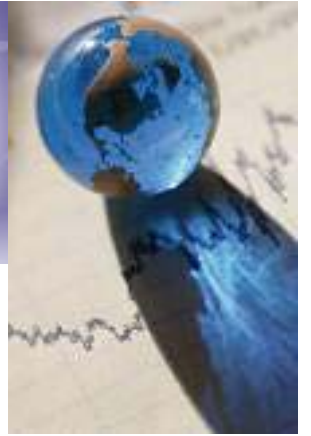




PC EXPRESS SOLUTIONS S.L.










PROYECTO DE IMPLANTACIÓN LEY DE PROTECCIÓN DE DATOS

INFORMACIÓN - DOCUMENTACIÓN



ÍNDICE

 Informe al asunto: Ley de Protección de Datos	3
 Proceso de Trabajo	4
 Contenido del Documento de Seguridad	5
 Razones para implantar la LOPD	6
 Noticias relacionadas	17
 Boletín mensual	34
 Tarifa de Precios	35

INFORME AL ASUNTO

Como consecuencia de la entrada en vigor de la **Ley Orgánica 15/1999 de Protección de datos de carácter personal**, se establece la obligación de todo empresario que tenga ficheros con datos de carácter personal registrados en soporte físico, de notificarlo a la Agencia de Protección de Datos y posteriormente inscribirlos en el Registro General de Protección de Datos, además de elaborar un Documento de Seguridad que contenga los artículos descritos en el Reglamento de Medidas de Seguridad de los ficheros automatizados que contengan datos de carácter personal, aprobado por el Real Decreto 994/1999 del 11 de Junio.

El objeto de esta Ley, no es otro que el de **garantizar y proteger**, en lo que concierne al tratamiento de los datos personales, las libertades públicas y los derechos fundamentales de las personas físicas, y especialmente de su honor e intimidad personal y familiar.

Asimismo, cabe señalar que la precitada ley es contundente en la aplicación de sanciones, estableciendo un régimen gradual de sanciones e infracciones. Así, las infracciones **leves** se sancionan con multa de 600 a 60.000 euros, las infracciones **graves**, como por ejemplo la falta de implantación de las medidas de seguridad, con multa de 60.000 a 300.000 euros y las infracciones **muy graves** con multa de 300.000 a 600.000 euros.

Hasta la fecha la Agencia de Protección de Datos sólo ha actuado en empresas multinacionales, las cuales poseen una gran cantidad de datos susceptibles de aplicación de procesos de seguridad.

Actualmente hay constancia de una campaña por parte de dicha agencia, para inspeccionar la situación del resto de empresas, ya sean grandes empresas, pymes, autónomos, etc.

Ponemos a su disposición un nuevo servicio a medida de cada perfil de empresa, para gestionar la regularización de todos los clientes en el menor tiempo posible, ya que consideramos que las sanciones están resultando lo suficientemente duras como para tener en cuenta una rápida actuación. No obstante aceptamos trabajar con su propia gestoría, la cual normalmente goza de su total confianza en estos aspectos.

PROCESO DE ADAPTACIÓN

- **Auditoría**

Detección de ficheros de datos de carácter personal. Obtención de datos para la elaboración de toda la documentación

- **Analítica de Seguridad**

Análisis de los procesos de seguridad física y lógica de la empresa en lo que a los ficheros se refiere.

- **Alta en la Agencia de protección de Datos**

Proceso de alta de los ficheros y su topología en la agencia oficial.

- **Documento de Seguridad**

Elaboración del documento de seguridad con los datos obtenidos en la auditoría.

- **Comunicados**

Elaboración de los comunicados a empleados (formación) , clientes, proveedores, etc..

- **Informe de medidas obligatorias**

Presentación de un informe detallado de las carencias detectadas y recomendaciones para solucionarlas.

- **Modificación de documentos**

Presentación de propuestas para la modificación de documentos de trabajo diario para la adaptación a la LOPD: correo electrónico, página web, mejoras recomendadas, etc.

CUADRO RESUMEN MEDIDAS DE SEGURIDAD

Reglamento de medidas de seguridad de los ficheros que contengan datos de carácter personal (RD 994/1999)

Nivel básico: Ficheros que contengan datos de carácter personal.

Nivel medio: Ficheros que contengan datos relativos a la comisión de infracciones administrativas o penales, Hacienda Pública, servicios financieros y los que se rijan por el artículo 29 de la LOPD (prestación de servicios de solvencia y crédito).

Nivel alto: Ficheros que contengan datos de ideología, religión, creencias, origen racial, salud o vida sexual así como los recabados para fines policiales sin consentimiento de las personas afectadas.

	NIVEL BÁSICO	NIVEL MEDIO	NIVEL ALTO
DOCUMENTO DE SEGURIDAD	<ul style="list-style-type: none"> - Ambito de aplicación. - Medidas, normas, procedimientos reglas y estándares de seguridad. - Funciones y obligaciones del personal. - Estructura y descripción de ficheros y sistemas de información. - Procedimiento de notificación, gestión y respuesta ante incidencias. - Proced. realización copias de respaldo y recuperación de datos. 	<ul style="list-style-type: none"> - Identificación del responsable de seguridad. - Control periódico del cumplimiento del documento. - Medidas a adoptar en caso de reutilización o desecho de soportes. 	
PERSO NAL	<ul style="list-style-type: none"> - Funciones y obligaciones claramente definidas y documentadas. - Difusión entre el personal, de las normas que les afecten y de las consecuencias por incumplimiento. 		
INCIDEN CIAS	<ul style="list-style-type: none"> - Registrar tipo de incidencia, momento en que se ha producido, persona que la notifica, persona a la que se comunica y efectos derivados. 	<ul style="list-style-type: none"> - Registrar realización de procedimientos de recuperación de los datos, persona que lo ejecuta, datos restaurados y grabados manualmente. - Autorización por escrito del responsable del fichero para su recuperación. 	
IDENTIFICACIÓN Y AUTENTICACIÓN	<ul style="list-style-type: none"> - Relación actualizada de usuarios y accesos autorizados. - Procedimientos de identificación y autenticación. - Criterios de accesos. - Procedimientos de asignación y gestión de contraseñas y periodicidad con que se cambian. - Almacenamiento ininteligible de contraseñas activas. 	<ul style="list-style-type: none"> - Se establecerá el mecanismos que permita la identificación de forma inequívoca y personalizada de todo usuario y la verificación de que está autorizado. - Límite de intentos reiterados de acceso no autorizado. 	
CONTROL DE ACCESO	<ul style="list-style-type: none"> - Cada usuario accederá únicamente a los datos y recursos necesarios para el desarrollo de sus funciones. - Mecanismos que eviten el acceso a datos o recursos con derechos distintos de los autorizados. - Concesión de permisos de acceso sólo por personal autorizado. 	<ul style="list-style-type: none"> - Control de acceso físico a los locales donde se encuentren ubicados los sistemas de información. 	
GESTIÓN DE SOPORTES	<ul style="list-style-type: none"> - Identificar el tipo de información que contienen. - Inventario. - Almacenamiento con acceso restringido. - Salida de soportes autorizada por el responsable del fichero. 	<ul style="list-style-type: none"> - Registro de entrada y salida de soportes. - Medidas para impedir la recuperación posterior de información de un soporte que vaya a ser desechado o reutilizado. - Medidas que impidan la recuperación indebida de la información almacenada en un soporte que vaya a salir como consecuencia de operaciones de mantenimiento. 	<ul style="list-style-type: none"> - Cifrado de datos en la distribución de soportes.
COPIAS DE RESPALDO	<ul style="list-style-type: none"> - Verificar la definición y aplicación de los procedimientos de copias y recuperación. - Garantizar la reconstrucción de los datos en el estado en que se encontraban en el momento de producirse la pérdida o destrucción. - Copia de respaldo, al menos semanal. 		<ul style="list-style-type: none"> - Copia de respaldo y procedimientos de recuperación en lugar diferente del que se encuentren los equipos.
RESPON SABLE		<ul style="list-style-type: none"> - Uno o varios nombrados por el responsable del fichero. - Encargado de coordinar y controlar las medidas del documento. - No supone delegación de responsabilidad del responsable del fichero. 	
PRUE BAS		<ul style="list-style-type: none"> - Solo se realizarán si se asegura el nivel de seguridad correspondiente al tipo de fichero tratado. 	
AUDITORIA		<ul style="list-style-type: none"> - Bianual, interna o externa. - Adecuación de las medidas y controles. - Deficiencias y propuestas correctoras. - Análisis del responsable de seguridad y conclusiones al responsable del fichero, - Adopción de las medidas correctoras adecuadas. 	
REGISTRO DE ACCESOS			<ul style="list-style-type: none"> - Registrar usuario, hora, fichero, tipo acceso y registro accedido. - Control del responsable de seguridad. Informe mensual. - Conservación 2 años.
TELE COMU NICACIONES			<ul style="list-style-type: none"> - Transmisión de datos cifrada.

- Los niveles son acumulativos y tienen la condición de mínimos exigibles.
- Los accesos a través de redes de telecomunicaciones deben garantizar un nivel de seguridad equivalente al de los accesos en modo local.
- La ejecución de trabajos fuera de los locales de la ubicación del fichero debe ser expresamente autorizada por el responsable del fichero y garantizar el nivel de seguridad.
- Los ficheros temporales deberán cumplir el nivel de seguridad correspondiente y serán borrados una vez que hayan dejado de ser necesarios.
- Los ficheros de nivel básico que contengan datos que permitan obtener una evaluación de la personalidad del individuo deberán garantizar, además de las medidas de nivel básico, las de nivel medio relativas a auditoria, identificación y autenticación, control de acceso físico y gestión de soportes.



PC EXPRESS SOLUTIONS S.L.



RAZONES PARA LA IMPLANTACIÓN DE LA LOPD





LISTADO DE RAZONES

Ley : Obligación – Desconocimiento - Despreocupación

AGPD : Denuncia - Inspección – Sanción

Adaptación : Actualización – Legalización – Implantación

Conocimiento : Mejora – Revisión – Control

Responsabilidad : Tratamiento - Confidencialidad

Seguridad : Sistemas Información Protegidos - Personal

Implantación : Auditoría – Consultoría – Mantenimiento

Producto : Servicio – Paquetes – Certificado

Mercado : Clientes – Competencia - Geografía



Ley : Obligatoriedad – Desconocimiento

- Obligación por la Ley Orgánica 15/1999
- El 100% de las empresas van a tener que legalizarse.
- El 93% de las empresas españolas no se han actualizado a la LOPD.
- A medida que las empresas vayan implantando la LOPD, el resto sentirá más la necesidad de adaptarse.

NOTICIAS RELACIONADAS:

1. **SÓLO EL 12% DE LAS FIRMAS VALENCIANAS CUMPLE LA LEY DE PROTECCIÓN DE DATOS**
 2. **EL 12% DE LAS EMPRESAS E INSTITUCIONES VALENCIANAS CUMPLEN CON LA LEY DE PROTECCIÓN DE DATOS**
 3. **LA DESCONOCIDA LEY DE PROTECCIÓN DE DATOS**
 4. **EL GOBIERNO PIDE AL CONGRESO QUE PROPONGA UN DIPUTADO PARA LA AGENCIA DE PROTECCIÓN DE DATOS**
 5. **DECLARACIONES DIRECTOR AEPD: CUATRO MILLONES DE EMPRESAS INCUMPLEN LA LOPD**
-



AGPD : Denuncia - Inspección – Sanción

- La Agencia de Protección de Datos ha aumentado su plantilla de inspectores sustancialmente.
- En caso de denuncia, la inspección es segura y la actualización y legalización resultará mucho más cara que la preventiva. Las mejoras serán obligatorias.
- El 70% de las empresas españolas desconocen la LOPD.
- El precio de las sanciones es exageradamente superior al precio de implantación.
- No interesa correr ningún tipo de riesgo con las administraciones.

NOTICIAS RELACIONADAS:

1. [LAS EMPRESAS DEBERÁN GASTAR 360 MILLONES HASTA EL AÑO 2010](#)
 2. [DECLARACIONES SECRETARIO GENERAL DE LA APD](#)
 3. [LA COMISIÓN DE LIBERTADES E INFORMÁTICA DENUNCIA A AMENA POR UTILIZAR DATOS PERSONALES DE CLIENTES LA DESCONOCIDA LEY DE PROTECCIÓN DE DATOS](#)
 4. [LA AGENCIA MULTA CON MÁS 360.000 EUROS A CÍRCULO DE LECTORES POR CESIÓN DATOS](#)
 5. [LA MULTA POR TIRAR LOS TESTS MÉDICOS A LA BASURA PUEDE SER DE HASTA 600.000 EUROS](#)
-



Adaptación : Actualización – Legalización - Implantación

- Asesores legales, empresas de informática y consultoría técnica aúnan esfuerzos para fomentar la adaptación de sus clientes a la LOPD sin provocar molestias de tipo organizativo o de trabajo diario.
- La actualización e implantación no es un hecho puntual, es un proceso continuo.
- La implantación de mejoras en el sistema informático no se hace de forma instantánea.
- La experiencia nos ha hecho detectar que el cliente utiliza la LOPD como una excusa para poder realizar aquellas mejoras que nunca había tiempo para hacer.
- Sector Informático ha desarrollado alianzas y relaciones más sólidas con aquellas firmas que permitan una mejora continuada en lo que a los sistemas de seguridad se refiere.

NOTICIAS RELACIONADAS:

1. **ALIANZA SECTOR – SERVINET**
 2. **BIT DEFENDER – FIREWALL – SOFTWARE AUDITORÍA.**
 3. **COPIA DE DATOS Y BACKUP ON-LINE.**
-



Conocimiento : Mejora – Revisión – Control

- Conocimiento más profundo de la propia empresa y del parque informático en uso.
- Conocimiento más profundo de los datos que se manejan y se protegen.
- Mejora del sistema de trabajo en varios aspectos técnicos.
- Mejora en la organización de la empresa y fácil revisión de los procesos de trabajo por auditoría.
- Los procesos de implantación siguen los consejos de profesionales externos, lo que garantiza independencia y objetividad.

NOTICIAS RELACIONADAS:

1. **LOS SISTEMAS DE INFORMACIÓN SON ÚTILES PARA PROTEGER LOS DATOS, PERO EL VERDADERO RETO ES EL CAMBIO ORGANIZATIVO**
-



Responsabilidad : Tratamiento - Confidencialidad

- La LOPD obliga a disponer de un responsable, encargado de velar por la seguridad de los datos de terceros.
- El tratamiento de los datos debe realizarse bajo un sistema que permita su protección desde el exterior.
- Los datos almacenados por la empresa deberán ser los necesarios para poder realizar su actividad diaria, excluyendo cualquier otro tipo de uso.
- Las empresas tienen que demostrar que los datos que manejan son tratados de manera confidencial.

NOTICIAS RELACIONADAS:

1. **LA RESPONSABILIDAD DEL DIRECTIVO ANTE LA LOPD.**
 2. **PROTECCIÓN DE DATOS ABRE UNA INVESTIGACIÓN SOBRE LOS TESTS MÉDICOS TIRADOS A LA BASURA.**
 3. **GOOGLE PODRÍA VULNERAR LA LOPD Y LA LSSI CON SU SERVICIO DE 'E-MAIL'.**
 4. **LA AGENCIA DE PROTECCIÓN DE DATOS ALERTA DE 'DEFICIENCIAS' EN EL TRATAMIENTO DE DATOS EN LOS HOTELES.**
-



Seguridad : Sistemas Información Protegidos - Personas

- La implantación mejora notablemente la seguridad informática de la empresa.
- Pequeñas modificaciones a nivel técnico pueden ayudar a adaptar a la empresa a la LOPD sin un coste demasiado elevado.
- Con los mismos recursos se actualiza la seguridad de la empresa y los procesos necesarios para legalizarse a la LOPD.
- La amortización del gasto en consultoría se produce de forma múltiple.
- La empresa dispone de sistemas legales que le permiten regular su personal en lo que al uso de la tecnología se refiere.
- El personal es formado con una serie de mejoras en sistemas de trabajo con la tecnología, que vienen especificados por ley.

NOTICIAS RELACIONADAS:

1. [EL PELIGRO DE PERDER UN PAPEL.](#)
2. [¿TIENE SU EMPRESA LOS DATOS BAJO LLAVE?](#)
3. [EL 90% DE EMPRESAS E INSTITUCIONES TIENEN SUS DATOS DESPROTEGIDOS](#)

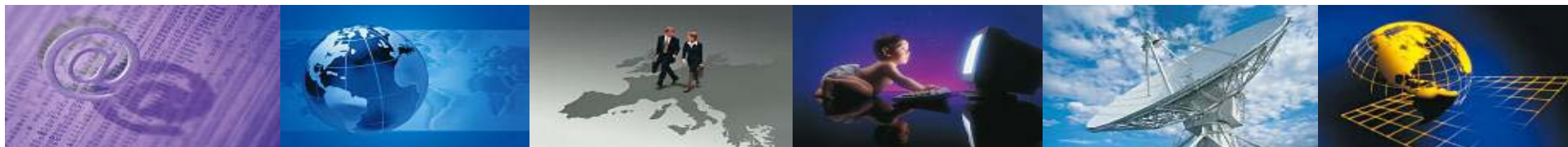


Implantación : Auditoría – Consultoría – Mantenimiento

- Modelos variados para la implantación del servicio según el perfil del cliente.
- Toma de decisiones conjuntamente con el cliente tras la recogida de datos de la empresa y detección de las carencias de la misma.
- Servicio “llave en mano” al cliente, incluido la consultoría y el mantenimiento del mismo.
- Para las empresas con el perfil de nivel de datos con seguridad de tipo medio y alto están obligadas por ley a realizar una auditoría bianual.
- La obligación de muchas empresas a realizar una auditoría cada dos años se regula con el sistema de mantenimiento.

NOTICIAS RELACIONADAS:

1. ***SE PREVÉE QUE LA DEMANDA DE CONSULTORÍA EN ESTE ÁMBITO GENERARÁ UN VOLUMEN DE NEGOCIO EN ESPAÑA DE 2.000 MILLONES DE EUROS, EN EL PERIODO 2004-2010.***
-



Producto : Servicio – Paquetes – Certificado

- La independencia del servicio garantiza la objetividad.
 - El servicio se tramita a través de un sistema de contratación.
 - La alianza entre servicios legales, jurídicos e informáticos garantiza una implantación profesional.
 - La variedad de paquetes de servicio permite la comercialización a diferentes niveles y tipos de cliente.
 - El cliente obtiene un certificado independiente que le permite venderse como empresa responsable y segura en el tratamiento de datos de terceros.
 - El contacto con el cliente no termina con la implantación, ya que con la contratación del servicio se obtiene un servicio de mantenimiento y de consultoría continuos para llevar el control del documento de seguridad.
 - La interacción entre clientes y sus propios clientes y proveedores permite una mayor difusión del servicio sin coste, ya que los propios clientes publicitan el servicio a través de su documentación diaria.
 - El estado permite desgravar el 10% del gasto en implantación de mejoras en sistemas de información directamente en el impuesto de sociedades.
-



Mercado : Clientes – Competencia - Geografía

- Fidelización del cliente e imagen y posicionamiento empresarial.
- Desmarcarnos del 95% de las gestorías, asesores legales y laborales pues están mal preparados o se desprecupan o asesoran de forma equivocada al cliente.
- Las consultoras o bufetes especializados acostumbran a volcarse en grandes proyectos corporativos y son demasiado caras.
- Poder vencer a la competencia con producto flexible y orientado a cualquier cliente.
- Posibilidad de dar servicio a cualquier cliente de todo el estado o delegaciones de clientes con proximidad.
- La alianza con un servicio de consultoría informático entendemos que es imprescindible.

NOTICIAS RELACIONADAS:

1. **LOS CONSUMIDORES TEMEN POR SUS DATOS PERSONALES**
 2. **ESPAÑA ES EL PAÍS DE LA UNIÓN EUROPEA QUE FIJA LAS MULTAS MÁS ALTAS EN PROTECCIÓN DE DATOS.**
-

NOTICIAS RELACIONADAS

Ley : Obligación-Desconocimiento-Despreocupación

** DIAPOSITIVA 3 **

SÓLO EL 12% DE LAS FIRMAS VALENCIANAS CUMPLE LA LEY DE PROTECCIÓN DE DATOS

El 12% de las empresas de la Comunidad Valenciana cumple la Ley sobre Protección de Datos, un porcentaje que, aunque es superior a la media nacional (10%), supone que en los próximos años deben invertir 360 millones de euros para proteger los datos. (Levante 15/7/2004)

La Comunidad es una de las zonas, junto a Cataluña y Madrid, con un mayor porcentaje de cumplimiento de la ley, pero todavía es pequeño el número de empresas y entidades que han registrado su información en la Agencia de Protección de Datos. La consultora, que presentó ayer estos datos, estima que las multas que deberán afrontar empresas e instituciones por el no cumplimiento de la ley asciende a un mínimo de 12 millones de euros en el periodo 2004-2010. El cumplimiento de la Ley asegura la protección de la información de carácter personal manejada por todo tipo de instituciones, tanto públicas como privadas. El grado de cumplimiento de la ley se debe al desconocimiento por parte de los empresarios de su existencia.

EL 12% DE LAS EMPRESAS E INSTITUCIONES VALENCIANAS CUMPLEN CON LA LEY DE PROTECCIÓN DE DATOS

El 12 por ciento de las empresas de la Comunidad Valenciana cumple con la legislación vigente en materia de protección de datos, a pesar de que este porcentaje está por encima de la media nacional, las empresas valencianas deberán asumir una inversión de 360 millones de euros para proteger sus datos según la normativa actual. (Europa Press 16/7/2004)

Esta consultora, especialista en el asesoramiento integral a empresas sobre políticas de seguridad y Ley Orgánica de Protección de Datos, prevé que la demanda de consultoría en este ámbito generará un volumen de negocio en la Comunidad Valenciana de 144 millones entre 2004 y 2010, lo que supone un 18 por ciento del mercado español (800 millones)

Asimismo, estiman que en este periodo las empresas e instituciones valencianas deberán afrontar multas por el no cumplimiento de la ley que ascenderán a "un mínimo de 12 millones de euros", aunque la Comunidad "aparece como una de las zonas geográficas más adelantadas en cuanto a cumplimiento de esta Ley".

Si la media nacional es de un 10 por ciento, en cuanto a empresas y organismos que cumplen esta ley, en la Comunidad Valenciana este porcentaje se eleva hasta un 12 por ciento, con lo que junto a Cataluña, con un 15 por ciento y Madrid con un 14 por ciento, son las tres autonomías con un mayor porcentaje de cumplimiento de esta ley.

En este sentido, destacaron que los datos más afectados por falta de seguridad, concretamente en más de un 90 por ciento de los casos, corresponde al manejo de datos en soportes tradicionales, como el papel.

La firma, que ofrece sus servicios con cobertura nacional, prevé que la demanda de consultoría en el campo de la Protección de Datos generará un volumen de negocio en la Comunidad Valenciana de 144 millones de euros, en el periodo 2004-2010, lo que supondrá un 18 por ciento del negocio total en España.

LA DESCONOCIDA LEY DE PROTECCIÓN DE DATOS

Sólo un 10% de las empresas españolas cumple hoy con los requisitos de la LOPD, que entró en vigor el año 2000. Autor: José Helguero (El Mundo 18/04/2004)

¿Cuántas veces hemos rellenado nosotros mismos o nuestros hijos esos cupones de los envases de cereales del desayuno para participar en un concurso? ¿Cuánta información contienen esos cupones? ¿Esa información queda almacenada?, ¿Es segura? La respuesta es no. Actualmente, las instituciones públicas y las empresas de servicios, concretamente las que atienden directamente a clientes, (es decir, nos proporcionan o les proporcionamos información personal), son los dos sectores más deficientes en cuanto al cumplimiento de una Ley, la de protección de datos. Esta Ley es prácticamente desconocida por la comunidad empresarial española a pesar de su obligatoriedad en cuanto a su cumplimiento. La actual Ley Orgánica de Protección de Datos entró en vigor en 2000 y cuatro años después sólo un 10% de las empresas españolas cumple con sus requisitos para la protección de sus datos. Actualmente, Cataluña, Madrid y Valencia son las tres zonas geográficas donde más número de empresas respeta la Ley. Navarra, Islas Baleares y Cantabria, son las más deficientes. Por ejemplo, en Cantabria, sólo 771 empresas cumplen con esta Ley, cifra ridícula comparada con su tejido industrial. Además del desconocimiento masivo de la Ley, el otro motivo fundamental que justifica este bajo índice de cumplimiento se basa en la falsa creencia de que los grandes agujeros de seguridad de los datos dentro de las empresas sólo hacen referencia a los sistemas de tecnología. En realidad los datos más afectados por falta de seguridad, concretamente en más de un 90% de los casos, corresponde al manejo de datos en soportes tradicionales, como el papel. De todos es conocido, el famoso caso de los currículos de candidatos a un puesto de trabajo de una conocida cadena de supermercados. Según se estima tras estudios realizados por consultorías en España, la inversión que deberá asumir el tejido empresarial español para adecuarse al cumplimiento de esta Ley asciende a 2.000 millones de euros. Igualmente, entre 2004 y 2010, las empresas españolas deberán afrontar multas por parte de la Agencia de Protección de Datos por valor de 40 millones de euros. Cabe mencionar que prácticamente todas las empresas que acuden a las consultoras especializadas en servicios para la adecuación de las sociedades a la Ley, lo hacen tras el anuncio, por parte de la Agencia, de una inspección y sorprendentemente, en muchos casos, declaran desconocer la existencia de la Ley y la obligatoriedad de su cumplimiento. Además, la norma establece sanciones económicas de hasta 601.002 euros, las más duras de toda la UE, por incumplimiento. Estas obligaciones, que en principio comportan un doble gasto; seguridad propia y seguridad para los datos de terceros, pueden servir a las empresas como punto de partida a la hora de replantearse la forma de poner en marcha sus sistemas de protección de una manera más efectiva y ventajosa. Un sistema que tenga como eje central de su desarrollo al titular de los datos y no a la empresa va a ser capaz de asegurar de golpe toda la información que maneja la empresa, la suya y la ajena. La LOPD implica tal cantidad de requisitos y disposiciones que una empresa al asegurarse de su cumplimiento estará obteniendo mecanismos válidos y útiles para cualquier tipo de información de la organización. Pero para ello es necesario tomar conciencia de que ajustarse a la norma necesita de un gran esfuerzo en términos de organización interna, informática y de concienciación y formación del personal. Un buen proyecto en ese sentido debe partir de la elaboración de una auditoría que, desde un enfoque multidisciplinar, más allá de los aspectos legales e informáticos, dé una verdadera imagen de la posición de la compañía. Posteriormente, ya en la fase de consultoría, se pondrían en marcha los mecanismos para la protección final de los datos. Por último se debe asegurar que la LOPD se cumple en el presente y en el futuro, que los mecanismos actúan también sobre el flujo de información de la empresa, para lo cual se tiene que establecer un sistema de gestión de ese flujo que asegure un rápido acceso a los datos y evite su fuga. En definitiva, la LOPD es una obligación para toda compañía, pero asegurar su eficaz cumplimiento puede brindarle un sistema que garantice la seguridad de su información crítica o vital más allá de la informática.

EL GOBIERNO PIDE AL CONGRESO QUE PROPONGA UN DIPUTADO PARA LA AGENCIA DE PROTECCIÓN DE DATOS

El Ministerio de Justicia ha remitido un escrito al presidente del Congreso, el socialista Manuel Marín, en el que le emplaza a proponer un candidato para formar parte del Consejo Consultivo de la Agencia de Protección de Datos durante los próximos cuatro años. Habitualmente este nombramiento se consulta entre los grupos, aunque el diputado suele proceder de la formación mayoritaria de la Cámara. (Europa Press 11/7/2004)

El Departamento que dirige Juan Fernando López Aguilar explica en su misiva, a la que tuvo acceso Europa Press, que con motivo de las elecciones generales del 14 de marzo y la constitución de la nueva Cámara Baja, hay que proceder al nombramiento de un nuevo vocal según lo establecido en el Estatuto de la Agencia de Protección de Datos. Por ello, solicita al Congreso que proponga a un diputado para su nombramiento por el Gobierno como vocal del citado Consejo Consultivo de la Agencia de Protección de Datos. Su mandato será de cuatro años.

El nuevo vocal sustituirá a Carmen Matador, que fue en su día propuesta por el Grupo Popular del Congreso. El Senado también deberá elegir un vocal para los próximos cuatro años para ocupar el puesto de Félix Lavilla, nombrado a instancias del Grupo Socialista en la pasada legislatura.

DECLARACIONES DIRECTOR AEPD: CUATRO MILLONES DE EMPRESAS INCUMPLEN LA LOPD

El director de la Agencia Española de Protección de Datos (AEPD), José Luis Piñar, reconoce que existe «menos preocupación de la que debería» sobre la protección de datos, pese a que hoy en día «hay mucha más información de la que los ciudadanos puedan saber sobre su persona, y que se pueda utilizar sin que lo sepan». (ABC 5/7/2004)

En una entrevista concedida a ABC, José Luis Piñar, y el subdirector general de la Inspección de Datos, Jesús Rubí, subrayan como retos de la AEPD la potenciación de la cultura de protección de datos. Recuerdan que en España «se ponen multas», pero en muchos otros países hay hasta penas de cárcel. Desde que se presenta una denuncia hasta que se investiga y se dictamina si ha existido infracción, pueden transcurrir como máximo seis meses. La AEPD cuenta con 93 trabajadores en plantilla, de los que 14 son inspectores. Piñar espera contratar a otros 36 trabajadores en 2005. Su labor no es grata ya que cuando se llega a una empresa hay cierto recelo, aunque los inspectores tienen autoridad y si se les niega la inspección pueden poner infracciones por obstrucción. Rubí concreta que se realiza una media de 1.000 investigaciones anuales. La ley obliga a todas las empresas a inscribirse en el registro de protección de datos. Las grandes, con más medios, están cumpliendo la normativa. El problema son las pequeñas y medianas, que «aún no son conscientes» de la necesidad de proteger las bases de datos que tienen. «Es un frente al que estamos prestando especial atención porque hemos constatado verdaderos intentos de estafa, que hemos puesto en conocimiento de la Fiscalía General del Estado», explica Piñar. Para mayor tranquilidad, Piñar asegura que una empresa registrada y con sus datos protegidos evita muchas denuncias, además de que protegerse «no es tan caro ni tan difícil». En este sentido, recuerda que cada vez existen más denuncias de empresas a las que se les ha robado sus bases de datos con el consiguiente riesgo de «competencia desleal», cuando todo sería tan sencillo como seguir los protocolos, poner claves de acceso a las bases de datos o realizar copias de seguridad, en su mayoría aplicaciones «muy

baratas». Sin embargo, de las cerca de cinco millones de empresas que existen en España, alrededor de cuatro millones, no tienen el «documento de seguridad». La AEPD para divulgar esta normativa ha firmado convenios con las Cámaras de Comercio, planes de oficio con los sectores -«se trata de auditorías preventivas de las que surgen recomendaciones», dice Piñar-. Pero también se está adaptando a las nuevas necesidades y buscando soluciones, por ejemplo, contra los «spam» de los correos de internet, para lo que están colaborando con la comisión federal de EE.UU. Igual ocurre con los mensajes por móvil, donde está empezando la colaboración internacional. Como explica Piñar «cada día se abre un frente nuevo», ocupando el sector de las telecomunicaciones la mayor atención. Además, la AEPD está realizando estudios en los sectores de «más riesgo», como es el hotelero, enseñanza o sanidad. La APD califica de «datos sensibles» los relacionados con la salud, la vida sexual, afiliación a sindicatos o partidos políticos, culto religioso y origen racial. Las multas oscilan entre los 600 y los 600.000 euros. La sanción media suele situarse en los 60.000 euros. Los incumplimientos más frecuentes son el tratamiento «sin consentimiento» de los datos para finalidades distintas a las que se tomaron, tratar la información de forma inexacta o vulnerar el derecho a guardar el secreto de los datos, pero también las cesiones ilícitas. La cesión de bases de datos con información sobre ciudadanos está prohibido por ley. Las multas por violar la norma oscilan entre 600 y 600.000 euros.

AGPD : Denuncia - Inspección – Sanción

** DIAPOSITIVA 4 **

LAS EMPRESAS DEBERÁN GASTAR 360 MILLONES HASTA EL AÑO 2010

Las multas por incumplimiento de la ley se multiplicarán por nueve y llegarán a 12 millones. A fecha de hoy, se denuncia menos del 5% de las infracciones. Las empresas de la Comunidad Valenciana deberán gastarse unos 360 millones para cumplir con la Ley Orgánica de Protección de Datos hasta 2010. (La Gaceta de los Negocios 15/7/2004)

De ellos, 144 millones se destinarán a consultoría y el resto a implementaciones tecnológicas y organizativas. Sólo el 12% de las firmas valencianas cumple con la ley; cifra que sitúa a la Comunidad al frente de la protección, junto a Madrid y Cataluña. Actualmente, menos del 5% de las infracciones acaban en denuncia.

Según un estudio, las empresas españolas deberán gastar 800 millones en consultoría de protección de datos en los próximos seis años. El 18% de dicho montante corresponderá al gasto de las firmas valencianas.

El montante de las multas por el no cumplimiento de la ley alcanzará los 40 millones hasta 2010. En la Comunidad se multiplicará por nueve y se situará en 12 millones. Los expedientes abiertos por la Agencia Española de Protección de Datos alcanzaron los 5,4 millones en 2003; 1,3 millones fueron desembolsados por firmas valencianas.

El problema de las multas radica en que la protección de la Agencia no valora el tamaño de la compañía. Por ello, las empresas valencianas podrían salir peor paradas, pues son pymes nada concienciadas. El 98% de sus infracciones se deben a la falta de concienciación o información. El 90% de las infracciones se efectúan por el mal uso del papel -expedientes, listados, historiales y análisis, entre otros-. Los sectores valencianos más afectados son el turismo, el sanitario, los seguros y los geriátricos.

LA COMISIÓN DE LIBERTADES E INFORMÁTICA DENUNCIA A AMENA POR UTILIZAR DATOS PERSONALES DE CLIENTES

La Comisión de Libertades e Informática (CLI), integrada por asociaciones de consumidores y sindicatos, ha denunciado a Amena por su campaña para hacer uso de los datos personales de sus clientes, al estimar que es contraria a la Ley de Protección de Datos, por dejar al usuario "la carga y el coste de la oposición al tratamiento". (Europa Press 26/7/2004)

En un comunicado, la comisión explicó que la operadora está enviando una carta a sus clientes para pedirles el consentimiento para la cesión de los datos personales que consten en sus ficheros a las otras empresas del grupo con fines publicitarios. Según la comisión, la recepción de la carta informativa supone que si en el plazo de un mes el cliente no se opone a ello (enviando una carta, con el coste que supone), Amena considerará otorgado el consentimiento.

La CLI estima que este tipo de prácticas, realizadas anteriormente por Telefónica, son contrarias a la Ley de Protección de Datos, dado que dejan al usuario la carga y el coste de la oposición al tratamiento de sus datos personales.

La comisión se basa en que Amena envía cartas no certificadas, por lo que muchos clientes pueden no estar informados sobre el uso de sus datos. Además, la operadora no habilita medios gratuitos y sencillos para que el usuario pueda oponerse al tratamiento de sus datos, de modo que la única forma de oposición es el envío de una carta costeada por el cliente. La comisión recordó que la Ley de Protección de Datos protege los derechos de los usuarios contra este tipo de abusos, con mecanismos como la denuncia ante la Agencia Española de Protección de Datos en los casos en que los usuarios no han tenido la posibilidad de oponerse al tratamiento.

LA AGENCIA MULTA CON MÁS 360.000 EUROS A CÍRCULO DE LECTORES POR CESIÓN DATOS

La Agencia de Protección de Datos (APD) ha impuesto a Círculo de Lectores una multa de 360.607 euros por una infracción "muy grave" de la Ley de Protección de Datos de Carácter

**Personal al haber cedido información personal a otra empresa para envío de publicidad.
(Agencia EFE 29-6-2004)**

Según el texto de la resolución, a la que tuvo acceso Efe y contra la que cabe recurso de reposición ante la APD o contencioso administrativo ante la sala correspondiente de la Audiencia Nacional, A.M.S, de Vigo (Pontevedra) denunció en noviembre de 2002 a Círculo de Lectores y a la entidad Arvato Services por cesión de datos a terceros y por utilización de los mismos. En mayo de este año, la APD resolvió que cabe imponer a Círculo de Lectores la multa citada y declarar la ausencia de responsabilidad de Arvato Services. La denunciante comunicó a la APD que había recibido a principios de noviembre de 2002 un envío publicitario de una entidad financiera, que advertía que el listado para realizar el mismo había sido elaborado por la empresa Bertelsmann Direct, a la que debía dirigirse para ejercer sus derechos de acceso, rectificación y cancelación. Tras ponerse en contacto con ellos, le comunicaron que los datos le habían sido facilitados por Círculo de Lectores a pesar de que ella no les había autorizado para que lo hicieran. En abril del año pasado, la APD comprobó que Círculo de Lectores tenía un contrato con Arvato Services ("anteriormente denominado Bertelsmann Direct"), que le permitía utilizar el fichero de ex socios de la empresa para la realización de campañas publicitarias de terceras compañías. Constataron que la afectada figuraba como socia desde enero de 2002 aunque la empresa no disponía de un contrato de alta como socia y que en el campo "LORTAD" constaba el valor "N", que "según los representantes del Círculo de Lectores significa que el socio no da su consentimiento para recibir publicidad de terceras personas", señala la resolución. A.M.S había comunicado a Círculo de Lectores que no quería recibir información u ofertas y la denunciada le comunicó a comienzos de noviembre de 2002 que atendía su petición. El fichero con los destinatarios de la campaña publicitaria objeto de la denuncia que incluía los datos de A.M.S fue creado el 30 de septiembre de aquel año. Círculo de Lectores alegó que no había habido cesión de datos sino "una mera inclusión" de los datos de la denunciante "en un listado de destinatarios de una campaña de publicidad contando con el consentimiento de la interesada, dado que la misma manifestó su oposición al tratamiento de sus datos con fines publicitarios después de haber recibido la publicidad". La APD acordó entonces sancionar a Círculo de Lectores con una multa de 300.506 euros por infracción del artículo 11 (comunicación de datos) de la Ley de Protección de Datos Personales; y con otra de 60.101 por infracción del artículo 6 (sobre el consentimiento del afectado), de la misma norma.

LA MULTA POR TIRAR LOS TESTS MÉDICOS A LA BASURA PUEDE SER DE HASTA 600.000 EUROS

La Ley de Protección de Datos tipifica como «infracción muy grave» arrojar a la basura documentos médicos con datos personales, como hizo el lunes un psiquiatra en una gasolinera de Pamplona. (Diario de Navarra 30/04/2004)

Estas infracciones se multan con entre 300.000 y 600.000 euros que, según fuentes jurídicas consultadas, podrían recaer sobre el departamento de Salud. Éste podría sancionar administrativamente al médico. El apartado 4 del artículo 44 de la Ley Orgánica de Protección de Datos tipifica como infracción muy grave «tratar los datos de carácter personal de forma ilegítima o con menosprecio de los principios y garantías que les sean de aplicación, cuando con ello se impida o se atente contra el ejercicio de los derechos fundamentales». En el capítulo de sanciones, la normativa establece que las infracciones muy graves serán sancionadas «con multa de 300.000 a 600.000 euros. Según fuentes jurídicas, el pago de la multa podría recaer sobre el departamento de Salud del Gobierno de Navarra. Éste, a su vez, podría aplicar las sanciones administrativas que estime pertinentes al psiquiatra que tiró los documentos. Éste arrojó el lunes a dos cubos de basura de una gasolinera de Pamplona 310 cuestionarios para detectar síntomas de depresión cumplimentados por menores de edad en Barañáin en 1997. En esas fechas, el facultativo trabajaba como médico residente para el Servicio Navarro de Salud (SNS). Los cuestionarios contaban con el sello del SNS y el texto «Centro de salud de Barañáin». Además, entre los documentos arrojados a la basura se encontraron dos informes médicos sobre pacientes con trastornos psiquiátricos. Uno de ellos es la historia clínica completa de una mujer que ingresó en el Hospital Virgen del Camino, e incluye el diario de su estancia hospitalaria y los exámenes a los que fue sometida, así como textos manuscritos de la paciente y sus respuestas a distintos tests psiquiátricos.

Tanto la Agencia Española de Protección de Datos como el departamento de Salud han abierto sendas investigaciones sobre lo ocurrido. El primero es el órgano competente para aplicar sanciones en materia de custodia y control de los datos personales y puede, si aprecia indicios de delito, remitir sus investigaciones al Ministerio Fiscal para que abra un proceso judicial. La Agencia de Protección de Datos puede requerir información a las partes implicadas en la aparición de los documentos en la basura, inspeccionar locales o recabar las declaraciones de las personas relacionadas con el hecho.

DECLARACIONES SECRETARIO GENERAL DE LA APD

Los usuarios de Internet pueden pagar multas de 600 a 600.000 euros por vulnerar datos privados, según la APD (Europa Press 5/04/2004)

Los usuarios de Internet que envíen correos electrónicos sin el consentimiento de los titulares pueden llegar a pagar sanciones que oscilan entre los 600 y los 600.000 euros, por considerarse una vulneración del derecho fundamental de la protección de datos, según informó el secretario general de la Agencia de Protección de Datos, Álvaro Canales Gil. La dirección de correo electrónico es considerada un "dato de carácter personal" amparada por la Ley, un hecho que desconoce el 81 por ciento de los ciudadanos europeos.

Cada internauta gasta más de 15 minutos del día en borrar los correos no deseados que recibe. Este es un hecho, que demuestran las conclusiones del primer informe elaborado en el 2003 por la Comisión Europea del seguimiento de la Directiva respecto a la confidencialidad en la Red, en donde se encuentran "datos reales y no optimistas" sobre la protección de datos en Internet. En este apartado, el 81 por ciento de ciudadanos europeos tienen un conocimiento "bajo a muy bajo" de la conciencia de la protección de sus datos de carácter personal.

La recepción de los correos no deseados puede provenir de agentes comerciales que utilizan los datos personales para otros fines diferentes a los comprendidos en un principio por el usuario. Asimismo existen situaciones más complicadas donde no es fácil llegar a la fuga de los datos de carácter personal. Para estos casos, la agencia dispone de una subdirección general de inspección que se desplaza por toda España con carácter de autoridad pública, con lo que pueden inspeccionar los sistemas informáticos de las empresas.

Desde la aplicación de la Ley General de Telecomunicaciones y de la Ley de Servicios de la Sociedad de la Información y de Comercio Electrónico (LSSI), las entidades financieras y aseguradoras son las primeras organizaciones que han aplicado medidas contra la vulnerabilidad de los datos confidenciales, ya que son las que más manejan datos de carácter personal de manera masiva, pero otras organizaciones e instituciones todavía se encuentran poco avanzadas en procedimientos de seguridad.

Con respecto a estas empresas que no cumplan la cláusula del "consentimiento informado", con la que se demuestra que la persona acepta el uso de sus datos personales, Canales Gil, ha avisado que el régimen sancionador es "estricto" para los que no respeten la protección de datos, así que deben asumir costosas multas, que desde principios de este mes serán más efectivas, ya que la agencia asumió nuevas competencias de revisión de correos electrónicos.

En este sentido, el secretario general hizo un llamamiento a todos los agentes sociales para que cumplan con la obligación de "trasladar la idea" de que todos los usuarios de Internet están amparados por este derecho fundamental, y que en caso de vulneración pueden denunciarlo, como así ha sucedido en Bélgica donde se han registrado más de 75.000 denuncias en dos meses.

LA LOPD PASA FACTURA A LAS EMPRESAS ESPAÑOLAS.

La sanción media por no cumplir con la normativa es de 60.000 euros, aunque hay casos en los que la infracción puede llegar a más de un millón de euros.

Prácticamente el cien por cien de las empresas manejan datos personales en el desarrollo de su actividad y están sometidas a la Ley Orgánica de Protección de Datos (LOPD). Sin embargo, más de la mitad de las compañías desconocen la existencia de esta normativa y están siendo sancionadas con multas altísimas por parte de la Agencia Española de Protección de Datos (AEPD). Así, de las 574 inspecciones realizadas por la AEPD durante 2003, se pasó a las 1.352 el año pasado, de las cuales se prevé que 188 acaben en procedimientos sancionadores.

La protección de datos ha recibido un importante impulso a lo largo del pasado año, si bien en 2005 será más acusado, debido a su inclusión en la nueva Constitución Europea como derecho fundamental y a la aprobación de un nuevo reglamento para la LOPD, que regulará formalmente todo lo dispuesto por la ley orgánica de 1999.

WWW.VNUNET.ES

Conocimiento : Mejora – Revisión – Control

** DIAPOSITIVA 6 **

LOS SISTEMAS DE INFORMACIÓN SON ÚTILES PARA PROTEGER LOS DATOS, PERO EL VERDADERO RETO ES EL CAMBIO ORGANIZATIVO

La adquisición y puesta en marcha de sistemas de información para la gestión de la confidencialidad de los datos sanitarios que la Ley de Protección de Datos clasifica como sensibles no es suficiente. (Diario Médico 26/7/2004)

‘Es útil y los medios que existen ahora son muy interesantes, pero si el tratamiento y vigilancia de la información no se basa en un cambio organizativo los avances son mínimos. El 90 por ciento de las inspecciones de la Agencia de Protección de Datos no derivan de fallos en los sistemas informáticos sino de cuestiones más tradicionales, como la entrega de pruebas diagnósticas en mano o la lectura de resultados analíticos por teléfono a los padres, madres o hermanos de los pacientes sin comprobar su identidad’. Se considera que la clave sigue siendo el papel. ‘No se puede apostar por la tecnología y no contemplar el impacto del papel porque el problema es organizativo. Cualquiera puede ir a un hospital -yo mismo lo he hecho en alguna ocasión- y reclamar los resultados de un análisis de sangre o de una prueba diagnóstica sensible: el personal del centro los entrega sin comprobar nada. Lo mismo ocurre con las historias clínicas: en los medios aparecen cíclicamente noticias sobre el descubrimiento de historias en contenedores de basura. Hay incluso quien los vende al peso y piensa que así se soluciona el problema’. El experto cree que el sector sanitario público no ha estado -ni está- a la misma altura que el sector privado, que ha invertido masivamente en protección de datos. ‘Ponerse al día cuesta entre 6.000 y 12.000 euros según el tamaño de la organización y las compañías lo entienden más como una inversión que como un gasto, sobre todo teniendo en cuenta que el año pasado las sanciones efectivas contabilizaron un total de 4 millones de euros. Además, el daño a la imagen supera con mucho a la sanción’.

Responsabilidad : Tratamiento – Confidencialidad

** DIAPOSITIVA 7 **

LA AGENCIA DE PROTECCIÓN DE DATOS ALERTA DE 'DEFICIENCIAS' EN EL TRATAMIENTO DE DATOS EN LOS HOTELES

La Agencia Española de Protección de Datos ha alertado de las "deficiencias" en el tratamiento de datos personales que cometen habitualmente las cadenas hoteleras que operan en España, manifestadas singularmente en torno a la confusión existente sobre quién debe responsabilizarse del tratamiento de los datos de clientes y cuál debe ser el destino final de éstos, según se recoge en las conclusiones del 'Plan de Inspección a Cadenas Hoteleras en España' desarrollado por la Agencia. (Europa Press 29-6-2004)

El organismo público subrayó que los hoteles deben informar expresamente a los clientes en el momento de recabar sus datos personales de si el tratamiento de los datos será procesado únicamente por el establecimiento con el que se firma el contrato de alojamiento o también por la cadena en la que está integrado el hotel, en cuyo caso habrá de solicitar el consentimiento explícito del cliente. La Agencia Española de Protección de Datos analizó el grado de adecuación del tratamiento de datos personales a lo previsto en la Ley Orgánica de Protección de Datos en el sector hotelero durante los últimos meses de 2002 y el conjunto de 2003, periodo en el que inspeccionó los servicios centrales y los hoteles más representativos de cuatro grandes cadenas hoteleras, así como las centrales de reservas y empresas que prestan algún servicio a los establecimientos. La Agencia ya ha transmitido a la Confederación Española de Hoteles y Alojamientos Turísticos (Cehat) y a las compañías auditadas una serie de recomendaciones para solventar estas deficiencias. En este sentido, la entidad recomienda incluir en los formularios que rellena el cliente información sobre la finalidad para la que se recaban los datos y sobre el destinatario de los mismos; de las consecuencias de la negativa a suministrar determinados datos; de la posibilidad de ejercitar derechos de acceso, cancelación, rectificación y oposición; sobre la posibilidad de cesión de los datos a terceros; y una clara diferenciación entre los campos que deben rellenarse obligatoriamente de los tan sólo voluntarios. Paralelamente, la Agencia ha constatado que algunas cadenas hoteleras pretenden tratar de forma simultánea y centralizada todos los datos personales recabados de los clientes durante su estancia en distintos establecimientos de la compañía, por lo que recordó que las cadenas sólo pueden realizar este tipo de tratamientos cuando cuenten con el consentimiento expreso del titular de los datos.

Por otra parte, el organismo público subrayó la obligatoriedad de que la información sobre el impago de deudas por parte de clientes debe reflejar con precisión si la deuda ha sido o no abonada, al tiempo que destacó que dicha información sólo puede ser accesible para los hoteles de la cadena cuya titularidad se corresponda con el responsable del fichero, no para terceros aunque utilicen la misma marca comercial. Asimismo, los datos personales relativos a reservas canceladas o a aquéllas que han concluido con la estancia del cliente pueden conservarse pero siempre que se bloqueen de forma que sólo puedan utilizarse para atender posibles responsabilidades administrativas o judiciales. Transcurrido el plazo durante el que pueden exigirse estas responsabilidades deberá procederse a la supresión definitiva de los datos.

LA RESPONSABILIDAD DEL DIRECTIVO ANTE LA LOPD

Autor: Abel González Lanzarote. Comisión de Seguridad de ASIMELEC y director de Desarrollo de Negocio de ESA Security. (El País 29/04/2004)

La incorporación a nuestra dinámica de empresa de la aplicación de la nueva Ley Orgánica de Protección de Datos Personales (LOPD) no deja de traernos bastantes preocupaciones. Está invadiendo nuestro día a día con un sinnúmero de aspectos y cuestiones que debemos tener en cuenta y que nos hacen perder la noción hasta del propio concepto que la inspira: el dato personal. Estos datos, que hasta ahora convivían con nosotros de forma pacífica, siendo manejados en nuestras tareas diarias como elementos corrientes en el desarrollo de nuestro trabajo, se convierten en algo extremadamente protegido y frágil. Lo son hasta tal punto que su incumplimiento acarrea consecuencias muy graves que pueden llegar a afectar al propio puesto de trabajo. Los responsables de las distintas áreas de las empresas empiezan a ser conscientes de las implicaciones de este problema. Se encuentran con algo que les afecta de lleno, que sobrepasa el ámbito de los responsables de informática y se extrapola a directivos de áreas claves como la financiera, administrativa, comercial, de marketing y especialmente la de recursos humanos. Para ser más concretos, podemos clasificar estas responsabilidades en cuatro grupos: laborales, administrativas, civiles y penales.

1. Laborales: No hemos dejado de ver en los diversos medios de comunicación las fortísimas sanciones que se imponen a las empresas por fugas de datos, y en esas noticias se destacan especialmente la cadena de fallos que los provoca, el área que los ha producido y la sanción laboral de su responsable. Todos recordamos el famoso caso de unos supermercados cuyos responsables de informática y recursos humanos se vieron afectados.

2. Administrativas: Las sanciones contempladas en la Ley Orgánica de Protección de Datos Personales.

3. Civiles: Los artículos del Código Civil 1902 y 1903 relativos a la responsabilidad contractual y extracontractual.

4. Penales: El Código Penal español contempla los delitos contra la intimidad en sus artículos 197 y siguientes. Recientemente, la Audiencia Provincial de Madrid ha condenado a un funcionario de la Seguridad Social a cinco años y tres meses de prisión, una multa de 330.556 euros y la inhabilitación especial de 11 años para empleo o cargo público por suministrar mediando precio datos de cotizantes a una empresa privada. Los delitos por los que ha sido condenado son los de cohecho y revelación de secretos.

Ante este panorama, las corporaciones se sienten desbordadas e intentando buscar recursos para ponerse al día con la LOPD.

Les preocupa especialmente que, después de tantos esfuerzos, el trabajo de implantación de los principios de protección de datos se quiebre por la falta de aplicación práctica de los mismos. Esa aplicación pasa por la concienciación de los directivos de área que tienen a su cargo una serie de personas y que son realmente los usuarios de los datos personales, ya que del incumplimiento de las normas de seguridad de la empresa en su hacer cotidiano no van a responder directamente los usuarios, sino sus responsables, y no frente a la Agencia Española de Protección de Datos, sino ante su propia Dirección. Por lo tanto, esta responsabilidad entra ya de lleno en el campo de objetivos que debe cumplir un directivo.

Se aprecia la imperiosa necesidad de formación de estos directivos encaminada a crear la sensibilización suficiente sobre el tema de la protección de datos. Debe tratarse también como una política más de su departamento en consonancia con la aplicación obligada de las normas de seguridad que la empresa impone, en cumplimiento del reglamento de medidas de seguridad que desarrolla la LOPD.

Se plantea, en definitiva, la necesidad de acudir a expertos tanto técnicos como jurídico-organizativos para abordar este tema, puesto que el problema es complejo y necesita de un equipo especializado y un trabajo coordinado para su solución. Estos expertos deben ayudar a las corporaciones a adecuarse a la LOPD. Deben también formar a los responsables, apoyarles y asesorarles para que conciencien a las personas que trabajan en sus áreas de la importancia del cumplimiento de la ley. Deben transmitirles las graves consecuencias de imagen y las pérdidas económicas que puede sufrir la empresa por su incumplimiento, e informarles de que si bien es la corporación la que responde frente a la Agencia de Protección de Datos del mal uso de los mismos, hay un tipo de responsabilidades laborales internas que afectan en cascada a todos los implicados en la gestión. Nuestra necesidad de despertar la conciencia de los directivos viene amparada por escuchar estas preocupaciones a diario en boca de quienes tienen que abordar seriamente el cumplimiento de la normativa sobre protección de datos.

PROTECCIÓN DE DATOS ABRE UNA INVESTIGACIÓN SOBRE LOS TESTS MÉDICOS TIRADOS A LA BASURA

La Agencia Española de Protección de Datos abrió ayer una investigación sobre el hallazgo en dos cubos de basura de Pamplona de 310 cuestionarios para detectar síntomas de depresión con los datos personales de menores de Barañáin que los cumplimentaron en 1997. Además, se encontraron los informes psiquiátricos de dos pacientes. (Diario de Navarra 29/04/2004)

El departamento de Salud envió ayer a la Agencia Española de Protección de Datos una copia de la información publicada ayer en Diario de Navarra en la que se daba cuenta del hallazgo de los documentos, que fueron arrojados «por error» a dos cubos de basura de una gasolinera por un psiquiatra. Además, Salud iniciará también una investigación sobre los hechos. La Agencia de Protección de Datos es el órgano competente en la salvaguarda de los datos personales en ficheros tanto de titularidad pública como privada. Tiene la potestad de investigar y sancionar a quienes vulneran la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal. En el artículo 7.3 de la ley se consideran datos «especialmente protegidos» aquellos «de carácter personal que hagan referencia al origen racial, a la salud y a la vida sexual» de las personas. Dos ciudadanos hallaron el lunes en dos cubos de basura de una gasolinera de Pamplona los 310 cuestionarios. Estos tests forman parte de un estudio realizado en 1997 en los institutos de Barañáin con

menores de entre 12 y 17 años para averiguar la prevalencia de este trastorno entre la juventud. Los tests cuentan con los nombres, apellidos, fecha de nacimiento, edad y número de hermanos de los menores que rellenaron el test. Los siete médicos que llevaron a cabo el estudio enviaron una carta a los padres de todos los alumnos solicitándoles su consentimiento informado. 152 de esos consentimientos, firmados por los padres, se encontraron también en los cubos de basura. En la carta enviada a los padres se aseguraba que los datos procedentes de los adolescentes encuestados «serán estrictamente confidenciales». Al tratarse de un estudio médico iniciado a instancias de los propios facultativos, el responsable de la custodia de los documentos es el propio médico (o equipo de médicos encargado de la investigación), según informó Salud. No precisan del consentimiento del Servicio Navarro de Salud para iniciar la investigación, cuyos resultados se presentaron en mayo de 1998 en un congreso médico en Ibiza.

GOOGLE PODRÍA VULNERAR LA LOPD Y LA LSSI CON SU SERVICIO DE 'E-MAIL'

La Federación de Consumidores en Acción (FACUA España) ha advertido a la filial española de la compañía de Internet Google que el servicio de correo electrónico sobre el que está trabajando, denominado 'Gmail', "vulneraría" la Ley Orgánica de Protección de Datos (LOPD) y la Ley de Servicios de la Sociedad de la Información y de Comercio Electrónico (LSSI). (Europa Press 6/04/2004)

Según recoge FACUA en un comunicado, la empresa estadounidense "pretende violar la privacidad de las comunicaciones de los usuarios tratando los datos de sus mensajes de correo electrónico para enviarles publicidad de productos relacionados con sus contenidos". Por ese motivo, la federación se ha dirigido a la filial española de Google "para advertirle de que su anunciado servicio de correo electrónico vulneraría" en España ambas leyes, puesto que con 'Gmail' la compañía "pretende violar la privacidad de las comunicaciones" de los usuarios, así como "mantener en sus sistemas los correos borrados por los usuarios". El máximo responsable de Google en España, Miguel de Reina, recordó que el producto está "en pruebas" y señaló que no existe "ninguna preocupación" en la matriz sobre esta cuestión. "No haremos nada que vaya contra la ley", dijo de Reina a Europa Press. FACUA explica que en un apartado del web de Google dedicado a la protección de la privacidad, 'Gmail' "pretende escudarse" en que "la correspondencia de los anuncios con el contenido [de los correos] es un proceso completamente automatizado realizado por ordenadores" y "ningún humano lee su correo electrónico para colocar los anuncios", pero la LOPD "reconoce el derecho de los usuarios a oponerse al tratamiento de sus datos con fines publicitarios, independientemente de que éste se realice de forma automatizada o no". Así, la federación explica que si en un 'e-mail' aparece alguna de las palabras clave compradas por los anunciantes clientes de Google, el usuario podrá encontrarse en la parte derecha de la pantalla con textos publicitarios ('Adwords'), ya que "los ordenadores tratan el texto en un mensaje y lo emparejan a anuncios o la información relacionada en la base de datos extensa de Google". Por ese motivo FACUA advierte de que, si Google decidiera poner en marcha este servicio en España, "obviaría aspectos básicos regulados por las citadas leyes como son el derecho de los usuarios a oponerse al tratamiento de sus datos con fines publicitarios, la prohibición de enviar publicidad no autorizada y la catalogación como datos especialmente protegidos de toda información que revele cualquier aspecto relativo a la ideología, afiliación sindical, religión, creencias, origen racial, salud y vida sexual de un ciudadano".

Por otra parte, FACUA recoge que Google advierte de que "las copias residuales de correo electrónico pueden permanecer sobre nuestros sistemas, incluso después de que usted los haya borrado de su buzón de correo o después de que cierre su cuenta". La asociación de consumidores considera que esta práctica es contraria al artículo 12 de la LSSI, que plantea que "los prestadores de servicios de alojamiento de datos deberán retener los datos de conexión y tráfico generados por las comunicaciones (...) por un período máximo de doce meses" --aspecto todavía pendiente de regulación--, pero "serán únicamente los necesarios para facilitar la localización del equipo terminal empleado por el usuario para la transmisión de la información" y "en ningún caso, la obligación de retención de datos afectará al secreto de las comunicaciones". El motor de búsqueda más utilizado en todo el mundo argumenta que sus empleados "no tienen acceso al contenido de ningún buzón a no ser que usted expresamente solicite que ellos lo hagan o de ser requerido por la ley, mantener nuestro sistema, o proteger a Google o el público".

En cualquier caso, la advertencia de FACUA no es la primera que se produce contra 'Gmail', puesto que a nivel internacional el servicio de 'e-mail' de Google ha recibido ya las críticas de ONGs como la británica Privacy International, la holandesa Bits of Freedom y las estadounidenses Commercial Alert, World Privacy Forum y Electronic Privacy Information Center. El pasado jueves, la compañía revolucionó el mercado de los proveedores de correo electrónico al anunciar que estaba probando 'Gmail', cuya principal novedad respecto a los de la competencia es que ofrece una capacidad prácticamente ilimitada para que los usuarios convencionales conserven sus mensajes.

Así, el servicio permitiría almacenar hasta 8.000 millones de bits de información, el equivalente a medio millón de páginas de 'e-mail'. Ofrece mil megabytes (1 GB), mientras que los servicios de correo

electrónico más populares, como 'Hotmail' y 'Yahoo', ofrecen 2 y 6 MB de espacio, respectivamente, aunque en sus modalidades de pago ofrecen mayor capacidad.

Seguridad : Sistemas Información Protegidos – Personas

**** DIAPOSITIVA 8 ****

EL PELIGRO DE PERDER UN PAPEL

Las empresas protegen a fondo sus datos informáticos, pero suelen olvidar los documentos (Cinco Días 5/05/2004)

Nueve de la mañana. Sentado en su despacho, un ejecutivo examina un grupo de currículos que uno de sus colaboradores ha depositado sobre su mesa. Como ninguno se ajusta al perfil que está buscando, los tira a una papelera que comparte con otro compañero y que se vacía en un simple contenedor. Diez de la mañana. Después de examinar el primer borrador de un contrato con uno de sus clientes, ese mismo ejecutivo imprime el documento. La impresora, como siempre, está atascada. Tras maldecirla por enésima vez, vuelve a su despacho prometiéndose mentalmente recoger el documento más tarde. Pero no lo hace. Estos son sólo dos ejemplos del descuido que existe en la mayor parte de las empresas y otras entidades a la hora de tratar los documentos en papel. Un agujero organizativo que puede traer consecuencias mucho más graves de lo que pueda parecer a simple vista. ¿La razón? En esos documentos no sólo puede recogerse información económica de la compañía, sino también datos personales de los trabajadores, clientes, proveedores y aspirantes a empleados de la empresa, entre otros. 'Las empresas se preocupan mucho por el aspecto tecnológico de la protección de datos. Todas hacen copias de seguridad e instalan cortafuegos. Sin embargo, nosotros por nuestra experiencia sabemos que es mucho más fácil meter la pata con el papel. Más del 90% de las inspecciones de la Agencia de Protección de Datos (APD) es por incumplimientos de la ley en cuanto a soportes en papel', señala José Prieto experto en LOPD. El año pasado, la APD ingresó más de cuatro millones de euros a través de 198 sanciones que oscilaron entre los 600 y los 600.000 euros. Entre esas actuaciones hubo muchos incidentes relacionados con el descuido hacia el papel. Fue el caso, por ejemplo, de la aparición de una caja con medio centenar de historiales médicos en un contenedor del polígono de El Campillo, en Abanto. O el descubrimiento en una calle de Madrid de 125 currículos de aspirantes a vendedor de una tienda de ropa juvenil. Las inspecciones de la Agencia se inician a menudo por sorpresa. 'A las empresas que consideran serias las avisan con 24 horas de antelación. En las desconocidas se hacen por sorpresa, para evitar que a nadie le de tiempo de quemar papeles o hacer desaparecer equipos informáticos', explica Helguero. Muchas compañías utilizan esas 24 horas de gracia para tratar de construir, a través de documentos, una apariencia frente a la Agencia de que están inmersos en pleno proceso de adaptación a la ley.

¿TIENE SU EMPRESA LOS DATOS BAJO LLAVE?

Blindar la información de clientes, proveedores o empleados evita riesgos Va con usted, aunque no se lo parezca. Aunque tenga una pequeña empresa con apenas dos empleados, aunque sea un profesional liberal y tenga un solo ayudante, aunque dirija un minúsculo negocio desde el salón de su casa. Va con usted porque, sea grande o pequeña, cualquier empresa que tenga algún cliente, proveedor o trabajador tiene que cumplir la legislación de protección de datos. (Cinco Días 5/7/2004)

'Creo que en estos momentos las pymes y los profesionales son nuestra asignatura pendiente. Muchos piensan que no va con ellos, que la ley no les afecta porque tienen pocos datos. Otros ni siquiera saben que lo que tienen en sus ordenadores son ficheros'. El diagnóstico, del director de la Agencia Española de Protección de Datos, José Luis Piñar, es compartido también por las Cámaras de Comercio, que hace dos años realizaron un sondeo cuyo resultado fue que el 85% de las pymes no cumplía con la legislación. 'Las pymes tardan en conocer las leyes unos 10 años. Pero se está haciendo un gran esfuerzo y el reto está en que asuman que cumplir la ley les dará una ventaja competitiva', explica Belén Veleiro, directora de la asesoría jurídica de las Cámaras. Otra razón para esforzarse son las posibles sanciones derivadas de una mala praxis en este terreno, aunque la Agencia recuerda a menudo que su labor es más preventiva que represiva. ¿Es tan difícil cumplir la ley? 'Ni es tan caro ni es tan difícil. Exige un cierto esfuerzo inicial, pero el mantenimiento es sencillo. Las auditorías son cada dos años y el registro es gratuito', afirma el director de la Agencia. El primer paso que deben dar las empresas es dar de alta los ficheros (relación de nóminas, listas de clientes,

proveedores...) en el registro de la Agencia de Protección de Datos. Además, las empresas deben solicitar siempre cualquier dato con el consentimiento informado de su titular, a ser posible por medio de cláusulas escritas que puedan servir de prueba en caso de conflicto. Para algunas informaciones especialmente sensibles (la orientación sexual, por ejemplo) el consentimiento deberá ser expreso. También hay que recordar que cualquier persona puede dirigirse a la compañía para conocer, rectificar o cancelar sus datos. Y que ésta debe responder con rapidez y eficacia. Todos los datos deben ser custodiados con la implantación de una medidas técnicas de seguridad que varían según la naturaleza de la información (medidas básicas, medias y altas) y que deben recogerse en un documento de seguridad. Ese documento se convertirá en la biblia de protección de datos de la compañía y deberá recoger aspectos como el ámbito de aplicación de las medidas, la estructura de los ficheros, los procedimientos de recuperación de datos o las obligaciones del personal. 'El personal que tenga acceso a los datos tiene que estar informado de sus obligaciones'. Las Cámaras aconsejan formar a esos empleados y hacerles firmar una cláusula que acredite que conocen la ley.

EL 90% DE EMPRESAS E INSTITUCIONES TIENEN SUS DATOS DESPROTEGIDOS

Presentación del Estudio sobre Cumplimiento de LOPD realizado por Consultores Independientes (El Norte de Castilla 12/03/2004)

El 90% de las empresas e instituciones incumplen la Ley de Protección de Datos, según un estudio presentado ayer por una consultora especializada. Empresas e instituciones deberían invertir unos 2.000 millones de euros para proteger sus datos de acuerdo con los criterios que marca la ley y en los próximos seis años el importe de las multas que deberán afrontar ascenderá a más de 40 millones de euros, según explicó el director de la consultora. Los principales incumplimientos, debidos sobre todo al desconocimiento de la ley, se centran en la ausencia de medidas organizativas para proteger el uso de la información y la carencia de medidas tecnológicas.

Implantación: Auditoría – Consultoría – Mantenimiento

**** DIAPOSITIVA 9 ****

PREVISIONES DE FUTURO

Se, prevé que la demanda de consultoría en este ámbito generará un volumen de negocio en España de 2.000 millones de euros, en el período 2004-2010.

Durante el período 2004 - 2010 se estima que las multas que deberán afrontar empresas e instituciones españolas por el no cumplimiento de la ley, ascenderá a un mínimo de 40 millones de euros. Se prevé que la demanda de consultoría en este ámbito generará un volumen de negocio en España de 800 millones de euros, en el período 2004-20010.

5 AÑOS DESDE LA ENTRADA EN VIGOR DE LA LEY.

El pasado 14 de enero se cumplieron los 5 años desde la entrada en vigor de la Ley Orgánica 15/1999 de Protección de Datos de Carácter Personal, parece pues un buen momento para valorar como se encuentra la implantación efectiva de esta ley en el ámbito de las empresas.

Según datos de la Agencia Española de Protección de Datos en Diciembre de 2004 se encontraban inscritos un total de 457.490 de ficheros de titularidad privada, en la misma fecha y según datos del Directorio Central de Empresas (organismo del INE) existían en España un total de 2.942.583 empresas (Sociedades Limitadas y Anónimas). Teniendo en cuenta que en ésta última cantidad no se reflejan ni autónomos, ni sociedades no mercantiles, ni otras entidades de ámbito privado cuyos ficheros deberían estar también inscritos en el Registro General de la Agencia Española de Protección de Datos, el grado de cumplimiento de esta obligación legal, es francamente desalentador. Tomando el número total de empresas contabilizadas por el Directorio Central de Empresas y considerando que la gran mayoría de empresas necesitan para su normal funcionamiento, como mínimo, un fichero de clientes y uno de proveedores y el 49% de éstas tienen al menos un asalariado, por tanto un fichero de trabajadores, podemos llegar a la conclusión que, como máximo, están inscritos en el registro el 6,2% de los ficheros de las empresas españolas. Éstas pírricas cifras, no tienen en cuenta, además, ficheros cada vez más habituales entre las empresas como el de los usuarios de su página web, clientes potenciales, currículums, etc... A todo esto debemos añadir, por si no fuera suficiente, que la inscripción de los ficheros no implica el cumplimiento efectivo por parte de la empresa de todo lo dispuesto por la LOPD, como por ejemplo que garantice el derecho de información de los titulares de los datos o que haya revisado sus contratos con prestadores de servicios que impliquen el tratamiento de datos o que haya implementado el preceptivo documento de seguridad.

Las frías cifras, por tanto, parecen demostrar que el grado de cumplimiento de lo que dispone la LOPD, está lejos de una situación, si quiera, razonable. Creemos necesario pues el lanzamiento de nuevas ideas y propuestas para que el cumplimiento efectivo de ésta ley empiece a consolidarse ya que el miedo que han generado algunas actuaciones de la AEPD, parece no ser suficiente, al menos para ciertas empresas o sectores de actividad.

Bajo mi opinión sería necesaria la interacción de cuatro sectores implicados para el definitivo relanzamiento de la cultura de protección de datos. Me estoy refiriendo a una distinta actitud del titular de los datos, un cambio de política de la AEPD y de las agencias autonómicas hasta el día de hoy creadas, así como de los responsables de los ficheros y encargados del tratamiento y, por último, del poder legislativo. Vayamos por partes.

Desde mi punto de vista resulta evidente la sensación generalizada entre los titulares de datos (es decir de todas las personas), de la falta de control que sobre sus propios datos tiene. Son constantes las llamadas, cartas, correos electrónicos nominales enviados por empresas con las que el titular de los datos no es consciente de tener relación alguna. La sorpresa o indignación en menos casos, de las personas acostumbra a morir en el momento en el que se cuelga el teléfono, se rompe la carta o se borra el correspondiente correo electrónico. A pesar de ese rechazo puntal, sus datos continúan en el

sistema que ha generado esa comunicación y al cabo de días o semanas, este vuelve a producirse, generando un círculo interminable. La gente se queja interiormente, pero no reclama a quien debe hacerlo. Nuestro país tiene tradición de quejarse mucho y reclamar poco. Es necesario que los titulares de los datos reclamen formalmente, por los cauces legalmente establecidos, sus derechos, lo que obligará a los responsables del tratamiento a guardar ciertas cautelas que en la actualidad no se toman en cuenta. En ese punto debería convertirse en básica la labor de las agencias de protección de datos (la estatal y las autonómicas) que hasta la fecha se han centrado, acertadamente a mi entender, en que los responsables de los ficheros conozcan la ley, sin llevar a cabo una divulgación efectiva de lo que es el derecho en sí entre sus titulares. Humildemente creo que ha llegado ese momento, el conocimiento del derecho debe generar un mayor cumplimiento de la ley. Esto exige, no puede negarse, mayores recursos de la AEPD, ya que un mayor conocimiento del derecho debe comportar más procedimientos de tutela de los mismos, lo que significa más recursos humanos y materiales para atenderlos. En ese plano creo imprescindible que el presupuesto de la AEPD vuelva a depender en exclusiva de las arcas públicas y deje de financiarse de las sanciones, circunstancia que, en la actualidad, coloca a la AEPD en una situación de juez y parte ciertamente incomprensible.

En cuanto a los responsables de los ficheros y encargados del tratamiento, creo que va siendo la hora que tomen medidas en cuanto a los cantos de sirena que últimamente están oyendo en relación a su necesidad de adecuarse a la LOPD. En su inmensa mayoría saben que deben aplicar la ley, pero pocos son los que lo hacen. Hasta día de hoy observan que las sanciones (el único argumento efectivo hasta la fecha), se aplican, casi exclusivamente, a las grandes empresas y creen que tardará en llegar su momento. A todos ellos les diría que este es el momento de adaptarse a la LOPD, básicamente, por qué entrarán en un reducido número de elegidos adaptados a la ley dejando de engrosar las empresas potencialmente sancionables. Por otro lado no podemos olvidar que la ley les obliga y, que tarde o temprano, deberán adecuarse. ¿Por qué no hacerlo ahora cuando el grado de paranoia sobre el cumplimiento de esta ley es aún moderado? Deben ser conscientes que un día llegarán las prisas, y que las prisas que no son buenas compañeras de viaje para ninguna de las partes implicadas: los propios responsables de ficheros, los auditores legales y la AEPD.

Por último creo que sería un error no buscar explicaciones del bajo grado de cumplimiento de la LOPD, en la propia ley. Creo francamente desacertado que la ley mida a todas las empresas por el mismo rasero, obligando del mismo modo y en la misma medida a una gran multinacional que a la pequeña tienda de ropa de la esquina. Dicho esto, es necesario añadir que las reformas en ese sentido, no pueden vulnerar el contenido esencial del derecho de protección de datos, ya que no será constitucionalmente tolerable que éste derecho fundamental tuviera mayor o menor eficacia en función del responsable del fichero. Por tanto teniendo en cuenta que el contenido esencial del derecho de protección de datos, no puede depender de la entidad que los trate, creemos que la flexibilización de los requisitos para ciertos responsables de ficheros, debe llevarse a cabo en los aspectos no orgánicos de la regulación. Estamos pensando en concreto en el próximo reglamento de medidas de seguridad que debe desarrollarse en cumplimiento de la LOPD. Esta norma debería flexibilizar los requisitos de seguridad para las empresas que objetivamente, son menos vulnerables. Por ejemplo pequeñas empresas que sólo trabajan con ordenadores sin conexiones remotas, o en una aislada estación de trabajo o incluso únicamente con ficheros en papel.

Victor Roselló Mallol, abogado

Mercado : Clientes – Competencia – Geografía

** DIAPOSITIVA 11 **

LOS CONSUMIDORES TEMEN POR SUS DATOS PERSONALES

Desconfían de la privacidad de acceso a sus datos. Estudio elaborado por Accenture en USA (Gaceta de los Negocios 17-2-2004)

El temor a la deficiente protección de los datos personales ha llevado a los consumidores a rechazar o cancelar transacciones con distintas compañías, según un estudio elaborado por Accenture entre consumidores y empresas de Estados Unidos sobre privacidad y acceso a los datos personales. El informe revela la existencia de un gran abismo entre los puntos de vista de consumidores y empresas reflejado en varias áreas. Por ejemplo, el 74% de las empresas culpa al miedo por la seguridad de perjudicar la confianza de los consumidores, mientras el 67% de los consumidores dirige sus críticas al marketing activo, acciones que afectan a la hora de dar su confianza a una empresa determinada.

Compañías y consumidores tienen también ideas diferentes sobre lo que genera la confianza. Las empresas citan con más frecuencia (43%) el servicio activo de atención al cliente como lo que más positivamente influye en la confianza, mientras que el 62% de los consumidores afirma que la confianza es, en la mayoría de los casos, el resultado de la reputación de una compañía o el fruto de la duración que tenga la relación. Aunque la mayoría de las empresas infravalora la importancia de sus políticas de confidencialidad y considera que es poco probable que influya en la percepción de los consumidores, más de la mitad de los consumidores encuestados (51%) afirma que evita tratar con compañías cuyas políticas de confidencialidad no le proporciona la seguridad necesaria. Al mismo tiempo, los consumidores sobreestiman la cantidad de información personal que las compañías pueden reunir sin su permiso. Los resultados sacan a la luz algunas paradojas entre las creencias de los consumidores y lo que realmente hacen con respecto a sus datos personales. Por ejemplo, aunque al 63% de los consumidores le preocupa que la cesión de información personal conlleve recibir correos electrónicos no solicitados (una práctica conocida como spam) más de las dos terceras partes de ellos afirman que están dispuestos a proporcionar de buena gana información personal a cambio de premios en metálico o comodidades en las compras. Desde la perspectiva europea y española, con diferencias significativas en el entorno legal pero con tendencias comparables en cuanto a la preocupación de la sociedad por la protección de los datos personales, estos resultados confirman el impacto real en el negocio que esta preocupación empieza a tener.

Según los resultados de este estudio de Accenture, los consumidores depositarían más su confianza y cederían sus datos privados a bancos y compañías de asistencia sanitaria, mientras que muestran mayores recelos con los comercios electrónicos y los supermercados. Para el socio de Accenture José Maixenchs, las compañías tienen que ocuparse de estas inquietudes extremadamente legítimas, ya que la importancia de la confidencialidad y la confianza en la protección de los datos personales seguirá aumentando, especialmente con la extensión del uso de tecnologías de identificación y localización, como por ejemplo la localización por radio frecuencia (RFID) que han suscitado preocupación entre los que piensan que las tecnologías pueden utilizarse para obtener información de los consumidores de forma encubierta.

MULTAS AEPD

España es el país de la UE que fija las multas más altas en protección de datos (El País 19-1-2004)

España es el país de la Unión Europea (UE) que ha fijado unas multas más altas a las empresas (hasta 600.000 euros) a la hora de proteger los datos confidenciales de los empleados. Así lo recoge un estudio realizado por del Consejo Superior de Cámaras que además critica la complejidad de la Ley de Protección de Datos. Sólo 400.000 empresas, de los dos millones que hay, se han adoptado a la norma.

Asimismo, el informe de las cámaras reclama que se cambie el actual sistema de financiación de la Agencia de Protección de Datos (a través de las multas a las empresas) para que se financie con una partida presupuestaria. Para las Cámaras, la complejidad y el desconocimiento de la ley hace que tan

sólo 400.000 empresas se hayan dado de alta hasta el momento en los ficheros de la Agencia de Protección de Datos.

Este dato fue manejado a modo de conclusión en la última reunión mantenida por las Cámaras con el director de la Agencia de Protección de Datos, José Luis Piñar. A este seminario asistieron especialistas de bufetes jurídicos como Cuatrecasas, Gómez Acebo y Pombo, Davara & Davara y firmas auditoras como Ernst & Young y PricewaterhouseCooper. También estuvieron presentes directivos de compañías relacionadas con el sector de la protección de datos personales como Equifax Ibérica, Informa, Camerdata, TPI, Páginas Amarillas, Marketing y Publicidad Directa, PDM, FECEMD y Consodata

La ley obliga a registrar en la Agencia todas aquellas bases de datos que contengan información de carácter personal, ficheros de clientes, o incluso la nómina de los empleados. Establece, asimismo, un tratamiento legal y leal de los datos, el deber secreto de cumplir medidas de seguridad de índole técnica y organizativa.

Según ha señalado Belén Veleiro, directora del Servicio Jurídico del Consejo Superior de Cámaras, es necesario hacer un esfuerzo para que las empresas conozcan el texto porque es el desconocimiento del mismo el principal escollo que argumentan las mismas compañías. Para Veleiro, se deberían fomentar los denominados códigos éticos o códigos tipo, que serían como una guía en el cumplimiento de la ley. Veleiro llama la atención sobre el riesgo de que ese desconocimiento de la ley por parte de las empresas haga que éstas paguen fuertes multas sin que haya intencionalidad de infringir la normativa.

Según las Cámaras, mientras que en Irlanda las sanciones económicas no superan 1.300 euros en España las sanciones pueden superar los 600.000 euros. Además, España penaliza hasta con siete años de pena de prisión la mala utilización de los datos. Grecia llega hasta los 10 años de prisión, la pena más alta en este aspecto, mientras que la multa máxima es de 146.735 euros.

LLAMADAS MOLESTAS

Un vecino, harto de la publicidad que abarrotaba, un día sí y otro también, el buzón de su piso, se dirigió a la Agencia de Protección de Datos para hacer valer ese derecho que todos tenemos a no recibir publicidad no deseada. El vecino, amparándose en la Ley Orgánica de Protección de Datos de Carácter Personal, realizó un escrito oficial en el que se oponía al uso publicitario o comercial de sus datos y se inscribió en una lista para que le diesen de baja y le borrarán de todas aquellas listas en las que figuraban sus datos personales. En otras palabras, se apuntó para que le desapuntasen.

Pasaron los meses, y su buzón, en teoría blindado a la publicidad, seguía prácticamente tan lleno como el mío, siempre abierto a las sugerencias del mercado. La diferencia era que mientras en mi buzón recibía cartas en las que se me decían cosas como «Estimado don Ramón: ¿Enhorabuena! Nos alegra escribirle para comunicarle que ha sido seleccionado, ¿ante notario!, para que le toque una millonada con la que ya se puede reír del mundo. Sólo tiene que comprar la cubertería X y participar en el concurso Y», en el suyo, o bien omitían siempre su nombre, o la publicidad era indiscriminada.

Me acuerdo del vecino y no porque la propaganda asalte el buzón, cosa a la que me resigno, sino porque asalta, a través del teléfono, mi casa. El teléfono, tal vez el mayor invento del siglo XX, puede llegar a ser el abanderado del intrusismo de la intimidad, el violador del domicilio. La publicidad a través del teléfono es incansable, no tiene horario, se adentra tanto en las casas de los descamisados, preguntando por los señores, como en las mansiones de los señores, anunciando ofertas para los descamisados. Eso sí, hay que reconocerle un don a la propaganda a través del teléfono: el de la inoportunidad.

Hasta las personas más educadas sucumben cuando en una tarde recibe tres llamadas indeseadas y seguidas, una anunciando una nueva función telefónica, otra ofreciendo un seguro de vida de película de intriga y otra solicitando no sé que datos para no sé cuál estadística. Por teléfono ni me interesan ni entiendo ni atiendo las ofertas. Lo único que quiero saber es adónde tiene que llamar uno para que no le llamen.

FUENTE: "EL COMERCIO DIGITAL" (ASTURIAS)

PRÓXIMAMENTE (15 de Diciembre) :

WWW.LOPD-PYME.COM

LA CESIÓN DE DATOS PARA PUBLICIDAD DEBE SER CONSENTIDA

La Agencia Española de Protección de Datos (AEPD) obligará a las empresas que realicen cesiones de datos de sus clientes a terceras empresas o que los utilicen para la promoción comercial de productos o servicios propios, a que precisen de forma "explícita" cuál es la finalidad del tratamiento de esos datos.

La AEPD advirtió de que "**no serán válidas expresiones genéricas**" por parte de las empresas a la hora de solicitar el consentimiento de sus clientes para la utilización de sus datos. Estas aclaraciones surgen tras la aparición de "**algunas informaciones difundidas en diversos medios de comunicación en relación a la Resolución de la Agencia Española de Protección de Datos**", en la que el pasado 11 de febrero se archivaron las denuncias interpuestas frente a Telefónica por la información que dirigió a sus abonados en 2003.

Para que el procedimiento sea lícito, "**tanto la normativa comunitaria como la española exigen que los abonados presten su consentimiento y que hayan sido informados previamente de la finalidad para la que se utilizan los datos**". Asimismo, recuerda que, según la normativa vigente, pendiente de ser sustituida por un nuevo Reglamento, se entiende que si en el plazo de un mes desde que el operador solicitó el consentimiento del cliente, "**éste no se hubiera pronunciado al respecto, se entenderá que consiente**".

Sin embargo, apunta la AEDP, la carga de la prueba sobre la recepción de la misiva en la que se solicita el consentimiento al abonado, recae sobre el operador, de modo que si el abonado niega haber **recibido la comunicación y prestado el permiso, será la empresa que utiliza los datos la que deberá acreditarlo**.

El consentimiento obtenido "será siempre revocable", aún en el supuesto de que el operador de telecomunicaciones acredite la recepción de una comunicación y el transcurso del plazo requerido para rechazar el tratamiento de sus datos.

Así, "el ciudadano podrá dirigirse al operador en cualquier momento para evitar el manejo de sus datos personales". Para denegar el consentimiento, los clientes no necesariamente deberán realizar el procedimiento por escrito, sino que podrán recurrir a fórmulas como la comunicación a través del servicio de atención al cliente o en las propias oficinas del operador.

FUENTE: DATOSPERSONALES.ORG

DEFENDAMOS NUESTROS DERECHOS

Continuamente oímos comentarios sobre las obligaciones que tienen las empresas de proteger los datos de sus clientes, proveedores, trabajadores, etc. pero, ¿a qué nos referimos exactamente cuando hablamos de protección de datos y cómo afecta a las empresas?

La informática ha avanzado tanto en los últimos años que las nuevas tecnologías hacen posible no sólo realizar tratamientos masivos de información referente a personas físicas, sino también manejar dicha información de tal manera que podamos saber aspectos de su vida que corresponden a sus ámbitos más íntimos y privados e incluso podríamos llegar a confeccionar sus perfiles de personalidad.

Este vertiginoso avance de las Nuevas Tecnologías en las empresas, ha desembocado en una urgente necesidad de proteger nuestra intimidad y nuestros datos personales. Tal es así que, para evitar que con la utilización de la informática se vulneren los derechos y libertades de las personas, nace la Ley Orgánica de Protección de Datos que sienta las bases para un adecuado tratamiento de los mismos.

En efecto, la Ley 15/1999 de Protección de Datos nace con la finalidad de proteger el derecho fundamental a la protección de nuestros datos, estableciendo obligaciones específicas a las empresas que traten este tipo de datos, pudiendo imponer la Agencia de Protección de Datos sanciones de importantes cuantías económicas a las empresas que no cumplan con las obligaciones que marca la ley.

Blanca Fdez-Galiano. Abogada

FUENTE : "EL HERALDO DE ARAGÓN"



PC EXPRESS SOLUTIONS S.L.

TABLA DE SERVICIOS DE CONSULTORÍA LOPD-LSSI						
TIPO DE EMPRESA (Personal+NºEquipos)/2	SOLUCIÓN Aplicada	PVP POR NIVEL		MANTENIMIENTO ANUAL		LSSI
		BÁSICO	MEDIO/ALTO	BÁSICO	MEDIO/ALTO	B/M/A
Hasta 10	TIPO A	850 €	950 €	215 €	250 €	250 €
Hasta 20	TIPO B	1.100 €	1.300 €	225 €	275 €	275 €
Hasta 30	TIPO C	1.500 €	1.700 €	255 €	300 €	300 €
Más de 30	TIPO D	ESTUDIO PREVIO DEL CLIENTE				

El tipo de solución aplicada (A,B,C y D) se calcula en concepto del tipo de empresa según el cálculo matemático establecido en la columna 1.

La cuota de mantenimiento anual está considerada a partir del segundo año. La cuota del primer año está incluida en la columna PVP por nivel.

Para las empresas con nivel de seguridad medio y alto existe la obligación de realizar una auditoría de forma bianual, no incluida en esta tarifa. (El precio de auditorías sucesivas se especifica en el presupuesto final al cliente, antes de la firma del contrato de servicios).