Sistemas de Información nas Administracións Públicas

Responsable: Alvaro M. Gómez Vieites

1. EL RETO DE COMPETIR EN LA NUEVA ECONOMÍA

La Nueva Economía, la Sociedad de la Información, la Era Digital, la Tercera Ola, la Economía en Red… son términos que constantemente aparecen en los medios de comunicación. La sociedad se está transformando a una velocidad vertiginosa, y los cambios en las relaciones económicas se traducen en nuevos modelos de negocio y en nuevas formas de competir. Las Tecnologías de la Información y las Comunicaciones se han convertido en herramientas básicas para las organizaciones de la Nueva Economía.

En esta nueva etapa dominada por Internet, la red de redes, los mercados adquieren una dimensión global, y las organizaciones deben trabajar en tiempo real, superando las barreras geográficas y temporales. Se ha intensificado la competencia en todos los sectores productivos, y están apareciendo empresas virtuales que lanzan productos y servicios innovadores que ponen en peligro los modelos de negocio tradicionales.

En la Economía Digital la innovación permanente se convierte en la única fuente de ventaja competitiva. El entorno se ha vuelto mucho más exigente, incierto y cambiante, por lo que las organizaciones deben desarrollar su capacidad para aprender y adaptarse a los nuevos modelos de negocio. Las organizaciones ágiles y flexibles son las que triunfan en este escenario: en la era de Internet, "*el pez grande ya no se come al pez chico; es el pez rápido el que se come al pez lento*".

La penetración de Internet a todos los niveles está provocando importantes cambios en la estructura de la mayoría de los sectores económicos: se alteran las relaciones entre los distintos participantes (empresas, proveedores, distribuidores, clientes…), los productos y servicios se vuelven más inteligentes al incorporar cada vez más información, surgen nuevos modelos de negocio que ponen en peligro los tradicionales en el sector, etc. Las empresas deben conocer y evaluar el impacto de estos cambios en su sector, y definir una estrategia de implantación gradual de Internet en sus procesos y en los servicios que ofrecen a sus clientes.

Por todos estos motivos, hoy más que nunca las empresas necesitan contar con profesionales cualificados, con los conocimientos, actitudes y habilidades necesarios para poder competir en este nuevo entorno que caracteriza la Economía Digital. Además, los continuos avances tecnológicos y la rapidez a la que se están produciendo los cambios en el entorno, obligan a un proceso de formación continua, de permanente actualización de sus conocimientos.

2. OBJETIVOS DE LA MATERIA

Para dar respuesta a algunos de los nuevos retos planteados por la Economía Digital, se propone el estudio de la materia de ***Sistemas de Información y Seguridad Informática***, cuyos objetivos se concretan en los siguientes puntos:

- Analizar las características que definen la Economía Digital y la Sociedad del Conocimiento, y justificar la importancia adquirida por la información y el conocimiento en esta nueva economía.

- Reflexionar sobre la posibilidad de incorporar las Tecnologías de la Información y la Comunicación (TICs) para mejorar los procesos.

- Analizar el papel de los Sistemas de Información y la complejidad asociada a la implantación de un Sistema de Información como soporte a los procesos de la organización.

- Analizar la problemática de la Seguridad de la Información.

- Conocer los principios básicos del marco legal de la protección de datos de carácter personal en España: LOPD

- Analizar las consecuencias que el incumplimiento de la LOPD podrían tener para una organización, prestando especial atención a los problemas más habituales: utilización de los datos de los empleados y de los clientes, adquisición de nuevas bases de datos, cesiones de datos a terceros, subcontratación de determinados trabajos (nóminas, selección de personal, mailings a clientes), etc.

3. DURACIÓN Y METODOLOGÍA

3.1. Duración

La materia se desarrolla en una única sesión de **6 horas**.

3.2. Metodología

La metodología docente de cada sesión se basará en exposiciones descriptivas por parte del profesor, con el análisis on-line de ejemplos y pequeños casos prácticos mediante una conexión permanente a Internet. Asimismo, se propondrá la discusión en grupos de trabajo de casos prácticos de mayor complejidad y duración, para fomentar el debate y la reflexión sobre los conceptos y cuestiones más importantes de cada sesión.

4. ESTRUCTURA DE LA MATERIA

1. La Sociedad de la Información

1.1. Características de la Sociedad de la Información
1.2. El papel de la información como recurso a explotar y gestionar
1.3. Creación de empresas en la Sociedad de la Información

2. El papel de las TIC's como motor del cambio

2.1. Desarrollo de las TICs e Internet en los últimos años
2.2. Resistencia a la implantación de las TICs
2.3. Aspectos organizativos y la clave del factor humano

3. Sistemas de Información

3.1. Revisión del papel de los Sistemas de Información
3.2. Gestión del proyecto de implantación de un Sistema de Información

4. Seguridad Informática

4.1. La importancia de la Seguridad Informática
4.2. Sistema de Gestión de la Seguridad de la Información

5. Protección de Datos de Carácter Personal

5.1. Principales características de la LOPD
5.2. Titular del fichero y encargado del tratamiento.
5.3. Inscripción de los ficheros con datos de carácter personal
5.4. Principios básicos de Protección de Datos: calidad de los datos, información a los afectados, cesiones y tratamientos encargados a terceros, solicitud del consentimiento, seguridad de los datos, etc.
5.5. Discusión de distintos ejemplos reales sobre las consecuencias del incumplimiento de estos principios básicos.
5.6. Derechos de los afectados: derechos de acceso, rectificación, cancelación u oposición.
5.7. Análisis de las medidas de seguridad a implantar en los ficheros
5.8. Infracciones y sanciones previstas por la LOPD.

5. DOCUMENTACIÓN ENTREGADA

- Diapositivas
- Casos
    1. Impacto de Internet en los servicios de información
    2. Ayuntamiento de Barataria (adaptación a la LOPD)
    3. Mueblibaño (sanciones incumplimiento LOPD)
- Artículos:
    1. La importancia de garantizar la protección de datos personales y la privacidad.
    2. Sistemas de Información
    3. Implantación de ERPs
- Material práctico:
    1. Modelo de contrato de tratamiento de datos de carácter personal.
    2. Ejemplos de sanciones de la Agencia de Protección de Datos.
    3. Cuadro resumen de las medidas de seguridad.

6. PROFESOR

Álvaro Gómez Vieites

(agomez@simce.com)

Ingeniero de Telecomunicación por la Universidad de Vigo. Especialidades de Telemática y de Comunicaciones. Número uno de su promoción (1996) y Premio Extraordinario Fin de Carrera.

Ingeniero Técnico en Informática de Gestión por la UNED (2004-2006). Premio al mejor expediente académico del curso 2004-2005 en la Escuela Técnica Superior de Ingeniería Informática de la UNED.

Actualmente completando las carreras de Licenciatura en Dirección y Administración de Empresas y de Licenciatura en Economía por la UNED (2006-2010).

Diploma de Estudios Avanzados (Curso de Doctorado) por la Universidad Politécnica de Madrid. Presentada la tesis doctoral sobre "*Estudio de los factores que inciden en el desarrollo de las actividades de I+D+I y de su impacto en los resultados empresariales*" en el Departamento de Análisis Económico I de la UNED.

"*Executive MBA*" y "*Diploma in Business Administration*" por la Escuela de Negocios Caixanova.

Ha sido Director de Sistemas de Información y Control de Gestión en la Escuela de Negocios Caixanova. Profesor colaborador de esta entidad desde 1996. Director del Master en Dirección de Empresas del Sector TIC desde 2000.

Socio-director de SIMCe y socio-consultor de EOSA. Consultor de empresas, con una amplia experiencia en la realización de proyectos y estudios relacionados con la gestión de la innovación y el impacto de las Tecnologías de la Información y la Comunicación en la gestión empresarial.

Libros y artículos publicados:

1. Libros:

1. "***Marketing na Internet e nos Meios Digitais Interactivos***" (marzo 2008), editado en Portugal por Vida Económica en colaboración con la Escuela de Negocios Caixanova (ISBN 978-972-788-244-1).

2. "***La Seguridad Informática y la Protección de los Datos de Carácter Personal en las Entidades Locales***" (diciembre 2006), editado por la Diputación de Ourense (ISBN 84-96503-35-6).

3. "***Enciclopedia de la Seguridad Informática***" (octubre 2006), editado por Ra-Ma en España (ISBN 84-7897-731-7) y por Alfaomega en Latinoamérica (ISBN 978-970-15-1266-1).

4. "***Marketing Relacional, Directo e Interactivo***" (abril 2006), editado por Ra-Ma en España (ISBN 84-7897-712-0). Libro prologado por Joost van Nispen.

5. "***Sistemas de Información. Herramientas prácticas para la gestión empresarial***" (febrero 2003), editado por Ra-Ma en España (ISBN 84-7897-553-5) y por Alfaomega en Latinoamérica (ISBN 970-15-0949-8). Segunda edición publicada en 2006 (ISBN: 84-7897-6949).

6. "***Redes de ordenadores e Internet. Funcionamiento, servicios ofrecidos y alternativas de conexión***" (enero 2003), editado por Ra-Ma en España (ISBN 84-7897-545-4) y por Alfaomega en Latinoamérica (ISBN 970-15-0900-5).

7. "***Las Claves de la Economía Digital***" (noviembre 2002), editado por Ra-Ma en España (ISBN 84-7897-537-3) y por Alfaomega en Latinoamérica (ISBN 970-15-0875-0).

8. "***Sistemas de Telecomunicación e Internet. Guía Práctica para los profesionales del nuevo milenio***" (junio 2002), editado por Tórculo en colaboración con SIMCe Consultores y la Fundación R (ISBN 84-8408-213-X).

9. "***Marketing en Internet y en los Medios Digitales Interactivos***" (abril 2002), editado por Tórculo en colaboración con la Escuela de Negocios Caixanova y Comunitel (ISBN 84-8408-203-2).

10. "***Comercio Electrónico y Economía Digital***" (abril 2002), editado por Tórculo en colaboración con la Escuela de Negocios Caixanova y Comunitel (ISBN 84-8408-204-0).

11. Participación con otros autores en la preparación del libro "***Las tecnologías de la información y la comunicación en las empresas gallegas***", Consellería de Industria, Xunta de Galicia, 2002 (ISBN 84-8408-209-1).

12. Participación con otros autores en la preparación de las guías prácticas "***Oportunidades de las TIC para la mejora de la empresa***", Consellería de Industria, Xunta de Galicia, 2002 (ISBN 84-8408-209-1).

2. Artículos:

1. "***La transición hacia los mercados hipercompetitivos y digitales***", revista *e-Deusto*, ISSN 1579-5934, nº3, noviembre de 2006, págs. 62-66.

2. "***Amazon vs Barnes & Noble***", revista *Harvard Deusto Márketing & Ventas*, ISSN: 1133-7672, nº75, julio/agosto de 2006, págs. 62-71.

3. "***Hacia un nuevo concepto de Marketing***", revista *Harvard Deusto Márketing & Ventas*, ISSN: 1133-7672, nº73, marzo/abril de 2006, págs. 36-44.

4. "***Seguridad informática: funciones y responsabilidades de los empleados y directivos***", revista *Capital Humano*, ISSN 1130-8117, nº 185, febrero de 2005, págs. 68-80.

5. "***Seguridad informática y protección de datos de carácter personal***", revista Dyna (Federación de Asociaciones de Ingenieros Industriales), ISSN 0012-7361, Vol. 80, Nº 8, 2005 , págs. 57-59.

6. "***El Impacto de Internet en el Marketing-Mix***", revista *Harvard Deusto Márketing & Ventas,* ISSN: 1133-7672, nº 51, julio/agosto de 2002, págs. 32-39.

7. "***Claves para conocer al cliente de la nueva economía***", revista *Harvard Deusto Márketing & Ventas*, ISSN: 1133-7672, nº 50, mayo/junio de 2002, págs. 24-29.

8. Varias decenas de artículos sobre Internet y Nueva Economía publicados en las revistas Indice, Club Financiero de Vigo o ECO, así como en varios portales de Internet como "documentalistas.org".

3. Ponencias:

1. Ponencia titulada "***La lucha contra el ciberterrorismo y los ataques informáticos***", presentada en la X Reunión Española sobre Criptología y Seguridad de la Información, en Salamanca del 2 al 5 de septiembre de 2008.

2. Ponencia titulada "***Las posibilidades ofrecidas por el Webmining***", presentada en el XI Congreso de Mundo Internet, en Málaga del 14 al 16 de mayo de 2007.

3. Ponencia titulada "***La importancia de explotar la información de los clientes y el modelo del lifetime value***", presentada en el XI Congreso de Mundo Internet, en Málaga del 14 al 16 de mayo de 2007.

4. Ponencia titulada "***Medios de pago en Internet***", presentada en el XI Congreso de Mundo Internet, en Málaga del 14 al 16 de mayo de 2007.

5. Ponencia titulada "***La importancia del factor humano y organizativo en los Sistemas de Información***", presentada en el II Simposium Internacional de Radiografía Digital, en Valencia el 18 de octubre de 2006.

6. Ponencia titulada "***Seguridad informática: funciones y responsabilidades de los empleados y directivos***", presentada en el X Congreso de Mundo Internet, en Madrid del 13 al 15 de abril de 2005.

TICs, Sistemas de Información y Protección de Datos

PARTE I
La Sociedad de la Información

La Sociedad de la Información

Sociedad de la Información: "*Estadio de desarrollo social caracterizado por la capacidad de sus miembros (ciudadanos, empresas y Administración Pública) para obtener y compartir cualquier información, instantáneamente, desde cualquier lugar y en la forma que se prefiera*".

(Informe 2002 de Telefónica sobre la Sociedad de la Información)

La Sociedad de la Información

- "*Nueva Economía*", "*Economía Digital*", "*Economía en Red*", "*Sociedad de la Información*", "*Tercera Ola*"…
- ¿Elemento desencadenante de esta nueva situación?

Uso intensivo de las Tecnologías de la Información y las Comunicaciones (TICs), a todos los niveles

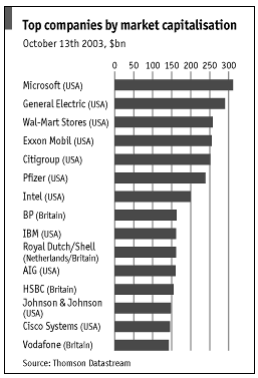
Convergencia de la Informática y de las Comunicaciones

La Sociedad de la Información

- Cambios drásticos y nuevos paradigmas:
  - ➪ De un flujo de actividades intermitente a un flujo continuo y globalizado
  - ➪ Eliminación barreras
    - ✎ Geográficas
    - ✎ Temporales
  - ➪ Autoservicio
    - ✎ El cliente trabaja para la empresa
  - ➪ Teletrabajo
  - ➪ Deslocalización

Empresas en la Sociedad de la Información

¿Apostaría por Bill Gates y su equipo en 1978?



Microsoft 25 años después

- La mayor empresa de software del planeta
- Tiene una plantilla de 55.000 empleados
- Presente en más de veinte países
- Fundada por Gates y Paul Allen, en Albuquerque (Nuevo México), en 1975
- Su producto estrella es Windows, presente en 9 de cada 10 ordenadores

Empresas en la Sociedad de la Información

- ¡¡Que no te "***amazoneen***"!!
  - ➪ Si no arriesgas, no ganas…¡el mayor riesgo es no arriesgar!
    - ✎ Ni *Barnes & Noble* ni *Borders* desarrollaron la tienda de venta on-line de libros más famosa: fue **Amazon**
    - ✎ Ni la *CNN*, ni *Newsweek* ni el *New York Times* crearon los Websites de información más acreditados: fue **Yahoo!** Google
    - ✎ Ni *IBM* ni *Compaq* ni HP desarrollaron el modelo de venta directa de PCs a través de Internet: fue **Dell**
    - ✎ Ni *Sotheby's* ni *Christie's* impulsaron el Website de subastas más concurrido: fue **eBay**
    - ✎ Ni *ATT* ni *MCI* pusieron en marcha el servicio de acceso a Internet más popular: fue **America Online**

"El que no aplica nuevos remedios debe esperar nuevos males, porque el tiempo es el máximo innovador" (Francis Bacon)

Internet y las Nuevas Tecnologías están abriendo un nuevo mundo de oportunidades y posibilidades de negocio

PARTE II
El papel de las TICs e Internet como motor del cambio

El papel de las TICs

- Ley de Moore: continuo avance en las prestaciones de los microprocesadores

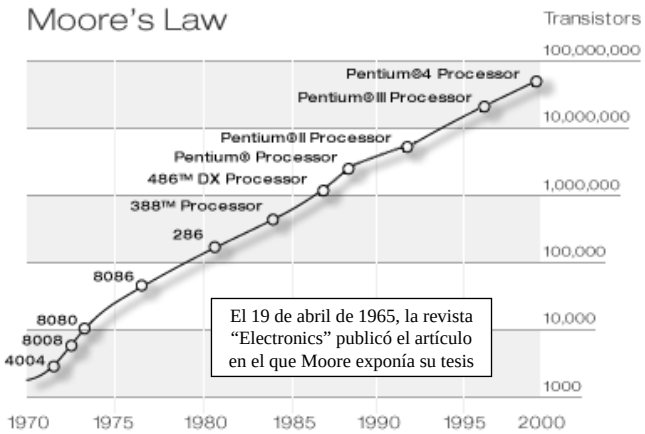
SMALL IS BEAUTIFUL

Chip makers continue the march toward miniaturization.

	2003	2005	2007
Smallest standard transistor feature, in nanometers*	90	65	45
Length of structure activating switching, in nanometers	50	35	25
Transistor size, in square micrometers	1.0	.57	.30
Transistors per consumer microprocessor, in millions	180	500	1,000

* By industry convention, each chip-technology generation is known by a standard measurement corresponding to half the distance between cells in a dynamic-random-access memory chip ("DRAM half pitch").

TechReview, 2004



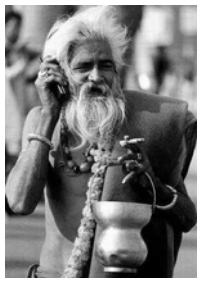
El camino hacia un mundo digital

- Digitalización de productos - Ventajas

Internet: un mundo de posibilidades

Marshall McLuhan
(sociólogo canadiense)

"La nueva interdependencia electrónica recrea el mundo a imagen de una ***Aldea Global***"



Anytime, Anywhere

"En estos momentos, cualquiera y nadie a la vez son el centro" (Galileo)

Internet: un mundo de posibilidades

Internet es un

medio de información

(prensa, radio, televisión…
personalizada, interactiva y multimedia)

Internet: un mundo de posibilidades

Internet es un

medio de comunicación

(e-mail, chat, telefonía IP, fax IP, videoconferencia, mensajería…)

Internet: un mundo de posibilidades

Internet es un

<u>medio de transacción</u>

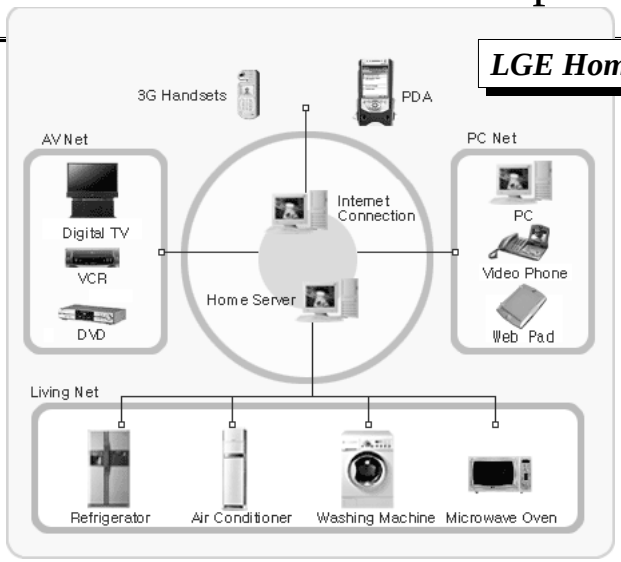
(comercio electrónico, distribución productos digitales, trámites con la Administración)

Internet: un mundo de posibilidades

- Universalización de Internet:
  - ➪ Acceso mediante todo tipo de dispositivos:
    - ✎ TV Interactiva (Internet-Box-TV)
      - – Conexión a Internet desde el equipo de TV
      - – Navegación utilizando un mando a distancia y un teclado específico
    - ✎ Teléfonos móviles (WAP, 3G)
    - ✎ PDAs y TabletPCs
    - ✎ Electrodomésticos: neveras, lavadoras, hornos, marcos…
    - ✎ Coches
    - ✎ Aviones y barcos

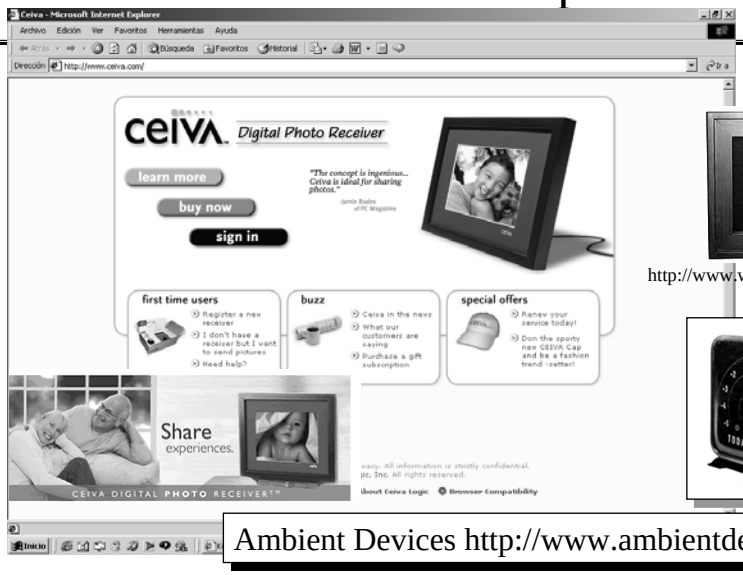
  - ➪ Proliferación de los cibercafés y de las cabinas especializadas en hoteles, aeropuertos, centros comerciales…

Internet: un mundo de posibilidades



LGE Home Network

Internet: un mundo de posibilidades

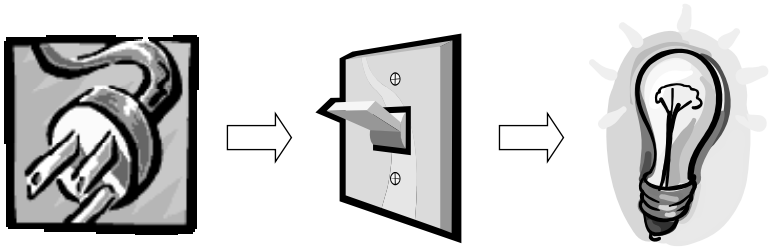


http://www.wallflower-systems.com/

Ambient Devices http://www.ambientdevices.com/

Internet: un mundo de posibilidades

- Universalización de Internet:
  - ➪ Hacia la "invisibilidad" de la tecnología que soporta la Red



Alan Kay: "la tecnología es tecnología sólo para quien ha nacido antes que ella"

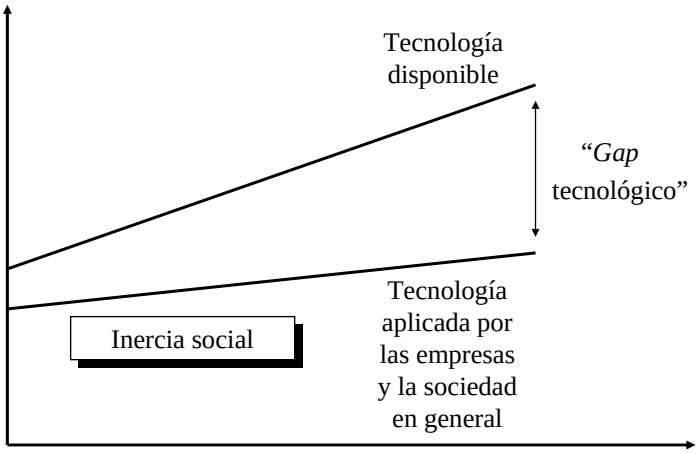
Internet: un mundo de posibilidades

- Hacia la universalización del uso de Internet
  - **Internet se ha convertido ya en el medio mas consumido en España, con 12,1 horas a la semana por internauta**, algo más de un punto por encima de la televisión cuyo consumo es de 11,7 horas por semana, un 11% menos que en el 2004.
  - Esta es una de las conclusiones del estudio europeo «Mediascope», realizado por la Asociación Europea de Publicidad Interactiva (EIAA), que ha realizado 9.000 entrevistas en 10 países europeos, 1.000 de ellas en España, realizadas entre el 1 y el 21 de septiembre de 2008. El consumo de radio es de 10,9 horas por semana, un 22% menos que en 2004, mientras que el de periódicos es de 4,4 horas por semana y el de revistas 3,6 horas.

La Voz de Galicia, 12/12/2008

El papel de las TICs

- Ley de "Demi-Moore": asimilación de la tecnología



El papel de las TICs

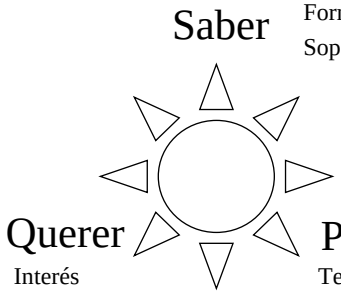
- Algunas frases célebres sobre las nuevas tecnologías:
  - "Este teléfono tiene muchas limitaciones para ser seriamente considerado como un medio de comunicación, el aparato no presenta ningún valor inherente para nosotros", memorándum interno de la Western Union (1876)
  - "Siendo más pesadas que el aire, las máquinas voladoras son imposibles", Lord Kelvin, presidente de la Royal Society (1895)
  - "Todo lo que se podía inventar ya ha sido inventado", Charles Duell, Director de la Oficina de Patentes de EEUU (1899)
  - "En el mundo sólo habrá mercado para cinco computadoras", Thomas Watson, director de IBM (1943)
  - "No existe razón para que alguien tenga un ordenador en su casa", Ken Olse, director de Digital Equipment Corporation (1977)

El papel de las TICs

- Algunas frases célebres sobre las nuevas tecnologías:
  - "Los aviones no tienen ningún valor militar", Mariscal Ferdinand Foch, 1912
  - "La caja musical sin cables no tiene ningún tipo de valor comercial. ¿Quién iba a pagar por un mensaje que no está siendo mandado a nadie en particular", David Sarnoff's Associates en respuesta a la propuesta de invertir en la radio, durante los años 20
  - "¿Quién demonios va a querer oír hablar a los actores", H. M. Warner, Warner Brothers, 1927
  - "La TV será un fracaso: la familia media americana no tiene tiempo para verla", New York Times, 1939
  - "640 Kb de memoria deberían ser suficientes para cualquiera", Bill Gates, 1981

Las tecnologías importan, pero no debemos olvidar las necesidades de las personas

Aspectos organizativos y el factor humano



Una persona hace lo que sabe hacer, lo que está motivada a hacer y lo que su entorno le permite hacer

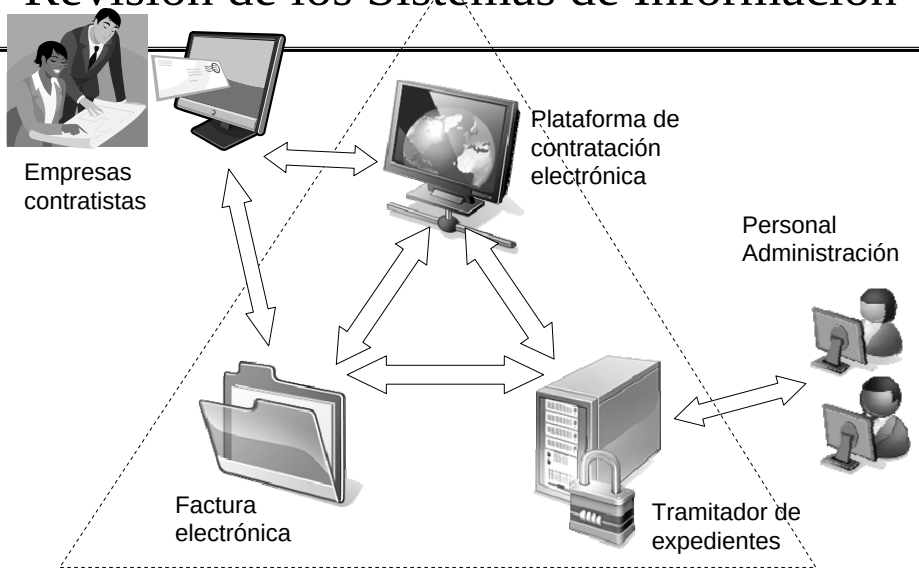
La introducción de nuevas herramientas tecnológicas produce cambios en el entorno de trabajo de una persona, afectando al equilibrio de estos tres factores (saber, querer y poder)

Según un estudio realizado en el Reino Unido, entre un 80 % y un 90 % de los proyectos de implantación de Sistemas de Información en los años noventa no consiguieron alcanzar los niveles de rendimiento esperados, entre otras razones porque no se presentaba suficiente atención a los factores humanos y organizativos

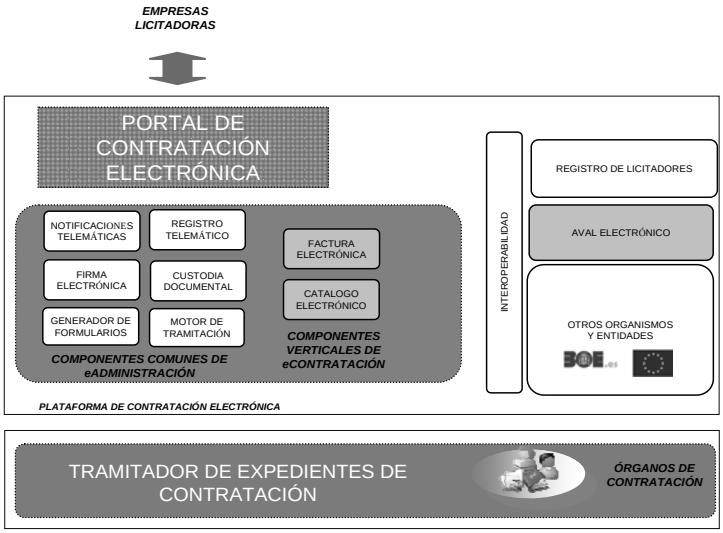
The Performance of Information Technology and the Role of Human and Organizational Factors, British Department of Trade and Industry

PARTE III
Implantación de Sistemas de Información

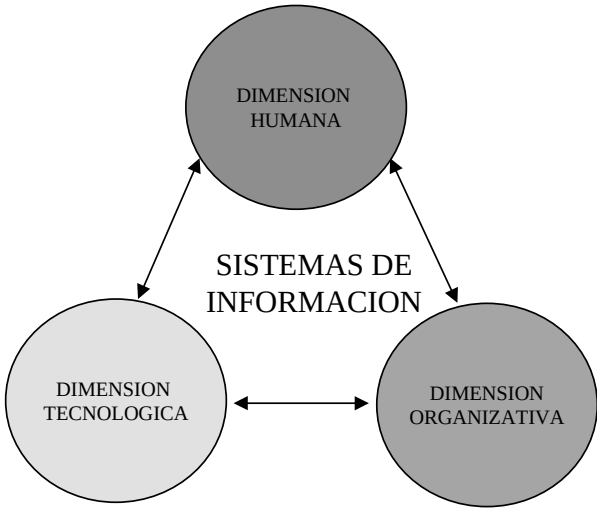
Revisión de los Sistemas de Información



Revisión de los Sistemas de Información

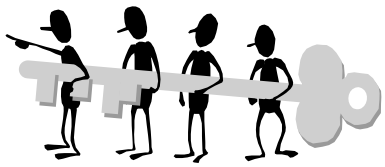


Revisión de los Sistemas de Información



Implantación de Sistemas de Información

- Factores Críticos para la Implantación (I)
  - Planificación realista, teniendo en cuenta las restricciones técnicas, económicas y organizativas
  - Utilización de herramientas de planificación y gestión de proyectos (con soporte de técnicas como Gantt o PERT)
  - Compromiso de la dirección con el proyecto
  - Definición precisa de los objetivos

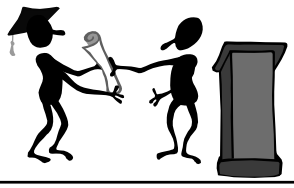


Implantación de Sistemas de Información

- Factores Críticos para la Implantación (II)
  - Análisis detallado de los requerimientos
    - Documentación de los procesos
    - Requisitos planteados por los usuarios finales
    - Interfaz de usuario
  - Definición de las especificaciones y requisitos técnicos
    - Diseño lógico y conceptual
    - Integración con otros sistemas
    - Migración de datos del entorno de trabajo anterior
  - Construcción del Sistema de Información

Implantación de Sistemas de Información

- Factores Críticos para la Implantación (III)
  - ➪ Equipo de implantación con experiencia en el sistema elegido y dedicación a tiempo completo, integrado por usuarios funcionales del sistema, técnicos informáticos propios y consultores externos
  - ➪ Formación y soporte técnico a los usuarios (redacción de procedimientos, diseño de manuales de usuario, diseño e impartición de cursos a usuarios finales, etc.)



Implantación de Sistemas de Información

- Factores Críticos para la Implantación (IV)
  - ➪ Gestión del cambio organizativo
    - ✎ Resistencia natural al cambio de las personas
      - – Vencimiento de los temores de los empleados ante la nueva situación
        - Pérdida de puestos de trabajo
        - Inseguridad ante el futuro
        - Pérdida de poder en la organización...
      - – Desconocimiento de los objetivos que se pretenden alcanzar y de cuáles son las causas que justifican el cambio
    - ✎ Promover la participación de los usuarios finales desde el principio
    - ✎ Medidas de sensibilización y de motivación (persuadir e implicar a los usuarios, retocar el sistema retributivo y de incentivos, etc.)
    - ✎ Análisis del impacto en la carga de trabajo de los distintos puestos y funciones, una vez se haya puesto en marcha el nuevo sistema
      - – Verificación de los nuevos métodos de trabajo

Implantación de Sistemas de Información

- Factores Críticos para la Implantación (V)
  - Pruebas y validación del nuevo sistema
  - Documentación del Sistema de Información y del proyecto
    - Documentación técnica del sistema
    - Manuales de procedimientos: pasos a seguir, codificación, etc.
    - Manuales de usuario final
    - Material de formación (ejemplos, casos prácticos, etc.)
  - Posterior mantenimiento y actualización del sistema, para hacer frente a los cambios en los procesos de negocio o en las necesidades de los Departamentos

PARTE IV
Gestión de la Seguridad de la Informacion (SGSI)

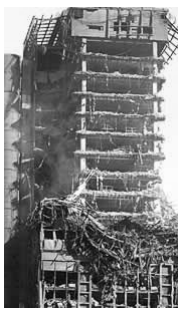
Seguridad de la Información

Activos Físicos

Datos e información sobre el negocio

Dependencia del negocio y de la actividad de una organización de los datos e información acumulados, así como del soporte de las TICs

Seguridad de la Información



Incendio de la Torre Windsor en Madrid, 12 de febrero de 2005

Edificio de 28 plantas dedicado a oficinas:

- La consultora y auditora Deloitte & Touche ocupaba 20 plantas
- El bufete Garrigues ocupaba 2 plantas

Seguridad de la Información

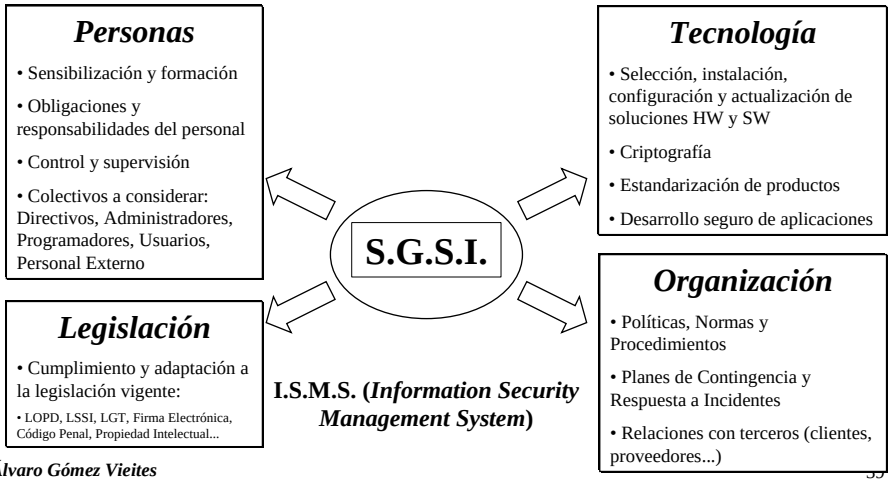
- Dificultades a tener en cuenta:
  - Intangibilidad de la información
  - Escasa formación en seguridad
  - Las medidas de seguridad no incrementan la productividad de la organización
  - Progresiva descentralización de los recursos informáticos
  - Problemas con el software (agujeros de seguridad)
  - Continuos cambios en el entorno tecnológico
  - Conexiones a Internet y accesos remotos

La Función de Seguridad

- Sistema de Gestión de la Seguridad de la Información
  - SGSI: Aquella parte del sistema general de gestión que comprende la política, la estructura organizativa, los procedimientos, los procesos y los recursos necesarios para implantar la gestión de la seguridad de la información en una organización
    - La gestión de la seguridad consiste en la realización de las tareas necesarias para garantizar los niveles de seguridad exigibles en una organización
    - Los riesgos no se pueden eliminar, pero sí se pueden gestionar
  - Política de Gestión de la Seguridad de la Información: Conjunto de normas reguladoras, procedimientos, reglas y prácticas que determinan el modo en que los activos, incluyendo la información considerada como sensible, son gestionados, protegidos y distribuidos dentro de una organización

La Función de Seguridad

Modelo para la Gestión de la Seguridad de la Información



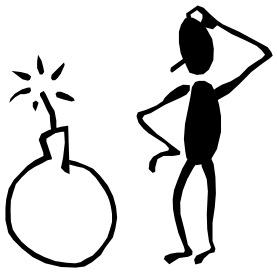
I.S.M.S. (*Information Security Management System*)

Estándares de Seguridad

- ISO/IEC 15408: *Common Criteria*
- ISO/IEC 17799: *Information Security Management*
  - Código de Buenas Prácticas, que incluye varios controles para mejorar la Gestión de la Seguridad de la Información
- ISO 27001 (SGSI)
- En España, serie de informes UNE 71501 y 71502 de AENOR
  - Establecer requisitos para proteger y gestionar la seguridad de los Sistemas de Información dentro de las organizaciones
    - UNE 71501-Parte 1: Conceptos y Modelos para la Seguridad de TI
    - UNE 71501-Parte 2: Gestión y Planificación de la Seguridad de TI
    - UNE 71501-Parte 3: Técnicas para la Gestión de la Seguridad de TI
    - UNE 71502: Especificaciones para los sistemas de Gestión de Seguridad de la Información (SGSI)

La importancia del factor humano

- "El enemigo está en casa en un 75 % de los casos"
  - Errores de los empleados: 50%
  - Empleados deshonestos: 15%
  - Empleados descuidados: 15%
  - Intrusos ajenos a la empresa: 10%
  - Integridad física de instalaciones: 10%
    - Fuente: *Datapro Research Corp.*



PARTE V
Protección de Datos de Carácter Personal (LOPD)

Protección de Datos Personales

- Cómo garantizar la protección de datos personales y la privacidad:
  - Postura de la Unión Europea y otros países, partidarios de una estricta regulación Estatal, con fuertes sanciones para aquellas empresas y organizaciones que incumplan las normas ("*hardlaw*")
    - También en Latinoamérica se ha reconocido recientemente el derecho fundamental a la protección de los datos personales de los ciudadanos
  - Países como EEUU que son mucho más permisivos con las actuaciones de las empresas, y que abogan por una autorregulación de la industria y la elaboración de códigos éticos de conducta, sin la intervención por parte de los Estados ("*softlaw*")
    - Fuertes presiones de las empresas y otros intereses económicos para impedir la intervención estatal

Protección de Datos Personales

- Servicios de venta de datos personales en EEUU
  - US Search (http://www.ussearch.com/)

¿Tiene el vecino antecedentes penales?
¿Está involucrado mi nuevo compañero de trabajo en una quiebra?
¿Dónde han vivido durante los últimos años los padres del nuevo amigo de mis hijos y qué propiedades tienen?
¿Con quién ha estado casada la nueva niñera de mis hijos, quiénes son sus familiares y dónde ha vivido en los últimos 10 años?

Protección de Datos Personales

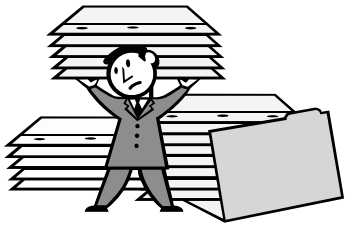
- Ley Orgánica de Protección de Datos Personales (LOPD), de 13 de diciembre de 1999
  - Art. 18.4 de la Constitución: La Ley limitará el uso de la informática para garantizar el honor, la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de los derechos
  - **LOPD**: Entrada en vigor el 15 de enero de 2000
    - Sustituye a la LORTAD
    - Transposición de la Directiva Europea 46/1995 de 24/11/1995
  - **Reglamento de la LOPD** (Real Decreto 1720/2007, de 21 de diciembre)
    - Entrada en vigor el 19 de abril de 2008
    - Desarrollo de disposiciones relativas a la potestad sancionadora de la Agencia de Protección de Datos, previstas en la LOPD, LSSI y LGT
    - Deroga el anterior Reglamento de Medidas de Seguridad de los Ficheros Automatizados (Real Decreto 994/1999, de 11 de junio)

Protección de Datos Personales

- Definiciones importantes
  - **Datos de carácter personal**: cualquier información numérica, alfabética, gráfica, fotográfica, acústica o de cualquier otro tipo concernientes a personas físicas identificadas o identificables
    - **Persona identificable**: toda persona cuya identidad pueda determinarse mediante cualquier información referida a su identidad física, fisiológica, psíquica, económica, cultural o social
  - **Fichero**: todo conjunto organizado de datos de carácter personal, que permita el acceso a los datos con arreglo a criterios determinados, cualquiera que fuere la forma o modalidad de su creación, almacenamiento, organización y acceso
  - **Tratamiento de datos**: cualquier operación o procedimiento técnico, sea o no automatizado, que permita la recogida, grabación, conservación, elaboración, modificación, consulta, utilización, cancelación, bloqueo o supresión, así como las cesiones de datos que resulten de comunicaciones, consultas, interconexiones y transferencias

Protección de Datos Personales

- Ámbito de aplicación (I)
  - "Organizaciones públicas y privadas que dispongan de fuentes de datos de carácter personal registrados en soporte físico, que los haga susceptibles de tratamiento, uso o explotación posterior"
  - Tratamiento efectuado en el territorio español de **datos personales** (automatizado o no)



Protección de Datos Personales

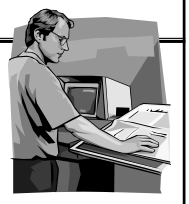
- Ámbito de aplicación (II)
  - No será aplicable a datos de personas jurídicas
    - Ni a los ficheros que se limiten a incorporar los datos de las personas físicas que presten sus servicios en aquéllas, consistentes únicamente en su nombre y apellidos, las funciones o puestos desempeñados, así como la dirección postal o electrónica, teléfono y nº de fax profesionales
  - Los datos relativos a empresarios individuales, cuando hagan referencia a ellos en su calidad de comerciantes, industriales o navieros, se entenderán excluidos del régimen de aplicación
  - Tampoco se aplica a los datos de personas fallecidas

Protección de Datos Personales

- Ámbito de aplicación (III)
  - Ficheros excluidos
    - Mantenidos por personas físicas para uso exclusivamente personal o doméstico (marco de la vida privada o familiar de los particulares)

    - Sometidos a la normativa sobre protección de materias clasificadas
    - Establecidos para la investigación de terrorismo y otras formas graves de delincuencia

Protección de Datos Personales



- Ámbito de aplicación (IV)
  - Fuentes de acceso público
    - Repertorio telefónico
    - Listas de personas pertenecientes a grupos profesionales
      - Deben contener únicamente los datos de nombre, título, profesión, actividad, grado académico, dirección e indicación de su pertenencia al grupo
    - Diarios y boletines oficiales
    - Medios de comunicación
    - Observación importante: las resoluciones judiciales no pueden ser consideradas como fuente accesible al público, sin perjuicio del principio de publicidad contenido en la Ley Orgánica del Poder Judicial

Protección de Datos Personales

- Ámbito de aplicación (V)
  - ➪ La inclusión en una página Web de datos personales debe cumplir el Derecho comunitario sobre Protección de Datos
    - ✎ Sentencia del Tribunal de Justicia de la UE, nov 2003: Caso LINDQVIST
      - – Este tipo de tratamiento de datos no se incluye en la categoría de actividades exclusivamente personales o domésticas

- La sentencia se refiere a una señora sueca que durante un período en el que fue catequista en una parroquia creó, en su domicilio y con su ordenador personal, varias páginas Web con el fin de que los feligreses de la parroquia que se preparaban para la confirmación pudieran obtener fácilmente la información que pudiera resultarles útil. Dichas páginas contenían información sobre ella y dieciocho de sus compañeros de la parroquia, incluido su nombre de pila y a veces el nombre completo. Además, se describía en un tono ligeramente humorístico las funciones que desempeñaban sus compañeros, así como sus aficiones. En varios casos se mencionaba la situación familiar, el número de teléfono e información adicional
- La señora en cuestión fue condenada a pagar una multa de aproximadamente 450 euros por haber tratado datos personales de modo automatizado sin haberlo comunicado previamente por escrito al organismo público para la protección de los datos transmitidos por vía informática, por haberlos transferido a países terceros sin autorización y por haber tratado datos personales delicados. La afectada interpuso un recurso de apelación contra esta resolución ante los tribunales suecos, quienes preguntaron al Tribunal de Justicia de la UE si las supuestas infracciones eran contrarias a las disposiciones de la Directiva relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos

Protección de Datos Personales

- Responsable del fichero y encargado del tratamiento
  - ➪ ***Responsable del fichero o tratamiento***: persona física o jurídica, de naturaleza pública o privada, que decide sobre la finalidad, contenido y uso del tratamiento
  - ➪ ***Encargado del tratamiento***: es el que sólo o conjuntamente con otros trate datos personales por cuenta del responsable del fichero
    - ✎ Tiene responsabilidad conjunta con el responsable del fichero sobre el establecimiento de las medidas de seguridad
    - ✎ Es el responsable de hacer efectivo el derecho de rectificación o cancelación en el plazo de 10 días
    - ✎ Obligación de indemnizar por los daños que los interesados sufran como consecuencia del incumplimiento por su parte de las obligaciones que le marca la LOPD

Protección de Datos Personales

- Relación entre el responsable del fichero y el encargado del tratamiento
  - Art. 12 de LOPD: "La realización de tratamientos por cuenta de terceros deberá estar regulada en un contrato que deberá constar por escrito o en alguna otra forma que permita acreditar su celebración y contenido, estableciéndose expresamente que el encargado del tratamiento únicamente tratará los datos conforme a las instrucciones del responsable del tratamiento, que no los aplicará o utilizará con fin distinto al que figure en dicho contrato, ni los comunicará, ni siquiera para su conservación, a otras personas" (de este modo, la LOPD impide una posible subcontratación del tratamiento de los datos)
  - "En el contrato se estipularán, asimismo, las medidas de seguridad a que se refiere el artículo 9 de esta Ley que el encargado del tratamiento está obligado a implementar"

Protección de Datos Personales

Responsable del fichero o tratamiento	**Persona física o jurídica, de naturaleza pública o privada, u órgano administrativo, que decida sobre la finalidad, contenido y uso del tratamiento.**
Encargado de Tratamiento	**Persona física o jurídica, autoridad pública, servicio o cualquier otro organismo que, sólo o conjuntamente con otros, trate datos personales por cuenta del responsable del tratamiento.**
Responsable de Seguridad	**Persona o personas a las que el responsable del fichero ha asignado formalmente la función de coordinar y controlar las medidas de seguridad aplicables.**

Protección de Datos Personales

- Creación de ficheros de titularidad privada
  - Notificación previa a la Agencia de Protección de Datos
    - Responsable del fichero
    - Finalidad del mismo
    - Ubicación
    - Tipo de datos de carácter personal que contiene
    - Medidas de seguridad
    - Indicación del nivel básico, medio o alto exigible
    - Cesiones de datos que prevean realizar

  - Inscripción en el Registro General de Protección de Datos
  - Comunicación de las posteriores modificaciones

Protección de Datos Personales

- Creación de ficheros de titularidad pública
  - Es necesaria una disposición general publicada en el BOE o en el Diario Oficial correspondiente (Art. 20 de la LOPD)
  - Disposiciones de creación o modificación de ficheros deben indicar:
    - La finalidad del fichero y los usos previstos para el mismo.
    - Las personas o colectivos sobre los que se pretenda obtener datos de carácter personal o que resulten obligados a suministrarlos.
    - El procedimiento de recogida de los datos de carácter personal.
    - La estructura básica del fichero y la descripción de los tipos de datos de carácter personal incluidos en el mismo.
    - Las cesiones de datos de carácter personal y, en su caso, las transferencias de datos que se prevean a países terceros.
    - Los órganos de las Administraciones responsables del fichero.
    - Los servicios o unidades ante los que pudiesen ejercitarse los derechos de acceso, rectificación, cancelación y oposición.
    - Las medidas de seguridad con indicación del nivel básico, medio o alto.

Protección de Datos Personales

- Principio fundamental de "***habeas data***"
  - Fijado en España por una Sentencia del Tribunal Supremo del 30 de noviembre de 2000: los datos personales son del ciudadano, no de la organización que decide crear un fichero en el que se incluyan dichos datos
  - Sentencia del Tribunal Constitucional número 292/2000: los derechos de acceso, rectificación, cancelación y oposición al tratamiento constituyen el haz de facultades que emanan del derecho fundamental a la protección de datos y "sirven a la capital función que desempeña este derecho fundamental: garantizar a la persona un poder de control sobre sus datos personales, lo que sólo es posible y efectivo imponiendo a terceros los mencionados deberes de hacer"

Protección de Datos Personales

- Principios de la protección de los datos (I)
  - Calidad de los datos (Art. 4 LOPD)
    - Datos adecuados, pertinentes y no excesivos en relación con el ámbito y las finalidades para las que se hayan obtenido
    - Datos exactos y puestos al día para garantizar la veracidad
    - Serán cancelados cuando hayan dejado de ser necesarios
  - **Seguridad de los datos** (Art. 9 LOPD)

    - El responsable del fichero, y, en su caso, el encargado del tratamiento deberán debe adoptar las medidas necesarias de índole técnica y organizativa para garantizar la seguridad de los datos de carácter personal y eviten su alteración, pérdida, tratamiento o acceso no autorizado
  - Deber de secreto (Art. 10 LOPD)

Protección de Datos Personales

- Principios de la protección de los datos (II)
  - Derecho de información en la recogida de datos (Art. 5)
    - La información debe abarcar:
      - Existencia, finalidad y destinatario de la información
      - Carácter obligatorio/facultativo de respuestas
      - Consecuencias de obtención o negativa a suministrarlos
      - Identidad y dirección del responsable del tratamiento

    - Se tendrá que llevar a cabo a través de un medio que permita acreditar su cumplimiento, debiendo conservarse mientras persista el tratamiento de los datos del afectado (art. 18 Reglamento)
      - Incorporación de esta información en todos los formularios y documentos utilizados para la recogida de datos

Protección de Datos Personales

- Principios de la protección de los datos (III)
  - Consentimiento del afectado (Art. 6 LOPD)
    - El tratamiento de los datos ***requiere el consentimiento inequívoco del afectado*** (y por escrito en datos especialmente protegidos)

      - El artículo 3.h) de la Ley Orgánica 15/1999 define el consentimiento del interesado como "*toda manifestación de voluntad, libre, inequívoca, específica e informada, mediante la que el interesado consienta el tratamiento de datos personales que le conciernen*"
      - Excepciones:
        - Datos obtenidos de fuentes accesibles al público
        - Datos necesarios para el ejercicio de funciones de la Administración
        - Datos de personas vinculadas por relación negocial, laboral, administrativa, contractual (cuando sean necesarios para mantener las relaciones o el contrato)
        - Cuando afecte a la Defensa Nacional, la seguridad pública o la persecución de infracciones penales
    - Se prohíbe la recogida por medios fraudulentos, desleales o ilícitos

Protección de Datos Personales

- Principios de la protección de los datos (IV)
  - Comunicación o cesión de datos a terceros (Art. 11 LOPD)
    - Se requiere el consentimiento previo del interesado (informado sobre la finalidad de la comunicación y las actividades del cesionario)
    - Excepciones:

      - Que se trate de una cesión autorizada por una norma con rango de ley o una norma de derecho comunitario Datos obtenidos de fuentes accesibles al público
      - Cesión necesaria para el desarrollo, cumplimiento y control de relación jurídica libre y legítimamente aceptada
      - Destinatario: Defensor del pueblo, Ministerio fiscal, Tribunales
      - Cesiones entre Administraciones con fines históricos, estadísticos o científicos
      - Razones de urgencia de datos relativos a la salud

Protección de Datos Personales

- Principios de la protección de los datos (V)
  - Comunicación o cesión de datos a terceros (Art. 11 LOPD)
    - Las cesiones o comunicaciones de datos entre empresas de un mismo grupo requieren consentimiento del interesado, siendo necesario identificar explícitamente las finalidades a las que se destinarán los datos
    - Responsabilidad para la empresa adquirente de los datos (Art. 11.5), que debe cumplir con todo lo dispuesto por la LOPD
  - Acceso a los datos por parte de terceros (Art. 12 LOPD)
    - Distinción entre comunicación de datos a un tercero y tratamiento de datos por cuenta del responsable del fichero
    - No se considerará cesión cuando el acceso a los datos sea necesario para la prestación de un servicio al Responsable del Fichero

Protección de Datos Personales

- Derechos de las personas (I)
  - Derecho de información en la recogida de los datos
  - Derecho de consulta al Registro General de Protección de Datos
    - Derecho a conocer del Registro la existencia de tratamientos de datos, sus finalidades y la identidad del responsable del tratamiento
  - Derecho de acceso de sus datos de carácter personal
    - Derecho a obtener gratuitamente información sobre:
      - Sus datos sometidos a tratamiento, el origen de dichos datos y las comunicaciones de los mismos
      - Plazo de 1 mes para hacerlo efectivo
      - Período de 12 meses para volver a ejercer este derecho

Protección de Datos Personales

- Derechos de las personas (II)
  - Derecho de rectificación y cancelación
    - Plazo de 10 días naturales para hacerlo efectivo y dar respuesta expresa al interesado
    - La cancelación dará lugar al bloqueo de los datos, conservándose disponibles para la Administración, Jueces y Tribunales durante el período de prescripción de las posibles responsabilidades
      - Supresión tras prescribir las responsabilidades

Plazos de prescripción comunes:

- Prescripción de las acciones personales en la legislación civil.
- Conservación de los datos de negocio impuesta por la legislación mercantil.
- Conservación de los datos de los empleados según los plazos marcados en la legislación laboral

    - En el caso de previa comunicación (cesión de datos), el responsable del fichero se encargará de comunicar la rectificación o cancelación a todas aquellas personas a las que haya comunicado los datos, para que procedan de igual modo

Protección de Datos Personales

- Derechos de las personas (III)
  - Derecho de oposición
    - El afectado podrá oponerse al tratamiento de sus datos aún cuando se trate de aquellos para los que no sea necesario su consentimiento (datos procedentes de fuentes accesibles al público)
      - El responsable del fichero excluirá del tratamiento los datos relativos al afectado
  - Derecho a indemnización (Art. 19 LOPD)
      - Las lesiones que el incumplimiento de los preceptos de esta Ley Orgánica pueda producir al afectado, en sus bienes o derechos generan derecho de indemnización, bien de acuerdo con el procedimiento establecido de responsabilidad de las Administraciones Públicas, en el caso de los ficheros de titularidad pública, o bien ante los Tribunales ordinarios para los ficheros de titularidad privada
  - Tutela de derechos por parte de la APD

Protección de Datos Personales

- Medidas de Seguridad para la Protección de los Datos
  - El Reglamento determina las medidas de índole técnica y organizativa necesarias para garantizar la integridad y seguridad de ficheros automatizados, centros de tratamiento, locales, equipos, sistemas, programas, así como de las personas que intervengan en el tratamiento automatizado de los datos
    - Las medidas también resultan aplicables a los ficheros en soporte no automatizado
    - No se registrarán datos de carácter personal en ficheros que no reúnan las condiciones que se determinen por vía reglamentaria con respecto a su integridad y seguridad y a las de los centros de tratamiento, locales, equipos, sistemas y programas (art. 9.2 de la LOPD)

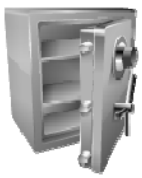
Protección de Datos Personales

- Medidas de Seguridad para la Protección de los Datos
  - Niveles de Seguridad para los datos:
    - ***Básico***: de aplicación a todos los ficheros de datos de carácter personal
    - ***Medio***: ficheros que contengan datos relativos a la comisión de infracciones administrativas o penales, ficheros de Hacienda Pública, ficheros de clientes de servicios financieros, ficheros de Entidades Gestoras y Servicios Comunes de la Seguridad Social, ficheros de mutuas de accidentes de trabajo y enfermedades profesionales de la Seguridad Social

      - Asimismo, cuando los ficheros contengan un conjunto de datos de carácter personal suficientes que permitan obtener una evaluación de la personalidad o del comportamiento del individuo

Protección de Datos Personales

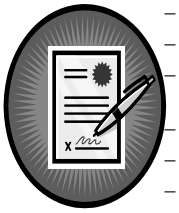
- Medidas de Seguridad para la Protección de los Datos
  - Niveles de Seguridad para los datos:
    - ***Alto***: ficheros que contengan datos de ideología, religión, creencias, origen racial, salud o vida sexual, así como los recabados para fines policiales y los de actos derivados de violencia de género



      - En caso de ficheros o tratamientos de datos de ideología, afiliación sindical, religión, creencias, origen racial, salud o vida sexual bastará la implantación de las medidas de seguridad de nivel básico cuando los datos se utilicen con la única finalidad de realizar una transferencia dineraria a las entidades de las que los afectados sean asociados o miembros
      - También podrán implantarse las medidas de seguridad de nivel básico en los ficheros o tratamientos que contengan datos relativos a la salud, referentes exclusivamente al grado de discapacidad o la simple declaración de la condición de discapacidad o invalidez del afectado, con motivo del cumplimiento de deberes públicos (nóminas, declaraciones IRPF, etc.)

Protección de Datos Personales

- Medidas de Seguridad para la Protección de los Datos
  - Elaboración de un documento de seguridad
    - Contenido:
      - Ámbito de aplicación del documento con especificación detallada de los recursos protegidos (ficheros declarados por la organización)
      - Medidas, normas y procedimientos para garantizar el nivel de seguridad
      - Funciones y obligaciones del personal con acceso a los datos
      - Estructura de los ficheros con datos de carácter personal y descripción de los sistemas de información que los tratan
      - Procedimiento de notificación y gestión de incidencias
      - Procedimientos de realización de copias de seguridad
      - Las medidas que sea necesario adoptar para el transporte de soportes y documentos, así como para la destrucción de los documentos y soportes, o en su caso, la reutilización de estos últimos
      - En caso de tratamiento de datos por cuenta de terceros, el documento de seguridad deberá identificar los ficheros o tratamientos que se traten en concepto de encargado, con referencia expresa al contrato o documento que regule las condiciones del encargo, así como de la identificación del responsable y del período de vigencia del encargo



Protección de Datos Personales

- Medidas de Seguridad de Nivel Básico (I)
  - Funciones y obligaciones del personal con acceso a datos
    - Las funciones y obligaciones de cada uno de los usuarios o perfiles de usuarios con acceso a los datos de carácter personal y a los sistemas de información estarán claramente definidas y documentadas en el documento de seguridad
    - También se definirán las funciones de control o autorizaciones delegadas por el responsable del fichero o tratamiento
    - El responsable del fichero o tratamiento adoptará las medidas necesarias para que el personal conozca de una forma comprensible las normas de seguridad que afecten al desarrollo de sus funciones así como las consecuencias en que pudiera incurrir en caso de incumplimiento

Protección de Datos Personales

- Medidas de Seguridad de Nivel Básico (II)
  - Identificación y autenticación de usuarios

  - El responsable del fichero o tratamiento establecerá un mecanismo que permita la identificación de forma inequívoca y personalizada de todo aquel usuario que intente acceder al sistema de información y la verificación de que está autorizado
  - Cuando el mecanismo de autenticación se base en la existencia de contraseñas existirá un procedimiento de asignación, distribución y almacenamiento que garantice su confidencialidad e integridad
  - El documento de seguridad establecerá la periodicidad, que en ningún caso será superior a un año, con la que tienen que ser cambiadas las contraseñas que, mientras estén vigentes, se almacenarán de forma ininteligible

Protección de Datos Personales

- Medidas de Seguridad de Nivel Básico (III)
  - Control de acceso
    - Los usuarios deben tener acceso únicamente a los datos que necesitan para el desempeño de sus funciones
    - Los mecanismos deben evitar el acceso a datos no autorizados
    - Debe existir una relación de usuarios o perfiles de usuarios con los accesos autorizados
    - Únicamente personal autorizado puede conceder y modificar los derechos de acceso

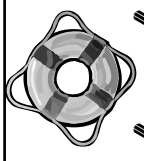
Protección de Datos Personales

- Medidas de Seguridad de Nivel Básico (IV)
  - Gestión de soportes informáticos (cintas, cartuchos, discos…) y documentos con datos de carácter personal que permita identificar, inventariar y almacenar la información

  - La salida de soportes y documentos (incluidos los adjuntos a un correo electrónico) fuera de los locales bajo el control del responsable del fichero o tratamiento deberá ser autorizada por el responsable del fichero o encontrarse debidamente autorizada en el documento de seguridad
  - En el traslado de la documentación se adoptarán las medidas dirigidas a evitar la sustracción, pérdida o acceso indebido a la información durante su transporte.
  - Siempre que vaya a desecharse cualquier documento o soporte que contenga datos de carácter personal deberá procederse a su destrucción o borrado, mediante la adopción de medidas dirigidas a evitar el acceso a la información contenida en el mismo o su recuperación posterior

Protección de Datos Personales

- Medidas de Seguridad de Nivel Básico (V)
  - Registro de incidencias
    - Deberá contener al menos, el tipo de incidencia, el momento en el que se produjo o en que se detecta, la persona que realiza la notificación, a quién se le comunica, los efectos que se hubieran derivada de la misma y las medidas correctoras aplicadas
  - Copias de seguridad



    - Existencia de procedimientos de generación y recuperación de las copias de seguridad, que deberán realizarse, como mínimo, semanalmente
    - Limitación de las pruebas con datos reales (pruebas anteriores a la implantación o modificación de los sistemas de información)

Protección de Datos Personales

- Medidas de Seguridad de Nivel Medio (I)
  - Identificación y autenticación
    - Limitación del número de intentos de acceso no autorizados al sistema
  - Control de acceso físico
    - Limitación del acceso a los locales donde se encuentran los equipos y soportes con los datos

  - Gestión de soportes informáticos
    - Registro de entradas y salidas de soportes con datos

Protección de Datos Personales

- Medidas de Seguridad de Nivel Medio (II)
  - Existencia de la figura del Responsable de Seguridad

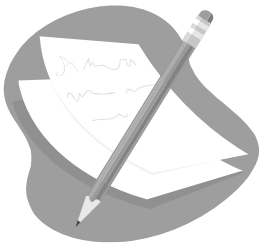
    - Responsable de adoptar las medidas de índole técnico y organizativas necesarias que garanticen la seguridad de los datos de carácter personal y eviten su alteración, pérdida, tratamiento o acceso no autorizado, habida cuenta del estado de la tecnología, la naturaleza de los datos almacenados y los riesgos a que están expuestos, ya provengan de la acción humana o del medio físico o natural
  - Registro de incidencias
    - Registro de procedimientos de recuperación de datos, que han de contar con la autorización por escrito del responsable del fichero

Protección de Datos Personales

- Medidas de Seguridad de Nivel Medio (III)
  - Auditoría interna o externa (al menos cada dos años)
    - El informe de auditoría deberá dictaminar sobre la adecuación de las medidas y controles al Reglamento, identificar sus deficiencias y proponer las medidas correctoras o complementarias necesarias
    - Deberá incluir los datos, hechos y observaciones en que se basen los dictámenes alcanzados y recomendaciones propuestas

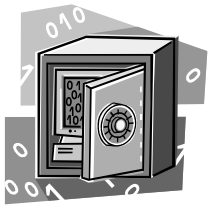
Protección de Datos Personales

- Medidas de Seguridad de Nivel Medio (IV)
  - Documento de seguridad (información adicional)
    - Identificación del responsable o responsables de la seguridad
    - Controles periódicos para verificar la seguridad
    - Procedimientos para el control de los registros de entradas y salidas de soportes
    - Plan auditor



Protección de Datos Personales

- Medidas de Seguridad de Nivel Alto
  - Distribución de soportes informáticos
    - Los datos deberán estar cifrados
  - Telecomunicaciones
    - Los datos deberán transmitirse cifrados
  - Registro de accesos
    - Identificación del usuario, fecha, hora, fichero accedido, tipo de acceso, resultado (autorizado o denegado), registro accedido
    - Mantenimiento durante al menos 2 años
  - Copias de seguridad
    - Deberán guardarse en un lugar diferente a los equipos



Protección de Datos Personales

- Tipos de Infracciones (I)
  - Leves
    - No atender una solicitud del interesado de rectificación o cancelación de los datos personales
    - No solicitar la inscripción del fichero de datos en el Registro General de Protección de Datos
    - Proceder a la recogida de datos de carácter personal sin proporcionar información a los afectados
    - Incumplir el deber de secreto

Protección de Datos Personales

- Tipos de Infracciones (II)
  - Graves
    - Proceder a la creación de ficheros de titularidad privada con finalidades distintas de las que constituyen el objeto legítimo
    - Proceder a la recogida de datos de carácter personal sin el consentimiento expreso de las personas afectadas
    - Mantener datos de carácter personal inexactos o no efectuar las rectificaciones o cancelaciones de los mismos que procedan
    - Mantener los ficheros, locales, programas o equipos que contengan datos de carácter personal sin las debidas condiciones de seguridad

Protección de Datos Personales

- Tipos de Infracciones (III)
  - Muy Graves
    - La recogida de datos en forma engañosa y fraudulenta
    - La comunicación o cesión de los datos de carácter personal, fuera de los casos en que estén permitidas
    - Recabar y tratar los datos de carácter personal especialmente protegidos sin cumplir los requisitos exigidos por la LOPD
    - La transferencia temporal o definitiva de datos de carácter personal con destino a países que no proporcionen un nivel de protección equiparable sin autorización del Director de la Agencia de Protección de Datos

Protección de Datos Personales

- Tipos de sanciones (I)
  - Infracciones leves: multa de **100.000** a **10.000.000** de pesetas (601 € a 60.101 €)
  - Infracciones graves: multa de **10.000.000** a **50.000.000** de pesetas (60.101 € a 300.506 €)
  - Infracciones muy graves: multa de **50.000.000** a **100.000.000** de pesetas (300.506 € a 601.012 €)
    - Potestad de inmovilización de los ficheros por parte de la APD
  - La cuantía de las sanciones se graduará atendiendo a:

    - La naturaleza de los derechos personales afectados; el volumen de los tratamientos efectuados; los beneficios obtenidos; el grado de intencionalidad; la reincidencia; los daños y perjuicios causados a las personas interesadas.

Protección de Datos Personales

- Tipos de sanciones (II)
  - Prescripción:
    - Leves: 1 año Graves: 2 años Muy graves: 3 años
  - El procedimiento sancionador se iniciará siempre de oficio mediante acuerdo del Director de la Agencia de Protección de Datos, bien por denuncia de un afectado o afectados o por propia iniciativa.
    - Las resoluciones de la APD agotan la vía administrativa (recurso contencioso- administrativo contra ellas)
  - Si las infracciones se cometen en ficheros de titularidad pública (art. 46 de la LOPD):
    - El Director de la APD podrá proponer la adopción de medidas disciplinarias, de acuerdo con lo establecido por el Régimen Disciplinario de las Administraciones Públicas.

Protección de Datos Personales

- Adaptación práctica a la LOPD
  - Sensibilización de los responsables
  - Auditoría de partida
    - Revisión de los tratamientos de datos realizados (aplicaciones informáticas internas y tratamientos realizados por terceros)
    - Análisis de los ficheros con datos de carácter personal (bases de datos y documentos en papel)
      - Estructura (qué datos utilizo), finalidad (para qué los utilizo), procedencia (cómo los obtengo), actualización de los datos, tiempo previsto para su conservación
  - Inscripción de los ficheros identificados en el RGPD
  - Redacción del Documento de Seguridad
  - Implantación en la práctica de las Medidas de Seguridad

Protección de Datos Personales

- Adaptación práctica a la LOPD
  - Revisión de tratamientos y de cesiones a terceros
    - Formalización mediante un contrato de los tratamientos, exigiendo la implantación de las medidas de seguridad adecuadas
    - Especial atención a las cesiones
      - ¿Qué datos? (proporcionalidad), ¿para qué? (finalidad) y ¿por qué? (legitimidad)
  - Revisión de los procedimientos relacionados con la protección de datos:
    - Información a los interesados sobre el tratamiento
    - Petición del consentimiento para el tratamiento
    - Respuesta a las peticiones de acceso, rectificación, cancelación u oposición, etc.

Protección de Datos Personales

- Adaptación práctica a la LOPD
  - Formación y sensibilización de los empleados
  - Clara definición de las funciones y obligaciones del personal
  - Otras cuestiones a considerar:
    - Posibles transferencias internacionales de datos
    - Aplicación de regulaciones sectoriales específicas sobre protección de datos (consultar instrucciones de la APD)

Comentarios, cuestiones, sugerencias...

agomez@simce.com

Muchas gracias por vuestra atención