de direccións dos clientes, localizándoos mediante SMB.

Se o cliente non está en liña durante o período de copia de seguridade normal, o servidor BackupPC non xera un erro a menos que transcorra un período de tempo establecido desde a última copia de seguridade. Neste punto, o servidor envíalle un email ao propietario do cliente e lémbrralle que se asegure de que a máquina está na rede para facer unha copia de seguridade. (O servidor tamén pode enviar calquera erro ao administrador.)

Os clientes que residen noutra LAN poden ser xestionados a escala local asumindo que hai conectividade entre as redes. Isto significa que se pode facer backup dos clientes conectados a través dunha rede privada virtual (VPN).

Se o usuario non desexa realizar copias de seguridade nun momento dado, conectaríase a través da interface web para cancelar a copia de seguridade.

- **Pool de Backups.** Cando os clientes utilizan o mesmo sistema operativo dúplícanse os arquivos respaldados. Se se quere manter

múltiples copias de seguridade completas aumenta o número de arquivos duplicados, o que aumenta os requisitos de capacidade de almacenamento para o servidor. BackupPC almacena unha árbore de directorios por cliente respaldado, pero comproba se os arquivos se almacenaron antes. Se é así, BackupPC utiliza un enlace que apunta ao ficheiro existente no conxunto de discos común, aforrando unha gran cantidade de espazo. Ademais, BackupPC pode comprimir opcionalmente para aforrar máis espazo.

- **Fácil configuración por cliente.** Unha vez que o administrador defina cales deberían ser as políticas de backup do sitio, é moi fácil anular calquera opción de configuración baseándose nun cliente. Isto permite unha gran flexibilidade sobre qué, cando, e cómo facer copia de seguridade dun cliente. Non hai clases de clientes por si mesmo.

#### *59.1.2.3 Ferramentas de código aberto - Bacula*

Bacula é un conxunto de programas Open Source, listos para ser utilizados nunha contorno doméstico e profesional, que permiten administrar os backups, restauración e verificación de datos nunha rede heteroxénea. Bacula é relativamente fácil de usar e eficiente, á vez que ofrece moitas funcionalidades avanzadas para a administración dos datos almacenados, o cal facilita atopar e recuperar arquivos perdidos ou danados. En termos técnicos, Bacula é un sistema de backups Open Source, orientado á rede e listo para a empresa.

É capaz de realizar copias de seguridade en disco, cinta ou medios ópticos. Bacula foi escrita orixinalmente por John Walker e Kern Sibbald no ano 2000. John deixou o proxecto non moito tempo logo da súa creación, e Kern, traballou nel desde mediados do 2000 ata o primeiro lanzamento

público de Bacula en abril de 2002. Desde entón, outros desenvolvedores contribuíron ao seu desenvolvemento.

Bacula está dispoñible baixo licenza AGPL versión 3. A páxina web do proxecto atópase en <http://www.bacula.org>, e os arquivos descargables e un repositorio CVS alóxanse en SourceForge.

### **Bacula Arquitectura**

Bacula é unha solución distribuída de backups. Isto significa que Bacula está composto por varios elementos, que poden ou non residir no mesmo host. Por exemplo, pódese ter un host co catálogo e noutro o storage.

Baséase nunha arquitectura Cliente-servidor que resulta eficaz e fácil de manexar, dada a ampla gama de funcións e características que brinda: copiar e restaurar ficheiros danados ou perdidos. Ademais, debido ao seu desenvolvemento e estrutura modular, Bacula adáptase tanto ao uso persoal como profesional.

Pódese utilizar TLS (Transport Layer Security) para protexer os datos durante a transmisión.

Os compoñentes principais desta arquitectura son:

- **Director (DIR)** é o encargado de xestionar de forma centralizada a lóxica dos procesos de backup e os demais servizos. Traballa tomando como base unha unidade básica denominada JOB (un cliente, un conxunto de arquivos, ...) de tal forma que o Director planifica, inicia e supervisa todos os jobs.

Tamén é o encargado de manter o catálogo, polo que o servidor da base de datos debe estar accesible desde a máquina que executa o Director.

- **Storage** é o encargado de xestionar os dispositivos de almacenamento; isto esixe que estea instalado na máquina que posúa a

conexión física aos dispositivos de almacenamento, tales como: discos locais, gravadoras, unidades de cinta, volumes NAS ou SAN, autocargadores ou librerías de cinta.

- **File Daemon** é o axente que corre ao lado do cliente, é dicir, na máquina cuxos datos ir a respaldar, e que ten como obxectivo empacar os datos e envialos ao Storage, onde serán almacenados.

- **Consola** é a ferramenta que lle permite ao usuario ou administrador controlar Bacula. Comunícase co director vía rede, iniciando os jobs, revisando a saída do job, facendo consultas e modificacións no catálogo.

Existen consolas en modo texto, modo GUI para Windows e Linux/UNIX e interfaces web.

- **Catálogo** é unha base de datos onde se garda información sobre os jobs e sobre os datos respaldados. O catálogo permite dúas cousas:

- o Por unha banda, como garda información dos jobs, pools e volumes, Bacula úsao para saber se hai un backup completo para un job, e se non o hai, realizará para ese backup unha copia completa.

- o Doutra banda, o catálogo ten todos os nomes de arquivo (e os seus atributos, como data de última modificación, etc.) que se respaldaron, e iso é o que permite facer unha recuperación selectiva, é dicir, seleccionar (marcar, na xerga de Bacula) individualmente qué arquivos e/ou directorios restaurar.

#### 59.1.2.4 Software Propietario CommVault Simpana

Simpana comezou como un proxecto dentro de AT & T Labs en 1987 e posteriormente foi adquirido pola empresa CommVault.

Simpania é un software de backup que realiza copias de seguridade de contornos Unix, Windows, Linux, servidores de correo Exchange, Lotus Notes, bases de datos Oracle, MySQL, SQLServer e máquinas virtuais



VMware. Ademais permite funcións avanzadas como pode ser o arquivado, a deduplicación e a replicación de ficheiros.

O funcionamento da aplicación baséase no uso dos bloques de disco, polo que todos os módulos non utilizan a información do arquivo, se non que traballa a máis baixo nivel. Con iso consegue mellores ratios de compresión e unha importante redución da fiestra de backup, ao utilizar unicamente os bloques modificados e non o ficheiro enteiro para realizar estas operativas.

Outra característica que incide no uso de almacenamento de baixo custo é a capacidade de xerar políticas como as de arquivado, mediante as que automaticamente permite mover ficheiros dun almacenamento a outro con maior capacidade a menor custo. Desta forma, por exemplo poderíanse pasar os datos dunha cabina de fibra a outra con discos SATA, podendo chegar a un terceiro nivel a cinta, tomando como base uns requisitos (data do arquivo, último acceso ao arquivo, etc.). Todos os movementos realízanse de forma transparente para o usuario, tanto no arquivado como na súa recuperación (se fose necesario).

A estas funcionalidades hai que sumarlle a capacidade de deduplicación, que realiza unha compresión dos datos aproveitando as duplicidades dos datos a escala de bloque, conseguindo alcanzar ratios de ata o 50% de aforro no uso de almacenamentos en datos de segundo nivel e ata o 90% nos de terceiro nivel.

Para terminar o repaso ás principais funcionalidades, a replicación, permite a utilización de snapshots a escala de cabina permitindo volver o almacenamento replicado a un estado anterior ou montar a imaxe snapshot como un recurso compartido.

Todo se administra desde unha única consola centralizada, que simplifica toda a administración da plataforma. Adicionalmente o motor de

busca ofrece a opción de buscar rapidamente e recuperar datos sen necesidade de saber onde se sitúan.

#### 59.1.2.5 *Software Propietario Symantec NetBackup*

Symantec NetBackup é actualmente o titular da maior cota de mercado da contorno de software de copia de seguridade.

Netbackup 7 é a nova versión da solución de copia de seguridade e recuperación de datos orientada a grandes corporacións. Esta ferramenta trata de simplificar a xestión da información reducindo o volume de almacenamento de datos con técnicas de deduplicación nos ordenadores cliente da rede ademais do propio servidor, ofrecendo protección para contornos virtualizados. Todo iso co único propósito de axilizar os procesos de backup e recuperación de datos.

A nova ferramenta inclúe eliminación de datos duplicados nativos dentro do cliente NetBackup e permítelles aos clientes multiplicar por dez a velocidade das copias de seguridade en oficinas remotas, o propio centro de datos e os contornos virtuais. Esta eliminación de datos duplicados no cliente e no destino ofrece unha maior cobertura con menos ferramentas.

O proceso de deduplicación contémplase para todos os sistemas físicos e virtuais, independentemente do método de copia de seguridade. Deste xeito intégrase unha maior protección para os cada vez máis estendidos contornos virtualizados baixo as plataformas Hyper-V e VMware. É no caso desta última na que se puido observar un incremento de velocidade de ata o 50% á vez que diminúe o volume de almacenamento necesario nun 40%.

Outro dos aspectos notablemente mellorados en Netbackup 7 é a velocidade de recuperación de datos ante desastres. Permitindo a restauración de grandes volumes de información en poucos segundos desde calquera lugar e punto no tempo. Esta xestión facilítaselle ao administrador de TI mediante un sistema centralizado de supervisión e

alerta, que integra a administración de varios dominios de arquivos coas súas respectivas políticas de salvagarda de datos.

A tecnoloxía incluída en NetBackup acelerará a transición a unha contorno virtual para as organizacións empresariais que instalen un gran número de máquinas virtuais ou que decidan crear unha infraestrutura de nube privada.

A solución NetBackup tamén ofrece unha elaboración de informes simplificada e un maior soporte ás aplicacións de bases de datos de Oracle e MySQL.

Algunhas das prestacións e beneficios incluídos na última versión da ferramenta son:

- A tecnoloxía Virtual Machine Intelligent Policy incorpora a automatización á localización e a protección de máquinas virtuais e minimiza os esforzos de administración necesarios para realizar copias de seguridade de máquinas virtuais VMware de alto rendemento.
- Un 50% máis de rapidez en copias de seguridade de máquinas virtuais grazas a que a tecnoloxía Granular Recovery Technology (GRT) se atopa agora dispoñible para sistemas Linux en contornos VMware. Isto permítelles aos clientes reducir os tempos comparables de copias de seguridade de máquinas virtuais nun 50%, ademais de simplificar a administración e mellorar a velocidade de recuperación de arquivos individuais.
- Recuperación “á carta” desde calquera lugar coa nova tecnoloxía de replicación de imaxe que permite aos clientes que replican datos entre múltiples sitios ou dominios de NetBackup realizar backups de datos nun sitio alternativo.
- Recuperación acelerada: NetBackup RealTime ofrece soporte a contornos VMware para eliminar o espazo de tempo entre copias de

seguridade, ademais de reducir o impacto para grandes hosts de VMware e permitir a recuperación case instantánea de sistemas completos.

- Satisfacer os requisitos normativos e de cumprimento para seguimento de auditorías.
- Incorpora informes mellorados das políticas do ciclo de vida do almacenamento, do seguimento das auditorías e do estado das licenzas.
- Deduplicación para Oracle mellorando o rendemento das copias de seguridade.
- Engádese un novo axente que presta soporte a MySQL para centralizar e automatizar as copias de seguridade e a recuperación de datos das bases de datos de MySQL.
- Actualización simplificada de clientes con LiveUpdate que permite melloras en equipos cliente para UNIX, Linux e Windows respecto de a versión NetBackup 6.5 e posterior desde unha política única controlada polo administrador de NetBackup.

### **59.2 ESTRATEXIAS DE BACKUP A DISCO**

As estratexias de backup definen o plan que se ha de seguir para garantir a integridade da información. Os motivos polos que se debe establecer unha correcta estratexia antes de comezar a realizar as copias de seguridade poden ser moi diversos, pero en esencia trátase de determinar o mellor xeito para asegurar a información tendo en conta as posibles dificultades de recuperación de parte dos datos, o custo dos medios que se empregasen e o tempo que se necesitase.

Como non todos os sistemas son iguais, non todas as estratexias de backup son adecuadas para todos os sistemas. Partindo dunhas características comúns, algunhas das propiedades básicas dunha estratexia backup son:

- Tempo de almacenamento. Define o tempo máximo que unha copia permanece almacenada nun dispositivo. Ao finalizar este tempo a copia pode cambiar de dispositivo ou ser borrada para liberar espazo no medio de almacenamento e poder facer uso do mesmo.
- Almacenamento alternativo. Posibilita realizar unha ou varias copias de seguridade nunha localización externa ao sistema e á localización xeográfica do mesmo, manténdoa durante un elevado período de tempo, aumentando a seguridade ante calquera catástrofe, xa sexa a escala de software ou de hardware.
- Protección ante fallo dos dispositivos. Establece o número de medios que se empregan. Canto maior é o número de medios utilizados, maior é a seguridade contra posibles perdas de información producidas por un fallo no dispositivo de almacenamento.

- Tempo de restauración. Esta característica especifica o tempo de rexeneración do sistema en caso de producirse algún fallo.
- O custo. Adoita ser un factor determinante á hora de seleccionar a estratexia a realizar.

As estratexias para a realización de copias de seguridade poden ser moi distintas, dependendo do sistema en cuestión sobre o cal se realizan.

Nalgúns casos, soamente se efectúa un backup de todo o contido. Isto prodúcese cando por algún motivo especial e moi específico ou por algún motivo técnico, cuestións de tempo ou por que existe un elevado risco para os datos. Algún destes casos especiais poden ser:

- Non dispoñer do software orixinal.
- Descoñecemento da localización dos ficheiros de configuración.
- Cambiar un disco de almacenamento ríxido.
- Realizar cambios nas particións dun ou máis discos de almacenamento ríxidos.

É habitual que este tipo de situacións concretas se produzan á hora de levar a cabo tarefas de reparación ou actualización sobre sistemas non controlados.

Cando se trata de cubrir algún destes casos a estratexia de backup a seguir é sinxela, realizar un resgardo ou copia de seguridade de todo o contido das unidades involucradas para así garantir que non se perderá ningunha información e que será posible realizar a restauración completa do sistema.

Doutra banda, cando realmente se deba deseñar un plan estratéxico para a realización das copias de seguridade dun sistema propio ou dunha organización externa, débense ter en conta unha serie de pautas que

axudan a que o plan estratéxico de backups sexa o máis conveniente e conseguir a mellor relación custo/beneficio posible.

Estas pautas achegan unha redución no tempo de resposta á hora de realizar unha recuperación no caso de que se produza calquera tipo de continxencia.

Ao intentar definir un plan de backups, xorden unha serie de dúbidas:

***Que datos se deberían resgardar en cada backup?*** Datos a resgardar.

É un factor determinante para unha estratexia de backup que se determine o grao ou graos de importancia da información, é dicir, establecer que información resulta de maior valor para a organización. Non teñen a mesma transcendencia un documento de traballo ca unha copia de respaldo da configuración dunha aplicación.

***Cada canto se debería efectuar un backup dos datos?*** Frecuencia do backup.

Para determinar a periodicidade coa que se deben realizar as copias de seguridade non existe un criterio claramente definido. Con todo, téñense en conta factores como:

- Tempo empregado na creación da información.
- Custo investido na creación da información.
- Posibles consecuencias derivadas da súa perda.

***Canto tempo deberían permanecer gardadas as copias de seguridade?*** Tempo de Almacenamento.

O período máximo de tempo de estancia dunha copia de seguridade nun dispositivo, é dicir, o tempo de retención, está directamente relacionado

cos medios de almacenamento dispoñibles, e por conseguinte polo orzamento da estratexia de backup.

Outra das decisións importantes a tomar durante a elaboración dunha estratexia para a realización de copias de seguridade é a de seleccionar e planificar os distintos tipos de copias de seguridade.

Os backups son copias exactas da información. Pódense definir como instantáneas dos datos nun momento determinado, almacenados nun formato estándar, pódese realizar un seguimento ao longo do seu período de utilidade e con cada nova copia mantense a independencia con copia inicial. Pódense crear múltiples niveis de backups, sendo os principais:

- **Copias de seguridade completas (Full backups):** representan unha copia exacta nun momento dado, dos datos que se pretende protexer. Proporcionan a base para todos os demais niveis de backup.
- Doutra banda, están dous niveis de backup que capturan unicamente os cambios realizados sobre unha copia de seguridade completa.
  - o **Copia de seguridade diferencial**, tamén coñecida como a *copia de seguridade incremental acumulativa*, captura copias de seguridade que se produciron desde o último backup completo e adoita utilizarse en contornos nos que non se produce un elevado número de cambios. A copia de seguridade diferencial débese utilizar con coidado debido a que pode crecer con rapidez e igualar e ata superar o tamaño da copia de seguridade completa.

A vantaxe de utilizar as copias de seguridade diferenciais vén dada no momento da restauración posto que no momento de restaurar unha copia de seguridade diferencial só se necesita o backup completo e a última copia diferencial realizada. Debido a que unicamente se precisan



dúas imaxes para a restauración, a probabilidade de que ambas imaxes sufran algún deterioro, perda, corrupción, etc., redúcese significativamente.

- o ***Copia de seguridade incremental***, é capaz de capturar os cambios que se produciron desde a última copia de seguridade realizada, independentemente do tipo que sexa. É a forma máis utilizada para a realización de copias de seguridade, evidentemente combinada cunha copia de seguridade completa.

Este tipo de copia de seguridade contén a menor cantidade de datos necesarios durante cada ciclo de backup, reducindo a cantidade de datos que se transfiren e o tempo que se necesita para a creación dunha copia de seguridade.

Con todo as copias de seguridade incrementais teñen aspectos negativos. Se se está recuperando un grupo de arquivos dun conxunto de copias de seguridade completas e incrementais, é probable que se requiran máis de dúas imaxes de copias de seguridade diferentes para completar a restauración, o que aumenta a probabilidade de que algunha destas partes sufra algún tipo de problema e non se poida completar a restauración.

### **59.3 DISPOÑIBILIDADE DA INFORMACIÓN RPO, RTO**

A información representa un dos activos máis importantes no contexto actual, e como tal, debe existir sempre un plan estratéxico e de

continxencia que proporcione os mecanismos necesarios para garantir a seguridade e dispoñibilidade da mesma.

Existen no mercado unha gran cantidade de solucións tecnolóxicas e metodoloxías que nos permiten aplicar ou instaurar protocolos específicos de protección e garantía de dispoñibilidade da información corporativa, independentemente da entidade na que nos atopemos. Para establecer un criterio de selección entre toda esta gran cantidade de solucións, existen un conxunto de indicadores técnicos que nos proporcionan un mecanismo estándar para poder establecer comparativas obxectivas sobre cal das diferentes solucións é a máis conveniente. Estes dous indicadores son o Obxectivo de Punto de Recuperación (RPO) e o Obxectivo de Tempo de Recuperación (RTO).

A grandes trazos, podemos definir ambos conceptos do seguinte xeito:

- Obxectivo de Punto de Recuperación ou RPO: É a cantidade máxima de información que pode ser perdida cando o Servizo é restaurado tras unha interrupción.
- Obxectivo de Tempo de Recuperación ou RTO: É o tempo máximo permitido para a recuperación dun servizo de TI tras unha interrupción.

Dentro dos plans de continxencia desenvolvidos para previr e paliar os casos de caída de servizo ou perda de información nunha organización, poden existir diferentes alternativas aplicables en función de determinados criterios relacionados co fluxo e a cantidade de información coa que se traballa. Para avaliar cales son as técnicas máis apropiadas, os conceptos anteriores marcan un punto inicial que se debe tomar como referencia para a implantación das políticas adecuadas no tratamento dos datos.

#### *59.3.1.1 Obxectivo de Punto de Recuperación*

O indicador RPO é un xeito obxectivo para comparar diferentes produtos, sistemas ou metodoloxías de recuperación de información cando

o que interesa controlar é a cantidade de información que podería chegar a perderse en caso de continxencia. Como se definiu con anterioridade, RPO establece un indicador que avalía a cantidade de información que pode chegar a perderse sen graves consecuencias, é dicir, é un indicador de risco.

Este indicador debe tomarse con cautela, dado que é altamente dependente do contexto no que se atope a organización, así como do seu volume de xeración de datos.

Para ilustrar o exemplo, preséntase a situación dunha organización na que se realiza unha copia de seguridade incremental cada noite. Neste escenario, a perda máxima de datos que poderían chegar a perderse en caso de continxencia (fallo dos servidores, etc...) sería como máximo un día hábil, dado que asumimos que cada noite se realiza a copia de seguridade incremental.

Esta medida pode ser válida para determinados modelos de negocio nos cales o volume de datos co que se traballa ao longo dun día hábil non é demasiado elevado. Con todo, o mesmo modelo aplicado a unha entidade bancaria na cal se realizan millóns de transaccións diarias, a perda máxima dun día hábil non é aceptable.

#### *59.3.1.2 Obxectivo Tempo de Recuperación*

O RTO determina o tempo de recuperación fronte a unha continxencia, é dicir, o tempo que se pode estar sen o servizo operativo. Para iso é necesario identificar ao comezo todas as funcións críticas do negocio e o seu apoio aos compoñentes de Tecnoloxías da información. Unha vez identificadas, podemos establecer o tempo necesario en caso de fallo para poder renovar as operacións normais.

O RTO é un indicador intimamente relacionado co BIA (Business Impact Analysis) e adóitase expresar en termos de tempo (horas, minutos,...). De feito, en moitas organizacións xa se establecen por norma primas sobre a dispoñibilidade dos sistemas e acceso a datos corporativos.

RTO e RPO están tamén enteiramente vinculados. Á hora de deseñar un plan de continxencia, é necesario saber qué estratexia RPO se implantará, dado que o volume de datos a recuperar en caso de fallo, que está ligado á estratexia RPO, inflúe directamente no indicador RTO, é dicir, no tempo que se tardará en recuperar o sistema.

#### **59.4 REPLICACIÓN LOCAL E REMOTA, ESTRATEXIAS DE RECUPERACIÓN**

A replicación é o proceso de creación dunha copia exacta dos datos. A creación dunha ou varias réplicas dos datos de produción é un dos xeitos de proporcionar continuidade ao do negocio (BC).

Estes modelos poden ser utilizados para operacións de recuperación e reinicio dos sistemas no caso de que se produza unha perda de datos.

Unha réplica debe proporcionar:

- **A capacidade de recuperación:** permite a restauración dos datos dos volumes de produción no caso de que se produza unha perda dos datos. Débese proporcionar un mínimo de e RTO e un RPO concreto que nos garantan a reanudación das operacións comerciais nos volumes de produción.
- **A capacidade de reinicio:** garante a coherencia dos datos da réplica, posibilitando a reanudación das operacións de negocio, utilizando para iso a información contida nas réplicas.

A replicación pódense clasificar en dúas grandes categorías: ***locais e remotos***

### **59.4.1 Replicación Local**

A replicación local fai referencia ao proceso creación de réplicas dentro do mesmo *array* de discos ou o mesmo centro de datos.

#### **59.4.1.1 *Tecnoloxías de replicación local***

As replicacións Host-based (baseadas en replicación en host local) e Storage-based (baseadas en almacenamento) son as dúas principais tecnoloxías adoptadas para a replicación local. A replicación de arquivos do sistema e a replicación baseada en LVM son exemplos da tecnoloxía Host-based de replicación local. A replicación de almacenamento baseada en matrices de disco pode levarse a cabo con solucións distintas, a duplicación de todo o volume, a replicación pointer-based de todo o volume, e a replicación baseadas en punteiros e virtual.

##### **59.4.1.1.1 Baseada en replicación en host local**

Neste tipo de replicación, os administradores do sistema levan a cabo o proceso de copia e restauración na propia máquina, podendo basearse a recuperación nunha replicación integral do volume mediante LVM (Logical Volume Manager), ou ben mediante instantáneas do sistema de ficheiros.

- Replicación do volume mediante LVM: O LVM encárgase de crear e controlar o volume de host a nivel lóxico e está formado por tres compoñentes: os discos físicos, os volumes lóxicos e os grupos de volumes. Na replicación de volumes baseado en LVM, cada partición lóxica nun volume asígnase a dous particións físicas en dous discos diferentes. Desesta forma conséguese un espello que permite redundancia e recuperación directa en caso de necesitar replicar.
- Instantánea de arquivos do sistema: Consiste en crear unha réplica a base de instantáneas do sistema de ficheiros mediante a utilización de metadatos almacenados nun mapa de bits. Estes metadatos van reflectindo o cambio que se vai producindo no

sistema de ficheiros e van almacenando un rexistro das direccións accedidas mediante operacións de lectura/escritura. Este sistema require dunha fracción do espazo utilizado polo sistema de ficheiros orixinal.

#### ***59.4.1.1.2 Baseada en arrays de discos***

Neste tipo de replicación faise uso de matrices de discos que poden estar distribuídas dentro do CPD. O contorno operativo é o que leva a cabo o proceso de replicación dun determinado sistema de ficheiros, sen necesidade de que os recursos de acollida (CPU e memoria) do anfitrión interveñan no proceso de replicación.

### **59.4.2 A replicación remota**

A replicación remota consiste no proceso de creación de réplicas do conxunto de datos en lugares con outra localización física. As réplicas remotas axudan ás organizacións a mitigar os riscos asociados ás interrupcións rexionais do servizo, que poden estar provocadas por diferentes causas, por exemplo, desastres naturais. A infraestrutura na que os datos se almacenan inicialmente chámase “fonte”. Á réplica, ou infraestrutura remota na que se almacena a copia chámasele “branco”.

#### ***59.4.2.1 Tecnoloxías de replicación remota***

A máis habitual é a tecnoloxía de replicación baseada en host remoto, que utiliza un ou máis compoñentes da máquina para realizar e xestionar a operación de replicación. Existen dous enfoques fundamentais para a replicación baseada en host remoto: Replicación remota baseada en LVM e replicación de bases de datos a través de transvase de rexistros.

##### ***59.4.2.1.1 Replicación remota baseada en LVM***

Neste modelo, a replicación efectúase e xestiona a escala de grupo de volumes. O LVM da máquina orixe é o encargado de xestionar e transmitir a información do volume ao LVM da máquina remota. O LVM da máquina remota encárgase de recibir os datos e realiza a operación de réplica do volume.

Antes do inicio da replicación, débense configurar os sistemas fonte e remoto para que os sistemas de arquivos, os volumes e a agrupación de volumes sexa idéntica en ambos. O punto de partida, ou sincronización inicial, pódese realizar de diferentes formas, sendo a máis frecuente a restauración no punto remoto dunha copia de seguridade dos datos de orixe.

Na replicación remota baseada en LVM sopórtanse dous modos de transferencia de datos, que son o sincrónico e o asíncrono. No modo asíncrono, as operacións de escritura vanse almacenando nunha cola de rexistros xestionada polo LVM e vanse enviando ao host remoto na orde no



que son recibidas. En caso de fallo da rede, as operacións seguen acumulándose na cola de rexistros.

Na replicación síncrona, as operacións de escritura deben estar comprometidas tanto en orixe como en destino. As operacións de escritura consecutivas non poden ocorrer en fonte nin destino ata que as operacións previas finalicen. Isto garante que os datos da fonte e destino sexan exactamente os mesmos en todo momento. Isto fai posible que o RPO en caso de fallo sexa cero ou próximo a cero. Con todo, como contraprestación ao nivel de seguridade, o tempo de resposta é moito maior. O grado de impacto no tempo de resposta depende da distancia entre ambos sitios (fonte e destino), do ancho de banda dispoñible e da infraestrutura de conectividade de rede.

#### **59.4.2.1.2 Baseada en transvase de rexistros**

A replicación de bases de datos a través de transvase de rexistros consiste na captura das transaccións realizadas na base de datos fonte, que son almacenadas en rexistros que se transmiten periodicamente dun host fonte a un host destino. O host destino recibe o conxunto de rexistros e realiza as operacións oportunas na base de datos replicada. O proceso inicial de produción e reprodución require que todos os compoñentes importantes da base de datos se repliquen no sitio remoto.

Os sistemas xestores de bases de datos permiten definir un intervalo de tempo para o envío dos ficheiros de rexistro, ou ben configurar un tamaño predeterminado dos mesmos. Cando un rexistro supera o intervalo de tempo establecido ou alcanza o seu tamaño máximo, péchase e ábrese un novo ficheiro para rexistrar as transaccións. Os rexistros pechados van sendo enviados desde a fonte ao destino garantindo que a base de datos replicada en destino sexa consecuente coa fonte ata o último rexistro pechado. O RPO no sitio remoto dependerá do tamaño do ficheiro de rexistro e da frecuencia de cambio de rexistro na fonte.

### **59.5 BIBLIOGRAFÍA**

- *System & Disaster Recovery Planning*. Richard Dolewski
- *Information Storage and Management: Storing, Managing, and Protecting Digital Information*. G. Somasundaram e Alok Shrivastava.
- *Backup & Recovery*. W. Curtis Preston e O'Reilly Media.

**Autor:** Francisco Javier Rodriguez Martínez

Subdirector de Sistemas Escola Superior Enxeñaría Informática Ourense

Colexiado do CPEIG



# **60. ADMINISTRACIÓN E XESTIÓN DE REDES E SISTEMAS DE ALMACENAMENTO. VIRTUALIZACIÓN DO ALMACENAMENTO. XESTIÓN DO CICLO DE VIDA DA INFORMACIÓN (ILM).**

Tema 60.- Administración e xestión de redes e sistemas de almacenamento. Virtualización do almacenamento. Xestión do ciclo de vida da información (ILM).

---

<b>60.1 Administración e xestión de redes e sistemas de almacenamento.</b>	<b>2</b>
.....	2
.....	2
60.1.1 Administrador de rede.....	2
60.1.2 Administración e xestión de redes.....	4
60.1.2.1 Tarefas da xestión de rede.....	5
60.1.2.2 Elementos da xestión de rede.....	7
60.1.2.2.1 Estrutura de Xestión da Información (SMI, Structure of Management Information):.....	7
60.1.2.2.2 A Xestión da Información Base (MIB, Management Information Base)	8
60.1.2.2.3 Protocolo SNMP (Simple Network Management Protocol).....	8
<b>60.2 Virtualización do Almacenamento.....</b>	<b>11</b>
60.2.1 Concepto de virtualización de almacenamento.....	12
60.2.2 Tipos de virtualización de almacenamento.....	14
60.2.3 Outros tipos de virtualización.....	15
60.2.3.1 Virtualización de Memoria.....	16
60.2.3.2 Redes de virtualización.....	16
60.2.3.3 Virtualización a nivel de servidores.....	17
<b>60.3 Xestión do Ciclo de Vida da Información (ILM).....</b>	<b>18</b>
60.3.1 Xestión do Ciclo de Vida dos Datos.....	18
60.3.2 Xestión do Ciclo de Vida da Información .....	19
60.3.3 Algunha solucións para a xestión .....	21
60.3.3.1 Microsoft.....	21
60.3.3.2 IBM.....	21
60.3.3.3 Oracle.....	22
<b>60.4 Bibliografía.....</b>	<b>23</b>

## **60.1 ADMINISTRACIÓN E XESTIÓN DE REDES E SISTEMAS DE ALMACENAMENTO.**

### **60.1.1 Administrador de rede**

Un administrador de rede como o seu nome indica "administra" unha rede, é dicir, encárgase de:

- Instalación e configuración da rede.
- Hardware de rede, conexións físicas, hubs, switches, routers, servidores e clientes.
- Software de rede, como os sistemas operativos de rede, servidores de correo electrónico, software para a realización de copias de seguridade, base de datos servidores e software de aplicación.

O máis importante, o administrador ten coidado dos usuarios da rede, respondendo ás súas preguntas, escoitando os seus problemas e resolvéndooos.

Cando as tarefas de administración se realizan nunha rede grande e complexa, este conxunto de tarefas debe abarcarse de xeito dedicado, é dicir, posuír unha ou varias persoas realizando unicamente as tarefas de administración da rede. Isto debe ser así debido a que as redes tenden a ser volátiles no sentido de:

- Os usuarios da rede cambian constantemente.
- Os equipos fallan.

- Prodúcese conflitos entre as distintas aplicacións.
- En xeral, unha rede complexa sofre continuos estados de crises.

Pola contra, as redes de menor tamaño e por iso menos complexas son xeralmente moito máis estables. Adoita ser habitual que unha vez posta en funcionamento unha rede sinxela, esta non teña que sufrir continuas e complexas tarefas de administración, xa sexan de hardware ou software.

Neste tipo de redes pequenas os problemas tamén aparecen, pero como interveñen un reducido número de equipos é normal que sexan sinxelos, poucos e distantes entre si.

Independentemente do tamaño dunha rede, un administrador debe cubrir as seguintes tarefas que son comúns a calquera tipo de rede:

- Involucrarse e formar parte na toma de decisións para a adquisición de novo equipamento, servidores, equipos, impresoras, etc.
- Establecer as accións necesarias para o correcto funcionamento cada vez que se engada un novo equipo, é dicir, un administrador de rede cando se integra un novo elemento á rede encárgase de introducir cambios na configuración do cableado, de asignar un nome de rede ao novo equipo, e de integrar a un novo usuario no sistema de seguridade garantindo ademais os seus privilexios.
- Estar ao corrente das actualizacións de software que publiquen os provedores e considerar se as súas novas características son suficientes para xustificar unha posible actualización.

Na maioría dos casos, a parte máis difícil dun proceso de actualización de software é a determinación do camiño a seguir, como levar a cabo a actualización de toda a rede, afectando o menos posible o funcionamento dos usuarios. Isto adoita ser aínda máis crucial se o software a actualizar é o sistema operativo de rede, posto que calquera cambio no pode afectar a toda a rede.

Dentro deste procesos de actualización tamén interveñen afectando en menor medida á estabilidade do sistema os parches e Service Packs que publican os provedores para actualizar as súas solucións e que liquidan problemas menores.

- Realizar tarefas rutinieras como a realización de copias de seguridade dos servidores, a administración do historial de datos ou a liberación de espazo nos discos duros. Gran parte da tarefas de administración dunha rede consisten en asegurarse de que todo funcione correctamente, buscando e corrixindo os problemas que poidan ter os usuarios.
- Recompilar, organizar e controlar o inventariado de toda a rede, para poder liquidar no menor tempo posible calquera imprevisto.

### **60.1.2      *Administración e xestión de redes***

O concepto de administración ten asociado moitos significados. Desde un punto de vista informal, a xestión de redes refírese ás actividades relacionadas co funcionamento dunha rede, xunto coa tecnoloxía necesaria para apoiar estas actividades. Outro aspecto de importancia na xestión dunha rede é a monitorización da mesma, é dicir, entender en todo momento qué é o que está sucedendo na rede.

Desde un enfoque software, a xestión de redes fai referencia ao conxunto de actividades, métodos, procedementos e ferramentas que interveñen nas operacións de administración, mantemento e aprovisionamento dos sistemas existentes dentro da rede.

Supón, ademais, garantir toda a oferta operativa de servizos mantendo a rede en marcha e funcionando sen problemas. Para conseguir isto faise imprescindible a utilización de ferramentas para a monitorización da rede, que ofrezan a detección de problemas o máis pronto posible, mesmo antes de que algún usuario se vexa afectado.

A administración abarca, á súa vez, as tarefas de seguimento dos recursos na rede e de como estes se asignan, facendo uso de todos os procesos ou accións de limpeza da rede que sexan necesarias para manter todo baixo o control do administrador ou administradores.

O proceso de mantemento, que se ocupa de realizar as operacións de reparación e mellora, ha de levar a cabo tarefas como a substitución dunha tarxeta de rede, actualización do sistema operativo dun router, engadir un novo switch ao entramado de rede. O mantemento tamén implica medidas para a corrección e prevención, por exemplo, o axuste dos parámetros necesarios dun dispositivo en función das necesidades que se soliciten ou intervir cando sexa necesario para mellorar o rendemento da rede en momentos puntuais.

Outro aspecto da administración dunha rede é o aprovisionamento, tarefa que atinxe á configuración e adaptación dos recursos de rede para dar soporte aos servizos ofertados. Un exemplo de aprovisionamento é o feito de engadir as configuracións necesarias nos sistemas para proporcionar o servizo de voz a un novo usuario.

#### *60.1.2.1 Tarefas da xestión de rede*

As tarefas de xestión dunha rede pódense caracterizar do seguinte xeito:

- QoS e Xestión do Rendemento: un administrador de rede debe supervisar e analizar periodicamente os routers, hosts e o



funcionamento dos enlaces e logo en función dos resultados obtidos realizar unha redirección do fluxo de datos para evitar a sobrecarga de certos puntos da rede. Para realizar esta tarefa de seguimento da rede, existen ferramentas que detectan rapidamente os cambios que se producen no tráfico dunha rede.

- Xestión de fallos pola rede: calquera fallo na rede, enlaces, nodos, routers, fallos de hardware ou software, debe ser detectado, localizado e respondido pola propia rede, é dicir, a propia rede debe posuír mecanismos para intentar liquidar por si soa o maior número de continxencias que se poidan producir.
- Xestión da configuración: esta tarefa implica o seguimento de todos os dispositivos baixo xestión e a confirmación de que todos os dispositivos están conectados e funcionan correctamente. Se se produce un cambio inesperado nas táboas de enrutamento, o administrador debe descubrir o problema de configuración e solucionalo canto antes para que ningún servizo nin usuario se vexa afectado.
- Xestión da seguridade: o administrador de rede é o responsable da seguridade da rede. Para poder manexar esta tarefa utilízanse principalmente os firewalls, posto que un firewall pode monitorar e controlar os puntos de acceso á rede informando sobre calquera intento de intrusión.
- Xestión de facturación e contabilidade: o administrador especifica os usuarios da rede os accesos ou restricións sobre os recursos e encárgase da facturación e dos cargos aos usuarios polo uso dos mesmos.

### 60.1.2.2 Elementos da xestión de rede

A xestión de rede está composta por tres compoñentes principais:

- **Centro de xestión:** composto polo administrador de rede e as súas oficinas ou centros de traballo. Normalmente o centro de xestión está composto por un grupo humano importante.
- **Dispositivos a xestionar:** conformado polo equipamento da rede, incluído a súa software, que é controlado mediante o centro de xestión. Calquera hub, bridge, router, servidor, impresora ou módem é considerado un dispositivo que debe ser xestionado.
- **Protocolo de xestión da rede:** é o conxunto de políticas que adopta o centro de xestión para controlar e manexar todos os dispositivos que conforman a rede. O protocolo de xestión de rede permítelle ao centro de xestión coñecer o estado dos dispositivos.

#### **60.1.2.2.1 Estrutura de Xestión da Información (SMI, Structure of Management Information):**

Define as regras para nomear os obxectos e para codificalos nun centro de xestión dunha rede, é dicir, é unha linguaxe mediante a cal se definen as instancias dentro dun centro de xestión de rede.

A linguaxe SMI tamén ofrece construcións da linguaxe de maior nivel que, habitualmente, especifican os tipo de datos, o estado e a semántica dos obxectos que conteñen a información necesaria para realizar as tarefas de xestión. Por exemplo, a cláusula STATUS especifica se a definición do obxecto é actual ou está obsoleta.

Traballa baixo o protocolo SNMP (Simple Network Management Protocol) definindo os conxuntos de obxectos dentro a xestión de información base (MIB).

#### **60.1.2.2.2 A Xestión da Información Base (MIB, Management Information Base)**

É un medio de almacenamento de información que contén os obxectos que mostran o estado actual dunha rede. Debido a que os obxectos teñen asociada información que se almacena no MIB, este forma coleccións de obxecto, nas que inclúe as relacións entre eles, no centro de xestión.

Os obxectos organízanse dunha forma xerárquica e identifícanse pola notación abstracta ASN.1, linguaxe de definición de obxectos. A xerarquía, coñecida como ASN.1, é unha árbore de identificadores de obxecto na cal cada póla ten un nome e un número, permitindo así á xestión de rede identificar obxectos por unha secuencia de nomes ou números desde a raíz ao obxecto.

#### **60.1.2.2.3 Protocolo SNMP (Simple Network Management Protocol)**

O Simple Network Management Protocol (SNMP) está deseñado para monitorar o rendemento dos protocolos de rede e dos dispositivos. As unidades de datos do protocolo SNMP (PDUs) poden ser transportadas nun datagrama UDP, polo que a súa entrega en destino non está garantida. Os dispositivos que se administran como os routers ou hosts, son obxectos e cada un ten unha definición formal e MIB adapta unha base de datos de información que describe as súas características. Con este protocolo, un xestor de rede pode atopar onde se localizan os problemas.

Execútase sobre UDP e utiliza unha configuración cliente-servidor. Os seus comandos definen cómo realizar as consultas sobre a información dun servidor ou cómo enviar esta cara a un cliente ou a outro servidor.

A tarefa principal do protocolo SNMP é a de transportar información entre os centro de xestión e os axentes que se executan en representación dos centros de xestión. Para cada obxecto MIB que se xestiona utilízase

unha petición SNMP para obter o seu valor ou para modificala. Se un axente recibe unha mensaxe non solicitada ou se unha interface ou dispositivo deixan de funcionar, entón o protocolo pode informar ao centro de xestión do fallo que se está producindo.

A segunda versión deste protocolo, SNMPv2, corre por encima de varios protocolos e ten máis opcións de mensaxería, o que resulta nunha xestión máis eficaz da rede. Ten sete unidades de PDU, ou mensaxes:

1. **GetRequest.** Utilízase para obter un valor de obxecto MIB.
2. **GetNextRequest.** Utilízase para obter o seguinte valor dun obxecto MIB.
3. **GetBulkRequest.** Recibe múltiples valores, o que equivale a GetRequests múltiples, pero sen necesidade de utilizar múltiples peticións.
4. **InformRequest.** É unha mensaxe de director a director de comunicación que se envían entre si dous centros de xestión a distancia o un do outro.
5. **SetRequest.** É utilizado por un centro de xestión para inicializar o valor dun obxecto MIB.
6. **Response.** É unha mensaxe de resposta a unha petición de tipo PDU.
7. **Trap.** Notifica a un centro de xestión dun evento inesperado.

Hai dous tipos de representación de PDUs, Get ou Set e Trap.

- O formato de PDU de Get ou Set é o seguinte:
  - o *PDU type*, indica un dos sete tipos de PDU.

- o *Request IDE*, é un IDE que se utiliza para verificar a resposta dunha solicitude. Polo tanto, un centro de xestión pode detectar peticións perdidas ou duplicadas.
- o *Error status*, só é usado por PDUs *Response* para indicar tipos de erros reportados por un axente.
- o *Error index*, é un parámetro que indica a un administrador o nome do obxecto que causou o erro.

Se as solicitudes ou respostas se perden, o protocolo non realiza un reenvío. Os campos *Error status and Error index* son todo zeros excepto para as PDUs *GetBulkRequest*

- O formato de PDU de Trap é:
  - o *Enterprise*, para usar en múltiples redes.
  - o *Timestamp*, para realizar as medicións de tempo.
  - o *Agentadress*, para indicar que a dirección do axente xestor está incluída na cabeceira PDU.

## **60.2 VIRTUALIZACIÓN DO ALMACENAMENTO**

Grazas á introdución de redes de gran capacidade e servidores de alto rendemento, combinado cos novos sistemas de almacenamento desenvolvidos en gran medida grazas ao avance das tecnoloxías neste campo, o campo da virtualización orientado ao almacenamento converteuse nun dos sectores máis dinámicos no campo das TIC.

A tendencia xeral nas grandes empresas e institucións hoxe en día oríéntase á disposición de tecnoloxías de almacenamento en rede, que permitan mantela accesible, á vez que protexida. As empresas, institucións e gobernos hoxe en día dependen da información, que non deixa de ser datos sen procesar ou interpretar, que en última instancia residen nalgún lugar dos medios de almacenamento. Polo tanto é necesario establecer os mecanismos adecuados para protexer esa información e facilitar o seu acceso ao tempo que se proporcionan os medios para simplificar a súa xestión.

Aproximadamente desde os anos 90, os sistemas de almacenamento foron sufrindo un proceso evolutivo constante. A introdución de tecnoloxía de fibra óptica propiciou o despregamento de sistemas de almacenamento distribuído, baseados en NAS (Network-Attached Storage), así como agrupación de servidores de discos ou acceso compartido aos sistemas de almacenamento de cinta. Cada un destes avances técnicos irá acompañado por unha ruptura nas prácticas anteriores, dado que a operativa para substituír e traballar con novos modelos de almacenamento, a medida implicaba un cambio operacional importante.

Actualmente as novas solucións tratan de simplificar este tipo de situacións aplicando técnicas de abstracción que permiten acceder de forma transparente aos recursos de almacenamento. Aquí é onde a

virtualización adquire un papel importante. A virtualización pretende abstraer de forma lóxica os sistemas de almacenamento físico, e polo tanto, cando está ben empregado, oculta a complexidade dos dispositivos e simplificando a xestión dos sistemas de almacenamento, o que axuda a reducir os custos de xestión.

Na actualidade non hai ningún organismo internacional que estea definindo un modelo estándar para os protocolos e arquitecturas relacionadas coa virtualización do almacenamento. O único traballo destacable é o realizado pola SNIA (Storage Networking Industry Association), que redactou un informe sobre o estado actual das tecnoloxías de virtualización.

### **60.2.1      *Concepto de virtualización de almacenamento***

O concepto de virtualización de almacenamento refírese ás ferramentas que se utilizan para dispoñer dun contorno de almacenamento con múltiples dispositivos e multilocalización de recursos, pero presentado de forma totalmente transparente ao usuario.

A virtualización de almacenamento a miúdo apóiase en servidores de discos ou servidores de almacenamento que combinen diferentes tipos de tecnoloxías de almacenamento, por exemplo medios de rotación, discos duros tradicionais, ou tecnoloxías de estado sólido, como SSD ou mesmo memoria de acceso aleatorio dinámico.

Segundo a taxonomía da SNIA (Storage Networking Industry Association) referente á virtualización do almacenamento, existen tres conceptos básicos que se deben destacar no sistema deste tipo:

- Que é o que se está virtualizando: A virtualización pódese aplicar a unha gran variedade de dispositivos de almacenamento. Os discos físicos, compostos de cilindros, pistas e sectores, virtualízanse conformando un disco virtual. Os sistemas de cinta, formados por unha ou moitas unidades de cinta, poden ser agrupados nunha

única unidade. Outro exemplo poden ser os sistemas de arquivo que, mediante virtualización, poden facer de forma transparente o acceso a puntos do sistema de ficheiros que se atopen en máquinas remotas.

- Ónde se realiza a virtualización: Refírese á localización espacial na cal se realiza a implementación, xa que esta pode concretarse mediante matrices de almacenamento, ou en rede a través de switches intelixentes ou dispositivos conectados a SAN.
- Cómo se implementa: Fai referencia a como proporcionar os medios para construír servizos de alto nivel que oculten a complexidade dos compoñentes subxacentes e permitan a automatización das operacións de almacenamento de datos.

A idea é que nin clientes nin servidores necesiten saber onde están os arquivos que se están procesando, escondendo a rede física que existe entre eles. Isto proporciona as seguintes funcionalidades:

- Permite sistemas de arquivos distribuídos.
- Os dispositivos de almacenamento remoto aparecen como se estivesen conectados directamente ao sistema.
- O sistema local non coñece onde se atopan ou que tipo de almacenamento son.

Un exemplo de virtualización de almacenamento baseado en host é a administración de volumes. A xestión de volumes permite presentar unha



única vista lóxica dun recurso de almacenamento que pode estar formado por distintos dispositivos físicos.

As principais vantaxes da virtualización do almacenamento inclúen a optimización e reaproveitamento da capacidade de almacenamento, a posibilidade de engadir ou eliminar almacenamento sen afectar á dispoñibilidade das aplicacións, e a migración de datos sen interrupción.

Aconséllase a implantación de virtualización do almacenamento nas organizacións cando se desexa alcanzar os seguintes obxectivos:

- Alta dispoñibilidade /Recuperación fronte a desastres.
- No caso de que exista virtualización de aplicacións.
- Cando se necesita un acceso continuo a aplicacións e datos e existe un só dispositivo e de almacenamento. Conectado en rede, mediante virtualización pódense mellorar as prestacións e a escalabilidade, ademais de ofrecer mecanismos de tolerancia a fallos.
- As políticas nas que se contemple procesamento paralelo, ou nas que se teña en conta unha escalabilidade global do sistema, deben contemplar virtualización do almacenamento.
- Cando múltiples sistemas traballan nunha tarefa contra unha única unidade de almacenamento, pode diminuír notablemente o rendemento da mesma. Mediante virtualización podemos conseguir que a carga de traballo se estenda por unha única unidade lóxica de almacenamento repartida en varias unidades físicas, o que proporciona un mellor equilibrio da carga de traballo.

### **60.2.2      *Tipos de virtualización de almacenamento***

A virtualización do almacenamento trata de proporcionar os mecanismos necesarios para asignar unidades de almacenamento lóxicas a usuarios e

aplicacións, independentemente da localización dos dispositivos físicos, realizando as operacións de forma transparente. A virtualización pode realizarse segundo a filosofía SAN ou NAS. A principal diferenza é que nos contornos de virtualización SAN, a virtualización se aplica a nivel de bloque, mentres que en NAS se aplica a nivel de arquivo.

- Virtualización a nivel de arquivo (NAS): a este nivel, a virtualización baséase na eliminación das dependencias entre os datos de acceso a nivel de arquivo e a localización onde se almacenan fisicamente. Isto permite optimizar a utilización do almacenamento e a consolidación de servidores para realizar migracións con seguridade.
- Virtualización a nivel de bloque (SAN): neste nivel proporciónase unha capa de tradución na SAN entre os usuarios e as matrices de almacenamento que albergan os dispositivos físicos de almacenamento. Cando se accede ás unidades de almacenamento, en lugar de redirixirse á matriz de almacenamento física identificada por un LUN (Logical unit number), rediríxese cara a un LUN virtual, que reorganiza as matrices de almacenamento físicas (identificadas polos LUN físicos), en función das necesidades organizacionais. O dispositivo de virtualización é o que se encarga de realizar a tradución entre os LUN virtuais e LUN físicos.

### **60.2.3      *Outros tipos de virtualización***

Ademais do almacenamento, a virtualización existiu na industria das Tecnoloxías da Información durante moitos anos, e en diferentes formas. A idea da virtualización representa, ademais dun mecanismo de abstracción, unha técnica para o aforro e a utilización eficiente de certos recursos

críticos da máquina. Dentro das técnicas de virtualización aplicables a outros factores, destacan a virtualización da rede, virtualización de memoria, e en combinación virtualización de servidores.

#### *60.2.3.1 Virtualización de Memoria*

Aínda que o custo da memoria diminuíu grazas aos avances tecnolóxicos, segue sendo un recurso custoso. A virtualización da memoria posibilita que as aplicacións dispoñan da súa propia memoria continua, de forma independente dos recursos de memoria física que exista na máquina anfitrión.

Unha das implementacións máis habituais de memoria virtual é a coñecida como paxinación. Nesta, o espazo de direccións da memoria divídese en bloques contiguos de tamaño fixo que se denominan marcos de páxinas. Á súa vez, os programas en execución divídense tamén en anacos ou páxinas. Isto permite que o sistema operativo dispoña dun proceso denominado Xestor de Memoria Virtual (VMM, Virtual Memory Manager) que permite optimizar o uso da memoria recuperando de forma eficiente os “anacos” das aplicacións en execución á memoria principal, e derivando a un almacenamento secundario os “anacos” inactivos.

O sistema asigna ao VMM un espazo no disco, coñecido como arquivo SWAP, ou partición SWAP. A SWAP conforma o espazo de intercambio, no que o VMM mantén almacenadas as páxinas nas que se dividen os procesos, gardando o seu contexto e información de estado. Esta parte do disco actúa como unha memoria física (RAM) para o sistema operativo.

#### *60.2.3.2 Redes de virtualización*

A virtualización de redes refírese ao feito de que cada aplicación que faga uso da rede para o seu funcionamento poida xerar a súa propia rede

lóxica e independente da rede física. Un exemplo concreto deste tipo de virtualización poderían ser as VLAN, que presenta un mecanismo de xestión das redes menos custosa e máis flexible.

Cunha virtualización de tipo VLAN, un conxunto de usuarios dunha rede cuns requisitos de acceso a recursos similares, pódense agrupar na mesma rede virtual, permitindo acceder aos recursos desa VLAN sen importar en que rede física real se atopen eses recursos. Isto implica que todas as conexións inter-rede que se teñan que realizar para o acceso aos recursos compartidos faranse de forma transparente, dando a impresión de que o acceso aos recursos se fai sempre a nivel local.

#### *60.2.3.3 Virtualización a nivel de servidores*

A virtualización de servidores aborda os problemas que existen nun contorno de servidor físico. A capa de virtualización axuda a superar conflitos de recursos que permiten illar aplicacións que se executan en diferentes sistemas operativos na mesma máquina. Ademais, a virtualización de servidores permite, de forma dinámica destinar os recursos de hardware ao lugar onde máis se necesiten.

## **60.3 XESTIÓN DO CICLO DE VIDA DA INFORMACIÓN (ILM)**

### **60.3.1 Xestión do Ciclo de Vida dos Datos**

A xestión do ciclo de vida dos datos ou DLM (Data Lifecycle Management) é un enfoque da xestión da información desde o punto de vista do manexo do fluxo dos datos dun sistema de información durante todo o seu ciclo de vida, desde que se crean e se produce o seu primeiro almacenamento ata que son declarados obsoletos e eliminados do sistema.

Os produtos para a xestión do ciclo de vida dos datos tratan de automatizar os procesos que forman parte deste ciclo de vida. Organizan os datos en distintos niveis seguindo unhas políticas especificadas e automatizan a migración ou intercambio dos datos entre uns niveis e outros, baseándose para iso nos criterios especificados de cada un.

Como norma xeral, os datos máis recentes e aqueles a os que se accede con máis frecuencia téndense a almacenar en medios de almacenamento máis rápidos, pero tamén máis caros, mentres que os datos dun nivel menos crítico se almacenan nos dispositivos máis baratos e máis lentos.

As arquitecturas que xestionan o ciclo de vida dos datos adoitan incluír un sistema de arquivos que indexa toda aquela información crítica e aquela considerada non tan crítica, pero que garda relevancia ou relación con esta. Con esta información crea copias de respaldo e almacénasas en localizacións seguras para evitar manipulacións, pero que poidan ser accesibles dun xeito seguro e fiable.

Estas arquitecturas tamén se encargan das posibles duplicacións de datos e da comprensión dos mesmos para garantir un correcto e eficiente uso do espazo de almacenamento dispoñible.

Desafortunadamente, moitas implementacións de DLM de negocios estancáronse, principalmente porque as empresas non lograron definir nin as políticas de migración adecuadas nin o arquivado de datos. Dado que esas políticas necesitan reflectir as prioridades de regulación e de negocio, nas súas definicións é necesario unha colaboración que involucre non só a membros do departamento de tecnoloxías da información, senón tamén a membros de diferentes departamentos do negocio.

Doutra banda, o criterio máis sinxelo para realizar unha migración da información a un sistema de almacenamento máis económico é o temporal, é dicir, os datos máis antigos nos sistemas máis lentos e baratos. Con todo, as empresas en industrias altamente reguladas a miúdo queren ir máis lonxe, establecendo a clasificación dos datos en función da rapidez coa que se precisen, ou a frecuencia coa que se accede a eles, ou baseándose en quen os enviou ou recibiu ou nun conxunto de palabras clave ou cadeas numéricas, etc. Daquela, o reto está en conseguir definilos de tal xeito que sexa viable realizalo no tempo e mediante a menor intervención humana.

### **60.3.2 Xestión do Ciclo de Vida da Información**

A xestión do ciclo de vida da información ou ILM (Information Lifecycle Management) é un enfoque integral para o manexo do fluxo dos datos dun sistema de información e os metadatos asociados desde a súa creación e almacenamento inicial ata o momento en que estes se volven obsoletos e son borrados.

A diferenza de anteriores enfoques para a xestión de almacenamento de datos ILM abarca todos os aspectos nos que se tratan os datos, partindo das prácticas dos usuarios, en lugar da automatización dos procedementos de almacenamento e en contraste cos sistemas máis antigos, ILM permite criterios moito máis complexos para a realización da xestión do almacenamento que a antigüidade dos datos ou a frecuencia de acceso a eles.

É importante destacar que ILM non é só unha tecnoloxía, senón que integra os procesos de negocio e TI co fin de determinar como flúen os datos a través dunha organización, permitíndolles aos usuarios e administradores xestionar os datos desde o momento que se crean ata o instante no que xa non son necesarios.

Aínda que os termos xestión do ciclo de vida dos datos (DLM) e xestión do ciclo de vida da información (ILM) ás veces se utilizan indistintamente, ILM a considérase un proceso máis complexo.

A clasificación dos datos en función de valores do negocio é unha parte integral e moi importante do proceso ILM. Isto quere dicir que ILM recoñece que a importancia dos datos non se basea unicamente na súa antigüidade ou na súa frecuencia de acceso, senón que ILM espera que sexan os usuarios e os administradores os que especifiquen distintas directivas para que os datos vaian variando dun xeito decrecente a súa relevancia ou grao de importancia para a organización, ou que poidan conservar a súa importancia durante todo o seu ciclo de vida, etc.

Para unha exitosa e eficiente implementación de IML necesítase que a organización identifique requisitos de seguridade dos datos críticos e incluílos nos seus procesos de clasificación. Os usuarios dos datos, tanto os individuos como as aplicacións, deben de ser identificados e categorizados en función das necesidades asociadas coas súas tarefas.

Algunhas das mellores prácticas relacionadas coa implementación de IML comparten enfoques como:

- Céntranse na produtividade do usuario, co fin de obter unha vantaxe estratéxica a través do acceso aos datos necesarios.
- Protexer os datos contra o roubo, a mutilación, a divulgación involuntaria, ou a eliminación.

- Crear múltiples capas de seguridade, sen crear unha xestión excesivamente complexa.
- Asegurarse que os procesos de seguridade están incorporados nos procesos xerais do negocio e nos procesos de TI.
- Utilizar estándares e modelos de referencias co fin de satisfacer unicamente as necesidades de seguridade da organización.

Por suposto, cada organización deberá desenvolver e implementar a súa propia solución de seguridade de almacenamento, que debe seguir evolucionando, adaptándose ás novas oportunidades, ameazas e capacidades.

### **60.3.3      *Algunha solucións para a xestión***

#### **60.3.3.1      Microsoft**

Microsoft Identity Lifecycle Manager ofrece unha solución integrada e completa para a xestión do ciclo de vida das identidades de usuario e as súas credenciais asociadas. Esta solución achega a sincronización de identidades, os certificados e administración de contrasinais e subministración de usuarios. A solución funciona baixo plataformas Windows e outros sistemas organizacionais.

#### **60.3.3.2      IBM**

As solucións de IBM para a xestión do ciclo de vida da información agrupáronse en cinco categorías (IBM, 2008):

- *Arquivo de correo electrónico* (IBM DB2 CommonStore, VERITAS Enterprise Vault, OpenText-IXOS Livelink)



- *Aplicación e base de datos de arquivo* (Arquivo Activo de Princeton Softech),
- *Xestión do ciclo de vida dos datos* (TotalStorage de IBM SAN File System)
- *Xestión de contidos* (repositorio de administración de contido, DB2 Content Manager)
- *Xestión de rexistros* (IBM DB2 Records Manager).

#### 60.3.3.3 Oracle

Oracle ILM Assistant é unha ferramenta que se basea nunha interface gráfica de usuario para a xestión de contorno de ILM. Ofrece a posibilidade de crear definicións de ciclo de vida, que se asignan ás táboas na base de datos. Posteriormente, baseándose nas políticas establecidas sobre o ciclo de vida, ILM Assistant informa sobre cando é o momento para mover, archivar ou suprimir os datos. Tamén mostra as necesidades de almacenamento e o aforro de custos asociados co cambio de localización dos datos.

Outras capacidades de Oracle ILM Assistant inclúen a habilidade de mostrar como particionar unha táboa baseada nunha definición do ciclo de vida, e poder simular os eventos para comparar o resultado no caso de que a táboa fose 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 Rodríguez Martínez

Subdirector de Sistemas Escola Superior Enxeñaría Informática Ourense

Colexiado do CPEIG



**61. REDUNDANCIA HARDWARE. ALTA DISPOÑIBILIDADE A NIVEL DE SISTEMA OPERATIVO. SISTEMAS DE CLÚSTER E BALANCEO DE CARGA. ALTA DISPOÑIBILIDADE EN SERVIDORES DE APLICACIÓNS E SERVIDORES DE BASES DE DATOS. ALTA DISPOÑIBILIDADE A NIVEL DE APLICACIÓN. DISPOÑIBILIDADE EN CONTORNOS VIRTUALIZADOS. CENTROS DE PROTECCIÓN XEOGRÁFICOS. PLANS DE CONTINXENCIA.**

Tema 61: Redundancia hardware. Alta dispoñibilidade a nivel de sistema operativo. Sistemas de clúster e balanceo de carga. Alta dispoñibilidade en servidores de aplicacións e servidores de bases de datos. Alta dispoñibilidade a nivel de aplicación. Dispoñibilidade en contornos virtualizados. Centros de protección xeográficos. Plans de continxencia.

---

## Índice

### **61.1 REDUNDANCIA HARDWARE**

#### 61.1.1 REDUNDANCIA EN DISCO RAID

##### 61.1.1.1 RAID 0

##### 61.1.1.2 RAID 1

##### 61.1.1.3 RAID 5

### **61.2 ALTA DISPOÑIBILIDADE A NIVEL DE SISTEMA OPERATIVO.**

#### 61.2.1 ALTA DISPOÑIBILIDADE

#### 61.2.2 ALTA DISPOÑIBILIDADE A NIVEL DE SISTEMA OPERATIVO

### **61.3 SISTEMAS DE CLÚSTER E BALANCEO DE CARGA.**

#### 61.3.1 CONCEPTO DE CLÚSTER

#### 61.3.2 TIPOS DE CLÚSTER

*Clúster HPCC (High Performance Computing Cluster): Cluster de Alto Rendemento*

*Clústers HA (High Availability): Cluster de Alta Dispoñibilidade*

#### 61.3.3 BALANCEO DE CARGA

### **61.4 ALTA DISPOÑIBILIDADE EN SERVIDORES DE APLICACIÓNS E SERVIDORES DE BASES DE DATOS.**

#### 61.4.1 ALTA DISPOÑIBILIDADE EN SERVIDORES DE APLICACIÓNS

#### 61.4.2 ALTA DISPOÑIBILIDADE A NIVEL DE BASES DE DATOS

### **61.5 ALTA DISPOÑIBILIDADE EN CONTORNOS VIRTUALIZADOS.**

#### 61.5.1 VIRTUALIZACIÓN DE HARDWARE

#### 61.5.2 VIRTUALIZACIÓN DE SISTEMA OPERATIVO

### **61.6 CENTROS DE PROTECCIÓN XEOGRÁFICOS**

### **61.7 PLANS DE CONTINXENCIA**

#### 61.7.1 CICLO DE VIDA

#### 61.7.2 CARACTERÍSTICAS

#### 61.7.3 O BXECTIVO

61.7.4 PUNTOS CLAVE

61.7.5 ELEMENTOS

## **61.8 BIBLIOGRAFÍA**

### **61.1 Redundancia Hardware**

A redundancia de hardware consiste na replicación de elementos hardware de reserva na configuración dun determinado sistema para proporcionar tolerancia a fallos, de forma que nun caso de continxencia por fallo dalgún dos compoñentes principais, algunha das réplicas se active para seguir proporcionando servizo sen que o sistema caia.

Dentro dos sistemas de protección contra fallos baseados na redundancia de hardware, existen un certo tipo de compoñentes determinados como críticos que adoitan ser os que se replican:

- *Fontes de alimentación:* A idea de replicación de fontes de alimentación consiste basicamente en replicar as fontes de alimentación interna do *servidor* ou máquina sobre a que estamos implementando a tolerancia a fallos. Ademais, e como medidas de apoio, poden instalarse unidades de alimentación eléctrica ininterrompida (SAI) para mitigar as caídas de subministro eléctrico da rede, ou mesmo, a instalación de grupos electrógenos alternativos para os casos nos que tratamos con centros de proceso de datos con varios servidores ou unidades que controlan sistemas críticos.
- *Núcleos de proceso:* É habitual, sobre todo coas novas unidades de microprocesadores multinúcleo, replicar as unidades de proceso que se integran nos servidores proporcionando mecanismos de control para a degradación do sistema que consisten en xestionar o fallo dos microprocesadores balanceando a carga de proceso ás unidades restantes que quedan activas.

- *Dispositivos de conexión á rede:* Do mesmo xeito que nos casos anteriores, a idea consiste en eliminar o colo de botella que pode supoñer o dispoñer dunha única toma de conexión á rede que presenta a interface de conexión á máquina e aos servizos que presta. Por iso, a tendencia adoita ser establecer como mínimo dúas interfaces de rede físicas na máquina para poder dispoñer dunha interface alternativa en caso de continxencia, que nos permita manter o sistema en liña.
- *Dispositivos de almacenamento:* En canto á replicación dos sistemas de almacenamento, a tendencia xeral consiste na replicación dos dispositivos de almacenamento masivo como os discos duros ou cintas magnéticas. No caso dos discos duros que se atopan nos servidores, a tendencia xeral é aplicar unha configuración de tipo RAID nalgún dos seus niveis avanzados, que presentan redundancia de datos e tolerancia a fallos con certas garantías.

Cómpre destacar que a maioría dos sistemas operativos sobre servidores deben implementar unha característica, de alta dispoñibilidade, que permita realizar mantemento e substitución de elementos hardware replicados que sufran algún fallo, sen necesidade de deter o sistema.

#### **61.1.1 Redundancia en Disco RAID**

As estratexias de backup que fan uso de discos, habitualmente seguen algún modelo de sistema RAID (Redundant Array of Independent Disks, conxunto redundante de discos independentes). A estratexia consiste en utilizar un conxunto de discos nos cales se distribúen ou replican os datos. Existen diferentes configuracións ou niveis de RAID que determinan as características da arquitectura e definen unha serie de vantaxes con respecto ao uso dun único disco ou ao uso doutros niveis de RAID

inferiores. Estas vantaxes están relacionadas coa integridade dos datos, a tolerancia a fallos, a capacidade e o rendemento.

Habitualmente os niveis de RAID se xestionan mediante controladoras especializadas a nivel de hardware, creando desde o nivel máis simple ata niveis complexos, matrices redundantes de discos independentes, que a alto nivel se reflicten como unidades lóxicas únicas.

Os modelos de RAID estándar son os Niveis 0 a 6, e as súas combinacións ou aniñamentos que dan lugar aos niveis 0+1 e 1+0 ou RAID10. Existen máis niveis de RAID por combinación ou aniñamento dos estándares existentes, así como solucións ou modelos propietarios. Dentro de todo o abano de posibilidades que existen, os máis habituais son os niveis RAID0, RAID1 e RAID5.

#### **61.1.1.1 RAID 0**

O nivel RAID 0, tamén coñecido como striping, consiste na utilización de dous ou máis discos entre os que se distribúe a información de forma equitativa. É un modelo ou nivel no que non existe información adicional de paridade nin se proporciona redundancia, polo que nalgúns círculos esta configuración non se considera como modelo de RAID orixinal. Como contrapartida, este modelo proporciona un alto rendemento dado que permite a escritura e acceso aos datos de forma simultánea en tantos dispositivos como estean configurados.

A configuración mostrará unha única unidade virtual (dous ou máis discos físicos subxacentes) cuxo tamaño total dependerá do disco físico que teña menor capacidade dentro do conxunto dos discos utilizados. É dicir, se dispoñemos dun nivel de RAID 0 con tres discos A, B e C, e cada un deles con 400GB, 350GB e 300GB respectivamente, o noso nivel RAID 0 presentará unha única unidade lóxica cunha capacidade de 900GB.



Isto implica que é posible a configuración dun nivel de RAID 0 con discos de diferente capacidade. Con todo, o recomendable sempre para este tipo de configuracións é o uso de capacidades similares.

Para determinar a fiabilidade dun RAID 0 existe unha fórmula sinxela que consiste en calcular a fiabilidade media de cada disco entre o número de discos utilizados na configuración.

#### **61.1.1.2 RAID 1**

En RAID 1, tamén coñecido como mirroring, créase unha copia exactamente igual dun conxunto de datos nun ou máis discos. Este modelo proporciona un alto rendemento en canto á lectura ademais de incrementar a fiabilidade global do sistema dado que ambos discos son unha copia exactamente igual. En contraposición existe un menor desaproveitamento do espazo dado que só se utiliza o equivalente ao espazo dun disco físico.

A implementación de técnicas de splitting ou duplexing, consistentes en configurar cada un dos discos en controladoras independentes, maximiza ese rendemento mellorado en canto á lectura de datos, dado que se poden estar lendo de ambos dispositivos de forma simultánea.

Para as operacións de escritura, o conxunto compórtase como un único disco dado que os datos deben ser escritos en todos os discos do RAID 1.

O RAID 1 proporciona unha gran vantaxe en canto á administración en contornos de produción continua, dado que permite a posibilidade de inactivar un dos discos espello para realizar sobre o mesmo copias de seguridade, sen necesidade de ter que apagar o sistema e proporcionando tempo de servizo extra para ese tipo de tarefas de mantemento.

#### **61.1.1.3 RAID 5**

O RAID 5 componse dun mínimo de 3 discos para a súa implementación. É un sistema RAID moi popular grazas a que proporciona, ademais de

eficiencia en operacións de lectura e escritura, redundancia a un custo realmente moi baixo.

RAID 5 realiza unha división dos datos en forma de bloques (stripes), distribuíndo cada bloque por un dos discos físicos que forman o RAID 5. Ademais, realiza un control de paridade de cada conxunto de bloques distribuídos polos discos. O almacenamento destes bloques de paridade vaise alternando entre os diferentes discos que forman o RAID, de xeito que permite establecer un sistema de redundancia con garantías.

A idea é que cada vez que un bloque de datos se escribe nun RAID 5, xérase un bloque de paridade dentro da mesma división. En caso de modificar os datos do bloque, ou engadir datos novos ao bloque, a paridade recálculase e escríbese no seu espazo asignado. O bloque utilizado para escribir a paridade está disposto en chanzos en cada división. Polo tanto todos os discos que forman parte dun RAID 5 albergan bloques de datos e bloques de paridade. De aí o termo de “bloques de paridade distribuídos”.

A desvantaxe deste nivel de RAID é que as operacións de escritura son custosas, dado que hai que realizar o coproceso de cálculo de paridade para a escritura. De feito, nas implementacións de RAID 5 preséntase un rendemento malo no caso de realizar moitas operacións de escritura cuxo tamaño do bloque é menor que o tamaño dunha división. Nas operacións de lectura, o bloque de paridade asociado non se le, a non ser que se produza un erro na comprobación de paridade dos datos lidos.

En caso de fallo dun dos bloques de datos durante a lectura, automaticamente se recupera a paridade asociada a ese bloque para recuperar os datos e reconstruír o sector erróneo de forma transparente ao usuario. Da mesma forma, se un dos discos de RAID 5 falla, os bloques de paridade restantes dos demais discos permiten reconstruír os bloques de datos baixo demanda do disco que fallou. Por iso é polo que polo menos se necesitan tres discos para unha implementación deste nivel de RAID. O

fallo dun segundo disco dentro de RAID 5 provoca a perda completa dos datos.

Teoricamente, en número máximo de discos que se poden utilizar para implementar un RAID5 é ilimitado, con todo a tendencia xeral consiste en limitar ese número dado que a maior cantidade de discos, maior probabilidade de fallo simultáneo.

## **61.2 Alta dispoñibilidade a nivel de sistema operativo.**

### **61.2.1 Alta dispoñibilidade**

O concepto de alta dispoñibilidade, ou High Availability en inglés, consiste no deseño de arquitecturas de sistemas cuxas implementacións aseguren un grao de continuidade das operacións que leven a cabo. Trátase fundamentalmente de prever continxencias que poidan desembocar na suspensión dos servizos proporcionados polo sistema que se diseña, de forma que poidan ser controlables, e os devanditos mecanismos de control permitan que o sistema manteña todas as funcionalidades que se poñen a disposición dos usuarios. Ademais de continxencias, trátase de prever e soportar outras tarefas que nun sistema normal provocan a suspensión temporal, como poden ser tarefas de mantemento ou actualización. Os sistemas que habitualmente necesitan garantir graos absolutos de alta dispoñibilidade son aqueles destinados ao control de tarefas críticas.

Como se detalla a seguir, existen diferentes orientacións á hora de dotar aos sistemas de alta dispoñibilidade, que poden estar implementadas a nivel de sistema operativo, a nivel de aplicacións, ou mesmo facendo uso transparente de redundancia de equipos mediante a configuración de clústers.

### **61.2.2 Alta dispoñibilidade a nivel de sistema operativo**

Os sistemas operativos proporcionan tamén os mecanismos necesarios para complementar as funcionalidades que proporcionan alta dispoñibilidade do sistema. Os máis habituais adoitan ser os seguintes:

- Capacidade para poder xestionar réplicas a nivel software de volumes ou particións do sistema. Consiste basicamente nunha simulación do nivel 1 de RAID baseado en software.
- O sistema de ficheiros ademais debe permitir a xeración de táboas coas que poida localizar arquivos redundantes noutras estruturas redundantes, de xeito que proporcione as operacións de acceso de maneira transparente

Algúns exemplos compoñentes software que proporcionan esta funcionalidade a nivel de sistema operativo son:

- HP MirrorDisk/UX baseada en Unix para servidores da casa HP.
- Sun Solaris Volume Manager para sistemas operativos baseados en Solaris de Sun
- Windows Disk Administrator para sistemas operativos Windows.

Todas estas ferramentas basean o seu funcionamento na xestión de discos dinámicos, facilitando a creación e xestión de volumes que proporcionan a creación de espellos, implementando un nivel de RAID 1 por software.

Nos sistemas operativos que se basean en Unix, a capacidade de xestionar un sistema de ficheiros que permite redundancia vén proporcionada polo sistema de ficheiros NFS (Network File System). Mediante a agrupación de máquinas en forma de clúster posibilitase a nivel hardware a alta dispoñibilidade mediante replicación de máquinas. O sistema operativo intervén ao implementar NFS como servizo, permitindo integrar no clúster servidores de ficheiros ofrecendo de forma transparente unha interface que permite utilizar un único sistema de ficheiros redundante sobre o clúster.

Outra característica a nivel de sistema operativo que proporciona a capacidade de alta dispoñibilidade consiste na implementación de journaling. O journaling é unha característica dos sistemas de xestión de ficheiros transaccionais que mantén un ficheiro de log no que se almacenan os cambios que se van producindo no disco. Isto proporciona a posibilidade de poder realizar unha recuperación dos datos no caso de que se produza un erro no sistema. En caso de fallo, o procedemento consiste na reconstrución dese ficheiro de log principal, comunmente chamado journal, para recuperar a integridade de todo o sistema de ficheiros. Entre os sistemas de ficheiros que implementan as características de journaling áchanse algúns como Ext3, Ext4 e JFS de Linux, NTFS de Windows, UFS de SUN Solaris, e HFS de Mac OS X.

Outras características que permiten manter unha alta dispoñibilidade dos sistemas consisten en:

- Capacidade para aplicación de parches e actualizacións sen necesidade de reiniciar o sistema. Isto fai que diminúa o tempo nas tarefas de mantemento así como evitar os cortes do servizo en caso de actualización.
- Capacidade do sistema operativo para a xestión de dispositivos hardware que poidan ser conectados e agregados en quente, é dicir, sen necesidade de ter que apagar o sistema.
- Outra característica implementada é a tolerancia a fallos provocados por hardware, implementando o que se coñece como sistemas degradables, que permiten xestionar estes fallos de hardware sen que se produza unha detención dos servizos proporcionados aos usuarios nin unha detención do sistema.

### **61.3 Sistemas de clúster e balanceo de carga.**

O concepto de clúster serve para definir un conxunto de ordenadores construídos utilizando compoñentes de hardware comúns e que se agrupan proporcionando a vista lóxica dun único equipo para realizar tarefas de procesamento. Grazas ao avance da tecnoloxía de clustering, actualmente esta filosofía de construción de centros de procesamento permite a súa aplicación en campos que abarcan desde a supercomputación, sistemas críticos, servidores Web ou comercio electrónico, ata bases de datos de alto rendemento. Na actualidade, os principios de clustering e a creación de agrupacións de máquinas para o procesamento de datos desempeña un papel importante para a resolución de problemas de cálculo e modelado de simulacións en todos os campos científicos e de coñecemento.

A utilización de clústers vén derivada do desenvolvemento tecnolóxico actual, no que a dispoñibilidade de microprocesadores económicos e infraestrutura de comunicacións de alta velocidade proporcionan a base hardware necesaria para o seu deseño, e o desenvolvemento de ferramentas de software para cómputo distribuído de alto rendemento proporciona os mecanismos para a posta en produción. Xa que logo, podemos entender os clústers como un conxunto de múltiples equipos interconectados a través dunha rede de datos habitualmente de alta velocidade, e que forman unha vista lóxica de equipo único. Esta vista lóxica proporcionada presenta un ordenador moito máis potente, e con certas capacidades intrínsecas que permiten proporcionar alta dispoñibilidade e gran capacidade de proceso, a un custo comparativo moito máis reducido que un equipo real coas mesmas características de procesamento.

Segundo o tipo de ordenadores que forman parte dun clúster, estes poden seguir tres tendencias:

- Se todos teñen os equipos, teñen a mesma configuración hardware e sistema operativo, falamos dun clúster homoxéneo.
- Se o hardware é distinto, pero a arquitectura e sistemas operativos son similares, entón falamos dun clúster semi-homoxéneo.
- Finalmente, se o hardware e sistema operativo de cada equipo é diferente falamos dun clúster heteroxéneo.

Esta versatilidade á hora de escoller entre as máquinas que finalmente formarán parte do clúster é o que proporciona flexibilidade económica e facilidade para a súa construción.

O último elemento que se necesita para que un clúster finalmente se poña en produción é o sistema de manexo do clúster. Este sistema será o que se encargue de interactuar co usuario e os procesos que corren no propio clúster, para optimizar o funcionamento distribuíndo as cargas de proceso e proporcionando ao usuario a vista transparente de equipo único.

Debido a que existen diferentes tipoloxías de clústers que se poden configurar, o tipo de software final que xestione esas capacidades debe ser específico. Independentemente das diferentes especializacións, existen dous modelos xerais á hora de desenvolver software que compón o clúster:



- Software a nivel de aplicación: No que habitualmente se utilizan bibliotecas que permiten realizar a abstracción dun nodo a un sistema integral, facilitando o desenvolvemento de aplicacións distribuídas. Estas bibliotecas proporcionan funcións para a construción de rutinas. Estas rutinas serán tratadas polo clúster como unidades que poden ser procesadas de forma independente en calquera dos nodos do clúster, realizando a comunicación a través da rede.
- Software a nivel de sistema: Neste tipo, habitualmente o propio sistema operativo conta con implementación interna para a xestión deste tipo de tarefas. Adoitan ser sistemas operativos específicos para a construción de clústers.

### 61.3.1 **Concepto de clúster**

A definición de clúster é complexa e para nada sinxela, ata o punto de que na actualidade, incluso o persoal especializado no campo da supercomputación e clustering ten problemas para delimitar realmente cales son os límites da definición.

A nivel xeral, podemos definir un clúster como un conxunto de ordenadores unidos por unha rede de alta capacidade e que realizan tarefas de procesamento conxunto. Segundo o tipo de tarefas ás que o clúster estea orientado, pódense distinguir clústers de alta dispoñibilidade, alto rendemento ou clústers dedicados ao balanceo de carga..

Tamén se fai referencia á arquitectura utilizada para a configuración dos clústers, distinguindo entre clústers SMP e clústers formados por nodos monoprocesadores. Hai arquitecturas clústers que se denominan constelacións e caracterízanse por que cada nodo contén máis procesadores que o número de nodos. Con todo, as constelacións seguen sendo clústers de compoñentes ou nodos avantaxados e caros. De feito, entre as máquinas que aparecen no top 500 existen uns poucos clústers que pertencen a organizacións que non son xigantes da informática, o cal indica o prezo que poden chegar a ter estes sistemas.

A definición que tomaremos como formal e máis aproximada ao conxunto de definicións que se poden atopar na bibliografía xeral que versa sobre o tema é a seguinte:

Un clúster consiste nun conxunto de máquinas denominadas nodos, que en conxunto alcanza unha gran capacidade de proceso e que está orientado ao procesamento paralelo de grandes cantidades de datos, realizándoo de forma transparente.

### **61.3.2 Tipos de clúster**

#### **Clúster HPCC (High Performance Computing Cluster): Cluster de Alto Rendemento**

Un clúster de alto rendemento será aquel tipo de clúster que está especialmente deseñado para ofrecer unha gran capacidade de cálculo. Á

hora de enfrontarse a un problema fundamentalmente baseado na realización de cálculo, as principais fortalezas que nos proporcionan os clústers están ligadas a dous aspectos:

- O tamaño do problema por resolver: En moitas ocasións, os problemas tenden a redefinirse e recalcularse, ou a xerar novas especificacións para validar, incrementando notablemente o tamaño do problema final que necesita ser procesado.
- O prezo da máquina necesaria para resolvelo: Se se suscitan especificacións necesarias sobre a capacidade de cálculo necesario para obter resultados nunha marxe de tempo aceptable, na maioría dos casos o custo asociado a unha única máquina que satisfaga esas especificacións é moi superior ao dun clúster formado por equipos de menor rendemento.

Outro aspecto que se debe ter en conta é que para garantir esta capacidade de cálculo os problemas necesitan ser paralelizables. Os clústers utilizan a división de tarefas e asignación aos diferentes nodos de proceso desas tarefas, como mecanismo para axilizar o proceso de cálculo. Os problemas deben ser subdivididos en problemas máis pequenos para que se poida distribuír o seu proceso entre os diferentes nodos de cómputo. Se un problema non cumpre con esa característica, entón o clúster non pode ser utilizado para resolvelo. O obxectivo, polo tanto é mellorar o rendemento na obtención de resultados dun problema, obtendo unha mellora do rendemento en base ao tempo de resposta ou en base á precisión dos propios resultados.

A implementación necesaria para abordar estes problemas segue dúas tendencias. Pódese implementar a nivel de sistema operativo e pódese implementar mediante o uso de librerías.

Dentro desta definición non se engloba restrición concreta. Isto supón que calquera clúster que faga que o rendemento do sistema aumente respecto ao dun dos nodos individuais pode ser considerado clúster HP. Xeralmente estes problemas de cómputo adoitan estar ligados a:

- *Cálculos matemáticos*
- *Renderizacións de gráficos*
- *Compilación de programas*
- *Compresión de datos*
- *Descifrado de códigos*
- *Rendemento do sistema operativo, (incluíndo nel, o rendemento dos recursos de cada nodo)*

Existen outros moitos problemas máis que se poden solucionar con clústers HP, onde cada un aplica dun xeito ou outro as técnicas necesarias para habilitar a paralelización do problema, a súa distribución entre os nodos e obtención do resultado. As técnicas utilizadas dependen de a que nivel traballe o clúster.

Habitualmente as tendencias de deseño de implementación de clústers a nivel de aplicación e a nivel de balanceo de carga son excluíntes, é dicir, se se constrúen a nivel de aplicación, non implementan o balanceo de carga. Adoitan basear todo o seu funcionamento nunha política de localización que sitúa as tarefas nos diferentes nodos do clúster, e comunícaaas mediante as librerías abstractas. Resolven problemas de calquera tipo dos

que se viron no apartado anterior, pero débense deseñar e codificar aplicacións propias para cada tipo para poderlas utilizar nestes clústers.

Outro tipo de implementación dos sistemas alto rendemento consiste en implementalos a nivel de sistema. Este tipo de clústers basea todo o seu funcionamento en comunicación e colaboración dos nodos a nivel de sistema operativo. Isto implica que xeralmente son clústers de nodos da mesma arquitectura, proporcionando unha vantaxe importante no relativo ao factor de acoplamento. Basean o seu funcionamento na compartición de recursos a calquera nivel, e no balanceo da carga de procesamento de xeito dinámico. Para iso utilizan funcións de planificación especiais que se encargan de xestionar os nodos de procesamento agregados ao clúster.

### **Clústers HA (High Availability): Cluster de Alta Disponibilidade**

Os clústers de alta dispoñibilidade son un tipo de clústers totalmente diferentes aos de alto rendemento, baseándose esta diferenza no obxectivo cara ao que están deseñados. A idea é que este tipo de clústers deben proporcionar unha mellora dos servizos ofrecidos, permitindo manter con garantía os devanditos servizos no tempo malia o incremento de factores que desvirtúen o rendemento ou mesmo malia que exista algunha continxencia. Este feito fai que sexan os clústers máis demandados actualmente polas empresas.

Estes clústers están deseñados para proporcionar a máxima dispoñibilidade sobre os servizos integrados que está proporcionando o clúster, e supoñen unha competencia que abarata os sistemas redundantes, ofrecendo unha serie de servizos durante o maior tempo

posible. Para poder dar estes servizos os clústers deste tipo se implementan en base a dous factores.

- **Alta dispoñibilidade de infraestrutura:** De producirse un fallo de hardware nalgunha das máquinas do clúster, o software de alta dispoñibilidade é capaz de arrancar automaticamente os servizos en calquera das outras máquinas do clúster (failover). E cando a máquina que fallou se recupera, os servizos son novamente migrados á máquina orixinal (failback). Esta capacidade de recuperación automática de servizos garántenos a alta dispoñibilidade dos servizos ofrecidos polo clúster, minimizando así a percepción do fallo por parte dos usuarios.
- **Alta dispoñibilidade de aplicación:** Se producirse un fallo do hardware ou das aplicacións dalgunha das máquinas do clúster, o software de alta dispoñibilidade é capaz de arrancar automaticamente os servizos que fallaron en calquera das outras máquinas do clúster. E cando a máquina que fallou se recupera, os servizos son novamente migrados á máquina orixinal. Esta capacidade de recuperación automática de servizos garántenos a integridade da información, xa que non hai perda de datos, e ademais evita molestias aos usuarios, que non teñen porque notar que se produciu un problema.

Gran parte da problemática asociada está ligada á necesidade de que o servizo proporcionado sexa ininterrompido, proporcionando total dispoñibilidade constante aos clientes ou usuarios do devandito servizo. En contorno de produción real adóitanse producir fallos inesperados nos servidores, e estes fallos provocan a aparición de dous eventos no tempo: o tempo no que o servizo está inactivo e o tempo de reparación do problema. Entre as opcións que solucionan este tipo de continxencias temos:

- Sistemas de información redundante

- Sistemas tolerantes a fallos
- Balanceo de carga entre varios servidores
- Balanceo de conexións entre varios servidores

A adopción deste tipo de sistemas está vinculada con dúas fontes de necesidade de calquera organización. A primeira é o poder dispoñer dun servizo activo e aforrar economicamente todo o que sexa posible. O servizo pode ser de diversa índole, desde un sistema de ficheiros distribuídos de carácter moi barato, ata grandes clústers de balanceo de carga e conexións para os grandes portais de Internet. Calquera funcionalidade requirida nun contorno de rede pode ser colocada nun clúster e implementar mecanismos para facer que esta obteña a maior dispoñibilidade posible.

Baséanse en principios moi simples que poden ser desenvolvidos ata crear sistemas complexos especializados para cada contorno particular. En calquera caso, as técnicas destes sistemas adoitan basearse en excluír do sistema aqueles puntos críticos que poden producir un fallo e por tanto a perda de dispoñibilidade dun servizo. Para isto adóitanse implementar desde enlaces de rede redundantes ata dispoñer de N máquinas para facer una mesma tarefa de maneira que si caen N-1 máquinas o servizo permanece activo sen perda de rendemento.

### **61.3.3      Balanceo de carga**

Aínda que o termo de balanceo de carga pode facer referencia a un tipo de clústering concreto, pode asumirse como unha característica que forma parte dun gran número de implementacións de clústering diferentes. O termo en si fai referencia á capacidade para subdividir o traballo de procesamento de forma equilibrada entre un conxunto de nodos que forman parte dun sistema multiproceso, sendo o termo aplicado a sistemas de clústering ou a outro tipo de sistemas multiproceso.

O balanceo de carga utilízase frecuentemente apoiándose na xestión dinámica do tráfico da rede existente entre distintos servidores. A aplicación máis común do balanceo de carga é evitar que un só servidor se encontre saturado mentres outros similares estean dispoñibles.

Mediante o uso de balanceo de carga, os servidores aparecen como un só para o usuario. Un servidor ou máquina realiza unha monitoración continua de cada servidor para determinar o mellor camiño a onde enrutar as peticións dos clientes de acordo aos recursos dos servidores que xestionan.

Desta forma conséguese que os sistemas sigan funcionando aínda que algún dos servidores non estea operativo. Se os servidores se atopan fisicamente en distintas localizacións o balanceo de carga convértese nunha forma de manter os sistemas funcionando aínda que un dos centros de datos non estea operativo.

O termo habitualmente confúndese co concepto de alta dispoñibilidade, e certamente, sistemas onde primen a alta dispoñibilidade ou o balanceo de carga habitualmente teñen obxectivos similares. Con todo, o concepto de balanceo de carga está ligado á unificación de sistemas separados.

No caso dos clústers de alta dispoñibilidade, poden entenderse como un conxunto de máquinas independentes baixo unha arquitectura distribuída que permite que se un nodo cae, outro en reserva se active para asumir as competencias do nodo que deixou de funcionar. Con todo, o concepto de



balanceo de carga, independentemente de que tamén proporciona redundancia e tolerancia a fallos, céntrase máis no uso compartido dos recursos para alcanzar metas globais.

## **61.4 Alta dispoñibilidade en servidores de aplicacións e servidores de bases de datos.**

### **61.4.1 Alta dispoñibilidade en servidores de aplicacións**

Un servidor de aplicacións defínese como un equipo ou máquina que contén un conxunto de aplicacións software que permiten ofrecer servizos de aplicación a diferentes clientes. Na actualidade o concepto está asociado a servidores de aplicacións baseados en Java, como J2EE (Java 2 Enterprise Edition), Websphere de IBM ou WebLogic de Oracle.

Na súa arquitectura interna, o servidor de aplicacións non é máis que un contedor de aplicacións formadas por compoñentes que interactúan entre si. Estes compoñentes teñen unha gran capacidade de reutilización permitindo a súa combinación para a implementación de novas aplicacións que acheguen diferentes servizos.

No caso dos servidores de aplicacións baseados en J2EE, este tipo de compoñentes están escritos en Java e clasifícanse segundo a funcionalidade que vaian desempeñar na arquitectura da aplicación, distinguíndose entre os Servlets, as Java Server Pages (JSPs) e para rematar os Enterprise Java Beans (EJBs). Estes elementos permiten construír aplicacións en diferentes capas, facilitando as operacións de reutilización, reimplementación, extensibilidade e escalabilidade das aplicacións. O deseño en capas das aplicacións permite separar a interface de usuario de funcións de lóxica de negocio, xestión das sesións do usuario ou o acceso

ás bases de datos do sistema. Ademais, no caso dos servidores de aplicacións baseados en Java, que seguen o estándar J2EE, permítese a creación de clústers de servizos ampliando as características de escalabilidade e proporcionando unha interface para integrar alta dispoñibilidade para o sistema de aplicacións baseado na xestión transparente de conxuntos de servidores.

Un exemplo concreto de servidor de aplicacións é o WebLogic Server, baseado en Java, que proporciona mecanismos para integrar un clúster de servizos, xerando copias replicadas de todos os servizos aos clientes do sistema. No caso de que un servizo caia, automaticamente se notifica e se redireccionan as solicitudes pendentes ás réplicas do servizo que existen no clúster.

Algúns dos requisitos que se deben cumprir para garantir a alta dispoñibilidade son:

- Que en cada instancia do servidor do clúster existan os mesmos compoñentes de aplicación.
- Que o mecanismo de recuperación poida determinar a localización no clúster de todos os obxectos da aplicación.
- Que se coñeza o estado de execución das distintas tarefas de cada un e dos compoñentes. Isto permite que se un compoñente falla, a tarefa poida completala outro servizo partindo do mesmo punto no que se detivo por fallo, e posibilitando que non se dupliquen os datos de carácter persistente.

#### **61.4.2 Alta dispoñibilidade a nivel de bases de datos**

A alta dispoñibilidade a nivel de bases de datos fai referencia á dispoñibilidade dos servizos de acceso ás bases de datos por parte dos clientes, garantindo un grao absoluto de funcionamento continuo dos sistemas xestores de bases de datos.

Existe un amplo repertorio de sistemas que necesitan alta dispoñibilidade de sistemas de xestión de bases de datos. Este tipo de sistemas abarcan desde sistemas de tempo real e sistemas embebidos ata aplicacións web ou outro tipo de sistemas online. Habitualmente estes contornos requiren un compromiso de nivel de servizo mínimo e robustez para facer fronte a posibles continxencias que eviten, non só a perda de datos, senón a suspensión do servizo.

Habitualmente, os sistemas de alta dispoñibilidade en xeral centran os seus esforzos en garantir que o servizo ofrecido se manteña de forma constante pese a que xurdan imprevistos ou fallos que deben controlarse. Con todo, na implementación da alta dispoñibilidade a nivel de bases de datos debe terse en conta un aspecto importante; non só se pretende manter o sistema activo, senón que se pretenden manter os datos actualizados e dispoñibles para todos os clientes. Debe de poder asegurarse a integridade da base de datos.

Os sistemas de alta dispoñibilidade que implementan os servizos de bases de datos deben cumprir as seguintes características:

- Robustez fronte a fallos do servidor e capacidade de recuperación.
- Tempo de caída do sistema ten que ser reducido ou eliminado.
- Niveis de servizo obrigatorios en caso de fallo ou alta densidade de tráfico.

Asociado aos sistemas de alta dispoñibilidade a nivel de base de datos entra en xogo o concepto de Punto de Fallo. Este termo fai referencia a determinados compoñentes do sistema que poden fallar, e cuxo fallo é independente doutros compoñentes. Polo tanto poden considerarse puntos de risco a ter en conta nunha planificación e deseño do sistema de alta dispoñibilidade.

Existen tres principais puntos de conflito ou Puntos de Fallo nunha implementación dun servizo de bases de datos:

- O propio servidor da base de datos, é dicir o motor software ou Sistema Xestor da Base de Datos e a plataforma hardware que o sustenta.
- A base de datos física, é dicir, o dispositivo ou dispositivos físicos que albergan os datos, como discos duros ou memorias.
- Os enlaces e conexións externas que permiten aos usuarios realizar as peticións, entendendo como tales enlaces físicos (rede cableada) e lóxicos (servizos levantados).

Cada compoñente ten o seu propio tipo de fallo e redución de servizo, así como os seus protocolos específicos de actuación para intentar reducir e/ou emendar as continxencias provocadas por eses fallos.

As principais solucións que intentan mitigar as posibles continxencias que se provoquen nos puntos de fallo consisten fundamentalmente en tres:

- Backup Online: Baséase en implementacións do server que permiten protexer os datos fronte a fallos do disco, mantendo rexistro de cambios do log en dispositivos separados.
- Replicación: implica a implementación doutro servidor xemelgo utilizando técnicas de mirroring. Mediante a duplicidade do servizo mediante un segundo punto de acceso, é posible derivar peticións entre servidores no caso de que un falle ou se produza un colo de botella que denegue o servizo a algún deles. O mecanismo de replicación utiliza dúas bases de datos diferentes; a principal (activa) e a secundaria (espello), que corren en máquinas diferentes, cada unha nun servidor, pero ambas contendo representacións idénticas dos mesmos datos.

- Recuperación ante fallos: A recuperación ante fallos consiste basicamente nunha mellora do mecanismo de replicación. Consiste en establecer os mecanismos necesarios para que, en caso de fallo, mediante a réplica situada noutra máquina, o sistema que caeu poida recuperar o punto actual mediante a sincronización automática dos sistemas.

## **61.5 Alta dispoñibilidade en contornos virtualizados.**

A alta dispoñibilidade en contornos virtualizados pode verse desde dúas ópticas distintas; a primeira delas implica alta dispoñibilidade de servidores que conteñen unha virtualización de servizos, ou ben desde o punto de vista de asegurar alta dispoñibilidade de servizos mediante a virtualización de servidores.

No primeiro dos casos, as medidas referentes á disposición de alta dispoñibilidade pasan pola implementación de solucións baseadas en redundancia de hardware, ou implementación de sistemas que garantan alto rendemento a nivel de sistema operativo.

En canto a asegurar alta dispoñibilidade mediante servizos de virtualización, é un campo complexo que tende a ser a idea xeral de implantación nos grandes centros de cómputo e proceso de datos, dadas as grandes vantaxes que presenta.

Mediante a virtualización pódense manexar todos os compoñentes que forman parte de cada un dos servidores ou nodos que van compoñer o centro de procesamento, permitindo interoperabilidade entre os compoñentes dos mesmos, e administrando e xestionando a memoria e recursos como CPU e discos. As dúas tendencias fundamentais que se seguen son a virtualización de hardware ou a virtualización de Sistema Operativo.

### **61.5.1 Virtualización de hardware**

Mediante a virtualización de hardware (Ilustración 4) emúlase o hardware orixinal do servidor en cada unha das máquinas virtuais. Unha vez emulada a máquina anfitrión, cada unha destas instancias virtualizadas converterase nun servidor privado que pode albergar diferentes sistemas operativos e diferentes servizos. O xestor de virtualización permitirá configurar políticas de recuperación fronte a fallos, permitindo levantar instancias e/ou recuperar instancias de máquinas que alberguen servizos e

que se detiveran en caso dalgunha continxencia.

### **61.5.2 Virtualización de sistema operativo**

Pola contra, na virtualización dos SO (Ilustración 5), establécese unha configuración base do sistema operativo sobre o hardware nativo da máquina, establecendo instancias dese sistema e virtualizado mediante a xeración de instancias idénticas ao hardware e sistema operativos orixinais da máquina. En última instancia, todos os recursos son procesados e controlados polo sistema operativo nativo, dado que non existe virtualización de hardware. Isto reduce a complexidade de configuración de diferentes dispositivos en diferentes sistemas operativos, pero ten como consecuencia que en caso de fallo dun dispositivo por mala configuración, veranse afectadas todas as instancias virtuais que corran sobre ese servidor físico.

## **61.6 Centros de Protección Xeográficos**

Cando é un requisito indispensable o feito de manter unha alta dispoñibilidade de determinados servizos de 24 horas ao día durante os 7 días da semana (24x7), é imprescindible facer uso de elementos que proporcionen respaldo da información ou dos recursos a distintos niveis: alta dispoñibilidade de servizos, redundancia de sistemas, replicación de datos e centro de respaldo.

Entón, para poder garantir que un servizo ou recurso vai ter unha dispoñibilidade de 24x7, será necesario empregar sistemas redundantes e estes deben de atoparse en localizacións físicas situadas a unha considerable distancia para ofrecer deste xeito resposta a certas situacións de continxencia de carácter moi grave producidas por un desastre a nivel

físico, como pode ser un incendio, un terremoto ou simplemente un fallo total nos sistemas de enerxía.

Á súa vez, a dispoñibilidade e integridade dos datos asociados aos servizos son vitais para poder garantir que os servizos teñan unha dispoñibilidade 24x7. Entón para garantir unha dispoñibilidade 24x7:

- Os datos teñen que estar replicados dun xeito eficiente entre os diferentes centros xeográficos, garantindo que no caso de que se produza calquera tipo de incidencia ou catástrofe se dispoña dunha copia exacta, fiable e actualizada dos mesmos. Esta réplica, á súa vez, ten que estar dispoñible para ser utilizada e poder facer uso dela nos servizos en produción.
- Os traballos para a recuperación dos servizos hanse de automatizar, diminuindo así os posibles tempos de indispoñibilidade. Para iso lévanse a cabo operacións nos servidores para a detección de fallos, para deter algún servizo e para levantar outros. Ademais, cómpre establecer unha coordinación entre os sistemas de almacenamento dos datos co fin de garantir tanto a dispoñibilidade do servizo como o feito de que a información se estea replicando dun xeito adecuado. Esta tarefa realízase co fin de ofrecer unha copia exacta da información nun estado óptimo para ser utilizada de forma automática unha vez ocorrido un desastre.

Seguindo estes puntos, un servizo que se atope en réxime de dispoñibilidade 24x7 no cal se ofrecen diversos centros xeográficos para a protección dos servizos e da información, hase de contemplar a alta dispoñibilidade dun xeito integrado. Esta alta dispoñibilidade ten que xestionar en bloque aquelas operacións que teñan relación tanto cos servizos, como cos sistemas ou co almacenamento dos datos.



Un exemplo onde o Centro de Datos 1 presta o servizo XYZ e ten asociados un conxunto de servidores e de dispositivos de almacenamento que se replican contra os dispositivos de almacenamento situados no Centro de Datos 2. No Centro de Datos 2, existen servidores que se atopan en disposición de proporcionar os mesmos servizos que no Centro de Datos 1, no caso de que neste se produza algún tipo de fallo ou desastre.

De producirse algún tipo de continxencia, todas as operacións que se levan a cabo no Centro de Datos 1 de servizos, de aplicacións, de servidores e de replicación de datos teñen que estar coordinadas e automatizadas para que se produza un cambio na execución dos servizos, é dicir, que o Centro de Datos 2 tome o mando dos servizos e comece a servir no menor tempo posible como se mostra na seguinte ilustración. Cando se produce este cambio e os servizos comezan a ser prestados desde o Centro de Datos 2, tamén se ten que producir un investimento no sentido da replicación dos datos.

## 61.7 Plans de Continxencia

Un plan de continxencia é unha ferramenta para empregar na xestión das Tecnoloxías da Información e as Comunicacións e aporta unha serie de regras ou medidas que proporciona unha garantía de continuidade do negocio e dos procesos dunha organización. Estas medidas poden ser:

- **Técnicas:** Extintores contra incendios, detectores de fume, saídas de urxencia, equipos informáticos de respaldo.
- **Humanas:** Formación de actuación ante un incendio, designación de responsables das salas, asignación de roles e responsabilidades para a copia de respaldo.
- **Organizativas:** Seguro de incendio, precontrato de aluguer de equipos informáticos e localización alternativa, procedemento de copia de respaldo, procedemento de actuación ante un incendio, contratación de servizos de auditorías de riscos laborais.

Podería definirse como unha planificación das accións a tomar cando se produza un evento ou condición que non estea recollido dentro do proceso de planificación formal. Trátase dunha serie de procedementos para o restablecemento dos procesos de negocio en caso de producirse un desastre.

Todo plan de continxencia ten que comprender tres subplans, que determinasen o conxunto de procedementos ou contramedidas que se aplicasen en cada momento en función da aparición dunha ameaza. Estes subplans son:

- **Plan de respaldo:** contramedidas antes da aparición dunha ameaza para evitar que se produza.

- **Plan de urxencia:** nel reflíctense os procedementos a seguir no momento que se produce unha ameaza ou xustamente despois para paliar os efectos que poida provocar a ameaza.
- **Plan de recuperación** tras un desastre: reflicte as contramedidas que se aplican unha vez a ameaza é controlada co fin de restablecer os danos ocasionados polo desastre, definindo desastre como toda interrupción do acceso á información ou do seu procesado, necesaria para o normal funcionamento de todos os procesos de negocio.

Un plan de continxencia divídese en tres partes segundo as tarefas que se leven a cabo:

- **Prevención:** Conxunto de accións que se teñen que realizar como prevención ante calquera posible problema que provoque a continuidade dos procesos de negocio de forma parcial ou total. Con iso minimizaranse os danos en caso de producirse o problema, proporcionando unha mellor resposta que restableza os servizos nun menor tempo.
- **Detección:** Grupo de accións encargadas de conter o impacto no momento da aparición dun problema intentando limitalos tanto como sexa posible.
- **Recuperación:** Accións que van desde o mantemento de partes críticas mentres se está producindo a perda dos servizos e os recursos, ata a súa recuperación ou restauración.

#### 61.7.1 **Ciclo de Vida**

Todo plan de continxencia ten que seguir un ciclo de vida iterativo, en continua evolución, PDCA (Plan-Do-Check-Act, Planificar-Facer-Comprobar-Actuar). Este ciclo de vida proporciona a identificación das ameazas que

poden provocar unha ruptura na continuidade dos procesos de negocio dunha organización.

Unha vez identificadas as ameazas establécense unha serie de medidas ou procedementos para afrontalas. O plan de continxencia recolle estas medidas ademais de indicar os recursos necesarios para poder executalas.

Ao longo do ciclo de vida dun plan de continxencia, este sofre numerosas revisións, que resultan dunha nova análise das posibles ameazas que se poden chegar a producir.

Cando se suscita unha ameaza, o plan de continxencia vese tamén afectado, provocando sobre o mesmo unha serie de actuacións:

- *Ameaza establecida e accións eficaces:* realízanse os cambios menores que se consideren para mellorar a eficacia do plan de continxencia ante o mesmo tipo de situacións.
- *Ameaza establecida e accións ineficaces:* vólvese a realizar unha análise das causas do erro e propóñense novas medidas a tomar.
- *Ameaza non prevista:* levásese a cabo unha nova análise de riscos, aínda que as medidas adoptadas contra unha ameaza non detectada fosen eficaces.

#### **61.7.2 Características**

O plan de continxencia ten que contemplar dous aspectos:

- Operacional: cada usuario debe coñecer que función desempeña unha vez detectado o problema e saber a quen avisar no caso de que este se produza. No plan de continxencia tamén hai que especificar os encargados da toma de decisións durante o proceso de recuperación e establecer a dispoñibilidade e o adestramento do persoal experimentado.

- Administrativo: no aspecto administrativo contémpase
  - o A definición dos riscos e as porcentaxes de aparición dos mesmos
  - o Os procedementos de recuperación da información
  - o Os responsables dos medios de respaldo
  - o A localización dos medios de respaldo e do software de reempazo.
  - o A especificación de alternativas de respaldo
  - o A información, bases de datos, servizos, etc. prioritarios que deben de ser restablecidos primeiro.

#### 61.7.3 **Obxectivo**

O obxectivo prioritario dun plan de continxencia é garantir que unha organización e os seus procesos e negocio ou actividades operacionais sigan en funcionamento malia producirse unha situación de desastre. Para poder conseguir isto, o plan de continxencia habilita á organización para poder responder e superar problemas críticos ou mesmo catastróficos, de tal xeito que permite unha pronta recuperación da situación normal de traballo.

#### 61.7.4 **Puntos Clave**

Os puntos clave dun plan de continxencia poden enfocarse cara a algunhas das seguintes áreas:

- **Facilidade de Destrución.** O equipo encargado de realizar a planificación ten que ter en conta que se pode producir unha total destrución dos sistemas organizacionais ou un colapso total dos servizos da mesma. O plan de continxencia tamén debe de contemplar revisións para realizar no caso de que se produza unha destrución parcial.

- **Disponibilidade do persoal.** Hase determinar no plan de continxencia un organigrama para unha situación de desastre, o cal deberá estar formado por persoal de toda a organización, identificando as posicións clave para a execución do plan.
- **Determinar os tempos do desastre.** Débense tomar as consideracións oportunas para cada un dos diversos momentos en que pode producirse un desastre, tratando de identificar os momentos nos que se poida producir un maior impacto para a organización. Este factor depende do tipo de organización, posto que unha organización pode desenvolver o 70 % da súa produción ou da súa actividade nas primeiras horas dun día, mentres que outras a súa maior actividade prodúcese de madrugada. Tamén se poden considerar períodos de tempo, maior impacto a principio de mes que a finais, etc.
- **Instalacións fóra do centro operacional.** Pódese ter en conta desastres que afecten por completo a partes do sistema presentes no centro de operacións. O feito de ter unha instalación externa, como un centro de almacenamento ou unha réplica do sistema, garante unha considerable redución do impacto que pode ocasionar unha continxencia ou un desastre.

Un plan de continxencia ten que ser dinámico e estar en continua evolución, véndose modificado cada vez que se produza, cambio de equipo de instalación cambio dalgún sistema, variacións nos contratos de mantemento, cambios de persoal, etc.

#### 61.7.5 Elementos

Nun plan de continxencia pódense identificar tres tipos de elemento ou tipos de accións que se poden identificar:

- ***Accións de Urgencia.*** Tratan de liquidar o dano no momento de ocorrer a incidencia, así como evitar o maior impacto posible.
- ***Accións de Recuperación.*** Realizan tarefas de mantemento durante a perda do servizo e recursos, e tarefas de recuperación.
- ***Accións de Respaldo.*** Lévanse a cabo unha vez que se presenta unha continxencia que afecte á continuidade operativa da organización co fin de reducir o seu impacto, posibilitando o restablecemento dos servizos interrompidos no menor tempo posible.

## 61.8 Bibliografía

- Alta disponibilidad de los servicios en la SGTIC do MEH. Emilio Raya López e Marcos Chama 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