

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
La AEPD rediseña su web e incorpora nuevas secciones	4
¿Puedo tener varios Documentos de Seguridad?	5



IMPORTANTE

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

En el procedimiento sancionador [PS/00746](#) 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.

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



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](#) 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.



IMPORTANTE

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

ACTUALIDAD LOPD

La AEPD rediseña su web e incorpora nuevas secciones y contenidos



Fuente: www.agpd.es

The screenshot shows the AEPD website interface. At the top, there is a header with the agency's name and logo, and a search bar. Below this is a navigation menu with categories like 'LA AGENCIA', 'CANAL DEL CIUDADANO', 'RESOLUCIONES Y DOCUMENTOS', etc. The main content area features a large banner with the headline 'La AEPD rediseña su web e incorpora nuevas secciones y contenidos que refuerzan la transparencia'. To the right of the banner are two columns of text: 'Ciudadanos' and 'Profesionales', each with a brief description and links to further information. Below the banner is a row of five smaller promotional tiles: 'THE PANDY', 'PROTEGE TUS DATOS EN INTERNET', 'RED IBEROAMERICANA PROTECCION DE DATOS', 'NOTIFICACIONES ELECTRONICAS A LA AEPD', and 'Sede electrónica'. A 'Destacados' section follows, containing three news items. The first item discusses the approval of common criteria for the 'right to be forgotten' by European authorities. The second item promotes a new 'Guía para una Evaluación de Impacto en la Protección de Datos Personales'. The third item announces the publication of the 2013 Annual Report by the AEPD.

La AEPD rediseña su web e incorpora nuevas secciones y contenidos que refuerzan la transparencia

La página incluye una estructura mejorada y una navegación adaptada a dispositivos móviles. La sección La Agencia permite acceder tanto a información institucional y organizativa como a la actividad que desarrolla y el empleo de los recursos públicos.



Ciudadanos

La protección de datos es un derecho fundamental. Conócelo.

[Conoce tus derechos](#)
[Consulta la guía del ciudadano](#)
[Canal del ciudadano](#)

Profesionales

Cumplir con la LOPD es fácil y gratuito. Descubre cómo.

[Cumple con tus obligaciones](#)
[Inscribe tu fichero](#)
[Canal del responsable](#)

Destacados



Las Autoridades europeas de protección de datos aprueban los criterios comunes para aplicar la sentencia sobre el 'derecho al olvido'

El documento del GT29 desarrolla los criterios interpretativos comunes que van a presidir la aplicación de la sentencia por parte de las Autoridades de los distintos Estados europeos.

[Acceso al documento \(EN\)](#)



La AEPD presenta la 'Guía para una Evaluación de Impacto en la Protección de Datos Personales'

La Agencia apuesta por promover nuevos enfoques proactivos entre las organizaciones. Una Evaluación de Impacto es un proceso que permite identificar los riesgos que un producto o servicio puede implicar para la protección de datos antes de que se materialicen.

[Acceso a la Guía](#)



La Agencia Española de Protección de Datos publica su Memoria 2013

El análisis de la actividad anual de la Agencia pone de manifiesto que ciudadanos y organizaciones son cada vez más conscientes de las garantías que pueden exigir o deben cumplir, respectivamente.

[Acceso a Memoria 2013 \(pdf\)](#)
[Acceso a Memoria 2013 \(ePub\)](#)



Las Autoridades europeas de protección de datos aprueban el primer Dictamen conjunto sobre internet de las cosas

El Dictamen identifica y alerta de los riesgos que estos productos y servicios pueden plantear para la privacidad de las personas, definiendo un marco de responsabilidades y realizando recomendaciones.

[Dictamen GT29 sobre internet de las cosas \(EN\)](#)

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.



IMPORTANTE

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