

LA LOPD EN EL DÍA A DÍA

¿Cuándo he de actualizar el Documento de Seguridad?

La LOPD establece que el Documento de Seguridad deberá mantenerse actualizado, de forma que **refleje** en todo momento la **realidad de la organización**.

A tal efecto, deberemos **estar atentos a los siguientes cambios** para actualizar el Documento de Seguridad:

- **Usuarios** que acceden a los ficheros.
- Modificaciones en los **procedimientos**.
- **Encargados** del tratamiento y servicios prestados.
- **Equipamiento** informático.
- Actualizaciones/instalaciones de **software**.
- **Incidencias** que se produzcan.
- **Personas autorizadas** para salidas de soportes, uso de portátiles, etc.
- **Administradores** de los ficheros y responsables de seguridad.
- **Comenzamos a recoger datos** que antes no se recogían (ej. Correo electrónico de los clientes).
- **Nuevos soportes** que deban incluirse en el inventario de soportes y documentos.

Contenido

¿Cuándo he de actualizar el Documento de Seguridad?	1
Sanción por envío de comunicaciones comerciales	2
Servicio recuperación de impagados	3
El Director de la AEPD subraya la importancia de...	4
¿Qué ventajas aporta un gestor documental para el...	5



IMPORTANTE

Se ha de realizar una revisión completa del Documento de Seguridad al menos una vez al año para verificar y actualizar los cambios producidos.

SANCIONES DE LA AEPD**Sanción por envío de comunicaciones comerciales**

En el procedimiento sancionador [PS/00618/2013](#) de la AEPD podemos ver la sanción que puede sufrir una empresa **por enviar correos electrónicos a destinatarios que no lo han solicitado previamente.**

Según los hechos, el 18 de Julio de 2013 tiene entrada un escrito en la AEPD de la Asociación Andaluza de Comercio Electrónico en el que indica que ha recibido varios correos electrónicos remitidos por ..@dest... Indica también que solicitó la baja y aún así le siguieron llegando correos.

El denunciado indica que se produjo un error al buscar otra empresa cliente que sí se deseaba enviar la información.

Asimismo, indica también que la dirección de la cuenta la obtuvo de la propia página web del denunciante, considerando que el hecho de que la dirección se encuentre publicada supone un consentimiento para su tratamiento y uso.

La LSSI en su artículo 21.1 prohíbe, de forma expresa el envío de comunicaciones publicitarias o promocionales por correo electrónico que no hayan sido previamente solicitadas o autorizadas por los destinatarios de las mismas.

Por otra parte, el hecho de que la dirección de correo esté publicada o no en la web es irrelevante de cara a la LSSI, pues lo que se debe obtener es el consentimiento previo para el envío de comunicaciones comerciales a dicha cuenta de correo. Su publicación en la web no otorga consentimiento para que cualquiera pueda mandar publicidad a dicha cuenta.

Resultado: Sanción de 1.800 € por vulneración del artículo 21 de la LSSI.

Todo el personal de la empresa ha de ser diligente en el cumplimiento de la LOPD.

**IMPORTANTE**

Antes de lanzar una campaña de marketing, es conveniente consultar con su asesor de protección de datos para evitar problemas.

LA AEPD ACLARA

Servicio recuperación de impagados



El informe [00376](#) de la AEPD resuelve la consulta planteada sobre si el servicio que se suministra a una empresa de **recuperación de impagados** se ajusta a la normativa de protección de datos.

La consulta en concreto se plantea sobre si la localización de teléfonos de morosos se adecúa a la LOPD, así como de la situación que se produce cuando dicha empresa contacta con un teléfono que no corresponde al deudor y para realizar la verificación de la identidad, se facilita el DNI del deudor y el importe de la deuda.

De dicho informe jurídico se extrae lo siguiente:

- a) La compañía que le busca el teléfono es **encargada del tratamiento** de la primera. Por tanto, debe de existir un contrato de acceso a datos por cuenta de terceros entre ambas.
- b) Siempre y cuando la búsqueda del teléfono sea en **fuentes accesibles al público**, no precisa del consentimiento de los titulares de los datos.
- c) Es este supuesto, la **comunicación de datos** a una persona distinta al titular de los datos, si no existe previo consentimiento del interesado, sería contrario a lo previsto en la LOPD.

**IMPORTANTE**

Siempre que suministremos datos a otra entidad, debemos extremar las cautelas y firmar el correspondiente contrato.

ACTUALIDAD LOPD

El Director de la AEPD subraya la importancia de “conciliar los beneficios de la tecnología con preservar los derechos y las libertades individuales”



Fuente: www.agpd.es



Nota de prensa

En el marco del curso ‘Protección de datos y nuevas tecnologías’ que arranca hoy en la UIMP

El director de la AEPD subraya la importancia de «conciliar los beneficios de la tecnología con preservar los derechos y las libertades individuales»

- El director de la AEPD, José Luis Rodríguez Álvarez, ha inaugurado hoy el curso ‘Protección de datos y nuevas tecnologías’, que se prolongará hasta el 4 de julio y contará con la presencia de destacados expertos en esta materia
- El big data, las cookies, las quiebras de seguridad, el derecho al olvido, las evaluaciones de impacto o el Reglamento europeo serán algunas de las cuestiones más destacadas del seminario
- Rodríguez Álvarez ha destacado en su conferencia inaugural que reforzar los derechos y las garantías es la receta principal para afrontar la situación actual de riesgos crecientes para la vida privada
- El programa completo [puede consultarse aquí](#)

(30 de junio de 2014). El director de la Agencia Española de Protección de Datos, José Luis Rodríguez Álvarez, ha inaugurado hoy el curso ‘Protección de datos y nuevas tecnologías’, que tiene lugar durante las Actividades de verano 2014 de la Universidad Internacional Menéndez Pelayo (UIMP) de Santander.

Puede ver más información en el siguiente enlace:

http://www.agpd.es/portalwebAGPD/revista_prensa/revista_prensa/2014/notas_prensa/common/jun_14/140630_NP_Curso_ProteccionDatos_UIMP.pdf

EL PROFESIONAL RESPONDE

¿Qué ventajas aporta un gestor documental para el cumplimiento de la normativa de protección de datos?

Un gestor documental aporta la seguridad de que cada persona involucrada en el tratamiento de la información **sólo accede a aquella información que necesita** para su trabajo, **facilitando** además la **aplicación de las medidas de seguridad** adecuadas a los diferentes niveles de datos (básico, medio y alto) dado que permite negar el acceso a determinada información a aquellas personas no autorizadas.

Además, **guarda un registro muy detallado del uso** que aquellos usuarios que tienen acceso hacen de los datos.

De esta forma podemos saber quién ha accedido a un dato, quien lo ha impreso, copiado, duplicado o borrado, por ejemplo.

En este sentido supone una **solución** para aquellas **empresas que manejan datos** en papel de **nivel medio o alto**, que muchas veces se enfrentan a un dilema para conciliar las medidas de seguridad obligatorias con el uso en el día a día de la información.

Por último, dado que toda la información está en formato electrónico, **es posible incluir la totalidad de los datos en la copia de seguridad** semanal.

**IMPORTANTE**

Se ha de revisar el software que se adquiere para verificar el nivel de seguridad que permite cumplir respecto a la LOPD.