RESUMEN
NOTICIAS DE ACTUALIDAD EN PROTECCION DE DATOS
Y
BOLETÍN LOPD EN LA EMPRESA

PRODASUR SOFTWARE Y SERVICIOS, S.L.L.
C.I.F. : B92656206
Domicilio Avda. Comandante Benitez, 15 Local 2
29001 - Málaga
prodasur@prodasur.es
www.prodasur.es

CONSULTORES EN PROTECCION DE DATOS PERSONALES
SOFTWARE Y SERVICIOS PARA EMPRESAS

PRESENTACIÓN:

Nuestra entidad es una organización integrada por un grupo de profesionales dinámicos especialmente formados para afrontar los retos que presenten nuestros clientes, ofreciendo efectivas soluciones en materia de protección de datos. Como cada año y con el fin de acercar cada vez más la Ley de Protección de Datos de Carácter Personal 15/1999, a la PYME, hemos recopilado una serie de noticias de actualidad relacionadas con la protección de datos de carácter personal, casos de sanciones, inspecciones, noticias aparecidas en prensa, que muestran como en el día a día la LOPD se encuentra presente en prácticamente cualquier sector, siempre que se esté tratando con datos de carácter personal.

No pretendemos más que ampliar su conocimiento en protección de datos, mantenerle informado de actuaciones de la AEPD y transmitirles cualquier novedad que estimemos pueda ser de su interés.

Las noticias a continuación expuestas son un exponente de la concienciación e interés que poco a poco esta legislación está alcanzando en España.

902. 15. 22. 25 . www.edorteam.net .
edorteam@edorteam.net
prodasur@prodasur.es

MEMORIA AEPD 2011:

Extractos de interés en estadísticas:

Denuncias y reclamaciones registradas.
Tutelas de derechos resueltas.
Inscripción de titularidad privada.
Ficheros de videovigilancia.

PRODASUR SOFTWARE Y SERVICIOS, S.L.L.
C.I.F. : B92656206
Domicilio Avda. Comandante Benitez, 15 Local 2
29001 - Málaga
prodasur@prodasur.es
www.prodasur.es

CONSULTORES EN PROTECCION DE DATOS PERSONALES
SOFTWARE Y SERVICIOS PARA EMPRESAS

Estructura de la Memoria 2011

AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS

MEMORIA 2011

La primera parte está dedicada a exponer las actividades desarrolladas por la Agencia, analizando y valorando aquellos datos o tendencias que pueden resultar más relevantes para conocer la evolución de la protección de los datos personales en España. En este sentido, resultan especialmente reseñables los incrementos producidos tanto en el número de denuncias presentadas (más de un 50%), como en el de consultas ciudadanas (casi un 30%), así como el crecimiento en un 22% de los ficheros inscritos, por cuanto son reveladores del mayor grado de conocimiento y de concienciación de la ciudadanía en relación con sus derechos y están en el origen de la notable intensificación de la actividad de la Agencia. En segundo lugar, se presentan las principales resoluciones del año 2011 y los informes más relevantes evacuados durante este periodo, junto con las novedades más significativas habidas el ámbito normativo y jurisprudencial. En un capítulo específico se analizan los grandes retos que actualmente tiene planteados la protección de datos y se expone el modo en el que la Agencia los está afrontando: la seguridad y la protección de la privacidad en Internet, las demandas de “derecho al olvido”, el nuevo paradigma de cloud computing, los riesgos derivados de la geolocalización y del reconocimiento facial, el crecimiento de los flujos internacionales de datos fruto de la globalización, son objeto de estudio individualizado. Finalmente, se da cuenta de la evolución europea e internacional en materia de protección de datos y de la contribución de la Agencia Española a esta evolución, sea directamente o en el marco de las instituciones que están promoviendo los nuevos desarrollos.

La segunda parte de la Memoria, que se presenta bajo el título la "Agencia en cifras", ofrece información estadística detallada y tabulada en función de distintos indicadores con el fin de proporcionar una “imagen fiel” de la actividad desarrollada por la institución en sus diferentes áreas durante el año 2011.

José Luis Rodríguez Álvarez
DIRECTOR DE LA AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS

DENUNCIAS Y RECLAMACIONES REGISTRADAS

TIPO	2009	2010	2011	% VAR. 2010/11
Escritos de reclamación de tutela	1.832	1.657	2.230	34,58
Escritos de denuncia	5.310	5.045	7.648	51,60
TOTAL	7.142	6.702	9.878	47,39

TUTELAS DE DERECHO RESUELTAS

	ESTIMATORIA	ESTIMATORIA FORMAL O PARCIAL	DESESTIMAT.	ARCHIVO POR INADMISIÓN O DESISTIMIENTO	TOTAL
Cancelación	242	158	102	551	1.053
Acceso	176	148	84	219	627
Rectificación	24	27	21	75	147
Oposición	55	28	22	83	188
TOTAL	497	361	229	928	2.015

NOTA: En cada procedimiento puede tutelarse más de un derecho ARCO.

INSCRIPCIÓN DE TITULARIDAD PRIVADA

DISTRIBUCIÓN DE FICHEROS

	RESPONSABLES		FICHEROS	
	2011	TOTAL	2011	TOTAL
Comunidad Autónoma de Andalucía	37.421	128.254	92.393	369.907
Almería	3.394	12.412	8.558	37.294
Cádiz	5.025	15.159	11.823	41.207
Córdoba	3.682	12.168	8.860	34.537
Granada	4.175	17.968	11.056	57.038
Huelva	1.758	5.650	4.288	16.713
Jaén	2.855	10.275	7.717	33.368
Málaga	7.830	28.855	19.905	76.302
Sevilla	8.741	26.395	20.186	73.448

FICHEROS DE VIDEOVIGILANCIA

Año de Inscripción	Titularidad Privada	Titularidad Pública	Total
1994 - 2006	1.004	15	1.019
2007	4.637	86	4.723
2008	8.974	171	9.145
2009	21.403	275	21.678
2010	31.716	791	32.507
2011	36.308	495	36.803
TOTAL	104.042	1.833	105.875

NOTICIAS DE PRENSA DE INTERÉS EMITIDAS EN 2012

CONSULTORES EN PROTECCION DE DATOS PERSONALES
SOFTWARE Y SERVICIOS PARA EMPRESAS

PRODASUR SOFTWARE Y SERVICIOS, S.L.L.
C.I.F. : B92656206
Domicilio Avda. Comandante Benitez, 15 Local 2
29001 - Málaga
prodasur@prodasur.es
www.prodasur.es

04/12/2011 – El Supremo condena al Opus Dei y le hace borrar los datos de una ex miembro. FUENTE: elpais.com

La Sala de lo Contencioso del Tribunal Supremo ha condenado al Opus Dei a cancelar los datos personales de una mujer que se dio de baja en la organización y que intentó en vano que la entidad religiosa la borrase de todos sus archivos. El Supremo confirma un pronunciamiento anterior de la Audiencia Nacional, que ya falló a favor de la demandante. La sentencia ha condenado al Opus a pagar las costas hasta un límite de 3.000 euros.

En agosto de 2006, M.I.M., que se había dado de baja en la organización, reclamó a la Prelatura que borrase sus datos de todos sus archivos, en aplicación de la legislación de Protección de Datos. La entidad respondió que los únicos datos que se referían a la demandante "son hechos históricos realizados voluntariamente, que no pueden anularse". "En anotación marginal", apuntó, "se hará constar su deseo de que no tengan trascendencia externa".

Ante la negativa del Opus Dei, la mujer acudió a la Agencia Española de Protección de Datos (AEPD) que, tras estudiar su caso, dictó una resolución por la que instaba a la entidad a que, en el plazo de 10 días, le remitiera una certificación en la que quedase patente que se había "procedido a la cancelación de los datos" de la reclamante que constaban en sus archivos. Frente a la resolución de la AEPD, el Opus Dei esgrimió el Acuerdo de 1979 sobre Asuntos Jurídicos entre la Santa Sede y el Estado español que "protege la inviolabilidad de los archivos, registros y demás documentos de las instituciones y entidades eclesiásticas".

La sentencia del Supremo examina el Acuerdo entre España y la Santa Sede e interpreta que lo que se protege son los archivos y registros de cualquier intromisión procedente del Estado, por lo que "resultan inviolables frente al mismo". Pero esa inviolabilidad "no es predicable frente al ciudadano, cuando ejercita un derecho fundamental" sobre sus propios datos personales.

El Supremo también rebate el argumento del Opus Dei de que los datos de la reclamante no están contenidos en un soporte informático, como tampoco lo estaban los relativos a los libros bautismales que el tribunal no obligó a modificar cuando lo pidieron los apóstatas. Según el tribunal, la diferencia estriba en que mientras el Opus Dei tiene los datos organizados y clasificados de forma que son fácilmente localizables, los libros bautismales son una "pura acumulación de datos" que no están ordenados ni alfabéticamente, ni por fecha".

05/12/2011 – Fin a la impunidad en Internet. FUENTE: abc.es

Las amenazas y la suplantación de identidad crecen, pero ya no salen gratis. Jueces y policías miran a la Red

El anuncio contra el ciberacoso, que tuvo una cierta repercursión en internet, retrata con precisión el espanto. Vemos a un grupo de alumnos reunidos en el salón de actos, a una niña que toma la palabra, a otra que escucha. Y todo empieza...

—Ok, Lindsay, es tu turno.

—Hoy vamos a hablar de Patty. La mejor característica de Patty es que es estúpida, estúpida y fea. Todo lo que hace es feo. Miren cómo come, miren su cara. Mírenla, tiene el pelo grasoso y uñas sucias, me dan ganas de vomitar...

Y, unos minutos después, el mensaje que se quiere transmitir: «**Si no lo dirías en persona, ¿por qué hacerlo por internet?** Borra el ciberacoso. No lo escribas. No lo reenvíes».

Internet ha sido (aún es, para qué engañarse) un paraíso para los «trolls» (traducción: persona que solo busca provocar intencionadamente a los usuarios o lectores). La red (foros, redes sociales, blogs) está llena de comentarios malsonantes, en el mejor de los casos, o incluso de amenazas directas que requieren la intervención de la Policía, como les ha ocurrido a Eva Hache y Juanma Castaño. «La Policía Nacional detiene a un tuitero e imputa a otros tres por amenazar de muerte a un prestigioso periodista deportivo», anunció vía Twitter la Policía el pasado martes.

«Existe una leyenda urbana por la que parece que en internet todo el mundo puede hacer lo que quiera, pero noticias como estas demuestran que nadie es impune, que esto no es la ley de la selva», asegura Víctor Domingo, presidente de la Asociación de Internautas. Domingo destaca que **todavía hay mucha gente que cree que «el mundo virtual no tiene relación con el real**, que es un territorio anónimo», y cita como ejemplo las redes de pederastia desarticuladas continuamente por la Policía. «Los pederastas siguen sin saber que se puede seguir su rastro».

En internet también se deja huella. Lo que se escribe puede tener consecuencias. Así parece que ocurre ahora con comentarios inoportunos o amenazantes. He aquí algunos ejemplos de estos días: el alcalde de Madrid, Alberto Ruiz Gallardón, destituyó a Fernando Autrán, coordinador general de Circulación, por considerar inaceptables sus comentarios en Twitter sobre el grupo Prisa; la candidata del PP al Senado por Mallorca Francisca Pol dimitió por publicar en Facebook un fotomontaje de la ministra Chacón semidesnuda; y, al cabo, la Policía detuvo a los autores de las amenazas a dos rostros conocidos de la televisión, Eva Hache y Juanma Castaño. «**No he denunciado insultos, esos ya los damos por incluidos en nuestro trabajo**. Sí frases como "vamos a acuchillar a ese gusano"», según explicó el presentador de Cuatro.

Los comentarios de las noticias sobre fútbol y política acostumbran a estar llenos de improperios. Varios periódicos deportivos tuvieron que cerrar sus foros recientemente por los insultos dirigidos al segundo entrenador del Barcelona, Tito Vilanova, tras pasar por el quirófano. Y la etiqueta #AnimoAznar, en Twitter, sirvió hace días para «festejar» con bromas de mal gusto la supuesta muerte del ex presidente del Gobierno. En Ecuador, el presidente Correa denunció mensajes como este en su Twitter: «Los que te vamos a matar te saludamos».

La Agencia Española de Protección de Datos (AEPD) ha tramitado en los últimos meses varios procedimientos sobre casos de suplantación de identidad en las redes sociales, una de las tendencias más «de moda» en el lado oscuro de internet (sobre todo en España, según los datos de Eurostat). Empieza a ser frecuente, por ejemplo, el caso de ex parejas que cuelgan fotografías, vídeos o mensajes agresivos. Un caso característico de estos nuevos tiempos se refleja en

la resolución R/01716/2011 de la AEPD. Según los hechos probados, «la actual

pareja de la ex pareja» de la denunciante creó un perfil en la red social Badoo en la que tecleó este anuncio: **«Quiero quedar y follar con un chico de 22-40»**. En el perfil se incluía una fotografía de la denunciante —que empezó a recibir todo tipo de llamadas imaginables— y una descripción relativa a sus preferencias sexuales. El caso se saldó con una sanción de 2.000 euros. La Policía Nacional, que tiene más de 61.000 seguidores en su cuenta de Twitter (@policia), recuerda que «las amenazas graves, como otras formas de ciberacoso demostrado, suponen un delito perseguido por la Ley». La Brigada de Investigación Tecnológica de la Policía Nacional y el Grupo de Delitos Telemáticos de la Guardia Civil monitorizan continuamente la Red en busca de comportamientos delictivos. Así se encontraron con la alerta lanzada por Eva Hache en Twitter. Eran solo cinco palabras: «Hola, buenas noches, señor agente», y adjuntaba un «pantallazo» con alguno de los «tweets» de su ciberacosador, como **«Yo que tu no saldría sola de casa»**, o «Voi al teatro i te apuñalo delante de todo el mundo» (sic).

28/12/2011 – La Agencia de Protección de Datos abre consulta sobre seguridad en la nube. FUENTE: expansión.com

Madrid, 28 dic (EFE).- La Agencia Española de Protección de Datos (AEPD) ha abierto hoy consulta pública sobre las implicaciones legales en materia de protección de datos de los servicios virtuales o computación en la nube, ya que considera que la adecuación de las normas de protección de datos a estos entornos es esencial.

La consulta estará abierta en la página web de la AEPD hasta el 27 de enero y a ella están invitados entidades prestadoras de estos servicios y usuarias, particulares, académicos, expertos y todos los interesados en la materia.

En nota de prensa esta agencia explica que la computación en la nube constituye un modelo de prestación de esta oferta de tecnología en auge y que su uso suscita interrogantes sobre las garantías aplicables en el marco de estos servicios.

Con esta consulta, la AEPD quiere tener un conocimiento preciso de las experiencias, opiniones y condicionamientos con los que se encuentran usuarios y prestadores de este tipo de oferta.

La agencia plantea preguntas sobre la legislación aplicable, garantías en el marco de las relaciones de prestación de servicios en nube o su impacto en el régimen que regula las transferencias internacionales. EFE.

10/01/2012 – La Agencia de Protección de Datos expedienta al Ayuntamiento de Málaga por sus cámaras de vigilancia. FUENTE: diariosur.es

La Agencia de Protección de Datos obliga a ello ya que captan imágenes de la vía pública. Las cámaras captan imágenes de los jardines de Pedro Luis Alonso o del Paseo del Parque, lo que no es legal.

JAVIER GARCÍA RECIO Las cámaras que el Ayuntamiento de Málaga tiene colocadas en el entorno de la casa consistorial, en la avenida de Cervantes, para vigilar los accesos al edificio infringen la ley, por lo que el equipo de gobierno del Ayuntamiento de Málaga va a proceder en los próximos días a la reubicación y adaptación de las mismas, en cumplimiento del requerimiento exigido por la Agencia Española de Protección de Datos (AEPD), según reconoció ayer lunes el concejal de Seguridad, Julio Andrade.

El Ayuntamiento tiene colocadas varias cámaras junto a las esquinas del edificio consistorial en unas torres de gran altura que tienen como misión vigilar los movimientos de entrada y salida del edificio. La Agencia de Protección de Datos, en una resolución del año pasado, requiere a las autoridades municipales para que «sustituyan o reubiquen» dichas cámaras. La AEPD entiende que la instalación de las cámaras infringe la Ley de Protección de Datos al abarcar más allá de lo que es el propio edificio y captar la vía pública y las zonas aledañas, lo que no está permitido, ya que las cámaras no pueden captar imágenes de la vía pública.

Algunas de las cámaras instaladas alcanzan incluso los jardines de Pedro Luis Alonso, mientras que otras captarían el paso de viandantes por el paseo del Parque e incluso por algunas de las calles laterales que rodean el edificio del Ayuntamiento.

Reubicar las cámaras

La ubicación y captación de imágenes de las cámaras están incumpliendo, según el organismo, el artículo 6 de la Ley de Protección de Datos, que señala que «el tratamiento de los datos de carácter personal requerirá el consentimiento inequívoco del afectado, salvo que la ley disponga otra cosa».

El concejal de Seguridad reconoció la irregularidad, «ya que el ángulo de visión de nuestras cámaras iba más allá del edificio».

Andrade explicó que el Ayuntamiento cumplirá en los próximos días el requerimiento de la Agencia de Protección de Datos, antes de que acabe el plazo instado por ésta, ya que de lo contrario se enfrentaría a una sanción económica por falta muy grave que podría llegar a los 300.000 euros.

En estos momentos los responsables del área de Seguridad están a la espera de un dictamen de la empresa encargada de la instalación y mantenimiento de las cámaras para «adoptar la solución que, dentro del respeto a la ley, sea más factible y, sobre todo, más económica».

Con todo, los técnicos ya han avanzado que lo más factible es la reubicación de las cámaras que sean necesarias, ya que su colocación en otros lugares sería más costosa.

23/01/2012 – La Agencia de Protección de datos alerta a menores sobre la privacidad en la red. FUENTE: abc.es

Con motivo de la celebración del Día Europeo de la Protección de Datos, la Agencia de Protección de Datos de la Comunidad de Madrid (Apdcm) ha difundido un vídeo para llamar la atención de los más jóvenes sobre la publicación de fotos, vídeos y otros datos personales en las plataformas sociales o sobre los riesgos del contacto con personas desconocidas en la Red.

Bajo el eslogan '¿Por qué hacerlo en Internet?', en el vídeo, a través de dos 'spot', se plantean situaciones en las que una persona joven se encuentra en una situación cotidiana con un extraño y le explica cuestiones privadas relativas a su vida íntima.

Concluye con una reflexión del director de la Apdcm, Santiago Abascal, sobre aquello que se divulga en la Red y que no se explicaría nunca, pública y presencialmente, en la vida cotidiana, y con una serie de recomendaciones para los jóvenes que fomenten un uso seguro de Internet y las redes sociales.

Además, la Apdcm ha querido lanzar una declaración en favor de la protección de la privacidad de los menores dado que, tal y como explica Abascal en un comunicado remitido a Efe, "los menores se encuentran entre los colectivos más expuestos a las amenazas relacionadas con la difusión pública de los datos privados en Internet".

Y añade: "La prematura incorporación de los más jóvenes a las redes sociales debe impulsar a todos los organismos implicados, desde la familia y las escuelas, hasta las Administraciones, hacia el desarrollo de iniciativas que faculten a los más jóvenes para saber identificar, distinguir y gestionar adecuadamente los peligros vinculados a las redes sociales".

15/02/2012 – Bancos podrán consultar bases de datos de solvencia sin consentimiento del afectado. FUENTE: europapress.es

Las entidades financieras podrán consultar bases de datos de solvencia antes de dar un crédito sin necesidad de recabar el consentimiento del interesado, aunque sí deberán informarle de este trámite, según una de las consecuencias de la sentencia del Tribunal Supremo sobre protección de datos destacada por la Asociación Nacional de Establecimientos Financieros de Créditos (Asnef).

De acuerdo a Asnef, la sentencia del Supremo permite que determinados tratamientos realizados por el sector financiero en los que existe claramente un interés legítimo por ayudar a cumplir con las normas comunitarias y nacionales sobre el crédito responsable, como es la consulta a bases de datos de solvencia y positivas, "pueden a partir del 24 de noviembre de 2011 ser legítimos sin necesidad de recabar el consentimiento del interesado, que debe ser adecuadamente informado sobre la existencia de este tratamiento".

Para Asnef, el Tribunal Supremo ha puesto fin a "una década de incoherencia" y ha armonizado la Ley Orgánica de Protección de Datos de Carácter Personal (LOPD) española a Europa, tras la Sentencia que el Tribunal de Justicia de la Unión Europea (TJCE) emitió en noviembre sobre la figura del consentimiento.

"Desde ayer, 14 de febrero, en España se ha producido una completa y adecuada armonización a la Directiva Comunitaria en materia de Protección de Datos ya que se puede realizar el tratamiento de los mismos además de cuanto exista consentimiento del interesado, cuando exista un interés legítimo tanto de la entidad que trate los datos como de los terceros a los que se cedan los mismos, siempre que no se vulneren los derechos y libertades de los afectados", señala la asociación.

Esta reivindicación que ASNEF ha abanderado desde el 2007, para no estar en desventaja con sus homólogos europeos, ha sido reconocida tanto por el Tribunal de Justicia de la Comunidad Europea1 como por el Tribunal Supremo español.

Por otra parte, y para que se produzca un punto de equilibrio, habrá de valorarse caso a caso cuando existe "de facto" interés legítimo para tratar/consultar datos sin el consentimiento del usuario.

20/02/2012 – El 66% de las empresas desconocen la obligación de proteger los datos de clientes. FUENTE: abc.es

El 66% de las empresas españolas podrían enfrentarse a sanciones debido al desconocimiento que reconocen tener sobre su obligación de proteger los datos de sus clientes, ha informado hoy la empresa Iurismática, citando datos del Instituto Nacional de Tecnologías de la Comunicación (Inteco).

Por este motivo, Iurismática y la patronal guipuzcoana Adegi han firmado un acuerdo "para la difusión del conocimiento en materia de Derecho de la Tecnologías de la información y Telecomunicaciones en las empresas" del territorio.

Gracias a este acuerdo, las compañías "podrán asesorarse de manera gratuita en materias como propiedad intelectual, propiedad industrial, factura y firma electrónica, protección de datos de carácter personal, comercio electrónico y redes sociales", entre otros ámbitos

09/03/2012 – Multa de 40.000 euros por anotar una deuda errónea de un céntimo. FUENTE: eleconomista.es

Mantener por un error informático una deuda en un fichero de morosos puede costar muy caro a una empresa, por pequeño que sea el pasivo que conste registrado.

Una reciente sentencia de la Audiencia Nacional condena a una conocida empresa de telecomunicaciones a pagar 40.000 euros a un particular **por no eliminar de su registro de datos una deuda de 0,01 euros, lo que supuso que siguiera constando como moroso** en el fichero de la Asociación Nacional de Establecimientos Financieros de Crédito (Asnef).

El fallo, del que es ponente la magistrada Buisán García, resuelve el caso de un cliente que constaba registrado por una deuda de 62,07 euros tanto en el fichero de la empresa como en el de Asnef. Tras reclamar la improcedencia del pago de dicha cantidad, la empresa rectificó y procedió a retirar la deuda. Sin embargo, por un error aritmético -provocado por el cálculo del IVA aplicable- la deuda no se eliminó totalmente, quedando un resto de 0,01 euros que provocó que el cliente siguiera constando como moroso para ambas entidades.

Irrelevancia de la cuantía

La sentencia, con fecha de 2 de diciembre de 2011, recuerda que "no es óbice a la comisión de la infracción del principio de calidad del dato el ínfimo importe de la deuda anotada, pues en definitiva, y a pesar de dicha cuantía, desde el momento en que existen datos de una persona en un fichero de morosidad, se está atribuyendo la condición de deudor moroso a la misma".

Del mismo modo, tampoco se toma en consideración que la empresa no hubiera dado de alta dicha deuda en el Asnef, ya que "con independencia de que dicha alta derivara de un mero error en la operativa aritmética tras la extinción del saldo de 62,07 euros, (...) **son las entidades gestoras de los datos personales (...) las responsables de su exactitud y puesta al día**".

27/04/2012 – La Justicia perdona a Telefónica una multa por mandar 46 millones de SMS de spam. FUENTE: lainformacion.com

La **Audiencia Nacional** ha eximido a la compañía presidida por **César Alierta** de pagar una sanción de miles de euros por haber realizado un envío masivo de 46 millones de mensajes de texto. La maniobra fue denunciada por la **Agencia de Protección de Datos**, tras alegar que los destinatarios no podían oponerse a recibirlos.

La **Justicia** ha dado la razón a Telefónica, que se ha librado de pagar una multa de miles de euros por mandar **publicidad** de manera masiva. Lo que se conoce como *spam*.

Y es que, tras dos años de pleitos judiciales, **la Audiencia Nacional ha reconocido que la compañía presidida por César Alierta actuó de forma correcta**, en contra de lo que alegaba la Agencia Española de Protección de Datos (AEPD).

Todo empezó en el año 2010, cuando la institución pública puso una **sanción de 50.000 euros** a la compañía.

El motivo de la multa era el **envío masivo ilegítimo de 46 millones de SMS publicitarios** con estos textos: "MoviStar publi. Este es tu SMS de la SUERTE. Puedes ganar 1MILLON de euros! Y 50.000 CADA DIA! Hoy mismo! Envia ahora MILLON al #### (1,2+IVA)". O bien, "MoviStar publi. Soy la suerte y quiero cambiar tu vida. MoviStar da 1MILLON y 50.000 euros hoy. Juega estoy de tu lado. Envia MILLON al #### (1,2+IVA)".

La Agencia de Protección de Datos consideró que dichos mensajes de texto no daban la posibilidad al destinario de oponerse a su recepción de manera fácil y gratuita.

Sin embargo, este argumento de la AEPD para sancionar a la multinacional no ha sido suficiente para la Justicia española.

¿El motivo? Telefónica recurrió la multa asegurando que los SMS sí que daban la posibilidad de paralizar su recepción. Los primeros SMS incluían el texto "*NO MÁS PUBLI AL 1010*", y los posteriores incluían la referencia "*Info:movistar.es*", esto es, la web en la que podrían informarse y frenar los envíos.

Esta justificación ha sido suficiente para la Audiencia Nacional, que ha estimado el recurso de Telefónica tras constatar que **una web en los SMS es suficiente para entender cumplido el deber de dar información para oponerse** a los envíos.

Según el despacho de abogados especializados en el anonimato en internet, **www.salirdeinternet.com**, "las sanciones por spam (o envíos comerciales no consentidos), son frecuentes y ya solo la cuantía de las multas desaconsejan utilizarlos. La AEPD ha llegado a sancionar a un infractor con 30.001 euros por enviar de cuatro correos electrónicos de este perfil".

05/05/2012 - Una procuradora, multada por hablar en su blog de una gijonesa. FUENTE: lne.es

Expuso en su blog personal un caso con nombres y apellidos e, incluso, foto. Y eso le ha traído consecuencias. La Agencia Española de Protección de Datos acaba de sancionar con 2.000 euros de multa a una procuradora de Cartagena que incluyó en una página web personal datos de una ciudadana que había iniciado un procedimiento penal en un Juzgado de instrucción de Gijón. La letrada ahora demandada llegó incluso a acompañar la información del caso con una foto de la víctima que había extraído de la página personal de Facebook de la mujer. Además, la procuradora había participado en distintos foros de internet relacionados con la violencia de género y las denuncias falsas.

El escrito colgado en la red contenía, en palabras de los responsables de la resolución de la Agencia Española de Protección de Datos, «variada información sobre las circunstancias personales de la demandante», además de su fotografía. «El tratamiento de datos de carácter personal que figuran en internet -como la fotografía de Facebook- por persona o entidad distinta a los interesados precisa el consentimiento previo de los mismos no pudiendo considerarse que tal fuente es de acceso público». Siguiendo este razonamiento, la actuación de la demandante no cumple, según los encargados del caso, con los condicionamientos y supone una vulneración de la Ley Orgánica de Protección de Datos al no constar que mediara en el procedimiento el consentimiento de la demandante.

«Es cierto que la realidad de internet requiere realizar una interpretación del principio de consentimiento que evite una aplicación estricta que la paralizaría o la convertiría en una red profusa en vulneraciones de datos personales de millones de personas», reflexionan los juristas. «De ahí que no sea conveniente realizar una interpretación maximalista del requerimiento del consentimiento», concluyen. De hecho, la letrada tenía la autorización

expresa del demandado para reproducir el escrito de alegaciones que había presentado en el caso que le enfrentaba con la mujer, pero no la de la demandante.

En este caso los datos son, además, «especialmente sensibles» al haber trascendido a la esfera pública circunstancias muy concretas de la demandante.

07/05/2012 – Protección de Datos multa con 200.000 euros a la productora de ANTENA3: Rico al instante. FUENTE; elpais.com

La Agencia Española de Protección de Datos (AEPD) ha impuesto una multa de 200.000 euros a la empresa Ocio Factory Time por el envío de publicidad masiva para un concurso de televisión. Esta compañía mandó casi 40 millones de mensajes a móviles, en muchos casos, sin el consentimiento de los destinatarios. Los SMS eran un reclamo para el espacio de Antena 3 *Rico al instante.*

Este aluvión de spam (publicidad no deseada) tuvo una rápida reacción por parte de los usuarios. Entre el 4 de enero y el 7 de febrero de 2011, la AEPD recibió 333 escritos de personas que denunciaban haber recibido en sus teléfonos móviles mensajes no solicitados en los que se promocionaba Rico al instante, un concurso que ofrecía la posibilidad de ganar 200.000 euros y solicitaba el envío de un SMS. Los mensajes eran sugerentes y tentadores: "(TF) Quieres ganar 200.000 E por lo mismo que cuesta 1 café? Ven al programa! Con solo responder RICO al 25354 podrías concursar en directo (1,42Eur.xsms)".

Rico al instante se emitió en Antena 3 en enero del año pasado. La cadena encargó la producción a Zed Worldwide, que más tarde se denominó Ocio Factory Time. Durante la campaña de promoción se remitieron 35.976.137 SMS y en noviembre la AEPD acordó iniciar un procedimiento sancionador por un eventual "envío masivo" de publicidad que podría vulnerar la ley. Zed alegó que no había incumplido la normativa, ya que los destinatarios de los mensajes se podían oponer a los envíos. Argumentó que la gran mayoría (el 99,8%) incluían la opción de rechazar más publicidad en el futuro ("Nomaspubli") y que solo en el caso de 8.170 mensajes (el 0,0022%) no se ofrecía esta posibilidad. "Dada la magnitud de la campaña", dijo, el porcentaje de supuestos incumplimientos es "sumamente ínfimo" y "denota" el propósito de cumplir la ley.

Pero la AEPD se ha mostrado inflexible. Percibe que la productora ha cometido dos infracciones graves. La primera —tras la tramitación de 330 denuncias, aunque llegaron 100 más— por 451 envíos de mensajes a teléfonos móviles sin consentimiento (50.000 euros). La segunda, por los 8.170 SMS en los que no se daba a los usuarios un medio de oposición "sencillo y gratuito" para recibir comunicaciones comerciales (150.000 euros).

La sanción pudo haber sido mayor, ya que la primera propuesta era de 230.000 euros. Miguel Cobacho, miembro del despacho de abogados salirdeinternet.com, afirma que es una de las mayores multas impuestas en España por estas prácticas. Mantiene que, si bien conviene poner coto a estas actividades, "lo cierto es que los empresarios en muchas ocasiones no saben qué sanción se les impondrá" y recuerda que la AEPD decretó una multa de 30.000 euros por enviar cuatro correos electrónicos y 50.000 por mandar 46 millones de mensajes.
Tras esta sanción, contra que la cabe recurso, la productora de *Rico al instante* ha pasado a ser pobre al instante.

21/05/2012 – El seguro crea un gran fichero para prevenir fraudes en el ramo de autos. FUENTE: Cincodias.com

La industria del seguro levanta una gran muralla contra la acción de los criminales especializados en simular siniestros para cobrar indemnizaciones. El sector ultima una gran base de datos que contendrá información sobre los vehículos que han desaparecido debido a un robo o que han quedado completamente siniestrados tras un golpe o un incendio. El fichero cuenta con el beneplácito de la Agencia Española de Protección de Datos (AEPD). Su función será identificar a los coches afectados por alguno de los supuestos citados. No tiene por objeto mantener un listado de las personas que han recibido el pago de una aseguradora. Los automóviles se monitorizarán a través del número de bastidor o Número de Identificación del Vehículo (VIN, por sus siglas en inglés).
Fuentes aseguradoras indican que se han adherido a la iniciativa 15 entidades que agrupan el 75% de las primas del ramo. El programa entrará en pleno funcionamiento en enero de 2013, cuando esté apuntado todo el sector. Tirea actúa como gestora. El alcance del fichero antifraude es, de momento, limitado. Solo afectará al ramo de autos. Quedan al margen otras líneas de negocio de peso como los seguros de vida riesgo, las pólizas industriales y otros ramos masa como el de hogar o el de salud.

Los seguros de automóviles han sido los elegidos como el primer paso porque constituyen la línea de negocio más relevante para el seguro y donde se concentran siete de cada diez intentos de fraude detectados. La ley exige que todo vehículo esté por lo menos cubierto ante las reclamaciones de terceros por una póliza de responsabilidad civil. A partir de ahí, se pueden sumar con carácter voluntario coberturas sobre los daños propios (lunas, robo...) hasta llegar al todo riesgo, con o sin franquicia. En España circulan unos 29 millones de automóviles. Se estima que medio millón de vehículos carecen del seguro preceptivo. La mayoría son motos y ciclomotores.

El fichero antifraude se centra en los casos por sustracción del vehículo en sí y donde el coche queda destrozado porque son siniestros susceptibles de ser simulados por bandas de crimen organizado al reportar indemnizaciones elevadas. Quedan al margen del escrutinio sectorial los golpes de chapa, los robos de elementos del vehículo y los accidentes con daños personales.

Vacas flacas en el seguro de autos

Las aseguradoras de autos facturaron 11.535 millones de euros en 2011, según Icea. Su volumen de negocio ha disminuido un 2,29% frente al año anterior. Sobre el gremio pesa como una losa la caída de las ventas de coches. Los grupos más importantes son Mapfre (21% del mercado), Allianz (11,62%), Axa (11,50%), Mutua Madrileña (11,25%) y Línea Directa (5,76%).

El seguro dispone de convenios destinados a agilizar el pago de indemnizaciones entre compañías en caso de accidentes (Cicos), conocer el historial de los conductores (Sinco) así como para realizar estudios sectoriales. La nueva Ley de Supervisión de Seguros Privados (LSSP) contempla en su artículo 103 sobre protección de datos personales la posibilidad de que se constituyan "ficheros comunes cuya finalidad sea prevenir el fraude sin que sea necesario el consentimiento del afectado".

Pero la norma, que entrará en vigor previsiblemente a finales de año, pone algunos límites. De entrada, será necesario comunicar al afectado "la introducción de sus datos, quién es el responsable del fichero antifraude y de las formas de

ejercicio de los derechos de acceso, rectificación y cancelación y oposición". En el ramo de salud es muy restrictivo el tratamiento de datos personales. En ese caso solo se podrá manejar información personal con el consentimiento expreso del afectado.

24/05/2012 – La subcontratación en el cloud computing. FUENTE: expansión.com

Uno de los principales problemas que encuentran las empresas españolas al intentar firmar contratos de cloud computing con empresas extranjeras, generalmente norteamericanas, está asociado a la estricta normativa que en materia de protección de datos personales rige en Europa.

Sin embargo, las empresas están encontrando soluciones que consisten en pactar con el proveedor de cloud computing unas medidas que tengan un efecto equivalente a las exigidas en la ley. La Agencia Española de Protección de Datos (AEPD) se ha pronunciado recientemente a favor de escapar de una interpretación literal de la Ley Orgánica de Protección de Datos (LOPD) y de su Reglamento (RLOPD), para buscar soluciones alternativas que se adapten a las peculiaridades del cloud computing y permitan garantizar la protección de los derechos de los afectados.

En este artículo analizaremos los puntos en los que se han producido ciertos avances.

1. Ubicación de los datos

Hoy en día el almacenamiento de datos ha sufrido una importante reducción de costes, debido principalmente a la caída del precio de los soportes informáticos. Ello ha generado una sana competencia entre los principales proveedores de servicios de hosting.

El crecimiento y la optimización de las redes y de los protocolos de comunicación y de compresión de datos también han influido en la existencia de una oferta económica y global.

La libre competencia en el mercado internacional y la amplitud de la oferta permite a las empresas de cloud computing escoger los proveedores de hosting que más les convienen en calidad y precio, pudiendo éstos encontrarse en cualquier país y latitud. Últimamente parece que están emergiendo las latitudes frías, donde el coste de refrigeración de los servidores es muy reducido.

Todo ello contribuye a que los datos gestionados por el proveedor de cloud computing puedan tener múltiples ubicaciones a lo largo de la vigencia del contrato. Si las oscilaciones en los precios del hosting son importantes, el proveedor de cloud computing podría cambiar la ubicación de los datos con una mayor frecuencia.

Todo ello tiene ventajas y desventajas. Un ventaja se produciría en materia de seguridad, ya que los posibles interesados en conseguir un acceso ilegal a los datos no podrían saber dónde se encuentran éstos en cada momento.

Una desventaja clara sería que, legalmente, la empresa cliente estaría obligada a saber dónde se encuentran los datos personales de sus clientes y trabajadores, para poder comprobar si se hallan en un país que ofrece una protección equivalente a la Unión Europea o que tiene un convenio de Puerto Seguro como Estados Unidos.

En caso de ser así, la empresa cliente debería solicitar una autorización al Director de la AEDP, al tratarse dicho hosting de una transferencia internacional de datos a un país sin protección equivalente a la de la UE. Durante el ejercio 2011 el Director de la AEPD autorizó 735 transferencias a estos países. De ellas, el 84,2% correspondió a transferencias de datos a encargados del tratamiento, es decir, a empresas de outsourcing, cloud computing, call centers externalizados y otros servicios con tratamiento de datos personales.

Avances

1. Desde un punto de vista legislativo, el avance que se está produciendo en esta materia es que el legislador está reconociendo el carácter global de las redes de telecomunicaciones y la necesidad de bajar el listón en relación a los requisitos exigidos para las transferencias internacionales de datos.

Pensemos que hay supuestos en que los es imposible cumplir estos requisitos. Por ejemplo, los sistemas de enrutamiento analizan en tiempo real los tiempos de salida y llegada de los paquetes IP y que, en cualquier momento pueden dirigir el tráfico a través de nodos situados en países sin protección equivalente. Aunque sería un tránsito efímero, la caché del router puede conservar esos datos durante un tiempo indeterminado.

2. Desde un punto de vista técnico, algunos proveedores de cloud computing están recurriendo a sistemas de informática distribuida en el que cada servidor tiene fragmentos o chunks tipo P2P. Ello hace que las cadenas de datos estén truncadas, y que sea imposible recuperar información útil desde un solo servidor.

Valorado jurídicamente, este sistema es mucho más potente que la disociación o la anonimización de los datos, ya que la dispersión de datos fragmentados en diferentes países permitiría eludir la figura de la transferencia internacional de datos.

En el caso de la disociación, los datos no podrían ser relacionados con las personas a las que van referidos, pero seguirían siendo datos inteligibles, con información suficiente, en algunos casos, para asociarlos a los afectados. En la fragmentación no existiría este riesgo, ya que cada fragmento incluiría datos ininteligibles.

Además, en la disociación, el tratamiento se realiza normalmente en bloque, y el proveedor tiene acceso inteligente a todos los datos. En cambio, en la fragmentación, el proveedor sólo tiene un acceso no inteligente a una parte de la base de datos. Es un acceso no inteligente porque se trata de un mero almacenamiento de bits no inteligibles y porque el proveedor no realizará ningún esfuerzo intelectual para tratar los datos.

2. Selección e identificación de las empresas subcontratadas

La LOPD y su Reglamento establecen requisitos muy claros y exigentes en relación a la cadena de custodia y tratamiento de datos personales por parte de

un proveedor que subcontrate los servicios de otras empresas. Estos requistos, detallados en el artículo 21,2 del RLOPD y en la Sentencia del Tribunal Supremo de 15 de julio de 2010, son los siguientes:

1. En el contrato con el proveedor se deben detallar los servicios que van a ser objeto de subcontratación.

2. También deben quedar identificadas las empresas subcontratadas.

4. El cliente debe autorizar cada una de las subcontrataciones.

3. Debe existir un contrato entre el proveedor y las empresas subcontratistas que incluya las mismas garantías y obligaciones del contrato principal.

Avances

1. Desde un punto de vista jurídico, la propia AEPD ha reconocido en diversas ponencias que las características particulares de los contratos de cloud computing impiden aplicar literalmente los requisitos de la subcontratación.

Por un lado, el proveedor de cloud computing presenta, en la mayoría de los casos, una oferta prediseñada con unas aplicaciones estándar. En función del tipo de servicio de cloud computing contratado habrá un distinto nivel de implicación del usuario y por lo tanto, el nivel de personalización del servicio y del contrato será también distinto. Tengamos en cuenta que estos servicios se regulan normalmente en un contrato de adhesión, y que el proveedor va a resistirse a cambiar sus cláusulas, dada la necesidad de disponer de un régimen uniforme para todos los clientes y para todos los países.

Por otra parte, el proceso de selección de las empresas que el proveedor de cloud computing contrata está basado en las oscilaciones de la oferta de servicios como el almacenamiento de datos, y por lo tanto esta sujeto a una evolución constante. Ello impide establecer una lista permanente de empresas subcontratadas como anexo al contrato. La AEPD en este sentido recomienda una remisión a una lista dinámica ubicada en el sitio web del proveedor, que vaya siendo actualizada constantemente.

2. Desde un punto de vista técnico debemos tener en cuenta varios puntos importantes. Las empresas de cloud computing se están convirtiendo en proveedores críticos de las empresas. Las empresas que administran infraestructuras críticas tienen que recurrir a medidas de ocultación como primera barrera de seguridad frente a ataques. Un ejemplo sería no dar a conocer la ubicación de sus CPD o pixelar las fotografías aéreas de sus instalaciones en Google Maps y otros servicios similares. De la misma manera sería interesante no desvelar la identidad del proveedor de cloud computing cuando éste administra recursos críticos.

En la tarea de crear esas primera barreras a un eventual ataque, la propuesta de relacionar a las empresas subcontratadas en el sitio web del proveedor de cloud computing no parece recomendable, salvo que ésta se encuentre en una zona privada a la que sólo el cliente tenga acceso.

Pensemos que, en materia de seguridad, una cadena es tan fuerte como el más débil de sus eslabones, y es inútil que una empresa concentre todos los recursos

posibles en la protección de sus activos intangibles y de los datos personales de sus clientes si después externaliza parte de su gestión a un proveedor que no realiza los mismos esfuerzos, o genera una cadena de subcontrataciones que van diluyendo, en cada nuevo nivel de subcontratación, el control sobre dichos activos. También hay que reconocer que el proveedor, como responsable frente a muchos clientes, puede haber invertido más en seguridad que el propio cliente, pero no podemos dejar de tener en cuenta la teoría del riesgo moral, que demuestra que nadie protege con tanto esmero sus activos como su propietario. Además, si miramos la casuística de los ataques, filtraciones, siniestros y descuidos en materia de seguridad que se han llegado a los medios de comunicación, veremos un incremento en la implicación de los proveedores en estos incidentes y una clara migración de estos ataques hacia ellos.

Estos factores de riesgo hacen aconsejable una labor de control sobre el proveedor de cloud computing y de éste sobre sus subcontratistas. El fenómeno de la externalización está haciendo que nuestros proveedores y sus subcontratistas se conviertan en gestores de nuestros activos intangibles y de nuestra reputación corporativa, por lo que no debe ser raro aplicar fórmulas de auditoría y control similares a las funciones de auditoría y control internos. Alguna empresas consideran suficiente solicitar el informe SAS70, pero en el caso del cloud computing sería necesario ampliar el alcance del control.

Otro factor importante a tener en cuenta es la **virtualización**. ¿Hasta qué punto podemos seguir hablando de hosting en entornos virtualizados gestionados directamente por el cliente? La fórmula se asemeja más a un housing virtual que a un hosting. Una máquina virtual es, como dice la palabra, una máquina, una unidad a la que el propietario del servidor físico no tiene acceso inteligente.

Si a ello unimos el proceso de cifrado y fragmentación de los datos, no debería seguir considerándose encargados o subencargados del tratamiento a los subcontratistas que simplemente dan alojamiento a una máquina virtual llena de datos ininteligibles. Aunque la LOPD incluye la simple conservación de datos personales en la definición de tratamiento, deberíamos preguntarnos si un paquete fragmentado de una gran base de datos puede seguir siendo considerado como un contenedor de datos personales, y si el simple almacenamiento de ese paquete fragmentado en una máquina virtual sin acceso inteligente del propietario del servidor es realmente una tratamiento de datos personales.

31/05/2012 - La Agencia de Protección de Datos denuncia a Sanidad por dejar filtrar datos de pacientes desde su web. FUENTE: leonoticias.com

La Agencia Española de Protección de Datos ha emitido una resolución en la que pone de manifiesto que la Consejería de Sanidad cometió dos infracciones de carácter grave contra la Ley de Protección de Datos de Carácter Personal, (LOPD), al permitir que se filtraran datos de pacientes a través de su web. En concreto, considera que vulneró el deber de secreto garantizado, al haber posibilitado que terceras personas tuviesen acceso a datos personales de usuarios, y que no impidió "de manera fidedigna" que un usuario accediera a datos de otros ciudadanos.

La resolución, conocida por Ical, pone fin a la vía administrativa, y se pondrá en conocimiento del Defensor del Pueblo. Según fuentes del despacho de abogados especializados en protección de datos www.salirdeinternet.com, esta infracción podría haber supuesto para una empresa una sanción de hasta 600.000 euros, teniendo en cuenta que, por ejemplo, Vodafone fue sancionada con 100.000 euros por una incidencia que provocó que se pudiera acceder a los datos de 22 clientes y que solventó en 24 horas.

Los hechos se remontan a marzo de 2011, cuando un usuario de Sacyl accedió a la web de la Consejería para realizar una reclamación, y comprobó que al cambiar en la URL el número de reclamación podía ver las presentadas por otros usuarios. Entre otros datos personales, relativos al nombre, apellidos, dirección, correo electrónico, se podían leer las reclamaciones o sugerencias y, en algunos casos, datos vinculados a su salud.

El denunciante, cumplimentó un documento alertando a la Consejería de la incidencia, y desde la Dirección General de Planificación, Calidad y Ordenación se le acusó recibo de la reclamación. Si bien, comprobó que el problema no se había subsanado, por lo que puso los hechos en conocimiento de la Agencia Española de Protección de Datos.

Tras una notificación de la Agencia, firmada por su director, José Luis Rodríguez Álvarez, la Consejería reforzó los sistemas de seguridad para blindar los accesos. De hecho, emitió un informe en el que puso de manifiesto que en seis años había sido la única incidencia denunciada, y en el que explicaba los diferentes sistemas de protección.

En concreto, la Consejería vulneró los artículos 9 y 10 de la Ley de Protección de Datos de Carácter Personal, tipificadas como graves en los artículos 44.3.h y 44.3.d de esta norma. Debido a que tomó las medias adecuadas para subsanar la incidencia, la Agencia de Protección de Datos ha decidido no instar a que adopte otras medidas.

25/06/2012 – Los centros sanitarios no conservan adecuadamente los datos personales. FUENTE; channelpartner.es

Un estudio de la Agencia Española de Protección de Datos muestra que las historias clínicas de unos 15 millones de españoles podrían tener lagunas de seguridad.

Según las conclusiones de un informe elaborado por la Agencia Española de Protección de datos, sólo un 22,5% de los hospitales ha realizado la última auditoría de sus datos personales en 2010; un 30,8% en 2009; un 10% en 2008, y un 7,4% en 2006 o años anteriores. **Un 29,3% de los centros no aporta información sobre la fecha de la última auditoría de seguridad** realizada. El estudio se ha llevado a cabo entre 654 centros hospitalarios (públicos y privados, de los 791 existentes en el país) que se encuentran en el ámbito de competencia de AEPD y se ha detectado que en un 32,5% de centros no se lleva a cabo la auditoría, y en un 85,6% de los centros que la realizan se han detectado en ella deficiencias de seguridad.

Cada vez que un español acude a su médico de cabecera, a urgencias, a un especialista de un hospital y, en general, a cualquier profesional de la salud, se le abre una historia clínica. Es un **documento válido desde el punto vista clínico y legal** donde se recoge la información necesaria (asistencial, preventiva y social) para la correcta atención de los pacientes. Debe recordarse que los tratamientos de datos de carácter personal que se realizan en el ámbito hospitalario y, en particular, los relacionados con la gestión de las historias clínicas o la investigación clínica, incluyen datos de salud, considerados datos sensibles o especialmente protegidos por la Ley (al mismo nivel que el origen racial y la vida sexual). y, como tales, tienen un régimen de garantías más fuerte.

Tal y como explica Ramona Stepan, del departamento jurídico de Alcatraz Solutions, una empresa experta en cumplimiento normativo, "los principios de respeto a la intimidad y a la confidencialidad de la información clínica de los pacientes están presentes en la legislación sanitaria y, además, en lo concerniente a la conservación de la documentación clínica, la Ley 41/2002 hace en su artículo 17 una referencia explícita a la Ley Orgánica de Protección de Datos (LOPD) y a su normativa de desarrollo, al establecer que "**son de aplicación las medidas técnicas de seguridad establecidas por la legislación reguladora de la conservación de los ficheros que contiene datos de carácter personal** y, en general, por La Ley Orgánica 15/1999 de Protección de Datos de Carácter Personal".

En 2009 se registraron un total de **123 denuncias y actuaciones previas de investigación** en el sector de la Sanidad en relación a la protección de datos. Dada la trascendencia y la importancia del derecho fundamental a la protección de datos en este sector, en el mes de marzo de 2010 la Agencia Española de Protección de Datos tomó la iniciativa de elaborar el Informe de cumplimiento de la LOPD en Hospitales y remitirlo a cada uno de los centros públicos y privados que componen el Catálogo Nacional de Hospitales, al objeto de conocer el nivel de cumplimiento de la LOPD y de su normativa de desarrollo en centros hospitalarios, para adoptar las medidas que resultasen pertinentes.

En el 88,7% de los centros hospitalarios las medidas previstas en el **documento de seguridad son las correspondientes al nivel alto**, que son las aplicables para los datos relativos a la salud de las personas, y el resultado fue desesperanzador e inquietante: un tercio de los hospitales españoles no está capacitado para salvaguardar la información de sus pacientes. Un porcentaje que trasladado al total de historias clínicas posibles nos daría una cifra aproximada de 15 millones de expedientes sanitarios con lagunas de seguridad.

Según los datos que aporta este informe, "**la implantación de algunas de las medidas de seguridad exigidas en el RLOPD para los datos de nivel alto es inferior al porcentaje que declara haberlas previsto en el documento de seguridad**. Así, el porcentaje de hospitales que dispone de un registro de accesos a toda la información es del 74,6%, mientras que el nivel de hospitales en los que se guarda la información exigida por el RLOPD de cada acceso realizado a los datos (identificación del usuario, fecha y hora del acceso, fichero accedidos, tipo de acceso e indicación de acceso autorizado o denegado) es ligeramente inferior, alcanzando el 70,5%. Es reseñable igualmente el hecho de que un 31% de los centros no almacena el registro de acceso durante el periodo mínimo preceptivo de dos años.

18/08/2012 – Facebook ahora sí eliminará las fotos. FUENTE: ideal.es

Facebook no deja de estar en boca de todos, y últimamente es reincidente en temas relacionados con la protección de datos personales, si hace poco os hablábamos del caso de Facebook con Alemania y los problemas que le está dando su programa de reconocimiento facial ahora os tenemos que hablar de otro tema relacionado con las fotografías. Finalmente **Facebook** eliminará las fotos que hayamos borrado.

Parece una perogrullada decir eso de que ahora sí que **Facebook** eliminará las fotos que borremos, pero es que hasta ahora no era así. Cuando los usuarios borraban las fotos que no deseaban que fueran vistas en la red social realmente estas fotos no se eliminaban del todo y se podría decir que seguían circulando por la red puede que por un fallo del sistema de servidores y no como algo intencionado.

Ahora el nuevo sistema de tratamiento de Facebook con las imágenes es diferente ya que cuando se borren estas sí que serán eliminadas, eso sí con un gran PERO y es que éstas no se borraran definitivamente hasta que hayan pasado 30 días cosa que a más de uno no lo hará mucha gracia y haga que se lo piense dos veces antes de volver a subir fotos a la reina de las redes sociales.

Más de 223.000 personas, muchas de ellas de Madrid, están inscritas en España en la Lista Robinson de exclusión publicitaria y ocho de cada diez es especialmente contraria a recibir propaganda por teléfono, ha explicado a Efe la asesora jurídica y responsable de este servicio, Sol Mestre.

De los 223.134 inscritos hasta la fecha, 177.067 no desean recibir propaganda a través del teléfono, fijo o móvil, lo que significa, ha dicho Mestre, que este canal de publicidad es el que más molesta a los ciudadanos, por encima de los mensajes o los SMS telefónicos, los correos electrónicos o el correo postal.

La Lista Robinson fue presentada en Madrid el 30 de junio de 2009 por la Agencia Española de Protección de Datos (AEPD) como un fichero de referencia para los usuarios hartos de recibir publicidad no solicitada y para las empresas que deben cumplir con la Ley de Protección de Datos.

Se trata de un servicio por Internet que permite a los consumidores inscribirse para no volver a recibir comunicaciones comerciales no deseadas por correo, teléfono fijo o móvil e Internet.

Madrid y Barcelona son las ciudades que tienen más personas inscritas, mientras que Teruel, Ávila y Soria son las que cuentan con menos presencia en la lista, y por sexos, predominan un poco más las mujeres, que suponen un 53 % de los inscritos.

A través de Internet, cualquier persona puede inscribirse en la Lista Robinson de forma gratuita y señalar el canal a través del cual no desea recibir publicidad de entidades con las que no mantiene ni ha mantenido algún tipo de relación.

Según Mestre, se pueden señalar todos los canales o sólo los que más molestan y los datos constatan que lo que peor tolera la gente, por lo que invaden, son las llamadas telefónicas.

En este sentido, ha puntualizado que se da el caso de que cuando las operadoras ponen en marcha campañas de propaganda agresiva a través del teléfono, es cuando más crece el número de personas que se apuntan a la Lista Robinson, "porque a los ciudadanos les molestan mucho las llamadas a horas intempestivas y que interfieren en su vida para ofrecerles algo que no han solicitado".

Contra el correo postal se han dado de alta en la lista hasta ahora 98.566 personas, contra los SMS o mensajes de teléfono 93.658 y 89.388 personas no quieren recibir correos electrónicos publicitarios.

El director de Desarrollo Corporativo de la Lista Robinson, César Tello, ha informado de que desde 2009 las entidades tienen la obligación de consultar la Lista Robinson, que está gestionada por la Asociación Española de la Economía Digital, antes de enviar comunicaciones comerciales.

Las empresas tienen también la obligación de excluir a las personas que están inscritas en ella, ya que su objetivo principal es garantizar y proteger, en lo que concierne al tratamiento de datos personales, las libertades públicas y los derechos fundamentales de las personas.

En el plazo máximo de tres meses, las personas inscritas dejan de recibir propaganda, pero si esto no sucede y la siguen recibiendo, el ciudadano puede denunciarlo a la Agencia de Protección de Datos (APD), que es la que tutela el derecho a la privacidad de los ciudadanos.

Tello ha añadido que cuando se constata que hay una vulneración del derecho a la protección de datos de una persona, la APD abre un expediente informador y, si procede, sancionador, con multas que pueden alcanzar hasta los 60.000 euros.

21/08/2012 – Torremolinos – Málaga: Sanción de 100.000 euros a Telefónica Móviles por una reclamación a través de la OMIC. FUENTE: andaluciainformacion.es

La Oficina Municipal de Información al Consumidor del Ayuntamiento de Torremolinos ha logrado con su reclamación que la Secretaría de Estado de Telecomunicaciones y la Agencia Española de Protección de Datos den la razón al vecino de la localidad, C.C.G. al que la empresa de telefonía móvil Movistar le había asignado sin su consentimiento dos líneas de teléfono en fraude de ley y lo había inscrito en un fichero de morosos por una deuda de 89,46 euros, pese a reconocer el error y anular la facturación.

De este modo, dicho vecino puso estos hechos en conocimiento de la Oficina Municipal de Información al Consumidor del Ayuntamiento de Torremolinos que elevó las correspondientes reclamaciones a la Secretaría de Estado de Telecomunicaciones por la contratación en fraude de ley y a la Agencia Española de Protección de Datos por incluirlo en un fichero de morosos.

Los mencionados hechos prueban que la empresa de telefonía le asignó dos líneas de teléfonos móviles y le contrató el 'Plan de Negocio 12 horas Plus' para ambas líneas cuando este vecino no tiene ningún tipo de negocio, reconociendo la empresa que la venta fue telefónica pero la grabación no demuestra que fuera cierto.

En consecuencia, los dos organismos le han dado la razón a este vecino de Torremolinos y el proceso ha dado lugar a que la Agencia Española de Protección de Datos imponga dos sanciones de 50.000 euros cada una a la empresa Telefónica Móviles, por su inclusión en el fichero de morosos.

04/09/2012 – «infracción grave» al enviar cartas electorales a los alumnos. FUENTE: diariodeleon.es

La Agencia Española de Protección de Datos (AEPD) ha calificado de grave la actuación llevada a cabo por el alcalde de Valencia de Don Juan, Juan Martínez Majo, durante las pasadas elecciones municipales, celebradas en mayo del 2011, por remitir una carta a las familias de unos 150 alumnos del colegio público Fray Bernardino Pérez, en las que el candidato por el PP a la Alcaldía de Coyanza denunciaba la «politización de la educación» al concurrir como candidato en otra formación política el propio director del centro. En la misiva también informaba de las actuaciones llevadas a cabo durante su mandato en los distintos colegios de infantil y primaria.

La intervención de la AEPD se produjo a principios de este año a raíz de la denuncia formulada por uno de los padres que recibió en su domicilio dicha carta dirigida a su hija de cinco años.

En su resolución, la AEPD concluye que aunque en la página web del colegio figura un listado con los nombres de los alumnos del colegio no se indica en ningún momento su dirección postal. Según consta en la propia resolución, Martínez Majo explicó que datos «fueron extraídos por varias personas, compañeros suyos, mediante la página web del colegio», pero no acredita que el domicilio, puerta y piso se hayan obtenidos de repertorios o guías telefónicas, lo que desmonta la defensa llevada a cabo por el regidor popular. Por este motivo, se imputa al alcalde de Valencia de Don Juan el tratamiento sin consentimiento de los datos personales de la hija del denunciante, infracción prevista en el artículo 6.1 de la LOPD.

La resolución destaca además que dado el contenido electoral de la carta «no existe un interés legítimo en el tratamiento de los datos de la menor y no se aprecia que deba prevalecer el derecho a comunicar información electoral utilizando los daos de la menor en el envío».

Por todo esto, la AEPD concluye que Martínez Majo, «utilizó los datos de los menores para enviar propaganda electoral» y le apercibe por cometer una «infracción grave» del artículo 6.1 de la LOPD. Contra esta resolución, que pone fin a la vía administrativa, los interesados podrán interponer recurso.

29/09/2012 –.Cómo proteger los datos en la nube y mantener los pies en la tierra. FUENTE; elmundo.es

La **computación en nube** es un modelo de informática totalmente diferente y una **revolución en la que Europa debe participar plenamente**.

Ya hay millones de internautas que disfrutan de las ventajas de servicios basados en la nube, como Facebook, Spotify o el correo electrónico. Pero para que el

conjunto de nuestra economía se beneficie de la informática en la nube, **las empresas y el sector público deberán adoptarla en masa**.

Para estas organizaciones, significa **una tecnología de la información más barata y más flexible**. Asimismo, ofrece **nuevas oportunidades** a aquellos que no disponen de capital para crear su propio centro de datos antes de poner en práctica su proyecto empresarial.

Asimismo, es la ocasión de ofrecer a los consumidores los contenidos numéricos que reclaman en toda Europa. A otros usuarios, como los científicos, la computación en nube les permite colaborar con personas en todo el mundo a una **velocidad y a una escala anteriormente impensable**.

En un momento en que los ordenadores son, junto con la aviación, la fuente de emisiones de carbono con crecimiento más rápido, **la utilización más eficiente de los recursos informáticos es un paso adelante en términos ambientales**. Todos los sectores de la economía que utilizan las TI pueden beneficiarse de este nuevo modelo.

Medidas coordinadas en Europa

Así pues, es necesario adoptar medidas coordinadas en Europa para que los derechos de los usuarios estén claramente establecidos y para **velar por que nadie se quede atrás**. De esta manera, todos podrán beneficiarse de una mejora del entorno jurídico que podría representar unos **beneficios estimados en 160000 millones de euros anuales**.

¿Cuál puede ser la aportación de la Unión Europea en el contexto de un mercado en constante y rápida evolución? La respuesta no es que los gobiernos o Bruselas deban controlar la nube. Pero cuando se trata de un recurso sin fronteras como este, es necesario disponer de una **reglamentación** igualmente sin fronteras y tan actualizada y tan estable como sea posible.

La falta de confianza es una barrera que debemos superar para el desarrollo de los servicios en la nube. Ya hemos comenzado a hacerlo con la presentación de una propuesta para dotar a los europeos de un conjunto único de normas de protección de datos adaptado a la era digital.

Reconocemos la **importancia crucial de los datos para nuestra economía digital**, incluidos los datos personales. Estos datos son como una moneda y deberían ser fiables y poder circular libremente.

Sin embargo, hoy por hoy, **es prácticamente imposible transportar sus datos en la nube de un proveedor a otro**. Los problemas más comunes son la falta de normas técnicas y la existencia de contratos incomprensibles y que nadie lee. Muchas personas y pequeñas organizaciones no son conscientes de los límites de los servicios que suscriben y se dan cuenta posteriormente de que no pueden cambiar de proveedor para su música o sus datos.

La **portabilidad de los datos**, la existencia de contratos con cláusulas sencillas y justas y la certificación de proveedores fiables pueden reforzar la confianza de los usuarios de la nube en los servicios que están comprando. También cometeríamos un error si subestimáramos el poder del **sector público**.

Se espera que dicho sector adquiera aproximadamente 11.000 millones de euros en servicios en la nube de aquí a 2014. Este gasto puede contribuir sobremanera a la hora de configurar el mercado europeo de servicios en la nube, haciéndolo más asequible y útil para todos los usuarios a largo plazo.

Reforma de las normas de protección de datos

Así pues, hemos propuesto una reforma de las normas de protección de datos de la UE a fin de aportar seguridad jurídica y establecer un conjunto de **normas armonizadas que promuevan las inversiones en la computación en nube**. El ahorro para las empresas podría estimarse en 2.300 millones de euros al año.

Asimismo, estamos estableciendo una Asociación Europea de Computación en Nube, con el fin de garantizar que los organismos públicos de toda la UE puedan intercambiar conocimientos y adoptar enfoques comunes en materia de contratación pública en este ámbito.

La computación en nube está destinada a cambiar la economía europea. La **creación de un mercado europeo de computación en nube más amplio, más fiable** y más eficiente podría marcar la diferencia entre el éxito o el fracaso de literalmente cientos de miles de pequeñas empresas.

La existencia de dicho mercado podría permitir desarrollar ciertos servicios públicos que, en su ausencia, podría ser necesario renunciar a prestar.

Pedimos a la industria de la tecnología, los gobiernos y los usuarios que colaboren con nosotros para trascender el concepto de fortalezas nacionales. Debemos instaurar un **clima de confianza**, de manera que podamos garantizar el impulso económico que necesita Europa.

22/10/2012 – Los historiales clínicos son las principales denuncias de protección de datos. FUENTE: europapress.es

Los historiales clínicos de los pacientes son las principales denuncias de protección de datos que se interponen. Y es que, a pesar de que en la inmensa mayoría (98 por ciento en el sector privado y 83 por ciento en el público) cumplen con la inscripción inicial de ficheros, todavía queda camino por recorrer en cuanto al cumplimiento del resto de obligaciones de la ley orgánica de protección de datos personales (LOPD) y la mejora de actuaciones que garanticen el correcto acceso a los datos de carácter personal que se manejan en los centros sanitarios españoles.

Por este motivo, la Asociación de Clínicas y Entidades sin Internamiento de la Comunidad de Madrid (Acesima) ha organizado una jornada sobre la LOPD en colaboración con la Agencia de Protección de Datos de la Comunidad de Madrid, la consultora especializada en protección de datos **Alaro Avant** y la correduría de seguros **Uniteco Profesional**.

"En los últimos años se ha detectado un aumento en el número de denuncias contra centros sanitarios por temas relacionados con el acceso a datos de carácter personal. Estos datos demuestran la necesidad de una mejor protección en este ámbito, que empieza por conocer mejor la ley y los requerimientos que

exige", ha comentado el director general de **Alaro Avant**, Alberto Martín San Cristóbal.

Dicho esto, el experto ha recordado que los datos personales que manejan los centros sanitarios son considerados **"especialmente protegidos"**, ya que la LOPD les otorga el mayor grado de sensibilidad de esta información y las medidas que se deben tomar para protegerlas

La historia clínica es casi una constante en las denuncias que han llegado hasta la Agencia de Protección de Datos en el ámbito sanitario. En concreto, estas quejas se refieren sobre todo a la difusión de datos de pacientes a través de Internet, aparición de expedientes médicos en contenedores en la vía pública, almacenamiento de documentación clínica en áreas sin restricción de acceso, pérdida de historiales clínicos o la utilización de los datos sanitarios para finalidades no autorizadas por los pacientes y la comunicación indebida a terceros.

PROCESOS JUDICIALES PENALES, CIVILES O CONTENCIOSO ADMINISTRATIVOS

Por otra parte, el subdirector general del Registro de Ficheros y responsable del ámbito sanitario en la Agencia de Protección de Datos de la Comunidad de Madrid, Ángel Igualada, ha destacado que la alta sensibilidad de los datos manejados en el ámbito hospitalario "propician no solo que las instituciones se expongan a sanciones económicas, sino también a afrontar procesos judiciales penales, civiles o contencioso administrativos

En este sentido ha recordado una reciente sentencia en la que un juez impuso la inhabilitación de un médico por nueve años, además de una pena de cárcel de tres años. "Hay que tener en cuenta que la LOPD no es la única vía sancionadora ya que puede tener implicaciones penales al vulnerar el derecho a la intimidad de los pacientes", ha manifestado Igualada, para recalcar que la mayoría de las sanciones impuestas van desde los 60.000 hasta los 300.000 euros.

LA SENSIBILIZACIÓN DEL PERSONAL ES OBLIGATORIA

Las principales recomendaciones de los expertos para evitar infringir la ley en este ámbito son formar correctamente al personal implicado en estas tareas y separar los datos personales de la información referida a esas personas.

De esta manera, las eventuales fugas de datos no serían tan graves al convertir en anónimos los datos referidos a cada persona. "El 70 por ciento de los incidentes de seguridad de datos se debe a factores internos de las empresas e instituciones así como a errores de los propios usuarios", ha comentado Martín San Cristóbal.

Por ello, ha asegurado que la "mejor" manera de reducir estos incidentes es formar mejor al personal implicado, concienciarles de la sensibilidad de los datos manejados, así como invertir los recursos necesarios para cumplir con los requisitos de la LOPD y mantenerse "permanentemente" adaptado a esta normativa.

26/10/2012 – Condenan a Renfe por violar la protección de datos con sus cámaras de vigilancia. FUENTE: lainformacion.com

La operadora ferroviaria ha sido sancionada por considerarse ilegal su sistema de videovigilancia instalado en diversas estaciones de **Sevilla**. La **Agencia Española de Protección de Datos**, tras una denuncia de la **Guardia Civil**, inició una investigación y constató varias grabaciones ilícitas.

El ojo que todo lo ve ha caído en su propia trampa de vigilancia. La operadora ferroviaria **Renfe** ha sido sancionada por considerarse **ilegal su sistema de videovigilancia** instalado en diversas estaciones de Sevilla.

Los hechos se remontan a una investigación que inició la Agencia Española de Protección de Datos (AEPD) tras recibir una denuncia de la Guardia Civil en mayo de 2011.

Estas pesquisas se centraron en 50 videocámaras instaladas por la compañía en diversas estaciones de Sevilla, varias de las cuales se ha constatado que realizaron varias grabaciones ilícitas.

Las estaciones inspeccionadas son las de Olivares-Villanueva, San Lucar la Mayor y **Benacazón**, en las que existían diversas **cámaras grabando espacios públicos** ajenos a Renfe, como sus parkings, produciéndose, según la mencionada Agencia, una captación de imágenes y registros desproporcionada.

En concreto, la AEPD constata que, "las cámaras exteriores situadas en las zonas de parking, dado que disponen de *zoom* y movimiento, pueden recoger imágenes de espacios públicos con acceso indiferenciado a personas y vehículos, **permitiendo identificar matrículas de vehículos**, personas que se bajen de dichos vehículos y personas que accedan a pie a las estaciones, con independencia de que dichos espacios sean o no titularidad de Adif (el gestor de la infraestructura ferroviaria que usa Renfe)".

Adis es propietaria de las tres estaciones ferroviarias de Cercanías denunciadas, pero la gestión integral de las mismas se encuentra cedida a Renfe desde septiembre de 2011, incluyéndose aquí las labores de seguridad y vigilancia.

Exceso de vigilancia

Según la Agencia, la cuestión a dilucidar se ha centrado en las cámaras que captan las imágenes de toda la extensión de los parkings, afirmando a este respecto que sería admisible un sistema que captara la parte mínima imprescindible para la seguridad del acceso o de la vigilancia de los muros, pero éste no es el caso.

En su opinión, la compañía ha ido mucho más allá, realizando un **tratamiento masivo de datos diario** que, además, se conserva al menos durante 15 días, sin que Renfe puedan especificar el periodo máximo de retención.

Según las investigaciones, las **imágenes se captan haciendo identificables a las personas y vehículos** en los espacios destinados a parkings, espacio de tránsito público generalizado, y en los espacios destinados al acceso a la estación, con la importante apreciación de que los vehículos que se aparcan son propiedad de particulares, el acceso es libre y no permanecen cerrados en ningún momento.

La Agencia considera que la titularidad privada de un terreno abierto no justifica *per se* la realización de grabaciones de imágenes en el caso de que se trate de un "lugar público".

Todo ello lleva a concluir a la AEPD que las videocámaras instaladas por Renfe realizan tratamientos de datos de carácter personal excesivos, vulnerando el artículo 6.1 de la Ley Orgánica de **Protección de Datos**, ante lo que ha decidido imponer una **sanción de 40.001 euros a la empresa pública** por una infracción tipificada como grave.

Samuel Parra, socio de la firma ePrivacidad, recuerda precisamente que **Renfe ya fue sancionada en ocasiones anteriores** por vulnerar la normativa de protección de datos.

Así por ejemplo, en mayo de 2010 fue multada con 6.000 euros por utilizar formularios de recogida de datos sin respetar las previsiones de información que estipula la Ley Orgánica de Protección de Datos.

17/12/2012 – Acceso y cancelación de antecedentes policiales mediante Internet. FUENTE: delitosinformaticos.com

La Policía Nacional ha informado en la Carta de Servicios Electrónicos sobre aquellas gestiones que los ciudadanos pueden realizar en Internet, como la consulta de los procedimientos relacionados con el certificado de residente o el acceso a los antecedentes policiales, entre otras.

Estos servicios electrónicos forman parte del Proyecto Policía 3.0, presentado por el director general de la Policía en el Congreso. Uno de sus objetivos es que el ciudadano realice los trámites a través de Internet, con plena garantía jurídica, de igual forma que si lo hiciera presencialmente en una comisaría.

Es interesante saber que la Dirección General de la Policía y de la Guardia Civil, disponen de un fichero de datos personales de gestión de antecedentes de las personas de interés policial, denominado fichero «**PERPOL**». Este fichero se encuentra inscrito en la Agencia Español de Protección de Datos Personales

Ahora, cualquier ciudadano que disponga de certificado digital podrá tener acceso, a través de las webs https://sede.policia.gob.es y http://www.060.es, a sus antecedentes policiales, derecho que sólo podrá ser ejercitado a intervalos no inferiores a doce meses, salvo que el interesado acredite un interés legítimo al efecto, en cuyo caso podrá ejercitarlo antes.

Según la AEPD para recabar y tratar datos recogidos en ficheros con fines policiales como el PERPOL, no es necesario el consentimiento del titular de los datos y por ello constituyen una excepción al principio básico en la normativa de protección de datos que exige tener el consentimiento del afectado para el tratamiento de datos de carácter personal.

No obstante, el resto de principios básicos recogidos en la LOPD deben ser respetados por este fichero, y entre ellos el deber de secreto regulado en el artículo 10 de la LOPD que obliga al responsable del fichero y a cuántos intervengan en el tratamiento de los datos, al secreto profesional sobre los mismos y al deber de guardarlos.

Según la Carta de Servicios Electrónicos, si algún ciudadano considera incumplido alguno de los compromisos de este documento podrá formular una reclamación y de forma inmediata se procedería a comprobar el hecho y emprender las gestiones necesarias para solucionar el incidente. La vulneración del deber de secreto en los ficheros con fines policiales dará lugar a la infracción calificada como muy grave del artículo 44.4 g) de la LOPD.

NOTICIAS DE PRENSA AEPD

PRODASUR SOFTWARE Y SERVICIOS, S.L.L.
C.I.F. : B92656206
Domicilio Avda. Comandante Benitez, 15 Local 2
29001 - Málaga
prodasur@prodasur.es
www.prodasur.es

CONSULTORES EN PROTECCION DE DATOS PERSONALES
SOFTWARE Y SERVICIOS PARA EMPRESAS

27/01/2012 – Conclusiones de la 4ª sesión anual abierta de la AEPD. FUENTE: agpd.es.

17/05/2012 – La AEPD pone en marcha su Sede electrónica para facilitar a ciudadanos, empresas y administraciones la realización de trámites a través de Internet. FUENTE: aepd.es.

Nota de prensa

En el marco de la 4ª Sesión Anual Abierta de la AEPD, celebrada en los Teatros del Canal de Madrid

Conclusiones de la "4ª Sesión Anual Abierta de la AEPD"

- **El director de la AEPD destaca la creciente concienciación ciudadana sobre la protección de sus datos, y pone de manifiesto que las denuncias y reclamaciones de tutela recibidas en 2011 crecieron en torno a un 50% y un 34%, respectivamente, respecto a 2010.**

- **Rodríguez Álvarez acoge con especial satisfacción que se reconozca expresamente la existencia de un derecho al olvido en Internet, "algo que hemos venido defendiendo e intentando materializar de forma continuada en los últimos años".**

- **También ha indicado que ante las cuestiones que plantea el Cloud Computing para la protección de los datos, la AEPD está desarrollando iniciativas como la consulta pública abierta para conocer las necesidades de prestadores y usuarios en España.**

- **El adjunto al director de la AEPD ha recordado que las empresas responsables de los datos y las empresas contratadas para prestar servicios de Cloud Computing, deben actuar con arreglo a lo establecido en la legislación de protección de datos.**

- **El subdirector general de Inspección de la AEPD ha explicado que entre el 3 de marzo y el 31 de diciembre de 2011, el 42 % de los asuntos en los que se apreciaba una infracción acabaron en apercibimiento, sin imposición de sanciones.**

(27 de enero de 2012). La Agencia Española de Protección de Datos (AEPD) ha celebrado hoy la "4ª Sesión Anual Abierta de la AEPD" en los Teatros del Canal de Madrid, a la que han acudido más de 800 expertos, organizada en el marco de la celebración mañana, 28 de enero, del Día de la protección de datos en Europa.

Durante el acto de apertura de la jornada, el director de la AEPD, José Luis Rodríguez Álvarez, ha destacado la creciente concienciación ciudadana acerca del valor de su información personal en nuestro país, y ha puesto de relieve que el número de denuncias recibidas en la AEPD ha crecido aproximadamente en un 50% con respecto al año 2010 y el de reclamaciones de tutela en más de un 34%. "Estos incrementos contrastan fuertemente con la relativa estabilización que se produjo en 2010 respecto del año anterior", ha añadido.

Asimismo, José Luis Rodríguez Álvarez se ha referido a la reciente presentación por parte de la Comisión Europea del **nuevo marco europeo de protección de datos**, subrayando que "esta iniciativa legislativa supone un importante avance para fortalecer la protección de los datos personales de los individuos en el territorio de la Unión Europea".

El director de la AEPD ha subrayado que la Agencia ha recibido con especial satisfacción que **se reconozca expresamente la existencia de un derecho al olvido en Internet**, "algo que hemos venido defendiendo e intentando materializar de forma continuada en los últimos años", ha añadido.

Rodríguez Álvarez también ha destacado el importante avance que supondrá **reforzar las Autoridades de Protección de Datos**, y equiparar sus poderes en todos los Estados Miembros, entre los que se incluye el de imponer sanciones económicas sobre la base de un régimen sancionador que también se armoniza para toda la Unión.

Además, el director de la AEPD ha recalcado que la posición jurídica y las garantías de los ciudadanos se ven también reforzadas en la medida en que el Reglamento establece expresamente su aplicación no sólo a las entidades establecidas en la UE, sino también a aquellas que, no estándolo, traten datos de residentes en la Unión para ofrecerles bienes o servicios o para monitorizar sus actividades. "Con ello se logrará poner fin a una práctica frecuente en los últimos tiempos de ciertas corporaciones que alegan que no les es aplicable el derecho europeo, negando con ello a sus usuarios europeos algunos derechos que éste les garantiza", ha añadido.

En cuanto al tema central de la jornada, -la Computación en Nube- el director de la AEPD ha recordado a los asistentes que, ante las cuestiones que plantean estos servicios en nube para la protección de los datos personales, **la AEPD está desarrollando diversas iniciativas**, entre las que se encuentran reuniones con las empresas prestadoras; la participación activa en la formulación de criterios generales en el Grupo de Autoridades Europeas de Protección de Datos, y la consulta pública abierta por la Agencia para conocer mejor las necesidades, experiencias y criterios de los prestadores y usuarios en España.

El primer bloque de la jornada, titulado **"Cloud Computing: sujetos que intervienen, ley aplicable, garantías. Transferencias Internacionales de Datos"**, ha contado con la participación del adjunto al director de la AEPD, Jesús Rubí, y la subdirectora general del Registro de la AEPD, Mª José Blanco.
Durante su intervención, Rubí ha repasado las distintas modalidades de Nubes y de servicios susceptibles de prestación en estos entornos, y ha recordado que la ley aplicable en este ámbito es la ley nacional del responsable del tratamiento datos o cliente.

Asimismo, el adjunto al director de la AEPD ha recordado que tanto las empresas responsables de los datos como las empresas contratadas para prestar servicios de Cloud Computing, deben actuar con arreglo a lo establecido en la legislación de protección de datos (la LOPD y su reglamento de desarrollo). En este sentido, deben existir en los contratos unas cláusulas contractuales que recojan las garantías que exige la legislación española de protección de datos -finalidad y usos de la información, seguridad, confidencialidad devolución o traslado a otro prestador de servicios.

Por su parte, Mª José Blanco ha centrado su intervención en abordar las implicaciones de la Computación en Nube en las transferencias internacionales de datos, y ha analizado régimen aplicable y los requisitos para cumplir con los principios establecidos en la LOPD.

En el segundo bloque, dedicado a abordar **las principales novedades en materia de protección de datos en el ámbito nacional e internacional,** el abogado del Estado-jefe de la AEPD, Agustín Puente se ha referido a consultas, informes y sentencias más relevantes de 2011. Entre otras sentencias se ha referido a la sentencia del Tribunal Supremo de 2 de diciembre de 2011, que si bien no cuestiona la sujeción de los órganos judiciales a la LOPD, establece que la competencia en este ámbito no corresponde a la Agencia sino al CGPJ, tanto en lo que respecta a los ficheros jurisdiccionales como a los no jurisdiccionales o gubernativos.

También se ha referido a la sentencia del Tribunal de Justicia de la Unión Europea (TJUE), que resuelve las cuestiones prejudiciales planteadas por el TS sobre la interpretación del artículo 7.f) de la Directiva Europea de Protección de Datos. Dicha sentencia proclama que el citado artículo tiene efecto directo en España y precisa el alcance del citado artículo, haciendo hincapié en la necesidad de ponderar caso a caso los derechos e intereses en conflicto. Puente ha indicado que, en la práctica, la incorporación de la doctrina del TJUE no debería llevar a un escenario sustancialmente distinto del actual, si bien, a partir de ahora será necesario proceder a un examen más exhaustivo de las circunstancias concurrentes en cada caso concreto y a su adecuada ponderación, con el fin de decidir sobre la legitimidad del tratamiento.

Por otra parte, este segundo bloque de la jornada ha abordado, de la mano del subdirector general de Inspección de Datos de la AEPD, José López Calvo, los principales casos tramitados en el último año en el área de inspección. López Calvo ha subrayado que en 2011 la entrada de denuncias y reclamaciones de tutela creció frente a 2010 en aproximadamente un 50% y un 34,5 %, respectivamente.

Asimismo, el subdirector general de Inspección de la AEPD ha hecho alusión a los primeros meses de aplicación del nuevo régimen sancionador de la LOPD aplicable tras la entrada en vigor en marzo de 2011 de la Ley de economía sostenible, que introdujo la figura del apercibimiento. En este contexto, López Calvo ha explicado que entre el 3 de marzo y el 31 de diciembre de 2011 se dictaron 394 resoluciones sancionadoras y 284 apercibimientos, es decir, que el 42 % de los asuntos en los que se aprecia una infracción acabaron en apercibimiento, sin imposición de sanciones, atendiendo a los criterios para la aplicación de esta figura contenidos en la Ley.

Posteriormente, la subdirectora general del Registro General de la AEPD ha presentado un nuevo modelo de cláusulas contractuales de transferencias internacionales de datos en respuesta a la demanda surgida por parte de empresas españolas prestadoras de servicios para poder dirigirse directamente a la Agencia para solicitar autorizaciones de transferencias internacionales de datos. Blanco ha puesto de manifiesto que si bien el criterio de la Agencia era que el exportador de los datos tenía que ser el responsable del fichero, la Decisión 2010/87 ofrece la posibilidad de ofrecer esta misma flexibilidad a los encargados de tratamiento nacionales, criterio que recoge el nuevo contrato presentado por la AEPD.

En el ámbito de los desarrollos internacionales, el coordinador del Área de Internacional de la AEPD, Rafael García, al igual que el director de la AEPD ha centrado gran parte de su intervención en el nuevo marco normativo europeo presentado por la Comisión Europea. Durante su intervención, ha valorado positivamente que la Comisión haya elegido la figura del Reglamento –norma aplicable directamente en toda la UE- como instrumento para lograr una mayor armonización y un marco uniforme del sistema europeo de protección de datos y superar las actuales diferencias que se derivan de las distintas aplicaciones nacionales de la Directiva.

Nota de prensa

Coincidiendo con la celebración del Día de Internet

La AEPD pone en marcha su Sede electrónica para facilitar a ciudadanos, empresas y administraciones la realización de trámites a través de Internet.

- **La Sede amplía la oferta de servicios de administración electrónica que ya viene ofreciendo la Agencia.**

- **Los interesados podrán realizar los trámites desde su propio ordenador utilizando un certificado electrónico.**

- **La plataforma permite solicitar la tutela de sus derechos reconocidos por la LOPD, presentar denuncias, realizar consultas, así como enviar quejas y sugerencias.**

- **En relación con la notificación de ficheros, la Sede añade a los servicios que ya ofrecía el sistema NOTA desde 2006, nuevas funciones como solicitar una copia de la inscripción o consultar su contenido.**

(Madrid, 17 de mayo de 2012). Hoy, coincidiendo con la celebración del Día de Internet, ha entrado en funcionamiento la **Sede electrónica de la Agencia Española de Protección de Datos (AEPD)**, una plataforma que facilita a ciudadanos, empresas y administraciones la realización de trámites, el envío de solicitudes y presentación de escritos a través de Internet.

La Sede electrónica amplía **la oferta de servicios de administración electrónica que ya viene ofreciendo la Agencia** desde hace años, como el sistema de Notificaciones Telemáticas de la Agencia (**NOTA)**, que funciona desde 2006.

A través de esta plataforma, los interesados **podrán comunicarse con la AEPD y realizar los trámites desde su propio ordenador a través de Internet**, **utilizando un certificado electrónico.** El certificado electrónico es un medio que permite identificar al firmante y garantizar que los contenidos no son alterados, al tiempo que asegura la confidencialidad, así como el correcto envío y recepción de los documentos**.**

Subsidiariamente se prevé la posibilidad **para quienes no dispongan de firma o certificado electrónico**, de realizar trámites cumplimentando los formularios disponibles en la Sede y enviándolos por Internet, aunque deberán remitir posteriormente un ejemplar firmado a la Agencia.

La Sede permite **solicitar la tutela de derechos** reconocidos por la LOPD **ante la Agencia, presentar denuncias,** consultar el **estado de los trámites en curso, efectuar quejas y sugerencias, y enviar consultas**. Existe además un espacio donde la Agencia dará cuenta de las **novedades** que afecten a la Sede.

Además, la Sede permite a los interesados **-particulares, empresas o administraciones- notificar ficheros de forma gratuita** a la AEPD, e incorpora a los servicios que ya se ofrecían**, nuevas funcione**s como la posibilidad de **solicitar una copia de la inscripción de ficheros o consultar el contenido** de la inscripción.

La Sede también cuenta con un **Registro Telemático**, mediante el cual se pueden presentar por vía electrónica aquellas solicitudes, escritos y comunicaciones **que no dispongan de un procedimiento electrónico específico** y tengan relación con actuaciones que requieren la intervención de la AEPD. El Registro Telemático de la AEPD es **accesible las 24 horas del día, todos los días del año.**

Facilidades de la Sede Electrónica

La Sede electrónica de la AEPD ha sido diseñada para facilitar un **rápido acceso** a la información. Así, en la sección izquierda del portal, los usuarios podrán encontrar enlaces a aspectos como: **"¿Qué es la Sede?", "Normativa", "Procedimientos electrónicos", "Consultas", "Firma electrónica" o "Novedades e incidencias".**

Para facilitar el acceso a los servicios, en el bloque central que se visualiza al acceder a la Sede electrónica figura un apartado de "**Destacados"**, que incluye los **procedimientos más utilizados** (presentación de denuncias, reclamaciones de tutela de derechos, solicitud de copia de la inscripción de ficheros, consulta del contenido de la inscripción –NOTA-, quejas y sugerencias). Debajo de este apartado figura otro llamado "**Otros procedimientos**", que da acceso a todos los procedimientos.

En la sección lateral derecha puede encontrarse un listado en el que se informa acerca de los **servicios** a disposición de los usuarios, como los canales de acceso -electrónico, presencial y telefónico-, la fecha, hora y calendario de días hábiles; quejas y sugerencias", así como la posibilidad de consultar el estado de los trámites en curso o los documentos aportados, entre otros.

La Sede Electrónica se complementa con un apartado de **enlaces a páginas de interés**, como el BOE; 060.es (oficinas de atención al ciudadano que informan sobre los servicios de las Administraciones Públicas); el DNI electrónico; el Registro Electrónico Común, o las Brigadas de Investigación Tecnológica de la Policía Nacional y la de Delitos Telemáticos de la Guardia Civil.

BOLETÍN LOPD EN LA EMPRESA 2012

PRODASUR SOFTWARE Y SERVICIOS, S.L.L.
C.I.F. : B92656206
Domicilio Avda. Comandante Benitez, 15 Local 2
29001 - Málaga
prodasur@prodasur.es
www.prodasur.es

CONSULTORES EN PROTECCION DE DATOS PERSONALES
SOFTWARE Y SERVICIOS PARA EMPRESAS

PRODASUR

LA LOPD EN EL DÍA A DÍA

Cómo proteger el acceso a los datos en formato automatizado (parte I)

El responsable del fichero debe establecer e implantar mecanismos que impidan el acceso por el personal no autorizado a los ficheros.

En el caso de ficheros automatizados, debe establecer mecanismos de seguridad con el **criterio de "todo lo que no está explícitamente autorizado, está prohibido".**

Para ello, se debe seguir una **política de "arriba-abajo"**, es decir, protegiendo el acceso al servidor y sus recursos, seguir con las aplicaciones de gestión utilizadas y terminar protegiendo el acceso a los puestos de trabajo.

Proteger el acceso al servidor

- **Proteger el acceso físico**: Se debe situar el servidor en una sala cerrada con llave o algún otro mecanismo similar. Únicamente debe disponer de la llave el personal informático debidamente autorizado.
- **Proteger el acceso lógico**: Se debe proteger el acceso al sistema operativo del servidor. Se debe eliminar o proteger con contraseña fuerte todas las cuentas que se crean por defecto, asegurándonos de que no queda ninguna sin proteger.

(Continuará)

Contenido

Cómo proteger el acceso a los datos en formato automatizado...1
Sanción por facilitar número de teléfono 2
Comunicaciones de datos en accidentes 3
Consulta Pública de la AEPD sobre Cloud Computing 4
¿Puedo tener varios Documentos de Seguridad? 5

A TENER EN CUENTA

Las cuentas por defecto, con contraseñas conocidas, son las que suelen aprovechar terceras personas para acceder a los recursos no autorizados.

SANCIONES DE LA AEPD

Sanción por facilitar número de teléfono

El consentimiento es uno de los principios fundamentales de la LOPD.

En el procedimiento sancionador PS/00746/2009 de la AEPD podemos ver la sanción que puede sufrir una entidad por **facilitar un número de teléfono de un asociado a otro sin obtener previamente su consentimiento para ello**.

Con fecha 15/07/2009, tuvo entrada en esta Agencia Española de Protección de Datos un escrito de D. C.C.C., en el que denuncia a la entidad Real Club Náutico de Gran Canaria (en lo sucesivo CLUB NÁUTICO), al que pertenece en calidad de socio, por la **indebida utilización de su dato personal relativo al número de telefonía móvil**, que, en fecha 13/10/2008, fue facilitado sin su consentimiento por el Presidente de dicha entidad a otro socio, con el propósito de que éste contactase con el denunciante para resolver unos incidentes personales acontecidos en el mencionado Club, según consta en la comunicación que el citado Presidente le remitió en fecha 08/06/2009, de la que aporta copia.

Durante la inspección, se pudo probar que el dato personal del denunciante relativo a su número de telefonía móvil, en fecha 13/10/2008, **fue facilitado sin su consentimiento por el Presidente del CLUB NÁUTICO a otro socio**, con el propósito de que éste contactase con el denunciante para resolver unos incidentes personales acontecidos en los locales del mencionado Club.

Resultado: **Sanción de 601,01 €** por vulneración del artículo 4.2 de la LOPD, relativo a la calidad de los datos, y en concreto a la utilización de los mismos para finalidades incompatibles con aquellas para las que los datos han sido recogidos.

IMPORTANTE

Antes de facilitar a otro cualquier dato personal de un individuo, hemos de preguntarnos si podemos (y debemos) hacerlo.

LA AEPD ACLARA

Comunicaciones de datos en accidentes

El informe 0411/2010 de la AEPD resuelve la consulta planteada sobre diversas dudas en relación con la aplicación de la LOPD a las **comunicaciones de datos relativos a accidentes de tráfico a las compañías aseguradoras o abogados defensores de los implicados en ellos.**

De dicho informe jurídico se extrae lo siguiente:

a) **No será preciso el consentimiento de los interesados para que puedan cederse los datos relativos a los accidentes de tráfico por la policía local a las compañías aseguradoras**, ya que las normas legales examinadas ampararían la cesión inconsentida, tal y como dispone 11.2.a) de la LOPD, en cuanto, como se señala en la Resolución transcrita, dichas compañías deben recabar y conservar la información necesaria en relación con la indemnización que debe abonarse a terceros como consecuencia de un seguro de responsabilidad civil.

b) **La cesión de los datos referidos al accidente a los particulares o sus representantes se encontraría habilitada** por lo dispuesto en el artículo 11.2.a de la LOPD **sin precisar el consentimiento del afectado**, dado que existen dos normas con rango de Ley que dan cobertura al acceso por el particular a los datos necesarios para exigir, mediante el ejercicio de una acción directa, el abono de la indemnización que proceda.

c) Respecto a qué datos pueden comunicarse, **deberá limitarse a los datos que sean necesarios**, en cada caso, en relación con las finalidades que justifican y habilitan dicha comunicación.

A TENER EN CUENTA

El envío de datos de nivel alto por medios telemáticos ha de hacerse cifrando dichos datos.

ACTUALIDAD LOPD

Consulta Pública de la AEPD sobre Cloud Computing

Fuente: www.agpd.es

Nota Informativa

Se podrá participar a través de la Web de la AEPD hasta el próximo día 27 de enero

La AEPD abre una consulta pública para conocer la opinión y experiencia de prestadores de servicios, usuarios y expertos sobre Computación en Nube

- **La AEPD pretende con esta iniciativa tener un conocimiento preciso de experiencias, opiniones y condicionamientos, desde la perspectiva de protección de datos, de prestadores y usuarios de los servicios de Computación en Nube.**
- **La AEPD invita a participar a entidades prestadoras y clientes de este tipo de servicios, así como a usuarios particulares, académicos y expertos, y todos quienes estén interesados en la materia.**
- **Ante el auge de la Computación en Nube, la aplicación y adecuación de las**

Puede descargarse más información aquí:

http://www.agpd.es/portalwebAGPD/revista_prensa/revista_prensa/2011/notas_prensa/common/diciembre/111228_NP_Consulta_Computacion_en_Nube.pdf

EL PROFESIONAL RESPONDE

¿Puedo tener varios Documentos de Seguridad?

Tal y como establece el RD1720/2007, el responsable del fichero o tratamiento, deberá elaborar un Documento de Seguridad que recogerá las medidas de índole técnica y organizativas acordes a la normativa de seguridad vigente, y será de obligado cumplimiento para el personal con acceso a los sistemas de información.

El Documento de Seguridad **podrá ser único y que comprenda todos los ficheros y tratamientos, o elaborar distintos documentos individualizados por cada fichero o agrupando varios** según las características de la organización.

De esta forma, se podrán elaborar documentos:

- Por fichero o tratamiento.
- Por áreas funcionales.
- Por áreas geográficas.
- Por sistemas de tratamiento.

En todo caso, el Documento de Seguridad tendrá carácter de documento interno de la organización, y se puede elaborar con el criterio que mejor convenga, pero no podemos olvidar que **debe estar actualizado en todo momento**.

Cuanta más dispersión exista, mayor dificultad presentará su actualización.

El Documento de Seguridad **deberá estar a disposición de la AEPD** en caso de que llegase a requerirlo.

A TENER EN CUENTA

El Documento de Seguridad **debe ser "manejable"**, ya que exige de una **actualización regular**.

PRODASUR

LA LOPD EN EL DÍA A DÍA

Cómo proteger el acceso a los datos en formato automatizado (parte II)

(Continuación)

Proteger el acceso a los recursos del servidor

- Los recursos (carpetas compartidas, aplicación de gestión, etc.) del servidor donde se ubiquen datos personales no deben tener, por defecto, el acceso permitido a nadie. Posteriormente se irá concediendo acceso a los usuarios autorizados que se den de alta.

Proteger el acceso a las aplicaciones

- Para poder acceder cualquiera de las aplicaciones que utilice la organización en las cuales se traten datos personales, se debe introducir el nombre de usuario la contraseña asociada al mismo.

Proteger el acceso a los puestos de trabajo

- Se debe limitar el acceso al sistema operativo de los puestos de trabajo a los usuarios debidamente autorizados. No se debe poder acceder a ningún sistema sin introducir el correspondiente nombre de usuario y contraseña de acceso o cualquier otro método alternativo que garantice que la persona que está accediendo está autorizada a hacerlo.

Contenido

Cómo proteger el acceso a los datos en formato automatizado...1
Sanción por no atender revocación de consentimiento 2
Plazo de conservación de datos personales 3
Nueva web de la Agencia Española de Protección de Datos 4
¿Es lo mismo un parte de baja que un parte de accidente... 5

A TENER EN CUENTA

No vale solo con tener documentados los procedimientos en el Documento de Seguridad. Han de cumplirse dichos procedimientos.

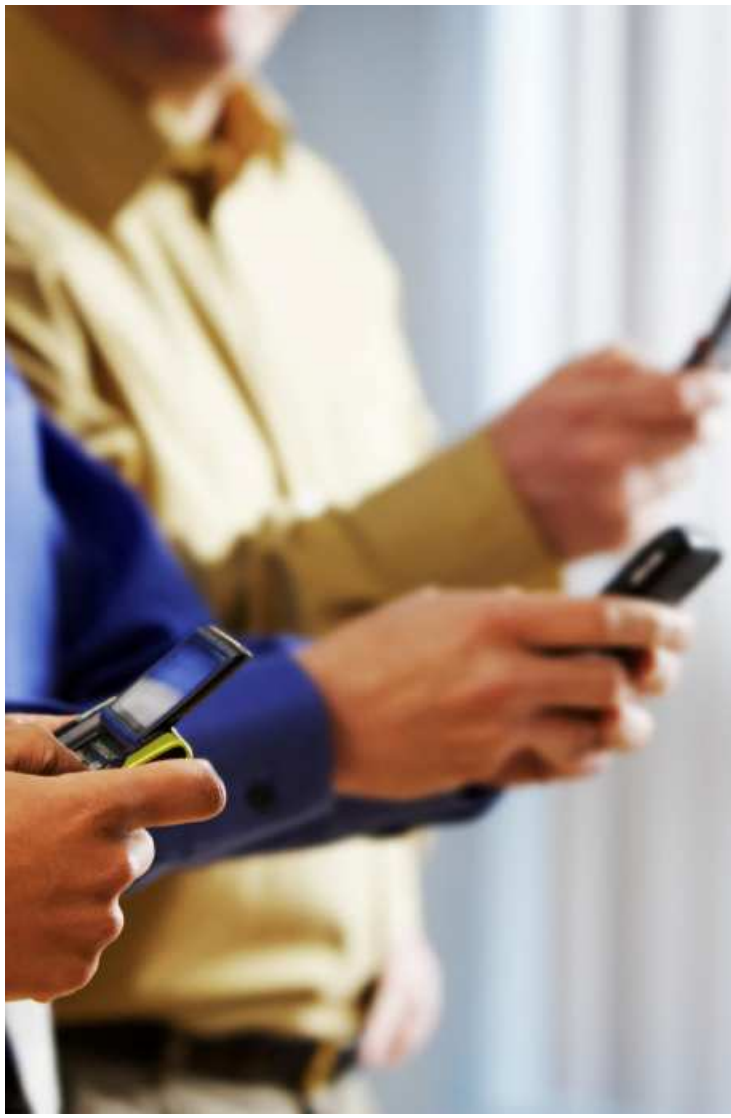
SANCIONES DE LA AEPD

Sanción por no atender revocación de consentimiento

La organización debe establecer procedimientos para el ejercicio de los derechos de los titulares.

En el procedimiento sancionador PS/00307/2011 de la AEPD podemos ver la sanción que puede sufrir una entidad por **no hacer caso a una revocación del consentimiento prestado para recibir SMS.**

Con fecha 11 de agosto de 2010 tiene entrada en la AEPD un escrito de D. A.A.A., en el que declara que tras haber sido usuario de GAY CONTACTOS (www.gay-contactos) ha estado recibiendo SMS sin autorización. A pesar de haber solicitado reiteradamente no recibir mensajes ha continuado recibiéndolos.



Durante la actuación inspectora de la AEPD ha quedado **acreditado** que el **usuario intentó por varios medios oponerse a la recepción de SMS**, siendo infructuosos sus esfuerzos, pese a la recepción de mensaje confirmando su baja.

A este respecto, en cuanto a las alegaciones relativas a la carencia de requisitos formales en las solicitud de cancelación realizada por el denunciante, concretamente a la no acreditación de la identidad, hay que señalar que la regulación que cita la entidad denunciada es para lo referente a la normativa de protección de datos de carácter personal, y en el presente caso, estamos ante un **incumplimiento de los derechos** de los usuarios de servicios de telecomunicaciones que tutela la LSSI.

En concreto, **ni se ofrecía un medio de oposición en cada comunicación comercial, ni se hizo caso al denunciante** cuando manifestó esta oposición por otros medios

Resultado: Sanción de 30.001 € por una infracción del artículo 21 de la LSSI, tipificada como grave.

IMPORTANTE

En cada comunicación comercial electrónica que se envíe a un destinatario debe indicarse el procedimiento para que pueda oponerse a seguir recibiendo dichas comunicaciones.

LA AEPD ACLARA

Plazo de conservación de datos personales

El informe 0408/2010 de la AEPD resuelve la consulta planteada sobre el **plazo legalmente establecido para poder proceder a la destrucción de la documentación** obrante en sus ficheros.

De dicho informe jurídico se extrae lo siguiente:

f) Resulta **imposible establecer una enumeración taxativa de los periodos en que el dato habrá de permanecer bloqueado**, está deberán fundamentarse en lo dispuesto "en las disposiciones aplicables" o a la "atención de las responsabilidades nacidas del tratamiento".

g) Los datos deberán, pues, **cancelarse una vez hayan dejado de ser necesarios para la finalidad para la que se recabaron**.

h) **Primero** deberán mantenerse **bloqueados** al menos durante el tiempo necesario para la prescripción de las acciones que pudieran derivarse de la relación jurídica que vincula a las dos partes, así como los derivados de la normativa tributaria, el plazo de prescripción de 3 años de la Ley Orgánica de Protección de Datos, o los establecidos en otras normas con rango de Ley que resulten de aplicación al caso.

i) **Por último**, una vez hayan transcurrido dichos plazos, se deberán **suprimir** los datos.

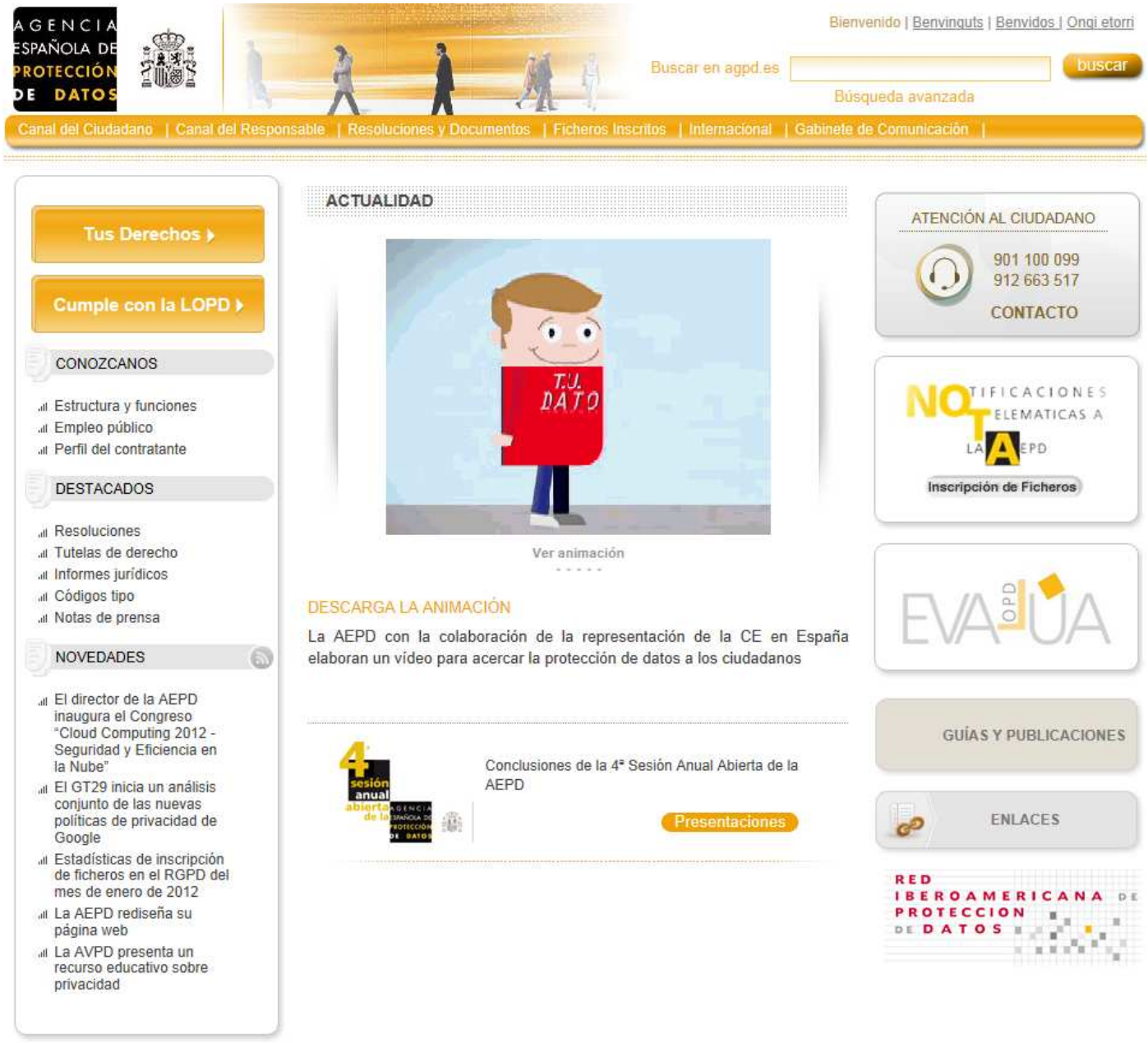
A TENER EN CUENTA

No hay una regla fija para la eliminación de datos personales.

ACTUALIDAD LOPD

Nueva web de la Agencia Española de Protección de Datos

Fuente: www.agpd.es



EL PROFESIONAL RESPONDE

¿Es lo mismo un parte de baja que un parte de accidente laboral de cara al nivel de seguridad a aplicar?

El parte de baja laboral que entrega un trabajador a la empresa no ha de contener más datos que la fecha y la situación de baja por enfermedad, pero sin dar datos concretos de la enfermedad que ha provocado la mencionada baja.

En este caso, podemos aplicar la excepción del art. 81.6 de RD1720/2007, que establece:

"También podrán aplicarme medidas de seguridad de nivel básico a los ficheros o tratamientos que contengan datos relativos a la salud, referentes exclusivamente al grado de discapacidad, o a la simple declaración de la condición de discapacidad o invalidez del afectado, con motivo del cumplimiento de deberes públicos".

Con lo cual, es posible aplicar **medidas de seguridad de nivel básico a dichos partes de baja** laboral.

En cambio, un **parte de accidente laboral** contiene más datos de los estrictamente mencionados antes (en concreto, contiene el accidente sufrido y las lesiones ocasionadas) que hacen que no sea posible acogerse a la excepción señalada en el párrafo anterior, siendo necesario **aplicar medidas de seguridad de nivel alto** a dichos datos.

A TENER EN CUENTA

Es muy importante segregar correctamente los ficheros para aplicar el nivel de seguridad que corresponde según los datos que contienen.

LA LOPD EN LA EMPRESA

Boletín 03/12

PRODASUR

LA LOPD EN EL DÍA A DÍA

¿Cómo se deben desechar los soportes que contengan datos personales?

Contenido

¿Cómo se deben desechar los soportes que contengan...	1
Sanción por enviar mails sin ocultar resto de destinatarios	2
Acceso al sistema de videovigilancia	3
Nueva aplicación de la AEPD para ficheros de titularidad...	4
¿Si mi empresa resulta sancionada por la AEPD, la persona...	5

Siempre que se **deseche** cualquier soporte o documento que contenga datos personales, deberá procederse a su **borrado o destrucción**.

En el caso de documentos en **papel**, se deberán desechar pasándolos por una **trituradora de papel** que los destruya totalmente (o procedimiento similar), haciendo imposible la posterior recuperación de la información que contenían.

Para **soportes y documentos electrónicos**, se debe utilizar alguna de las abundantes herramientas que existen para realizar un **borrado seguro** de la información, de forma que sea totalmente imposible realizar un recuperado posterior.

Este proceso de destrucción y borrado es de aplicación también a los equipos informáticos obsoletos que se desechan, ya que antes de deshacerse de ellos o destinarlos a otro fin, se debe eliminar toda la información que contienen a través de alguna herramienta de borrado seguro de disco que haga imposible recuperar su contenido.

A TENER EN CUENTA

Nunca debe depositarse un equipo obsoleto en el punto limpio sin antes borrar de forma segura la información que contenía.

SANCIONES DE LA AEPD

Sanción por enviar mails sin ocultar resto de destinatarios

La organización debe establecer procedimientos para formar al personal.

En el procedimiento sancionador PS/00565/2011 de la AEPD podemos ver la sanción que puede sufrir una entidad por **enviar correos electrónicos a varios destinatarios sin ocultar la cuenta de correo de los demás destinatarios.**

Con fecha 25 de agosto de 2011 tiene entrada en la AEPD un escrito de D. B.B.B., en el que manifiesta que en el mes de mayo de 2009 contrató un servicio de hospedaje en el Hostal Puerta de Bisagra de Toledo, para lo cuál, facilitó su cuenta de correo electrónico. Posteriormente, el 4 de julio de 2011 recibió un correo comercial no solicitado de dicho hostal. **En el correo podía verse, tanto su dirección de correo como la del resto de los destinatarios** junto con los nombres y apellidos de los mismos.

El hostal reconoció los hechos, alegando que no disponían de autorización para la comunicación de la cuenta de correo des denunciante a otros destinatarios y no fue su intención realizar dicha comunicación, ya que su intención era enviar la comunicación a una selección de contactos e incluir dicha selección en el campo de copia oculta (CCO). **El envío fue debido a un error humano e involuntario** y se han adaptado las medidas necesarias para que este hecho no se vuelva a producir.

La empresa comunica a la AEPD que con anterioridad a los hechos, ya poseía ficheros inscritos en la AEPD y Documento de Seguridad, reconociendo los hechos y solicitando se le sancione con la mínima multa.

Resultado: Sanción de 1.000 € por una infracción del artículo 10 de la LOPD, tipificada como grave.

IMPORTANTE

Siempre que se han de mandar correos a varios destinatarios debe ser utilizando CCO (campo de copia oculta).

LA AEPD ACLARA

Acceso al sistema de videovigilancia

El informe 0135/2010 de la AEPD resuelve la consulta planteada sobre si la creación de un nuevo sistema de videovigilancia, en virtud del cual **el cliente puede acceder a las imágenes**, del lugar donde se encuentran instaladas las cámaras, incluso de las últimas 48 horas, y cuyo fichero está dado de alta por la entidad consultante, obliga a que el cliente nuevamente dé de alta el fichero según la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de datos de Carácter Personal.

Según el contenido de la consulta, el cliente si quiere puede acceder a las imágenes, conectándose por control remoto al servidor de la entidad consultante. Por tanto, puede deducirse que el cliente, más que crear su propio fichero, lo que se le permite es acceder al sistema de la empresa de seguridad.

De dicho informe jurídico se extrae lo siguiente:

l) **No procede** que el cliente **dé de alta un nuevo fichero**.

m) Sin embargo, la entidad consultante sí debe considerar al **cliente** como un **usuario del sistema**, cuyo acceso debe estar regulado de la misma forma que si el acceso fuese realizado por su propio personal.

n) Todo ello debe **aparecer reflejado** en el Documento de Seguridad.

o) Ese **cliente** solo debe tener **acceso a los recursos precisos y autorizados**, limitándose al acceso al resto de recursos.

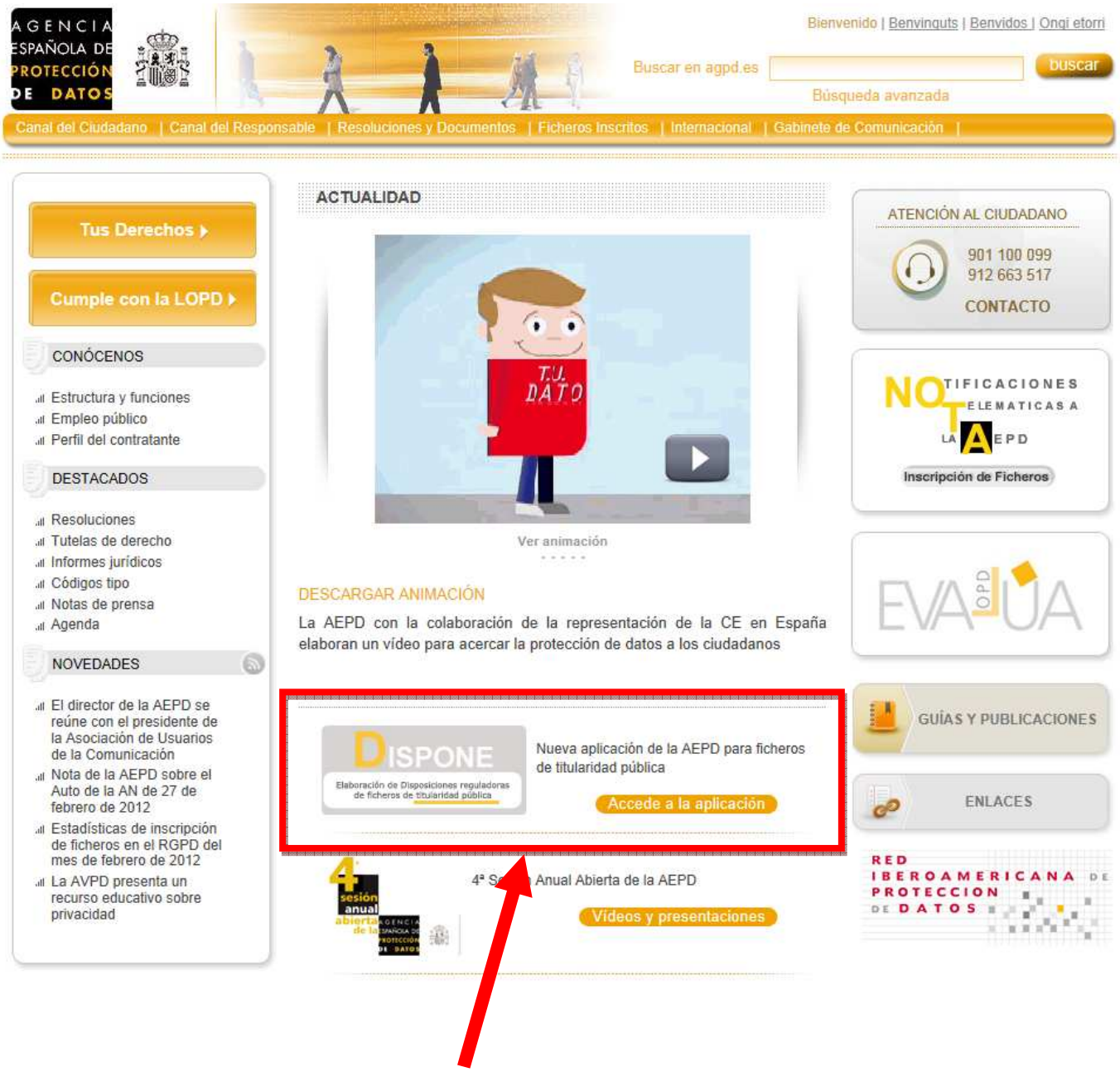
A TENER EN CUENTA

Debe controlarse al acceso tanto del personal propio como del personal externo.

ACTUALIDAD LOPD

Nueva aplicación de la AEPD para ficheros de titularidad pública

Fuente: www.agpd.es



Permite crear las disposiciones reguladoras de los ficheros de titularidad pública.

EL PROFESIONAL RESPONDE

¿Si mi empresa resulta sancionada por la AEPD, la persona denunciante puede pedirme algún tipo de indemnización?

Tal y como establece la LOPD, **los afectados** que, como consecuencia de un incumplimiento de lo dispuesto en la LOPD por el responsable o el encargado del tratamiento **sufran daño o lesión** en sus bienes o derechos tendrán derecho a ser **indemnizados**.

Cuando se trate de ficheros de titularidad pública, la responsabilidad se exigirá de acuerdo con la legislación reguladora del régimen de responsabilidad de las Administraciones Públicas.

En el caso de ficheros de titularidad privada, la acción se ejercitará ante los **órganos de jurisdicción ordinaria**.

Es decir, que si resultamos sancionados por la AEPD y la persona que ha resultado afectada (denunciante) considera que se le ha perjudicado de alguna forma, puede, con la resolución del procedimiento sancionador de la AEPD acudir a un tribunal ordinario a solicitar una indemnización por parte del responsable para resarcir el daño causado.

A TENER EN CUENTA

Denunciar a una entidad ante la AEPD no conlleva ningún coste al denunciante.

LA LOPD EN LA EMPRESA

Boletín 04/12

PRODASUR

LA LOPD EN EL DÍA A DÍA

¿Qué medios no son adecuados para ejercer los derechos de los afectados?

Contenido

¿Qué medios no son adecuados para ejercer los derechos de... 1
Sanción por recoger datos de menores sin consentimiento 2
Publicación de datos en web de Ayuntamiento 3
Dictamen sobre las propuestas de reforma para la normativa... 4
¿Qué tengo que hacer si quiero colgar de la web de la... 5

La normativa establece que debe concederse al interesado un medio sencillo y gratuito para el ejercicio de los derechos de acceso, rectificación, cancelación y oposición (ARCO). El ejercicio de los derechos ARCO también debe ser gratuito para el interesado.

A tal efecto, **no se consideran conformes** los siguientes supuestos:

- El envío de **cartas certificadas** o semejantes.
- La utilización de **servicios** de telecomunicaciones que impliquen **tarificación adicional**.
- Cualquier medio que implique un **coste excesivo** para el interesado.

De esta forma, sería **acorde a la normativa**:

- El **envío de una carta** siempre que no fuese obligatorio que fuese certificada.
- Disponer de un **número de teléfono** siempre que **no fuese 807** o similar.
- El envío de un **correo electrónico**.

A TENER EN CUENTA

La entidad debe establecer procedimientos eficaces para el ejercicio de los derechos ARCO en tiempo y forma.

SANCIONES DE LA AEPD

Sanción por recoger datos de menores sin consentimiento

En el procedimiento sancionador PS/00339/2011 de la AEPD podemos ver la sanción que puede sufrir una entidad por **recoger datos de menores de edad sin obtener el consentimiento paterno.**

La organización debe establecer procedimientos para recoger datos personales y ejercer los derechos.

Con fecha 1 de febrero de 2011 se recibe en el registro de la Agencia Española de Protección de Datos escrito de reclamación de D. A.A.A., en el que pone de manifiesto que durante el mes de diciembre de 2010 y comienzos de enero de 2011, **el canal infantil de televisión TDT BOING** promocionaba la **asistencia a la Cabalgata de Reyes** en una carroza patrocinada por la cadena. **Para participar** en el concurso, **se debía cumplimentar un formulario disponible en la web www.boing.es**, el cual recogía datos personales de menores puesto que en las bases de la promoción figuraba que iba dirigido a niños entre 7 y 12 años, **no obstante, no se solicitaba el consentimiento del tutor legal ni se facilitaba claramente la finalidad de la recogida ni la información necesaria para ejercitar los derechos ARCO.**

En la inspección de la AEPD se comprueba que **aunque el sitio web www.boing.es es un portal dirigido a un público juvenil cuya información facilitada en la recogida de datos se realiza cumpliendo la LOPD**, sin embargo, **en la recogida de datos para participar**, en fechas del 15 de diciembre hasta el 26 de diciembre de 2010, en la promoción de la **Cabalgata de Reyes** en Madrid para menores entre 7 y 12 años, era necesario **rellenar un formulario con datos personales, no existiendo ninguna opción para solicitar la autorización** del padre/madre/tutor, **ni consta la información establecida por la LOPD**.

Resultado: Sanción de 20.000 € por una infracción del artículo 6.1 de la LOPD.

IMPORTANTE

Se ha de ser especialmente cauto a la hora de recoger datos personales de menores.

LA AEPD ACLARA

Publicación de datos en web de Ayuntamiento

El informe 0119/2012 de la AEPD resuelve la consulta planteada sobre **si resulta conforme** a lo dispuesto en la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de datos de Carácter Personal, y su Reglamento de desarrollo, aprobado por Real Decreto 1720/2007, de 21 de diciembre, la **publicación en la página web** de la Corporación consultante **de los datos contenidos en el "fichero de facturas**", remitido al Ministerio de Hacienda y Administraciones públicas **en cumplimiento de lo dispuesto en el artículo 4 del Real Decreto-Ley 4/2012**, de 24 de febrero, por el que se determinan obligaciones de información y procedimientos necesarios para establecer un mecanismo de financiación para el **pago a los proveedores de las entidades locales**.

De dicho informe jurídico se extrae lo siguiente:

p) **La publicación en Internet** de los datos contenidos en el denominado por la consultante "fichero de facturas" referidos a quienes no tengan la condición de personas jurídica o se refieran a comerciantes, industriales o navieros el ámbito exclusivo de su actividad empresarial, de forma que la información sea libremente accesible por cualquier persona **implica una cesión de datos que no encuentra amparo, sin el consentimiento del interesado**, ni en el artículo 11 de la LOPD ni en el artículo 7 f) de la Directiva 95/46/CE.

q) **La inclusión de estos datos en Internet** únicamente **sería posible si el acceso quedase limitado** al propio interesado mediante la inclusión previa de varios datos que sólo él pudiera, en principio, conocer.

A TENER EN CUENTA

La publicación de datos personales en internet es una cesión de datos.

ACTUALIDAD LOPD

Dictamen sobre las propuestas de reforma para la normativa europea de protección de

Fuente: www.agpd.es

Nota Informativa

En el transcurso de la última reunión plenaria del grupo celebrada en Bruselas con la participación del director de la AEPD

Las Autoridades europeas de protección de datos aprueban un Dictamen sobre las propuestas de reforma de la normativa europea protección de datos

(Madrid, 30 de marzo de 2012). El grupo de **autoridades europeas de protección de datos (Grupo de Trabajo del Artículo 29) ha aprobado**, durante su sesión plenaria del 22 y 23 de marzo celebrada en Bruselas con la participación del director de la AEPD, **José Luis Rodríguez Álvarez**, un **dictamen** sobre las **propuestas de reforma del marco normativo europeo de protección de datos de la Comisión Europea.**

El Grupo de autoridades ofrece en el dictamen sus conclusiones generales tras el análisis de las propuestas y **pone de relieve las áreas de preocupación y sugerencias de mejora.**

En líneas generales el Grupo de **autoridades europeas de protección de datos da la bienvenida a las propuestas presentadas por el Comisión Europea,** que buscan reforzar los **derechos de los interesados**, para **mejorar la responsabilidad de las empresas** y fortalecer la posición de las autoridades de protección de datos, a nivel nacional e internacional.

Puede descargarse más información aquí:

https://www.agpd.es/portalwebAGPD/revista_prensa/revista_prensa/2012/notas_prensa/common/marzo/120330_NP_Reforma.pdf

EL PROFESIONAL RESPONDE

¿Qué tengo que hacer si quiero colgar de la web de la empresa fotos del personal de la misma?

En el supuesto de que **se desee incluir fotos de los trabajadores en la web de la empresa** o en otras publicaciones (revistas, periódicos, etc.), hemos de tener en cuenta varios factores:

- **El tratamiento de la imagen de los trabajadores con fines de promocionar la empresa**, sus actividades, o los miembros que la componen, **no está enmarcado dentro de la, estrictamente, gestión laboral del personal** (que sí es, en cambio, realizar las nóminas, seguros sociales, etc.).
- Que la **publicación de la imagen de los trabajadores en la web de la empresa supone una cesión de datos** que debe ser consentida por dichos trabajadores.
- Que **el trabajador es libre de prestar dicho consentimiento**, no pudiendo ser obligado al mismo.

Debemos, pues, **obtener el consentimiento de todos y cada uno de los trabajadores** que vamos a mostrar en la web antes de poder publicar su imagen.

También hemos de tener en cuenta que **el consentimiento otorgado** por los trabajadores **es revocable en cualquier momento**, debiendo la empresa en ese momento de retirar dicha imagen de la web.

A TENER EN CUENTA

Publicar la foto de un trabajador en la web de la empresa sin obtener su consentimiento puede acarrear una sanción.

LA LOPD EN LA EMPRESA

Boletín 05/12

PRODASUR

LA LOPD EN EL DÍA A DÍA

¿Qué tratamientos de datos están incluidos dentro de la LOPD?

Según establece la Ley, *la LOPD será aplicable a los datos de carácter personal registrados en soporte físico, que los haga susceptibles de tratamiento, y a toda modalidad de uso posterior de esos datos por los sectores público y privado*.

Están incluidos dentro de esta Ley tanto los datos de carácter personal en soporte informático, como los registrados en soporte papel.

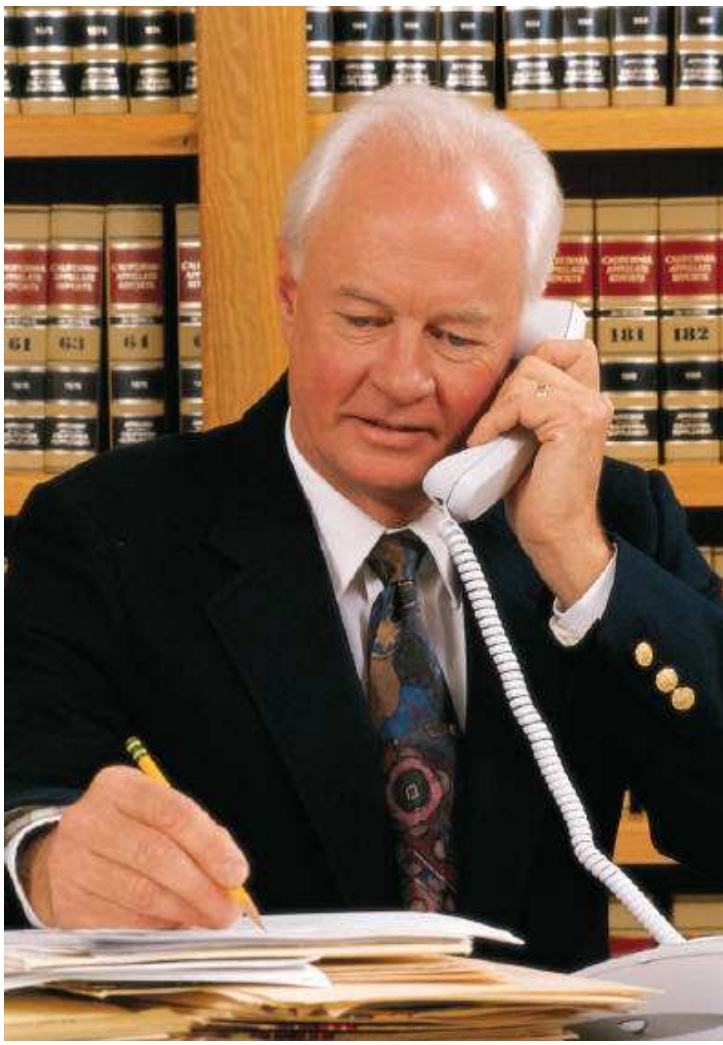
La LOPD es de aplicación tanto para las entidades privadas, como para los organismos públicos.

Por tanto, la LOPD es de obligado cumplimiento para:

- Empresas (sea cual sea su tamaño).
- Autónomos.
- Profesionales liberales.
- Asociaciones, Fundaciones.
- Comunidades de vecinos.
- Organismos y administraciones públicas.
- Entidades sin ánimo de lucro.
- Cualquier organización que maneje datos de carácter personal.

Contenido

¿Qué medios no son adecuados para ejercer los derechos de... 1
Sanción por recoger datos de menores sin consentimiento 2
Publicación de datos en web de Ayuntamiento 3
Dictamen sobre las propuestas de reforma para la normativa... 4
¿Qué tengo que hacer si quiero colgar de la web de la... 5



A TENER EN CUENTA

Cualquier organización, empresa o autónomo que recoja, almacene o manipule datos personales ha de cumplir con la LOPD.

SANCIONES DE LA AEPD

Difusión por email de fichero con datos personales

En el procedimiento sancionador PS/00559/2011 de la AEPD podemos ver la sanción que puede sufrir una entidad por **enviar de forma accidental un fichero que contenía datos personales adjunto a un correo electrónico.**

La organización debe formar adecuadamente al personal que trata datos personales.

Con fecha 15/06/2011, tuvo entrada en esta Agencia un escrito de DÑA. B.B.B. en el que denuncia a la entidad O2 CENTRO WELLNESS PLENILUNIO, S.L. (en lo sucesivo O2 CENTRO WELLNESS), de la que fue cliente, por **haberle remitido un correo electrónico de 17/05/2011 que contenía un fichero adjunto con datos de 9.293 personas**, incluyendo los suyos. Dicho fichero contiene datos personales de las personas afectadas relativos a nombre, apellidos, domicilio, teléfono (línea fija y móvil), dirección e-mail, Número de DNI y sexo.

Durante las actuaciones quedó acreditado que O2 CENTRO WELLNESS **remitió a terceros un documento en el que figuran los datos personales de abonados de la entidad** relativos a nombre, apellidos, domicilio, teléfono (línea fija y móvil), dirección e-mail, Número de DNI y sexo. **Esta información no puede ser facilitada a terceros, salvo consentimiento de los afectados** o que exista una habilitación legal que permita su comunicación, que no concurren en el presente caso.

Por tanto, queda acreditado que por parte de dicha entidad, se **vulnera el deber de secreto** garantizado en el artículo 10 de la LOPD, al haber posibilitado que terceras personas tuviesen acceso a datos personales de los afectados.

Resultado: **Sanción de 3.000 €** por vulneración del artículo 10 de la LOPD relativo al deber de secreto.

IMPORTANTE

Se ha de ser especialmente cauto a la hora de recoger datos personales de menores.

LA AEPD ACLARA

Recogida de datos del DNI por la Policía Local

El informe 0512/2010 de la AEPD resuelve la consulta planteada sobre la **posible vulneración de lo dispuesto en la LOPD**, y a su Reglamento de desarrollo, por el hecho de que la **policía local que controla el acceso a las dependencias municipales** donde se celebran los Plenos del Ayuntamiento (Sala de Juntas), **recoja los datos de nombre, apellidos, D.N.I. y lugar al que se dirigen de las personas** que pretendan presenciar dichos Plenos, siendo la finalidad de su recogida el control de seguridad de acceso al edificio.

De dicho informe jurídico se extrae lo siguiente:

s) **La Policía Local forma parte de las Fuerzas y Cuerpos de Seguridad** del Estado pues así lo dispone el artículo 1.4 de la Ley Orgánica 2/1986, de 13 de marzo, de Fuerzas y Cuerpos de Seguridad.

t) En consecuencia, si el Ayuntamiento tiene atribuida la prestación del servicio de **seguridad y control de acceso** al edificio a la unidad correspondiente de la **policía local**, **no estaríamos ante un supuesto de vulneración de la LOPD**.

u) No obstante, **ello implica**, que el **Ayuntamiento, como responsable del fichero, deberá asumir el cumplimiento de todas las obligaciones establecidas en la LOPD**, incluida la inscripción del fichero en el Registro General de Protección de Datos.

v) Debería **indicarse al interesado qué dependencia municipal va a ser responsable del tratamiento**, ante la que poder ejercitar sus derechos y la finalidad del fichero.

A TENER EN CUENTA

Siempre que se traten datos personales han de implantarse las medidas de seguridad.

ACTUALIDAD LOPD

La AEPD pone en marcha su Sede electrónica para facilitar la realización de trámites a través de Internet

Fuente: www.agpd.es

Puede acceder desde este enlace:

http://sedeagpd.gob.es/sede-electronica-web/

EL PROFESIONAL RESPONDE

¿La normativa sobre protección de datos es antigua, o es de reciente creación?

Respecto a la **evolución de la normativa** sobre protección de datos, hemos de destacar las siguientes fechas:

- **1977 Alemania**. Aparece la "Ley De Protección Contra el Abuso de Datos Personales, en el Proceso de Datos"
- **1978 Constitución Española.** En su artículo 18 relativo al Derecho al honor, a la intimidad personal y familiar y a la propia imagen, así como a la limitación en el uso de la informática para garantizar esto.
- **1992 España**. Aparece la "Ley Orgánica De Regulación Del Tratamiento Automatizado De Datos" (LORTAD).
- **1999 España**. Aparece la "Ley Orgánica De Protección De Datos De Carácter Personal" (LOPD).
- **2007 España**. Aparece el Reglamento de Desarrollo de la LOPD (RD1720/2007).

¿Qué nos depara el futuro?

- **Armonización** de la normativa en todos los países de la **Unión Europea**.
- Se está **implantado** esta normativa en los países de **Latinoamérica**.

A TENER EN CUENTA

La normativa sobre protección de datos es una normativa que en el futuro tendrá un alcance global.

LA LOPD EN LA EMPRESA

Boletín 06/12

PRODASUR

LA LOPD EN EL DÍA A DÍA

¿Qué debo hacer cuando recibo un Curriculum Vitae en la empresa?

Contenido

¿Qué debo hacer cuando recibo un Curriculum Vitae en la... 1
Difusión de parte medico en red social 2
Publicación de datos de profesores en web 3
La AEPD convoca la XVI edición de los "Premios Protección... 4
¿Qué son los Códigos Tipo y para qué se utilizan? 5

Es normal recibir en las empresas Curriculum Vite de posibles candidatos que quieren optar a un puesto de trabajo, ya sea a través de un proceso de selección de personal que la empresa haya iniciado o sin que dicho proceso se haya producido.

Una vez recibido el Curriculum hay dos posibles alternativas:

a) **Que NO nos interese**: en este caso hemos de destruir el Curriculum con una trituradora o sistema similar, de forma que no sea posible recuperar esos datos (si lo hemos recibido por mail, borraremos el correo).

b) **Que SÍ nos interese**: en caso de que guardemos el Curriculum hemos de informar al titular del mismo que vamos a guardar dichos datos para procesos de selección de personal e indicarle quién es el responsable del fichero y cómo puede ejercer sus derechos de acceso, rectificación, cancelación y oposición.

Hemos de tener en cuenta que a los Curriculum que guardemos les hemos de aplicar las **medidas de seguridad de nivel medio**.

A TENER EN CUENTA

Debemos analizar las distintas fuentes de entrada de datos personales en la entidad.

SANCIONES DE LA AEPD

Difusión de parte medico en red social

En el procedimiento sancionador PS/00369/2012 de la AEPD podemos ver la sanción que puede sufrir una entidad por **al publicarse en Facebook un parte médico de incapacidad temporal de un trabajador de dicha entidad, manteniéndose durante un periodo de entre 24 y 48 horas.**

Con fecha 14/10/2010, tuvo entrada en la AEPD un escrito de DÑA. B.B.B. en el que denuncia a la entidad LITTE CUP S.L. La denunciante ha aportado a la Agencia una copia impresa (el 7 de septiembre de 2010) de una fotografía colgada (desde un teléfono móvil) en el álbum del perfil TAZZINA MANRESA de la red social Facebook. En la fotografía se aprecia un documento en cuyo encabezamiento figura la leyenda "BUROFAX MANRESA" y fecha 06/09 2010, junto a un literal parcialmente ilegible: "…INCAPACITAT TEMPORAL PER CONTINGENCIES COMUNES". El documento contiene el nombre y apellidos de la denunciante, junto con su número de tarjeta sanitaria, número de afiliación a la Seguridad Social, número de DNI y domicilio. Asimismo se incluye el nombre de la empresa: LITTLE CUP, S.L. y datos asociados a la baja médica: 60 días, "malaltia comuna", fecha de baja: 08/09/2010.

La empresa alega que desconoce las circunstancias por las cuáles una fotografía del citado parte fue publicada en el perfil de la red social Facebook y que en cuanto detectó la difusión del documento, decidió su retirada y el cambio de contraseñas de acceso a dicha red, ya que los empleados tenían acceso al perfil.

Resultado: Sanción de 2.000 € por vulneración del artículo 6.1 de la LOPD relativo al consentimiento y tipificada como infracción grave.

La organización debe formar adecuadamente al personal que trata datos personales.

IMPORTANTE

La entidad ha de prestar mucha atención a lo que publica en las redes sociales.

LA AEPD ACLARA

Publicación de datos de profesores en web

El informe 0223/2011 de la AEPD resuelve la consulta planteada sobre si la consultante **puede proceder a publicar en la página web de la Universidad los datos de contacto de sus profesores** consistentes en el número de teléfono y correo electrónico de la Universidad **sin su consentimiento**, con la finalidad de favorecer la actividad docente a través de la interrelación con los alumnos, incluso si alguno manifiesta su oposición, de acuerdo con lo dispuesto por la LOPD, y el artículo 2.2 del RD1720/2007 (RLOPD), teniendo además en cuenta el RD1791/2010, por el que se aprueba el Estatuto del Estudiante Universitario.

De dicho informe jurídico se extrae lo siguiente:

w) **La publicación planteada implica la existencia de una cesión** o comunicación **de datos de carácter personal**.

x) El RD1720/2007, en su artículo 2.2 establece que "Este reglamento **no será aplicable** a los tratamientos de datos referidos a **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 número de fax profesionales**."

y) En consecuencia, si los datos de contacto a los que se refiere la consulta se enmarcan en el **entorno profesional** del afectado y su actividad en el marco de su integración profesional en la persona jurídica (Universidad) **no será necesario registrar dicho fichero** al encontrarse **excluido del marco de aplicación de la Ley** y por consiguiente **no se precisaría el consentimiento** de los profesores para la comunicación de sus datos de contacto a través de Internet en la página web de la Universidad.

A TENER EN CUENTA

Siempre que se cedan o comuniquen datos hemos de ser extremadamente cautos.

ACTUALIDAD LOPD

La AEPD convoca la XVI edición de los "Premios Protección de Datos Personales"

Fuente: www.agpd.es

La AEPD convoca la XVI edición de los "Premios Protección de Datos Personales"

- **Se convocan en las categorías de "Investigación" y "Comunicación".**
- **Los premios quieren reconocer aquellos trabajos que supongan una aportación destacada en la difusión del derecho a la protección de datos.**
- **Los premios de cada categoría cuentan con una dotación económica de 3.000 euros y los accésit están dotados con 1.500 euros.**
- **El 15 de octubre de 2012 concluye el plazo para presentar las candidaturas tanto al premio de comunicación como al de investigación.**

(Madrid, 15 de junio de 2012). La Agencia Española de Protección de Datos (AEPD) ha convocado la XVI edición de los **"Premios Protección de Datos Personales"**, en las categorías de "**Investigación" y "Comunicación".**

La Agencia convoca estos premios con el objetivo de **reconocer aquellos trabajos que, ya sea en el campo de la comunicación o en el de la investigación, supongan una aportación destacada a la promoción del derecho fundamental a la protección de datos**, y contribuyan a fomentar la concienciación de quienes manejan información personal sobre sus responsabilidades en esta materia.

El **PREMIO PROTECCIÓN DE DATOS PERSONALES DE COMUNICACIÓN, dotado con 3.000 euros, así como un accésit de 1.500 euros,** tiene por objeto reconocer los trabajos de medios y profesionales de la comunicación que hayan contribuido de forma destacada a promover el conocimiento de los ciudadanos de sus derechos en materia de protección de datos personales.

Puede acceder desde este enlace:

http://www.agpd.es/portalwebAGPD/revista_prensa/revista_prensa/2012/notas_prensa/common/junio/120615_NP_Convocatoria_Premios.pdf

EL PROFESIONAL RESPONDE

¿Qué son los Códigos Tipo y para qué se utilizan?

Los **Códigos Tipo** son **acuerdos sectoriales**, convenios administrativos o decisiones de empresa en los que se establecen, en función de los principales problemas de un determinado sector para cumplir la normativa sobre protección de datos, unas **pautas de actuación** así como una definición de criterios uniformes de aplicación de la LOPD entre las organizaciones agrupadas a dicho Código Tipo.

Los Códigos Tipo tienen el carácter de códigos deontológicos o de buena práctica profesional, y **son vinculantes** para quienes se adhieran a los mismos.

El objetivo de los Códigos Tipo es redactar y cumplir las **mejores prácticas de la LOPD** en las organizaciones agrupadas.

Para ello, los Códigos Tipo deben:

- **Identificar** los **principales problemas de un sector** determinado para cumplir la normativa sobre protección de datos.
- **Concretar criterios** específicos de aplicación de la normativa.
- **Definir** la **aplicación de las medidas** de seguridad atendiendo los riesgos de ese sector en concreto.

A TENER EN CUENTA

La adhesión de una organización a un Código Tipo es voluntaria.

LA LOPD EN LA EMPRESA

Boletín 07/12

PRODASUR

LA LOPD EN EL DÍA A DÍA

¿Por qué están aumentando las amenazas hacia los datos personales?

Las amenazas y los incidentes de seguridad que afectan a los datos personales que las entidades almacenan **están aumentando notablemente** debido a los siguientes factores:

c) **Mayor dependencia** de los sistemas, servicios de información y tecnologías asociadas.

d) Complejidad y vulnerabilidad de la **tecnología** empleada.

e) **Volumen de información** cada vez más importante.

f) **Crecimiento exponencial** de las redes y usuarios interconectados.

g) **Aumento de las bases de datos** on-line.

h) Uso masivo del **cloud computing**.

i) **Inmadurez** de las nuevas tecnologías.

j) Alta disponibilidad de las **herramientas automatizadas para ataques** a la seguridad.

k) Técnicas de **ingeniería social**.

l) **Falta de concienciación** y formación del personal.

m) **Rentabilidad de los ataques**.

Contenido

¿Por qué están aumentando las amenazas hacia los datos... 1
Pérdida de historia clínica 2
Acceso a los datos de personas fallecidas 3
La AEPD y CGAE presentan un informe sobre la utilización... 4
¿Qué es la Ingeniería Social? 5

A TENER EN CUENTA

En el determinado mercado negro, los datos personales son moneda de cambio.

SANCIONES DE LA AEPD

Pérdida de historia clínica

En la resolución de administraciones públicas PA/00016/2010 de la AEPD se detalla el **extravío de la historia clínica de un paciente** del Hospital Clínico Universitario de Valladolid, demostrándose que carece de las medidas de seguridad que la Ley exige al responsable del fichero.

Con fecha 26 de enero de 2010 tiene entrada en la AEPD un escrito de Dña. B.B.B. en el que declara que el Hospital Clínico Universitario de Valladolid ha extraviado su historia clínica, indicando que se dirigió por escrito al hospital solicitando su historia clínica. Manifiesta la denunciante que en la respuesta del Director Gerente del hospital se le informa de "que en dicho hospital se está a la espera de la localización de mi historia clínica, mencionándose en el indicado escrito una reconstrucción mínima y parcial de la misma con aquellos documentos últimos que se encuentran digitalizados".

En este caso concreto lo constatado es que la paciente solicitó el derecho de acceso a su historia clínica, que no se pudo satisfacer en ese momento porque no se localizó, que se solicitó que le entregase a su paciente una copia de su historia clínica en diez días y que el hospital manifiesta que cumplimentó este requerimiento transcurridos 20 días, sin que hasta la fecha se tenga constancia de la conformidad de su paciente que se solicitó en pruebas.

Resultado: DECLARAR que la Gerencia Regional de Salud de Castilla y León- Hospital Clínico Universitario de Valladolid ha infringido lo dispuesto en el artículo 9.1 de la LOPD, con una infracción tipificada como grave y REQUERIRLA para que implante las medidas que impidan que esto vuelva a ocurrir.

La organización debe implantar las medidas de seguridad recogidas en el Documento de Seguridad.

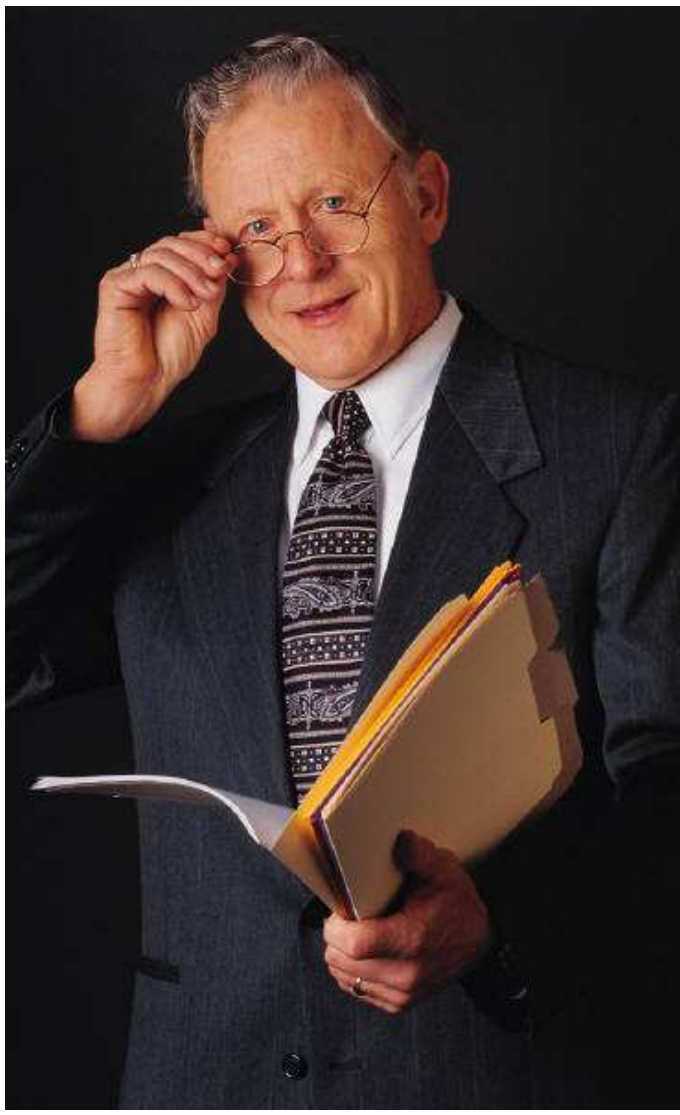
IMPORTANTE

Si esto mismo le ocurre a una clínica privada, en lugar de a un hospital público, el resultado hubiese sido, casi con seguridad, una fuerte sanción.

LA AEPD ACLARA

Acceso a los datos de personas fallecidas

El informe 0523/2010 de la AEPD resuelve la consulta planteada sobre **la posibilidad de acceso por un investigador privado al expediente de un médico fallecido hace ya veinticinco años, y si puede fotocopiarlo o fotografiarlo**, de acuerdo con lo dispuesto en la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (LOPD) y a su Reglamento de desarrollo, aprobado por el Real Decreto 1720/2007, de 21 de diciembre.



De dicho informe jurídico se extrae lo siguiente:

aa) **La protección** conferida por la Ley Orgánica 15/1999 **no se extiende a los datos de las personas fallecidas**, así lo indica expresamente el Reglamento de desarrollo de dicha Ley, aprobado por Real Decreto 1720/2007, por consiguiente el acceso a los datos a ellas referidas contenidos en los documentos que forman parte del Patrimonio Documental no se encuentra tutelado por dicha Ley Orgánica.

bb) Todo ello sin perjuicio de que la normativa que regule dicho Patrimonio establezca determinados plazos para permitir el acceso a sus datos.

cc) En concreto, la consulta de los documentos constitutivos del **Patrimonio documental Español** se atendrá a las de índole policial, procesal, clínico, o de cualquier otra índole que puedan afectar a la seguridad de las personas, a su honor, a la intimidad de su vida privada y familiar y a su propia imagen, y no podrán ser públicamente consultados sin que medie consentimiento expreso de los afectados o hasta que **haya transcurrido un plazo de 25 años desde su muerte** si su fecha es conocida o, en otro caso, de 50 años a partir de la fecha de los documentos.

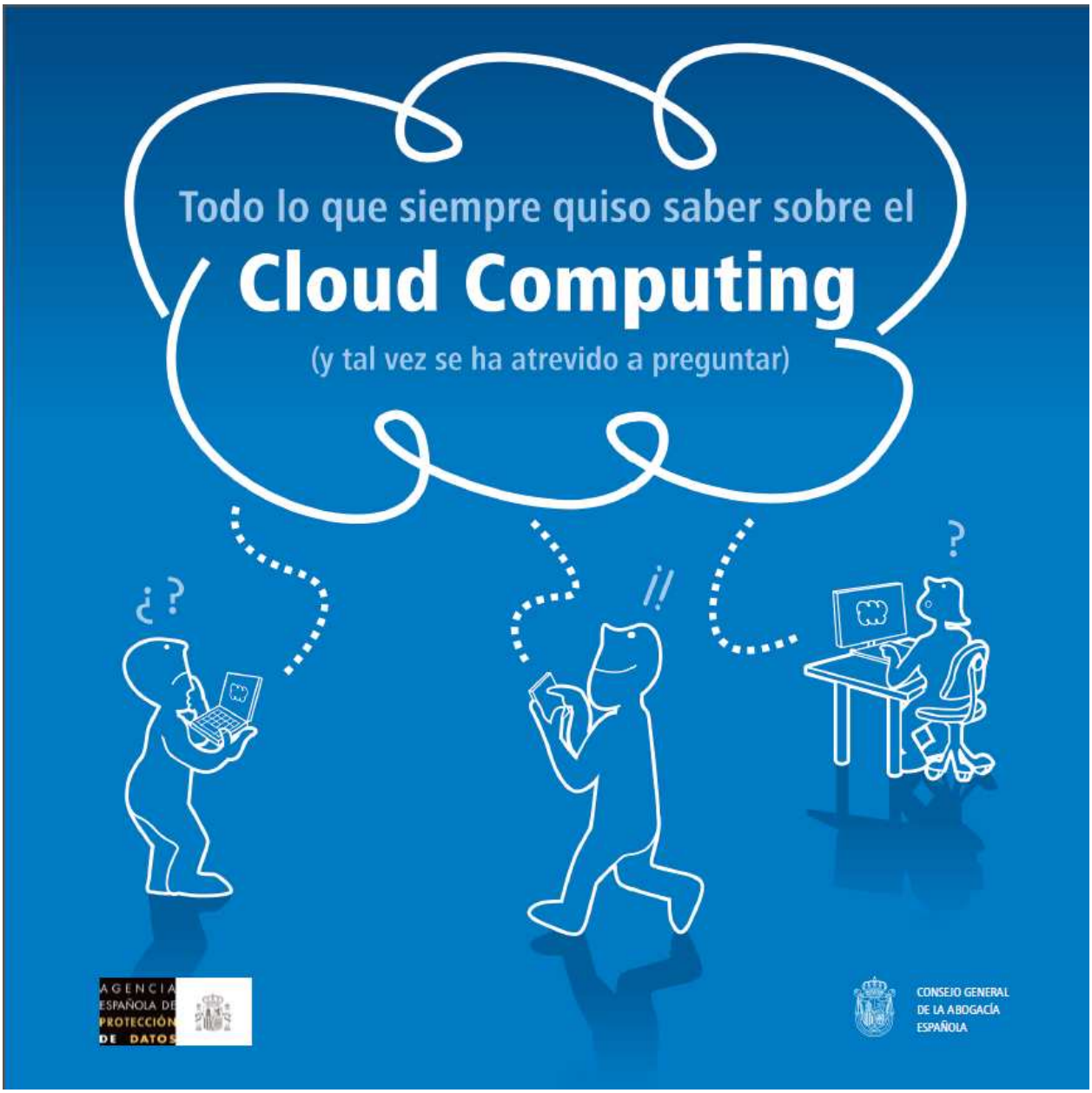
A TENER EN CUENTA

Siempre que se cedan o comuniquen datos hemos de ser extremadamente cautos.

ACTUALIDAD LOPD

La AEPD y CGAE presentan un informe sobre la utilización del cloud computing por los despachos de abogados.

Fuente: www.agpd.es



Puede acceder desde este enlace:

http://www.agpd.es/portalwebAGPD/revista_prensa/revista_prensa/2012/notas_prensa/common/junio/Diptico_CLOUD.pdf

EL PROFESIONAL RESPONDE

¿Qué es la Ingeniería Social?

La Ingeniería Social es un conjunto de **acciones que se realizan con el fin de obtener información** a través de la manipulación de usuarios legítimamente autorizados para acceder a la misma.

Es un conjunto de trucos, engaños y artimañas que permiten confundir a una persona para que entregue información confidencial, ya sea la propia información, los datos necesarios para acceder a ésta o la forma de saltar la seguridad de un sistema.

Se dice que el único ordenador seguro es el que está desenchufado… en una caja fuerte, con una cerradura sellada y enterrada bajo hormigón… y aun así existen riesgos.

Los entendidos en Ingeniería Social, responden que siempre existirá un ser humano dispuesto a enchufarlo…

¿Cómo prevenirlo?

La mejor manera de estar prevenido, es tener el conocimiento sobre la Ingeniería Social. Para ello:

- Todo el **personal** debe ser **concienciado**, desde los usuarios al personal de limpieza.
- **No informar telefónicamente** a nadie de las características técnicas de la red, personal, etc.
- **Controlar el acceso físico** al sitio donde se encuentra los equipos informáticos y comunicaciones.

A TENER EN CUENTA

"El factor humano es el eslabón más débil de la seguridad de la información".

LA LOPD EN LA EMPRESA

Boletín 08/12

PRODASUR

LA LOPD EN EL DÍA A DÍA

Consentimiento en el marco de una relación contractual para otros fines

Si el responsable del tratamiento **solicita el consentimiento** del afectado durante el proceso de formación de un contrato **para finalidades que no guardan relación directa** con el mantenimiento, desarrollo o control de la relación contractual, deberá permitir que el afectado **manifieste expresamente su negativa** al tratamiento o cesión de datos.

En particular, se entenderá cumplido tal deber cuando se permita al afectado la **marcación de una casilla** claramente visible y que no se encuentre ya marcada en el documento que se le entregue para la celebración del contrato o se establezca un procedimiento equivalente que le permita manifestar su negativa.

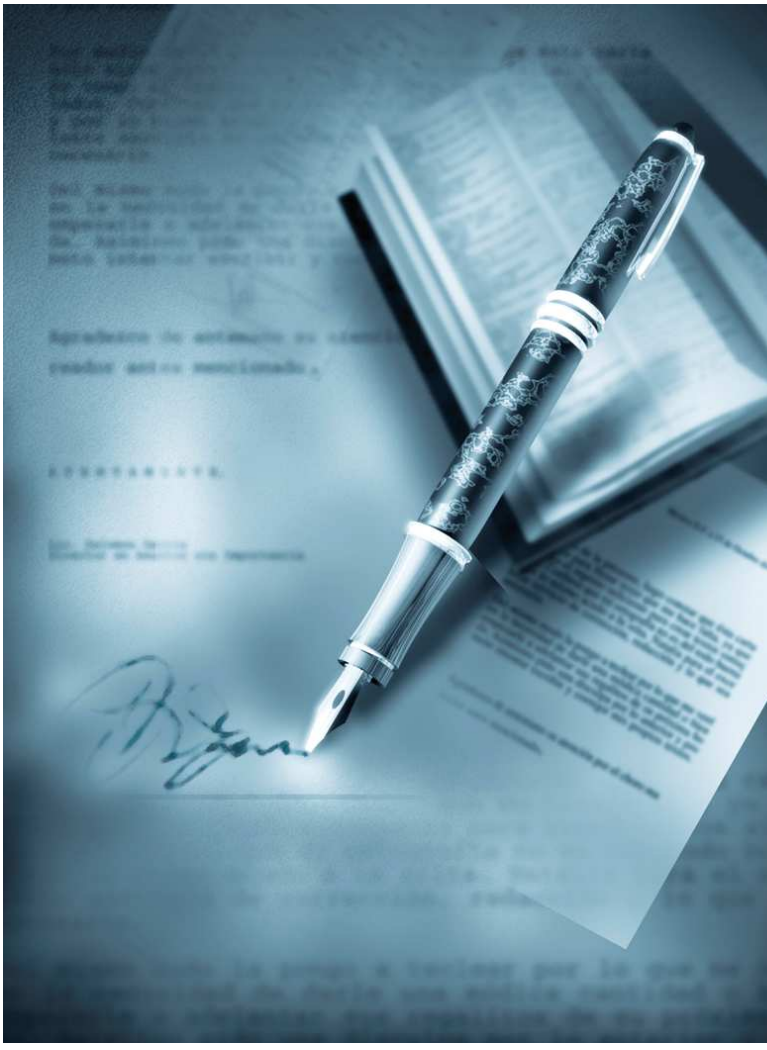
EJEMPLOS

[ ] Si no desea permitir el tratamiento de sus datos conforme la finalidad indicada, marque esta casilla.

[ ] Si no desea que realicemos la cesión de sus datos, marque esta casilla.

Contenido

Consentimiento en el marco de una relación contractual...	1
Cámara sin cartel informativo para controlar trabajadores	2
Publicación de datos personales en foro	3
Reunión del consejo consultivo de la Agencia Española...	4
¿Qué es el código malicioso?	5



A TENER EN CUENTA

El consentimiento es uno de los pilares principal sobre los que se asienta la LOPD.

SANCIONES DE LA AEPD

Cámara sin cartel informativo para controlar trabajadores

En procedimiento sancionador R/00630/2011 de la AEPD se puede ver la sanción que puede sufrir una empresa por colocar **cámaras para controlar a los trabajadores sin** los pertinentes **carteles informativos**.

Con fecha 18 de febrero de 2010, tuvo entrada en esta Agencia **escrito del Ministerio de Trabajo e Inmigración (Inspección provincial de Trabajo y Seguridad Social de Pontevedra) (en lo sucesivo el denunciante)** en el que comunica la instalación de **cámaras de videovigilancia** en un centro en Vigo de Cortefiel S.A. (en lo sucesivo el denunciado) **sin cumplir los requisitos** exigidos en la LOPD.

En su escrito el denunciante manifiesta que, en el citado centro de trabajo del denunciado, **no hay ningún cartel que indique la existencia de cámaras** de videovigilancia y que las cámaras están **disimuladas como detectores de humos**.

Una vez realizada la inspección de la AEPD, ha quedado acreditado que el día de la visita de la Inspección de Trabajo (23/12/2009) **no existía cartel informativo** de grabación de imágenes a los clientes de la tienda, aunque si existían cámaras que graban las **imágenes de los clientes.**

Se puede observar, entonces, que el denunciado ha recabado datos personales de sus clientes **sin facilitar a sus titulares la información** que señala el artículo 5 de la LOPD por lo que debe considerarse que ha incurrido en la infracción leve descrita.

Resultado: Sanción de 2.000€ por una infracción del artículo 5.1 de la LOPD, tipificada como leve.

El principio de información es vital para el cumplimiento de la LOPD.

IMPORTANTE

Como podemos ver en este procedimiento, **quien ha denunciado es la propia Inspección de Trabajo**, no un trabajador de la empresa.

LA AEPD ACLARA

Publicación de datos personales en foro

El informe 0023/2010 de la AEPD resuelve la consulta planteada sobre **si para el tratamiento y publicación de datos personales en el foro de la página web de la Asociación de enfermos consultante, es preciso incluir una cláusula en la que se recoja la política de privacidad de la Asociación, de acuerdo con la LOPD.**

De dicho informe jurídico se extrae lo siguiente:

ff) **La actividad objeto de la consulta supone un tratamiento de datos** de carácter personal cuya publicación en el foro constituye una cesión de datos a terceras personas.

gg) **Será obligación de la Asociación** consultante como responsable de los datos aludidos, la de **obtener el consentimiento** del interesado para dicho tratamiento.

hh) **Este consentimiento**, por tratarse de un foro de afectados por una determinada enfermedad, y siendo posible que se traten **datos de salud**, deberá ser además **expreso**, entendiendo por tal, aquél que se obtiene de una declaración clara e inequívoca por parte del interesado que acepta o rechaza la cesión y uso de sus datos mediante la expresión de su voluntad de forma que permita su constancia y prueba indubitada.

En conclusión, **no solamente resulta obligado el aviso legal**, sino que parece conveniente que el mismo se incluya en la página de gestión del foro, **impidiéndose la inclusión de dato personal alguno sin que se haya aceptado el mismo**, lo que, puede constituir la prueba de que se ha obtenido el consentimiento expreso e informado del interesado para el tratamiento y publicación de los datos.

A TENER EN CUENTA

Siempre que se cedan o comuniquen datos hemos de ser extremadamente cautos.

ACTUALIDAD LOPD

Reunión del consejo consultivo de la Agencia Española de Protección de Datos el pasado 19 de Julio de 2012

Fuente: www.agpd.es

AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS

Bienvenido | Benvinguts | Benvidos | Ongi etorri

Buscar en agpd.es buscar

Búsqueda avanzada

Canal del Ciudadano | Canal del Responsable | Resoluciones y Documentos | Ficheros Inscritos | Internacional | Gabinete de Comunicación |

- Notas de prensa
- Agenda
- Revista de prensa

Agenda 2012

Madrid, 19 de julio de 2012

Reunión del Consejo Consultivo de la Agencia Española de Protección de Datos

El Consejo Consultivo de la Agencia Española de Protección de Datos (AEPD) se reúne el 19 de julio para analizar las principales actividades de la institución durante el primer semestre de 2012.

El Consejo Consultivo es el órgano colegiado que tiene como funciones el asesoramiento del director de la AEPD, emitir informes en relación a las cuestiones que le someta el director y formular propuestas sobre temas relacionados con las materias de competencia de la Agencia.

A la reunión asisten José Luis Rodríguez Álvarez, director de la Agencia Española de Protección de Datos; Santiago Abascal, director de la Agencia de Protección de Datos de la Comunidad de Madrid; José Ignacio Pariente de Prada, director de la Agencia Vasca de Protección de Datos; Meritxell Batet, a propuesta del Congreso de los Diputados; María Rosa Vindel, a propuesta del Senado; Francisco Díaz, como vocal de la Administración Local; Feliciano Barrios, a propuesta de la Real Academia de la Historia; Antonio Troncoso, a propuesta del Consejo de Coordinación Universitaria; Alejandro Perales, como vocal de los consumidores y usuarios, y Belén Veleiro, como vocal del sector de ficheros privados.

Asistentes a la reunión del Consejo Consultivo de la Agencia Española de Protección de Datos

subir

Gabinete de Prensa | English Resources | Página de inicio | Enlaces | Contacto | Sugerencias web | Glosario

Agencia Española de Protección de Datos © 2010 | Política de Privacidad | Requisitos técnicos | Aviso legal

Puede acceder desde este enlace:

http://www.agpd.es/portalwebAGPD/agenda/2012/news/2012_07_19-ides-idphp.php

EL PROFESIONAL RESPONDE

¿Qué es el código malicioso?

Se denomina código malicioso a cualquier programa escrito para producir inconvenientes, destrucción o violar la política de seguridad de un sistema.

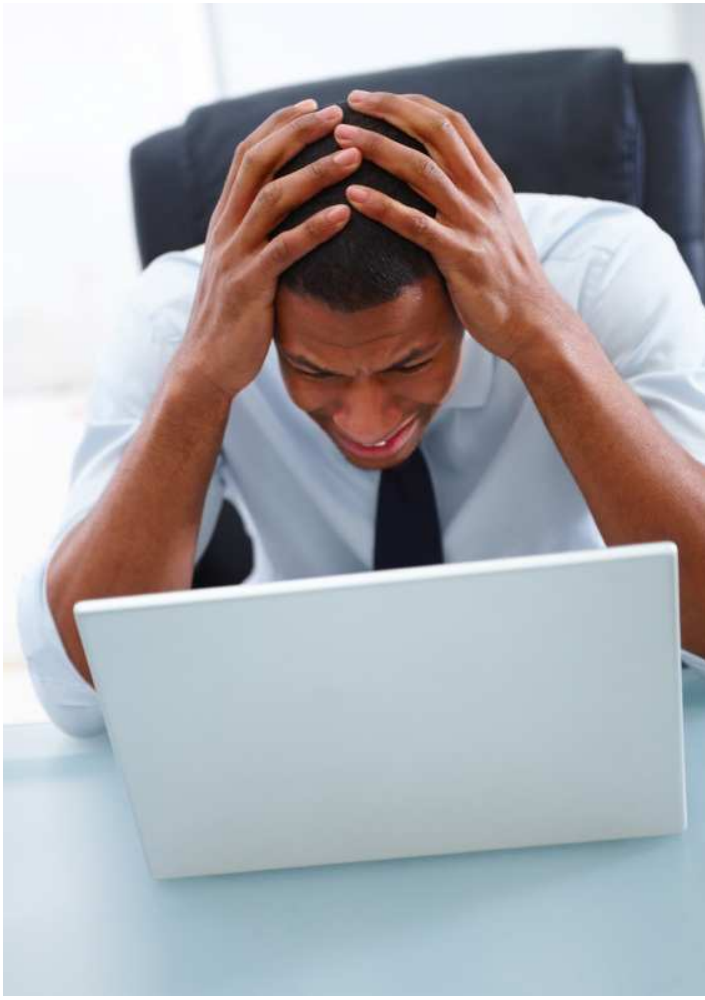
Hay diversos tipos de código malicioso, como virus, troyanos, spywares, keyloogers, etc.

El código malicioso puede realizar diversas acciones en los sistemas (hacer daño, obtener información, capturar nuestro equipo para su uso, etc.).

En función de la finalidad que pretenda, el código malicioso puede:

- **Borrar archivos** del disco duro para que el ordenador quede inoperativo.
- Infectar un sistema y usarlo para **atacar a otros**.
- **Obtener información** de usted: sitios que visita y hábitos en el uso.
- **Grabar sus conversaciones** activando el micrófono o grabar su **imagen** activando su webcam.
- **Ejecutar comandos** como si lo hubiese hecho usted.
- **Robar archivos** del equipo, por ejemplo, aquellos con información personal, financiera, contraseñas, fotos, etc.

Hay que tener en cuenta que ningún antivirus puede detectar todo el código malicioso.



A TENER EN CUENTA

"El factor humano es el eslabón más débil de la seguridad de la información".

LA LOPD EN LA EMPRESA

Boletín 09/12

PRODASUR

LA LOPD EN EL DÍA A DÍA

El Documento de Seguridad y las medidas de seguridad que contiene

El **Documento de Seguridad** describe las **medidas** que la organización tiene implantadas para **garantizar la seguridad** de los datos personales y cuyo objetivo es evitar:

- La pérdida de datos.
- La alteración no autorizada de los mismos.
- El acceso o difusión no autorizada.

Para ello, se debe tener en cuenta:

- La naturaleza de los datos almacenados.
- El estado de la tecnología.
- Los riesgos a que están expuestos dichos datos.

Es decir, no serán las mismas medidas de seguridad las que deberán implantarse para el tratamiento de datos meramente identificativos (nombre, apellidos, domicilio, etc.), que para el tratamiento de datos especialmente protegidos (salud, ideología, vida sexual, etc.).

El tratamiento de datos más comprometidos requiere de más medidas de seguridad.

Contenido

El Documento de Seguridad y las medidas de seguridad...	1
Error en el ensobrado de dos informes médicos	2
Prevención del Blanqueo de Capitales y LOPD	3
Nueva sección con recomendaciones para usuarios de...	4
¿Qué ocurre si no puedo aplicar todas las medidas de...	5

A TENER EN CUENTA

El responsable del fichero debe asegurarse de que las medidas de seguridad se aplican.

SANCIONES DE LA AEPD

Error en el ensobrado de dos informes médicos

En el procedimiento sancionador PS/00159/2012 se puede ver la sanción que puede sufrir una empresa por **un error a la hora de realizar el ensobrado e intercambiar dos informes médicos**.

Con fecha de 12 de abril de 2011 tiene entrada en la AEPD un escrito de Dª. A.A.A. en el que declara que tras acudir en fecha 14/02/2011 para una **revisión ginecológica** a los **servicios de prevención de IBERMUTUAMUR**, el día 17/03/11 **recibió, vía postal, el resultado de su citología y el informe médico de la revisión realizada a Dª. B.B.B.**. Al día siguiente la denunciante contacta con ella a través de los datos de trabajo que, junto a los datos médicos, obraban en el informe. **Dª. B.B.B. le informó que, a su vez, ella disponía del informe de la denunciante**.

Aunque IBERMUTUAMUR **envió el Documento de Seguridad a la AEPD y alegó que ese incidente era un caso aislado**, ya que se realizan envíos de forma cotidiana y no ha habido nunca ningún problema, en el procedimiento sancionador se hace referencia a la sentencia de la Audiencia Nacional en la que se impone la **obligación de resultado**. Es decir, que se adopten las medidas necesarias para evitar que los datos se pierdan, extravíen o acaben en manos de terceros, siendo insuficiente con acreditar que adopta una serie de medidas, pues es también **responsable de que las mismas se cumplan y se ejecuten con rigor**.

En definitiva, IBERMUTUAMUR, no actuó con la diligencia debida al **no adoptar las medidas de seguridad necesarias** y suficientes para impedir el acceso a la información de carácter personal.

Resultado: Sanción de 4.000€ por infracción del art. 9.1 de la LOPD, relativo a la seguridad de los datos y tipificada como grave.

El Documento de Seguridad debe detallar las medidas aplicadas.

IMPORTANTE

Las medidas de seguridad no solo deben estar en el Documento de Seguridad, han de implantarse de forma efectiva. El responsable ha de vigilar que se cumplan.

LA AEPD ACLARA

Prevención del Blanqueo de Capitales y LOPD

El informe 0517/2010 de la AEPD resuelve la consulta planteada sobre **cuál es el régimen jurídico aplicable a las cesiones de datos en el seno de los Sistemas Institucionales de Protección SIP (mecanismo de consolidación de Entidades de crédito para su autoprotección), para el cumplimiento de las obligaciones de prevención del blanqueo de capitales y de la financiación del terrorismo, en relación a la LOPD.**

De dicho informe jurídico se extrae lo siguiente:

ii) El artículo 24 de la Ley 10/2010 traspone al derecho español lo dispuesto en el artículo 28 de la Directiva 2005/60/CE, del Parlamento Europeo y del Consejo, relativa a la prevención de la utilización del sistema financiero para el blanqueo de capitales y para la financiación del terrorismo, cuyo apartado 1 dispone que **las entidades y personas sujetas a lo dispuesto en la presente Directiva, así como sus directivos y empleados, no revelarán al cliente de que se trate ni a terceros que se ha transmitido información** ni que está realizándose o puede realizarse una investigación sobre blanqueo de capitales o financiación del terrorismo.

jj) No obstante, la Directiva, dispone que **esta prohibición no impedirá la comunicación entre entidades de los Estados miembros, o de terceros países**, siempre que cumplan las condiciones establecidas en el artículo 11, apartado 1, que pertenezcan al mismo grupo.

En conclusión, **la cesión de datos entre las entidades que conforman un sistema institucional de protección con la finalidad de prevención del blanqueo de capitales y la financiación del terrorismo se encuentra amparada por el art. 11.2 a) de la LOPD**, en conexión con el artículo 24.2 a) de la Ley 10/2010 y, particularmente, del artículo 28.3 de la Directiva 2005/60/CE.

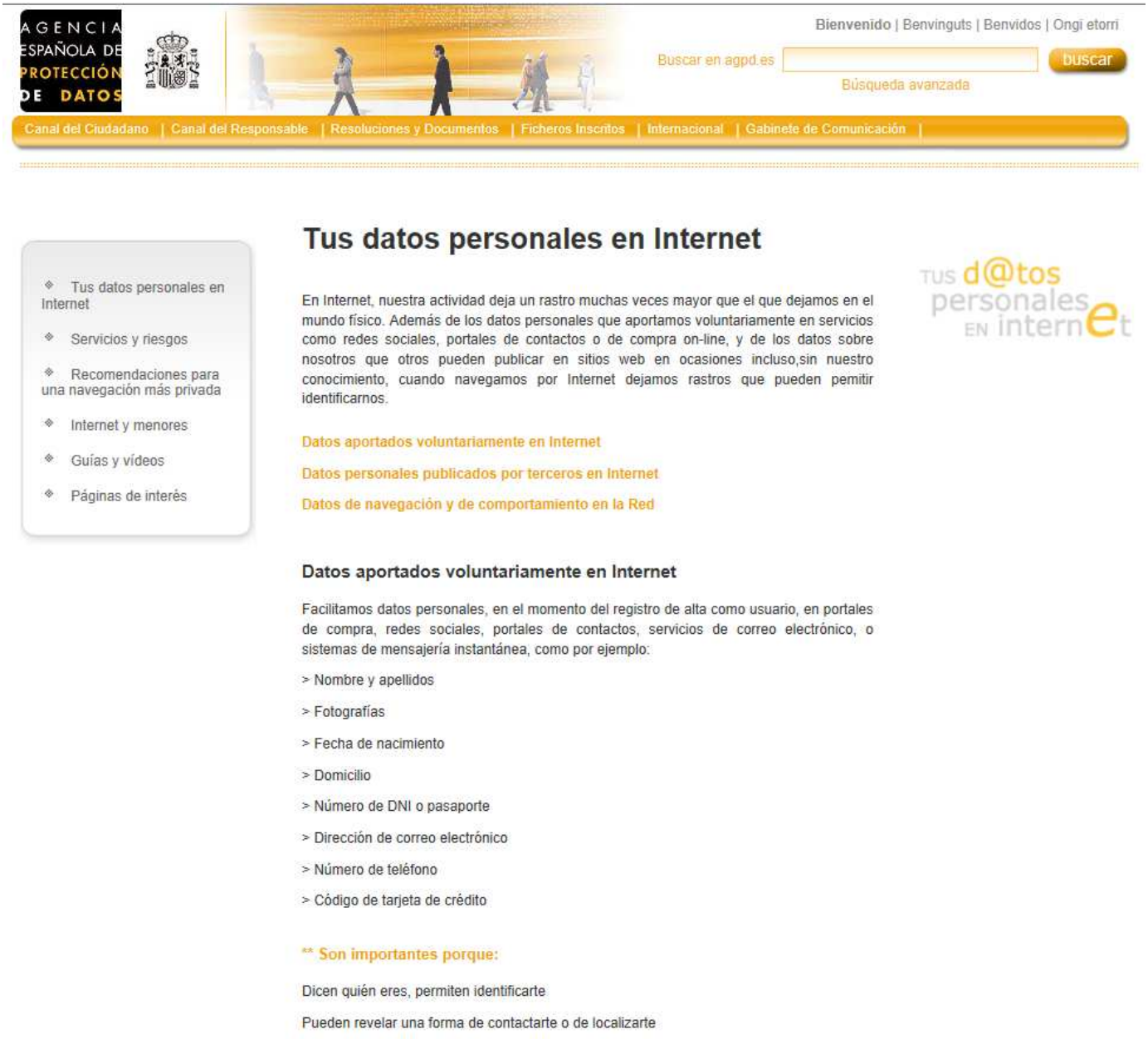
A TENER EN CUENTA

Siempre que se cedan o comuniquen datos hemos de ser extremadamente cautos.

ACTUALIDAD LOPD

Nueva sección con recomendaciones para usuarios de Internet en la web de la Agencia Española de Protección de Datos

Fuente: *www.agpd.es*



Puede acceder desde este enlace:

http://www.agpd.es/portalwebAGPD/jornadas/dia_internet_2012/tus_datos_personales_en_internet-ides-idphp.php

EL PROFESIONAL RESPONDE

¿Qué ocurre si no puedo aplicar todas las medidas de seguridad a todos los datos personales que trato?

Una de las obligaciones que tiene el responsable del fichero es **proteger los datos personales** que trata.

Los riesgos a que están expuestos los ficheros pueden venir, tanto de la acción humana, como de circunstancias naturales, o de accidentes fortuitos.

Resulta necesario que el responsable del fichero adopte las medidas adecuadas y necesarias para garantizar la protección de datos de carácter personal para evitar su destrucción, pérdida, alteración, difusión o acceso no autorizado.

FICHEROS QUE NO REUNAN LAS CONDICIONES DE SEGURIDAD

No se registrarán datos de carácter personal en ficheros que no reúnan las condiciones requeridas respecto a su integridad y seguridad y las de los centros de tratamiento, locales, equipos, sistemas y programas.

Es decir, que **no tenemos excusa**. Si tratamos datos personales hemos de **aplicar las medidas de seguridad** descritas en el Documento de Seguridad.

A TENER EN CUENTA

El responsable del fichero debe asegurarse de que las medidas de seguridad se aplican.

LA LOPD EN LA EMPRESA

Boletín 10/12

PRODASUR

LA LOPD EN EL DÍA A DÍA

El ciclo de vida de los datos

En el tratamiento de los datos personales tenemos cuatro momentos fundamentales:

1. Recogida de los datos

Es el momento en que se recogen los datos. Puede ser del propio interesado, de un Tercero o de fuentes accesibles al público.

2. Conservación y utilización de los datos

Es el momento en que introducimos los datos recogidos en el fichero y los utilizamos para una finalidad específica. Por ejemplo, elaborar facturas, nóminas, contratos, etc.

3. Comunicación de los datos

Es el momento en que comunicamos los datos, o el resultado del tratamiento a Terceros. Esto es conocido como "cesión o comunicación de datos", ya sea a otra entidad o a la administración.

4. Supresión de los datos

Es el momento en que eliminamos definitivamente los datos porque ya no son necesarios o pertinentes para la finalidad para la cuál fueron recabados en su momento.

En cada uno de estos momentos existen unas obligaciones específicas y definidas que han de ser cumplidas.

Contenido

El ciclo de vida de los datos	1
Sanción por no atender requerimiento de la AEPD	2
Uso de cámaras para controlar asistencia	3
Las denuncias de los ciudadanos a la AEPD han aumentado...	4
¿Qué es un plan de contingencias?	5

A TENER EN CUENTA

El responsable del fichero es responsable en todos y cada uno estos momentos de lo que se hace con los datos.

SANCIONES DE LA AEPD

Sanción por no atender requerimiento de la AEPD

En el procedimiento sancionador PS/00101/2012 se puede ver la sanción que puede sufrir una empresa **por no atender debidamente el ejercicio de los derechos de los ciudadanos, máxime, cuando la AEPD lo ha requerido para ello.**

El afectado, si no se atienden sus derechos, puede pedir tutela a la AEPD

Con fechas 4 y 13 de enero de 2012, tuvieron entrada la AEPD escritos de Don B.B.B. (en lo sucesivo el enunciante), en los que denuncia que Don A.A.A. (en lo sucesivo el denunciado) **no ha cumplido el requerimiento del Director de esta AEPD**, relativo a la Resolución de la tutela de derechos nº TD/00706/2010, por la que se estimaba su reclamación y se instaba al denunciado para que en el plazo de diez días facilitase el acceso a sus datos sanitarios contenidos en sus ficheros o, en su defecto, denegase motivada y fundamentadamente dicho acceso.

En fecha 2 de abril de 2012, se intentó la notificación del citado acuerdo de **inicio de procedimiento sancionador** al denunciado, por medio del servicio de correos, con el resultado de "**Ausente en reparto**". Se envió para su notificación el citado acuerdo de inicio de procedimiento sancionador al denunciado, mediante su exposición en el Tablón de edictos del Ayuntamiento de Valencia. El edicto estuvo expuesto en el Tablón de edictos del Ayuntamiento de Madrid desde el 25 de abril al 15 de mayo de 2012. El 27 de abril de 2012 se publicó en el Boletín Oficial del Estado, otorgándose al denunciado plazo para efectuar alegaciones a dicho acuerdo.

La **falta de atención** al requerimiento del Director de la AEPD al imputado en este procedimiento, **establece la base de facto para fundamentar la imputación de la infracción**.

Resultado: Sanción de 5.000€ por infracción del art. 37.1.a) de la LOPD.

IMPORTANTE

Es sumamente importante atender los derechos de los ciudadanos en tiempo y forma para evitar problemas futuros.

LA AEPD ACLARA

Uso de cámaras para controlar asistencia

El informe 0392/2011 de la AEPD resuelve la consulta planteada sobre **la conformidad con lo dispuesto en la LOPD, y su Reglamento de Desarrollo, del tratamiento de los datos necesarios para el reconocimiento de los alumnos de un determinado centro universitario a través de programas de reconocimiento facial, que se utilizarán para el control de su asistencia a las clases y la identificación de los mismos en la realización de las correspondientes pruebas.**

De dicho informe jurídico se extrae lo siguiente:

ll) Para comprobar si una medida restrictiva supera el juicio de proporcionalidad, y por tanto, puede aplicarse, se ha de constatar que cumple estas tres condiciones:

   a. Si tal medida es susceptible de **conseguir el objetivo** propuesto (juicio de idoneidad).

   b. Si, además, es necesaria, en el sentido de que **no exista otra medida más moderada** para la consecución de tal propósito con igual eficacia (juicio de necesidad).

   c. Y finalmente, si la misma es ponderada o **equilibrada**, por derivarse de ella más beneficios que perjuicios (juicio de proporcionalidad en sentido estricto).

mm) La finalidad, propuesta, **control de asistencia, podría lograrse** igualmente a través de **otros mecanismos** utilizados habitualmente y menos intrusivos.

En conclusión, dicho tratamiento de los datos **vulnera**, a juicio de la AEPD, **el principio de proporcionalidad** y, en segundo lugar, **genera unos riesgos innecesarios** derivados del propio tratamiento de los datos que no se concilian fácilmente con las normas reguladoras del derecho fundamental a la protección de datos de carácter personal.

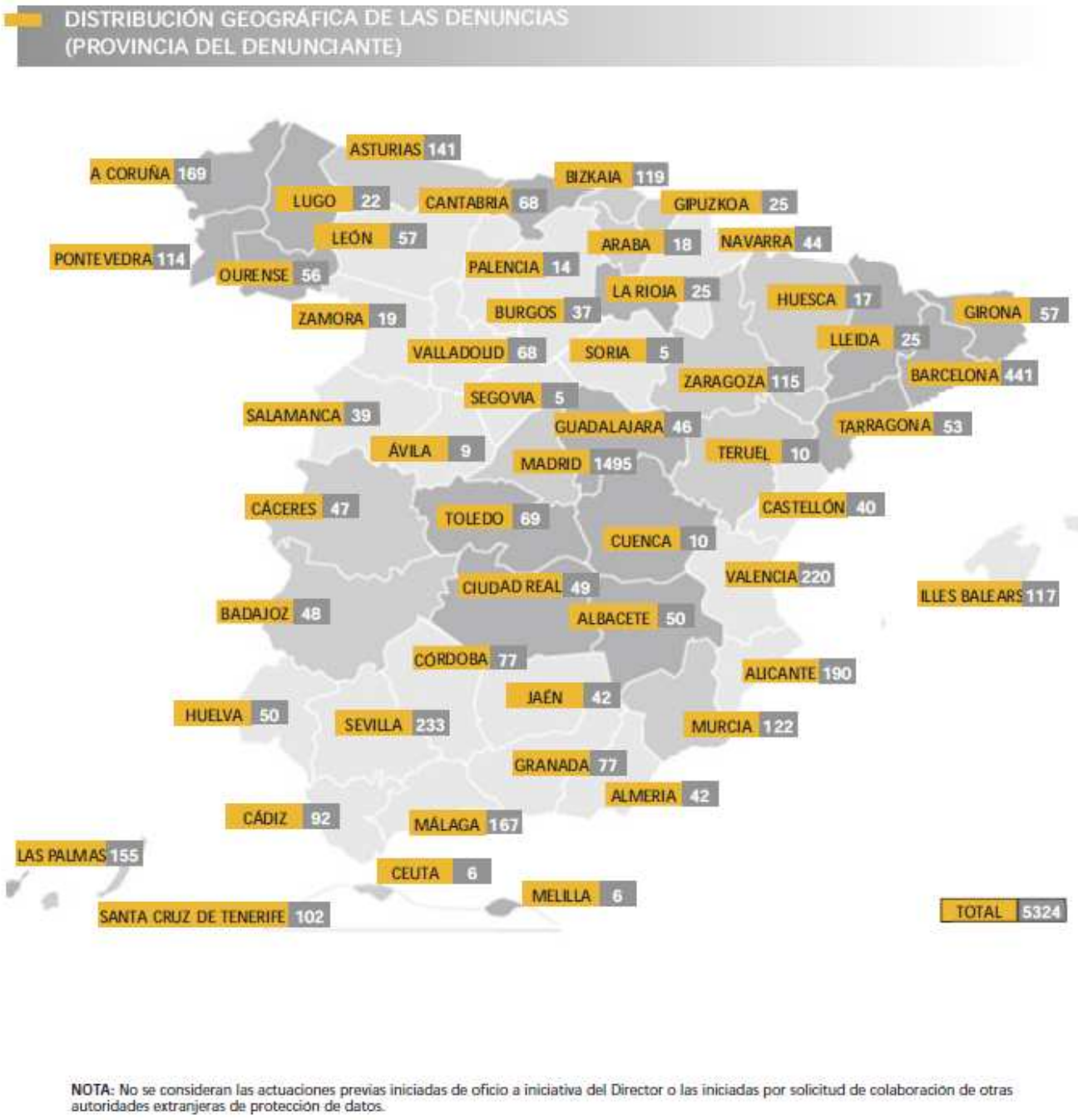
A TENER EN CUENTA

El uso de cámaras de vigilancia y reconocimiento facial es algo que debe estar debidamente justificado.

ACTUALIDAD LOPD

Las denuncias de los ciudadanos a la AEPD han aumentado un 51,60% en 2011

Fuente: *www.agpd.es*



NOTA: No se consideran las actuaciones previas iniciadas de oficio a iniciativa del Director o las iniciadas por solicitud de colaboración de otras autoridades extranjeras de protección de datos.

Puede acceder desde este enlace:

http://www.agpd.es/portalwebAGPD/canaldocumentacion/memorias/memoria_2011/common/Memoria_2011.pdf

EL PROFESIONAL RESPONDE

¿Qué es un plan de contingencias?

El plan de contingencias y continuidad de negocio puede definirse como el **conjunto de procedimientos que permiten un rápido retorno a una situación suficientemente normalizada** para que la actividad de la organización recupere un nivel aceptable después de una interrupción no prevista de sus sistemas de información.

Dicho plan contiene las medidas técnicas, humanas y organizativas necesarias para **garantizar la continuidad del negocio y las operaciones** de la organización ante un evento desafortunado.

Por ejemplo: si en su organización se avería el servidor y no es posible dar servicio a sus clientes:

a) **¿Dispone de medidas de respaldo preventivas?**
   Como por ejemplo, copias de seguridad de la información ACTUALIZADAS.

b) **¿Dispone de un plan de acción en función del origen del problema?**
   No es igual la avería de la placa base que el disco duro.

c) **¿Sabe cuánto es el tiempo máximo que puede estar inoperativo antes de comenzar a perder clientes?**

d) **¿Dispone de recursos alternativos que le permitan dar un servicio aceptable mientras se soluciona la situación?**

Un plan de contingencias y continuidad de negocio responde estas preguntas y **le permite estar preparado ante situaciones críticas.**

A la izquierda hemos planteado una serie de preguntas.

Intente responderlas, a lo mejor se sorprende.

LA LOPD EN LA EMPRESA

Boletín 11/12

PRODASUR

LA LOPD EN EL DÍA A DÍA

Almacenamiento de la documentación en formato papel (facturas, albar., etc.).

Los dispositivos utilizados para el almacenamiento de los documentos que contengan datos personales deben **disponer de mecanismos** que **obstaculicen su apertura** a las **personas no autorizadas** para acceder a dicha documentación.

Es decir, se debe almacenar dicha documentación (los archivadores con las facturas, albaranes, nóminas, etc.), en armarios, cajoneras, etc. que dispongan de cerradura con llave u otro dispositivo similar. Obviamente, solo deben disponer de la llave las personas autorizadas a acceder a dicha documentación y los dispositivos deben permanecer cerrados mientras no sea necesario acceder a los documentos almacenados en ellos.

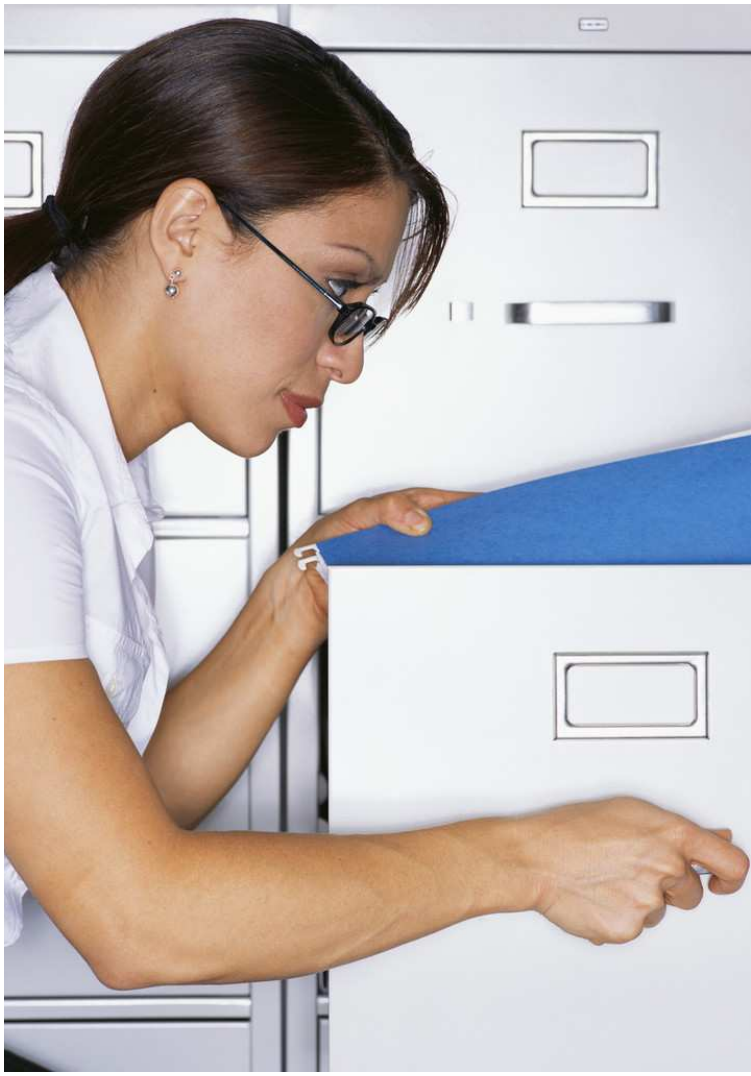
¿Y qué hacemos si los armarios no disponen de cerradura?

En este caso, la normativa nos indica que si las características físicas no permiten adoptar esta medida, el responsable del fichero adoptará medidas que impidan el acceso de personas no autorizadas.

Estas medidas pueden ser **trasladar toda esta documentación a un recinto aparte cerrado con llave**, u otra similar, que garantice que los documentos no van a ser accedidos por alguien no autorizado.

Contenido

Almacenamiento de la documentación en formato papel...	1
Sanción por compartir fichero con datos por eMule	2
Cambio de sexo y protección de datos	3
Las Autoridades Europeas de Protección de Datos...	4
¿Qué son etiquetas las RFID y qué relación tienen con la...	5



A TENER EN CUENTA

Las medidas de seguridad descritas en el Documento de Seguridad deben cumplirse.

SANCIONES DE LA AEPD

Sanción por compartir fichero con datos por eMule

En la resolución R/02437/2012 de la AEPD se puede ver la **sanción que puede sufrir una empresa por no tener implantadas las medidas de seguridad que exige la LOPD**.

Los usuarios han de ser formados en el uso adecuado de la informática.

Con fecha 16 de julio de 2007, tuvo entrada en la AEPD un correo electrónico de la Policía Local del Concello de Ourense, **en el que manifiesta que el día 10 de ese mes han encontrado y descargado un archivo de un usuario de Internet, en entorno compartido Emule, siendo el nombre del archivo "PONFERRADA AFILIADOS FIA BIERZO ACCESS 2000.MDB"**. En fecha 10/7/2007 a las 16:21 horas se identificó la IP del usuario de emule que compartía el citado archivo, resultando ser la ***IP.1.

Una vez realizada la inspección de la AEPD, se verifica que la base de datos se compone de diferentes tablas entre las que se encuentran las denominadas "AFILIADO" y "EMPRESAS", verificando que la primera se compone de 2.890 registros. Dicha base de datos corresponde a una aplicación informática utilizada para la gestión del fichero que se encuentra alojada en un servidor ubicado en la propia secretaría de la organización sindical donde se realiza la inspección. El problema se ocasionó porque un **usuario permitió que el archivo pudiera ser compartido por otros a través de eMule**, aunque no está probado que el mismo lo hiciera conscientemente y con la intención de dar a conocer o difundir este archivo, ni que con ello pretendiera perjudicar a los afiliados o a la organización sindical FIA-UGT de la comarca del Bierzo.

Resultado: **Sanción de 6.000€** a la FEDERACIÓN ESTATAL DE INDUSTRIAS AFINES DE LA UNIÓN GENERAL DE TRABAJADORES **por una infracción del artículo 9.1 de la LOPD**, tipificada como grave.

IMPORTANTE

No deben instalarse aplicaciones para compartir archivos en equipos utilizados para el tratamiento de datos personales.

LA AEPD ACLARA

Cambio de sexo y protección de datos

El informe 0268/2011 de la AEPD resuelve la consulta planteada sobre el **modo en que deberán aplicarse las previsiones de la LOPD**, y su Reglamento de desarrollo, en el supuesto en que una **persona que ha sido sometida a un tratamiento de transexualidad ha solicitado la rectificación de sus datos**, de forma que aparezcan recogidos en la historia clínica de la paciente con su **nuevo nombre**. En particular, se plantea si debería modificarse el nombre de la paciente en los datos relacionados con episodios de la historia clínica acaecidos **mientras la paciente era hombre**.

De dicho informe jurídico se extrae lo siguiente:

oo) La necesidad de que los **datos relacionados con el paciente** aparezcan en la historia clínica en su **situación actual**, de forma que la información aparezca vinculada con la misma.

pp) No obstante, los **episodios contenidos en la historia** deberán **conservarse con la debida exactitud e integridad**, a fin de poder garantizar una adecuada asistencia sanitaria al paciente a tenor de toda la información sanitaria disponible, teniendo particularmente en cuenta las peculiaridades que pudieran derivarse, en relación con determinadas dolencias, del sexo del paciente, dado que en la consulta se señala que "el modo de enfermar es diferente en función del género", existiendo además determinadas dolencias vinculadas exclusivamente a un género determinado.

Consecuencia de todo ello será que **si bien la información contenida en la historia clínica** deberá figurar en su denominación bajo el **nombre de la paciente**, los **concretos episodios contenidos** en la misma deberán **conservar la información necesaria que garantice** el **conocimiento** por los facultativos que accedan a la historia de que la paciente en el momento de desarrollarse **dicho episodio era del género masculino**.

A TENER EN CUENTA

Cuando se tratan datos de personales relativos a la salud hemos de ser extremadamente cautos.

ACTUALIDAD LOPD

Las Autoridades Europeas de Protección de Datos concluyen su investigación sobre la nueva política de privacidad de Google

Fuente: *www.agpd.es*

Liderada por la Autoridad francesa de protección de datos (CNIL)

Las Autoridades Europeas de Protección de Datos concluyen su investigación sobre la nueva política de privacidad de Google

- **Reclaman a Google que informe de una forma más clara a sus usuarios y le piden que ofrezca un mayor control sobre la combinación de datos entre sus numerosos servicios.**
- **Solicitan a la empresa que modifique las herramientas que emplea para evitar una recogida excesiva de datos.**

(Madrid, 16 de octubre de 2012). Las Autoridades europeas de protección de datos han publicado sus conclusiones respecto de la nueva política de privacidad implementada por Google el pasado mes de marzo, tras meses de investigación liderada por la Autoridad francesa de protección de datos (CNIL).

Tras analizar las respuestas y la documentación proporcionada por Google, las Autoridades concluyen que Google **no proporciona suficiente información a los usuarios** sobre sus operaciones de tratamiento de datos. Asimismo, considera que Google **no ofrece al usuario un control sobre el modo en que sus datos se combinan entre los diferentes servicios** de Google.

Puede acceder desde este enlace:

http://www.agpd.es/portalwebAGPD/revista_prensa/revista_prensa/2012/notas_prensa/common/octubre/121016_NP_conclusiones_Google.pdf

EL PROFESIONAL RESPONDE

¿Qué son las etiquetas RFID y qué relación tienen con la protección de datos personales?

La Identificación por Radio Frecuencia o RFID es una tecnología que permite **identificar un objeto gracias a una onda emisora incorporada en el mismo** que transmite por radiofrecuencia los datos identificativos del objeto (etiquetas de seguridad, chips, carnet biblioteca, tarjeta de control de trabajadores, pulseras chip, etc.).

Si bien esta tecnología mejora la eficiencia y comodidad de los sistemas de uso diario, a veces plantea **riesgos para la seguridad y la privacidad** de los usuarios.

En los casos en los que las etiquetas **contengan información personal** o asociada a personas físicas, serán de aplicación las normas sobre protección de datos personales, en concreto, la **LOPD**.

Los usuarios deben **conocer la tecnología**, interesarse por el uso que se va a hacer de ella, conocer el modo de ejercer sus derechos y trasladar a los responsables del uso de estas tecnologías la necesidad de respetar su derecho fundamental a la protección de datos en los procesos de diseño de nuevos servicios de RFID.

El INTECO ha **editado una guía sobre la tecnología RFID** y sus implicaciones en la normativa de protección de datos que puede descargarse desde aquí.

A TENER EN CUENTA

Antes de utilizar una nueva tecnología hay que ponderar sus beneficios contra las implicaciones que tiene de cara a la privacidad.

Boletín 12/12
LOPD EN LA EMPRESA
AUTOR: JULIO CÉSAR MIGUEL PÉREZ

LA LOPD EN EL DÍA A DÍA

Cuidado con las selecciones de personal y la protección de datos personales

Contenido

Cuidado con las selecciones de personal y la protección de... 1
Sanción por no facilitar derecho de acceso 2
Cesión de datos a los registros de cáncer 3
La AEPD autoriza un nuevo modelo de transferencia... 4
¿Qué es el Registro General de Protección de Datos de la... 5

Últimamente está apareciendo una nueva picaresca en relación con la LOPD y los procesos de selección de personal.

La operativa es la siguiente:

- Su empresa publica un anuncio en el cuál solicita el Curriculum Vitae para seleccionar candidatos para un puesto de trabajo.
- Un candidato nos entrega su Curriculum Vitae.
- Pasado un tiempo nos pide la devolución del mismo, al tiempo que nos indica que, como no le hemos informado tal, y como establece la LOPD de la identidad del responsable y la finalidad a la que va a destinar los datos, nos va a denunciar a la AEPD.
- **Se ofrece a no denunciarnos a la AEPD a cambio de una compensación económica.**

Por tanto, debemos ser especialmente escrupulosos en los procesos de selección de personal con el cumplimiento de la LOPD, ya que no sabemos quién nos está proporcionando sus datos.

A TENER EN CUENTA

El momento de la recogida de los datos es crucial para el buen cumplimiento de la LOPD.

SANCIONES DE LA AEPD

Sanción por no facilitar derecho de acceso

En la resolución R/01627/2012 de la AEPD se puede ver la **sanción que puede sufrir una empresa por no facilitar el derecho de acceso a un ciudadano**.

Hemos de contestar a un requerimiento de derechos ARCO rápidamente.

Con fechas 4 y 13 de enero de 2012, tuvieron entrada en la AEPD escritos de Don B.B.B. (en lo sucesivo el denunciante), en los que denuncia que Don A.A.A. (en lo sucesivo el denunciado) **no ha cumplido el requerimiento del Director de la AEPD, relativo a la Resolución de la tutela de derechos nº TD/00706/2010**, por la que se estimaba su reclamación y se instaba al denunciado para que en el plazo de diez días facilitase el acceso a sus datos sanitarios contenidos en sus ficheros o, en su defecto, denegase motivada y fundamentadamente dicho acceso.

Anteriormente, y con fecha 7 de octubre de 2010, el Director de la Agencia Española de Protección de Datos, en la TD/00706/2010 resolvió: <<ESTIMAR la reclamación formulada por Don B.B.B. e instar a Don A.A.A. para que, en el plazo de los diez días hábiles siguientes a la notificación de la presente resolución, remita al reclamante certificación en la que se facilite el acceso completo a sus datos, o deniegue motivada y fundamentadamente el acceso solicitado, pudiendo incurrir en su defecto en una de las infracciones previstas en el artículo 44 de la LOPD. Las actuaciones realizadas como consecuencia de la presente Resolución deberán ser comunicadas a esta Agencia en idéntico plazo>>.

El denunciado **hizo caso omiso** a dicha resolución, no ejerciendo el derecho que acceso que se le requería en la misma.

Resultado: **Sanción de 5.000€ por una infracción del artículo 37.1.a) de la LOPD**, tipificada como grave.

IMPORTANTE

El hacer caso omiso a los requerimientos de la Agencia Española de Protección de Datos puede acarrear una fuerte sanción.

LA AEPD ACLARA

Cesión de datos a los registros de cáncer

El informe 0262/2011 de la AEPD resuelve la consulta planteada sobre si resulta conforme a lo dispuesto en la LOPD, la **comunicación de datos de diversos tipos de tumores**, solicitada al laboratorio de anatomía patológica consultante por la Consejería de Salud de su Comunidad Autónoma, requiriéndose, asimismo, los datos necesarios para la correcta **identificación de los pacientes** (nombre, apellidos, DNI, fecha de nacimiento, domicilio, etc.), para ser incorporados al registro de cáncer de dicha Comunidad Autónoma.

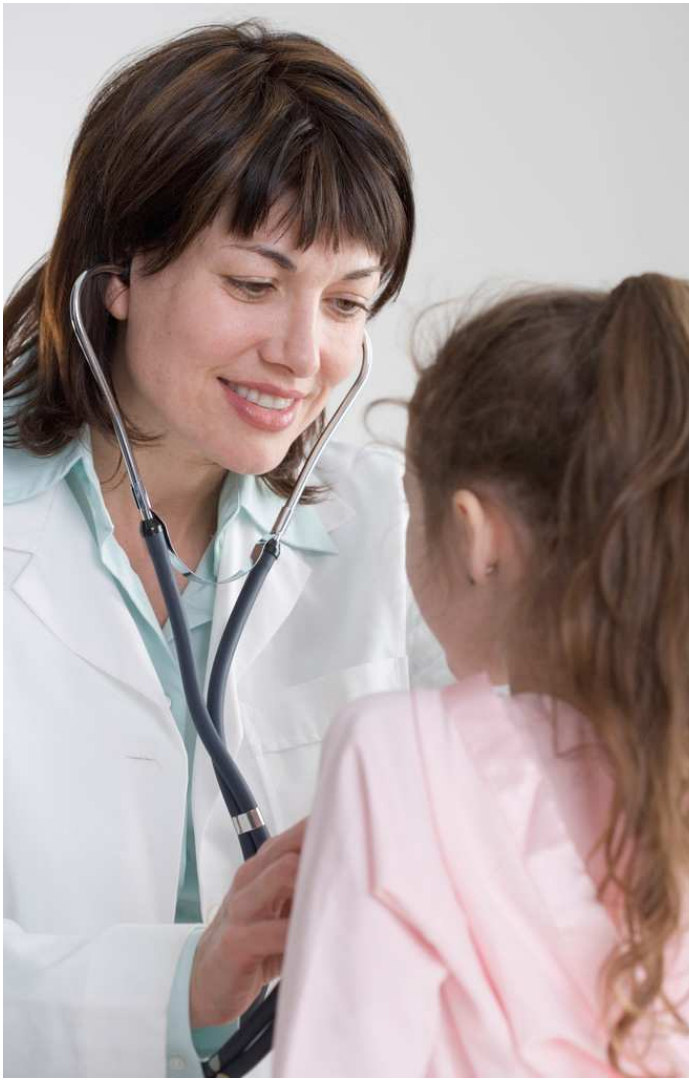
De dicho informe jurídico se extrae lo siguiente:

rr) La transmisión de datos así requerida constituye una **cesión de datos** de carácter personal, en este caso, **datos de nivel alto**.

ss) El Decreto 297/2007, de 18 de diciembre, por el que se crea y regula el Registro de Cáncer de Andalucía, tiene como objeto, entre otros, conocer la **incidencia de la enfermedad del cáncer** y su evolución.

De este modo, en lo que a los registros de cáncer se refiere la necesidad de conocer datos tales como la supervivencia o la evaluación clínica, entre otros aspectos, parece requerir el **conocimiento y la incorporación a los citados registros de datos identificativos de los pacientes**, viniendo, así a constituir un supuesto encuadrable en lo previsto en el último párrafo del artículo 16.3 de la Ley 41/2002, de 14 de noviembre, básica reguladora de la Autonomía del Paciente y de Derechos y Obligaciones en materia de Información y Documentación Clínica, que ampararía la comunicación de datos a que la consulta se refiere sin necesidad de consentimiento del interesado de conformidad con lo previsto en los artículos 41 de la Ley 33/2011, de 4 de octubre, General de Salud Pública y 11.2. f) de la LOPD.

Por otro lado, esto **no excluye el deber de información en la recogida** de los datos a los interesados, indicando quienes son los **destinatarios** de la información.



A TENER EN CUENTA

Cuando se tratan datos de personales relativos a la salud hemos de ser extremadamente cautos.

ACTUALIDAD LOPD

La AEPD autoriza un nuevo modelo de transferencia internacional de datos en el marco de una subcontratación de servicios

Fuente: www.agpd.es

La AEPD autoriza un nuevo modelo de transferencia internacional de datos en el marco de una subcontratación de servicios

El director de la Agencia Española de Protección de Datos ha dictado una resolución por la que, por primera vez, se autoriza una **transferencia internacional de datos** de carácter personal entre un prestador de servicios/exportador de datos, establecido en España, y un subcontratista/importador de datos, situado en un país que no garantiza un nivel adecuado de protección de datos personales, **en el marco de una subcontratación de servicios**.

Esta decisión **establece un nuevo modelo de transferencias internacionales de datos de carácter personal que proporciona mayor flexibilidad** a los prestadores de servicio establecidos en España para la subcontratación con entidades establecidas fuera del ámbito de la UE/EEE, al ser suficiente una sola autorización de la Agencia Española de Protección de Datos para realizar todas aquellas transferencias de datos, derivadas de los contratos de prestación de servicios con los responsables de los tratamientos, siempre que se ajusten al marco de la autorización y se notifique con carácter previo al Registro General de Protección de Datos los ficheros cuyos datos vayan a ser objeto de transferencia, evitándose así que cada responsable tenga que solicitar una autorización como venía haciéndose hasta la fecha.

En el procedimiento de autorización de la transferencia internacional de datos **se han aportado las garantías adecuadas a través del contrato suscrito entre el exportador e importador de datos, cuyas cláusulas han sido elaboradas por la AEPD** con la finalidad de garantizar a los afectados la protección de sus datos personales y el pleno ejercicio de sus derechos en caso de vulneración.

Puede acceder desde este enlace:

https://www.agpd.es/portalwebAGPD/canalresponsable/transferencias_internacionales/common/121023_Nota_TI.pdf

EL PROFESIONAL RESPONDE

¿Qué es el Registro General de Protección de Datos de la Agencia Española de Protección de Datos?

El Registro General de Protección de Datos (RGPD) es un órgano cuyo objetivo es **garantizar la publicidad de la existencia de ficheros** de datos de carácter personal, de los tratamientos aplicados a dichos ficheros y de sus principales características; tiene por finalidad hacer posible el ejercicio de los derechos ARCO de los interesados.

Son objeto de inscripción en el RGPD:

- Los ficheros de que sean titulares las administraciones públicas.
- Los ficheros de titularidad privada.
- Las autorizaciones de transferencias internaciones de datos.
- Los Códigos Tipo.
- Los datos relativos a los ficheros que sean necesarios para el ejercicio de los derechos de información, acceso, rectificación, cancelación y oposición.

Este registro es de **pública consulta**, es decir, cualquiera puede entrar en la web de la AEPD (www.agpd.es) y consultar, en el momento y de forma totalmente gratuita los **ficheros** que una empresa tiene **registrados** introduciendo el nombre de la empresa o su CIF.

A TENER EN CUENTA

El registro de ficheros de una empresa en la AEPD ha de coincidir con lo descrito en su Documento de Seguridad.