El nuevo Reglamento General de Protección de Datos (RGPD)

Comisión de Economía Digital y Nuevas Tecnologías

Martes 22 de mayo de 2018

economistas
Colegio de Valencia

Javier Nogueroles Olaizola - Compliance Officer

1er

Director Compliance en Quicksand SL

Valencia y alrededores, España | Servicios jurídicos

Actual	Auditor Externo, Quicksand SL
Anterior	BCR, Beoptimus, Compliance Ibérica CB
Educación	Universidad de Valencia

Enviar un mensaje

más de 500 contactos

https://es.linkedin.com/in/javiernogueroles | Información de contacto

Trayectoria profesional y académica

Experiencia

Auditor de calidad Servicio // Mistery Shopper

Auditor Externo

abril de 2015 – actualidad (1 año 9 meses) | Valencia y alrededores, España

Auditorías de calidad y servicio para velar por el cumplimiento y estándar exigidos por el cliente.

Director Compliance

Quicksand SL

enero de 2016 – actualidad (1 año) | Valencia

Socio Director área Comliance:

Protección de Datos (LOPD)
Prevención Blanqueo de Capitales (PBCFT)
Seguridad Gestión Sistemas Información (SGSI - ISO 27001)
Responsabilidad Penal Empresarial
Registro de marcas.

Otros servicios prestados traducción jurada a todos los idiomas.

QUICKSAND

QUICKSAND

Me presento

apep

¿QUÉ ES LA PROTECCIÓN DE DATOS?

Es la **salvaguarda** del **derecho al honor, la intimidad y la propia imagen de las personas físicas** ante el uso ilegítimo de sus datos de carácter personal.

¿Por qué proteger nuestros datos de carácter personal?

- Por el **uso abusivo de los mismos** que se ha venido realizando, tanto por la Administración como por particulares y empresas privadas.
- Porque el problema se ha **acrecentado con la aparición de Internet** y el desarrollo de nuevas tecnologías de comunicación.
- Porque la protección de datos redunda, al fin y al cabo, en una **salvaguarda de nuestra libertad**.

Ley Orgánica Protección Datos 15/1999, de 13 de diciembre (LOPD).

Esta norma se ha caracterizado por una perspectiva **estática**: se ha articulado mediante la consideración de los **ficheros** como **algo poco variable y notificados para su inscripción** a la Agencia **Española** de Protección de Datos (AEPD).

Real Decreto 1720/2007, de 21 de diciembre por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999.

Nos indicaba las medidas de seguridad aplicar en función del nivel de los datos: básicos, medios o altos

Proyecto de Ley Orgánica de Protección de Datos del 10 de noviembre de 2017.

Legisla aquellos aspectos que no cubre el RGPD

Se acaban de presentar 360 enmiendas y surgen voces indicando que igual para final de año tenemos la ley que derogue la 15/99

LOPD vs RGPD

Reglamento General de Protección de Datos (RGPD) 25 mayo 2016

- Regulación armonizada y uniforme de obligado cumplimiento en toda la **Unión Europea**.
- Perspectiva más **dinámica**, al atender a los **flujos de los datos** personales que merecen protección.
- Obligatorio para todas las **empresas** que oferten productos o servicios a **ciudadanos que pertenezcan al territorio europeo.**

Definiciones

LOPD

Datos de carácter personal: Cualquier información concerniente a **personas físicas identificadas o identificables.**

Es decir, cualquier dato que tengamos almacenado y podamos relacionar con otras personas, ya sean clientes, proveedores, trabajadores de la empresa y terceros.

Cualquier información **numérica, alfabética, gráfica, fotográfica, acústica** o de cualquier otro tipo concerniente a personas físicas **identificadas o identificables**.

RGPD

"toda información sobre una persona física **identificada o identificable** ("el interesado"); se considerará persona física identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un identificador, como por ejemplo un nombre, un número de identificación, datos de localización, un identificador en línea o uno o varios elementos propios de la identidad física, fisiológica, genética, psíquica, económica, cultural o social de dicha persona.

3 niveles de datos vs 2 tipologías de datos

LOPD: Datos de nivel **básicos**, **medios** y **altos**

RGPD: Categorías **especiales** de datos personales que están subordinados a un régimen más estricto. Datos referentes a:

- ideología,
- afiliación sindical,
- religión, creencias,
- origen racial,
- salud o vida sexual,
- **datos genéticos,**
- **datos biométricos**

Mayor seguridad jurídica **(Consentimiento Explicito)**

Evaluaciones de Impacto de Privacidad si alto riesgo para los derechos y libertades

- **Fichero**: Todo **conjunto organizado de datos** de carácter personal, cualquiera que fuere la **forma o modalidad de su creación, almacenamiento, organización y acceso.**

- **Tratamiento de datos**: operaciones y procedimientos técnicos de carácter automatizado o no, que permitan la recogida, grabación, conservación, elaboración, modificación, bloqueo y cancelación, así como las cesiones de datos que resulten de comunicaciones, consultas, interconexiones y transferencias.

- **Cesión o comunicación de datos**: toda revelación de datos realizada a una persona distinta del interesado.

Ficheros vs Tratamiento de datos

Desaparece la obligación de **INSCRIBIR** los FICHEROS ante la AGPD (Clientes, proveedores, empleados, curriculums, …) de la LOPD

Pasando a ser necesarito confeccionar el **REGISTRO DE ACTIVIDADES DE TRATAMIENTO** del RGPD. De este modo la empresa es consciente de la tipología de datos que trata, sus finalidades y las obligaciones que deberá cumplir.

El **registro de actividades del tratamiento del responsable** deberá contener la información siguiente:

1. El nombre y los **datos de contacto del responsable** y, en su caso, del corresponsable, del representante del responsable, y del delegado de protección de datos.
2. Los **fines** del tratamiento.
3. Una descripción de las **categorías** de **interesados** y de las categorías de datos personales.
4. Las **categorías** de **destinatarios** a quienes se comunicaron o comunicarán los datos personales, incluidos los destinatarios en terceros países u organizaciones internacionales.
5. En su caso, las **transferencias** de datos personales a un tercer país o una organización internacional, incluida la identificación de dicho tercer país u organización internacional, así como la documentación sobre garantías adecuadas para determinados casos.
6. Cuando sea posible, los **plazos** previstos para la **supresión** de las diferentes categorías de datos.
7. Y cuando sea posible, una descripción general de las **medidas técnicas** y organizativas de **seguridad** que el responsable aplique para garantizar la integridad y confidencialidad de los datos.

DERECHO DE INFORMACIÓN y TRANSPARENCIA

LOPD: Establece las siguientes **obligaciones** respecto de la información que se ha de facilitar a las personas interesadas en el momento en que se soliciten los datos:

1. La existencia del fichero o tratamiento, su finalidad y destinatarios.
2. El carácter obligatorio o no de la respuesta, así como de sus consecuencias.
3. La posibilidad de ejercitar los derechos de acceso, rectificación, cancelación y oposición.
4. La identidad y datos de contacto del responsable del tratamiento.

RGPD: ***requisitos adicionales*** en cuanto a la necesidad de informar a las personas interesadas, generalizando el concepto de “Tratamiento”, e incorporando, en líneas generales, los siguientes detalles:

1. Los datos de contacto del Delegado de Protección de Datos, en su caso,
2. La base jurídica o legitimación para el tratamiento,
3. El plazo o los criterios de conservación de la información,
4. La existencia de decisiones automatizadas o elaboración de perfiles,
5. La previsión de transferencias a Terceros Países
6. El derecho a presentar una reclamación ante las Autoridades de Control

INFORMACION POR CAPAS

El enfoque de información multinivel consiste en lo siguiente:

- ✓ presentar una ***información básica*** en un primer nivel, de forma ***resumida***, en el mismo momento y en el mismo medio en que se recojan los datos,
- ✓ remitir a la ***información adicional*** en un segundo nivel, donde se presentarán ***detalladamente*** el resto de las informaciones, en un medio más adecuado para su presentación, comprensión y, si se desea, archivo.

Nuevos derechos de los ciudadanos

LOPD: Derechos ARCO (Acceso, Rectificación, Cancelación, Oposición)

Nuevos derechos **RGPD**:

1. **Transparencia** de la información
2. **Olvido** … solicitar la eliminación de sus datos en determinadas circunstancias: se han recogido ilícitamente, si ya no son necesarios o si se ha retirado en la forma adecuada su consentimiento.
3. **Limitación** … se puede limitar el tratamiento de los datos cuando: se impugne la exactitud de los datos personales, sea un tratamiento ilícito y el interesado se oponga a la supresión de los datos, el responsable no necesite los datos personales, pero el interesado los necesite para la defensa de reclamaciones.
4. **Portabilidad** … se pretende obligar a la empresa que gestione los datos de una determinada persona a enviarlos en los formatos adecuados para poder pasarlos a otro proveedor, o incluso ser ella misma la que los transfiera cuando esto sea posible.

Principio Accountability – responsabilidad proactiva

Deja de ser obligatorio el **Documento de Seguridad**, donde queda constancia de las diferentes medidas de seguridad

Accountability

- Documentación/registro de los **tratamientos**.
- Aplicar **medidas de seguridad** adecuadas
- Privacidad por **defecto** y privacidad desde el **diseño**.
- **Análisis de impacto de la privacidad** (PIA)
- Seguridad y **análisis de riesgos**. Notificación de incidentes.
- Los **códigos de conducta**
- Designación **Delegado de Protección de Datos**
- Notificación de **Quiebras de Seguridad**

Delegado Protección de Datos

Obligatorio para aquellas organizaciones que pertenecen a los siguientes sectores entre otros:

- Los **Organismos públicos**
- Los colegios profesionales y sus consejos generales.
- Los **centros docentes** y las Universidades públicas y privadas.
- Las entidades que exploten redes y presten **servicios de comunicaciones electrónicas**.
- Los **prestadores de servicios de la sociedad de la información** que recaben información de los usuarios de sus servicios.
- Las entidades de ordenación, supervisión y solvencia de entidades de crédito.
- Los establecimientos **financieros de crédito**.
- Las entidades **aseguradoras y reaseguradoras**.
- Las empresas de **servicios de inversión**.
- Los distribuidores y comercializadores de **energía eléctrica**.
- Las entidades responsables de ficheros comunes para la evaluación de la **solvencia patrimonial y crédito** o de los ficheros comunes para la gestión y prevención del fraude.
- Las entidades que desarrollen **actividades de publicidad y prospección comercial** que realicen actividades que impliquen la elaboración de perfiles de los mismos.
- Los **centros sanitarios** obligados al mantenimiento de las historias clínicas de los pacientes según la Ley básica reguladora de la autonomía del paciente y de derechos y obligaciones en materia de información y documentación clínica.
- Las entidades que tengan como uno de sus objetos la emisión de **informes comerciales** acerca de personas y empresas.
- Los operadores que desarrollen la **actividad de juego** a través de canales electrónicos, informáticos, telemáticos e interactivos.
- Quienes desempeñen las actividades de **Seguridad Privada**.

- Empresas con más de **250 empleados**

Las **funciones** que debe desarrollar un DPO son:

- **Informar y asesorar** al responsable o al encargado del tratamiento y a los empleados de las obligaciones del RGPD y de otras disposiciones de protección de datos;
- **Supervisar el cumplimiento del RGPD**, de otras disposiciones de protección de datos y de las políticas del responsable o del encargado del tratamiento en materia de protección de datos personales, incluida la asignación de responsabilidades, la concienciación y formación del personal, y las auditorías correspondientes;
- Supervisar y asesorar para **determinar el registro de actividades** de tratamiento,
- Analizar y comprobar la **conformidad de las actividades** de tratamiento
- Asesorar en los casos de **evaluaciones de impacto** y supervisar su aplicación
- **Cooperar con la autoridad de control**
- Actuar como **punto de contacto** de la autoridad de control.
- Prestar la debida atención a los **riesgos asociados** a las operaciones de tratamiento, teniendo en cuenta la naturaleza, el alcance, el contexto y fines del tratamiento.
- Supervisar la **asignación de responsabilidades**.
- Supervisar la **concienciación y formación del personal** que participa en las operaciones de tratamiento
- Supervisar las **auditorías** correspondientes;
- Rendir cuentas directamente al más alto nivel jerárquico del responsable/encargado.
- **Atender a los interesados** que se pongan en contacto con el DPO para cuestiones relativas al tratamiento de sus datos personales y al ejercicio de sus derechos. (asumiendo funciones de atención al cliente o interesado en materia de privacidad)

Legitimación tratamiento de datos

a) el interesado dio su **consentimiento** para el tratamiento de sus datos personales para uno o varios fines específicos;

b) el tratamiento es necesario para la **ejecución de un contrato** en el que el interesado es parte o para la aplicación a petición de este de medidas precontractuales;

c) el tratamiento es necesario para el cumplimiento de una **obligación legal** aplicable al responsable del tratamiento;

d) el tratamiento es necesario para **proteger intereses vitales** del interesado o de otra persona física;

e) el tratamiento es necesario para el cumplimiento de una misión realizada **en interés público** o en el ejercicio de poderes públicos conferidos al responsable del tratamiento;

f) el tratamiento es necesario para la satisfacción de **intereses legítimos** perseguidos por el responsable del tratamiento o por un tercero, siempre que sobre dichos intereses no prevalezcan los intereses o los derechos y libertades fundamentales del interesado que requieran la protección de datos personales, en particular cuando el interesado sea un niño (salvo poderes públicos).

Consentimiento

Consentimiento RGPD: toda manifestación de voluntad **libre**, **específica**, **informada** e **inequívoca** por la que el interesado acepta el tratamiento de datos personales que le conciernen.

Mediante una **declaración** o una clara **acción afirmativa**

- **Pilar básico** de la regulación actual.
- **NO se admite** el consentimiento **tácito**.
  - El silencio
  - Las casillas premarcadas
  - La inacción
- En caso de tratarse de **datos especialmente protegidos** el consentimiento debe ser **expreso** y en algunos casos –ideología, religión, creencias-, recogido por escrito.
- Existen excepciones a este principio general.
- Se cumple conjuntamente con el deber de información en los impresos y formularios utilizados

Relaciones responsables - encargados

- Obligación general de diligencia debida en selección de encargado
- Regulación más detallada y asimilada a nuestra LOPD
  - En el contenido del instrumento que exterioriza la relación jurídica
  - En las obligaciones del encargado
  - En el régimen de posible subcontratación
- Peculiaridades
  - Previsión de que el responsable “realice auditorías y contribuya a ellas, incluidas las inspecciones dirigidas por el responsable o por otro auditor autorizado por dicho responsable
  - Fin de la prestación implica borrado o devolución de datos, sin incluir transferencia a otro encargado
  - Obligación de informar al responsable “si, en su opinión, una instrucción infringe el presente Reglamento o disposiciones en materia de protección de datos

Brechas de seguridad

Definición según los considerandos del RGPD

“Toda violación que ocasione la destrucción, pérdida o alteración accidental o ilícita de datos personales transmitidos, conservados o tratados de otra forma, o la comunicación o acceso no autorizado a dichos datos”

Deben ser notificadas a la Autoridad de Control **cuando la misma constituya un riesgo para los derechos y libertades de las personas físicas.**

Deberemos notificarla en un plazo máximo de **72 horas** a contar desde que **tengamos conocimiento de la brecha.**

En la LOPD no viene regulado expresamente, habla de incidencia y no había obligación de notificación.

Sanciones

Los Estados miembros establecerán las normas en materia de otras sanciones aplicables a las infracciones del RGPD, en particular las infracciones que no se sancionen con multas administrativas y adoptarán todas las medidas necesarias para garantizar su observancia.

CARACTERÍSTICAS DE LAS SANCIONES:

- Efectivas.
- Proporcionadas.
- Disuasorias.

economistas
Colegio de Valencia

Infracción: muy grave **prescripción**: 3 años

QUICKSAND

a) Tratamiento de datos personales **vulnerando los principios y garantías** establecidos en el art. 5 RGPD
b) Tratamiento de datos personales **sin** que concurra alguna de las condiciones de **licitud** del tratamiento establecidas en el art. 6 RGPD
c) El incumplimiento de los requisitos exigidos por el artículo 7 del RGPD para la validez del **consentimiento.**
d) La utilización de los datos para **una finalidad que no sea compatible** con la finalidad para la cual fueron recogidos, sin contar con el consentimiento del afectado o con una base legal para ello.
e) El tratamiento de datos personales de las categorías a las que se refiere el artículo 9 del RGPD, sin que concurra alguna de las circunstancias previstas en dicho precepto y en el artículo 10 de LOPD.
f) El tratamiento de datos personales relativos a **condenas e infracciones penales** o medidas de seguridad fuera de los supuestos permitidos por el artículo 10 del RGPD y en el artículo 20 de LOPD.
g) El tratamiento de datos de carácter personal relacionados con **infracciones y sanciones administrativas** fuera de los supuestos permitidos por el artículo 4.
h) La **omisión del deber de informar** al afectado acerca del tratamiento de sus datos de carácter personal conforme a lo dispuesto en los artículos 13 y 14 del RGPD y 21 de LOPD.
i) La vulneración del **deber de confidencialidad** establecido en el artículo 6.
j) La exigencia del **pago de un** canon para facilitar al afectado la información a la que se refieren los artículos 13 y 14 del RGPD o por atender las solicitudes de ejercicio de derechos de los afectados previstos en los artículos 15 a 22 del RGPD, fuera de los supuestos establecidos en su artículo 12.5.
k) El **impedimento o la obstaculización** o la no atención reiterada del ejercicio de los derechos establecidos en los artículos 15 a 22 del RGPD
l) La **transferencia internacional de** datos de carácter personal a un destinatario que se encuentre en un tercer país o a una organización internacional, cuando no concurran las garantías, requisitos o excepciones establecidos en los artículos 44 a 49 del RGPD.
m) El **incumplimiento de las resoluciones** dictadas por la autoridad de protección de datos competente en ejercicio de los poderes que le confiere el artículo 58.2 del RGPD.
n) El **incumplimiento de la obligación de bloqueo** de los datos establecida en el artículo 29 cuando la misma sea exigible.
o) No facilitar el acceso del personal de la autoridad de protección de datos competente a los datos personales, información, locales, equipos y medios de tratamiento que sean requeridos por la autoridad de protección de datos para el ejercicio de sus poderes de investigación.
p) La **resistencia u obstrucción** del ejercicio de la función inspectora por la autoridad de protección de datos competente.

a) El tratamiento de datos de carácter personal de un **menor de trece años sin recabar su consentimiento,** cuando tenga capacidad para ello, o el del titular de su patria potestad o tutela, conforme al artículo 8 del RGPD.

b**) No acreditar la realización de esfuerzos razonables para verificar la validez del consentimiento** prestado por un menor de trece años o por el titular de su patria potestad o tutela sobre el mismo, conforme a lo requerido por el artículo 8.2 del RGPD

c) El **impedimento o la obstaculización o la no atención reiterada de los derechos** de acceso, rectificación, supresión, limitación del tratamiento o a la portabilidad de los datos en tratamientos en los que no se requiere la identificación del afectado, cuando éste, para el ejercicio de esos derechos, haya facilitado información adicional que permita su identificación.

d) **La falta de adopción de aquellas medidas técnicas y organizativas** que resulten apropiadas para aplicar de forma efectiva los principios de protección de datos **desde el diseño y por defecto** e integrar las garantías necesarias en el tratamiento, en los términos exigidos por el artículo 25.1 del RGPD

e) **La falta de adopción de las medidas técnicas y organizativas** apropiadas para garantizar que, por defecto, **sólo se tratarán los datos personales necesarios para cada uno de los fines específicos del tratamiento**, conforme a lo exigido por el artículo 25.2 del RGPD

f) El **incumplimiento de la obligación de designar un representante** del responsable o encargado del tratamiento no establecido en el territorio de la Unión Europea, conforme a lo previsto en el artículo 27 del RGPD

g) La **falta de atención** por el representante en la Unión del responsable o del encargado del tratamiento de las **solicitudes efectuadas por la autoridad** de protección de datos o por los afectados.

h) La contratación por el responsable del tratamiento de un **encargado de tratamiento que no ofrezca las garantías suficientes** para aplicar las medidas técnicas y organizativas apropiadas conforme a lo establecido en el Capítulo IV del RGPD

i) Encargar el tratamiento de datos a un tercero sin la previa formalización de un contrato u otro acto jurídico escrito con el contenido exigido por el artículo 28.3 del RGPD

j) La **contratación** por un encargado del tratamiento de otros encargados **sin contar con la autorización previa del responsable,** o sin haberle informado sobre los cambios producidos en la subcontratación cuando fueran legalmente exigibles.

k) La infracción por un encargado del tratamiento de lo dispuesto en el Reglamento (UE) 2016/679 y la presente ley orgánica, al determinar los fines y los medios del tratamiento, conforme a lo dispuesto en el artículo 28.10 del citado reglamento.

l) No disponer del registro de actividades de tratamiento establecido en el artículo 30 del RGPD

m) No poner a disposición de la autoridad de protección de datos que lo haya solicitado, el registro de actividades de tratamiento, conforme al apartado 4 del artículo 30 del RGPD

n) No cooperar con las autoridades de control en el desempeño de sus funciones en los supuestos no previstos en el artículo 72 de LOPD.

o) El tratamiento de datos de carácter personal sin llevar a cabo una previa valoración de los riesgos que el mismo pudiera generar en los derechos de los afectados, y en particular en su derecho a la protección de datos de carácter personal, conforme a lo dispuesto en el artículo 30.

p) El incumplimiento del deber del encargado del tratamiento de **notificar al responsable del tratamiento las violaciones de seguridad** de las que tuviera conocimiento.
q) El **incumplimiento del deber de notificación** a la autoridad de protección de datos de una **violación de seguridad** de los datos personales de conformidad con lo previsto en el artículo 33 del RGPD
r) El **incumplimiento del deber de comunicación al afectado de una violación de la seguridad** de los datos de conformidad con lo previsto en el artículo 34 del RGPD si el responsable del tratamiento hubiera sido requerido por la autoridad de protección de datos para llevar a cabo dicha notificación.
s) El tratamiento de datos de carácter personal sin haber llevado a cabo la evaluación del impacto de las operaciones de tratamiento en la protección de datos personales en los supuestos en que la misma sea exigible.
t) El tratamiento de datos de carácter personal sin haber consultado previamente a la autoridad de protección de datos en los casos en que dicha consulta resulta preceptiva conforme al artículo 36 del RGPD o cuando la ley establezca la obligación de llevar a cabo esa consulta.
u) El **incumplimiento de la obligación de designar un delegado de protección de datos** cuando sea exigible su nombramiento de acuerdo con el artículo 37 del RGPD y el artículo 33 de LOPD.
v) No posibilitar la efectiva participación del delegado de protección de datos en todas las cuestiones relativas a la protección de datos personales, no respaldarlo o interferir en el desempeño de sus funciones.
w) La utilización de un sello o certificación en materia de protección de datos que no haya sido otorgado por una entidad de certificación debidamente acreditada o en caso de que la vigencia del mismo hubiera expirado.
x) Obtener la acreditación como organismo de certificación presentando información inexacta sobre el cumplimiento de los requisitos exigidos por el artículo 43 del RGPD
y) El desempeño de funciones que el RGPD reserva a los organismos de certificación, sin haber sido debidamente acreditado conforme a lo establecido en el artículo 40 de LOPD.
z) El incumplimiento por parte de un organismo de certificación de los principios y deberes a los que está sometido según lo previsto en los artículos 42 y 43 de RGPD.
aa) El desempeño de funciones que el artículo 41 del RGPD reserva a los organismos de supervisión de códigos de conducta sin haber sido previamente acreditado por la autoridad de protección de datos competente.
bb) La falta de adopción por parte de los organismos acreditados de supervisión de un código de conducta de las medidas que resulten oportunas en caso que se hubiera producido una infracción del código, conforme exige el artículo 41.4 del RGPD

Infracción: leve **prescripción**: 1 años

a) El **incumplimiento del principio de transparencia de la información** o el derecho de información del afectado por no facilitar toda la información exigida por los artículos 13 y 14 del RGPD.

b) La exigencia del pago de un canon para facilitar al afectado la información exigida por los artículos 13 y 14 del RGPD o por atender las solicitudes de ejercicio de derechos de los afectados previstos en los artículos 15 a 22 del RGPD, cuando así lo permita su artículo 12.5, si su cuantía excediese el importe de los costes afrontados para facilitar la información o realizar la actuación solicitada.

c) No atender las solicitudes de ejercicio de los derechos establecidos en los artículos 15 a 22 del RGPD, salvo que resultase de aplicación lo dispuesto en el artículo 72.1.k) de LOPD.

d) No atender los derechos de acceso, rectificación, supresión, limitación del tratamiento o a la portabilidad de los datos en tratamientos en los que no se requiere la identificación del afectado, cuando éste, para el ejercicio de esos derechos, haya facilitado información adicional que permita su identificación, salvo que resultase de aplicación lo dispuesto en el artículo 73.c).

e) El incumplimiento de la obligación de notificación relativa a la rectificación o supresión de datos personales o la limitación del tratamiento exigida por el artículo 19 del RGPD.

f) El incumplimiento de la obligación de informar al afectado, cuando así lo haya solicitado, de los destinatarios a los que se hayan comunicado los datos personales rectificados, suprimidos o respecto de los que se ha limitado el tratamiento.

g) El incumplimiento de la obligación de suprimir los datos referidos a una persona fallecida cuando ello fuera exigible conforme al artículo 3.

h) La falta de formalización por los corresponsables del tratamiento del acuerdo que determine las obligaciones, funciones y responsabilidades respectivas con respecto al tratamiento de datos personales y sus relaciones con los afectados al que se refiere el artículo 26 del RGPD o la inexactitud en la determinación de las mismas.

i) No poner a disposición de los afectados los aspectos esenciales del acuerdo formalizado entre los corresponsables del tratamiento, conforme exige el artículo 26.2 del RGPD.

j) La falta del cumplimiento de la obligación del encargado del tratamiento de informar al responsable del tratamiento acerca de la posible infracción por una instrucción recibida de éste de las disposiciones del RGPD o de LOPD, conforme a lo exigido por el artículo 28.3 del citado reglamento.

k) El incumplimiento por encargado o subencargado de las estipulaciones impuestas en el contrato o acto jurídico que regula el tratamiento o las instrucciones del responsable del tratamiento, salvo que esté legalmente obligado a ello conforme al RGPD y la LOPD en los supuestos en que fuese necesario para evitar la infracción de la legislación en materia de protección de datos y se hubiese advertido de ello al responsable o al encargado del tratamiento.

l) Disponer de un Registro de actividades de tratamiento que no incorpore toda la información exigida por el artículo 30 del RGPD.

m) La notificación incompleta o defectuosa a la autoridad de protección de datos de la información relacionada con una violación de seguridad de los datos personales de conformidad con lo previsto en el artículo 33 del RGPD

n) El incumplimiento de la obligación de documentación de cualquier violación de seguridad, exigida por el artículo 33.5 del RGPD.

o) El incumplimiento del deber de comunicación al afectado de una violación de la seguridad de los datos que entrañe un alto riesgo para los derechos y libertades de los afectados, conforme a lo exigido por el artículo 34 del RGPD, salvo que resulte de aplicación lo previsto en el artículo 73.q) de LOPD

p) Facilitar información inexacta a la Autoridad de protección de datos, en los supuestos en los que el responsable del tratamiento deba elevarla una consulta previa, conforme al artículo 36 del RGPD

q) No publicar los datos de contacto del delegado de protección de datos, o no comunicarlos a la autoridad de protección de datos, cuando su nombramiento sea exigible de acuerdo con el artículo 37 del Reglamento (UE) 2016/679 y el artículo 35.3 de esta ley orgánica.

r) El incumplimiento por los organismos de certificación de la obligación de informar a la autoridad de protección de datos de la expedición, renovación o retirada de una certificación, conforme a lo exigido por los apartados 1 y 5 del artículo 43 del Reglamento (UE) 2016/679.

s) El incumplimiento por parte de los organismos acreditados de supervisión de un código de conducta de la obligación de informar a las autoridades de protección de datos acerca de las medidas que resulten oportunas en caso de infracción del código, conforme exige el artículo 41.4 del Reglamento (UE) 2016/679.

Las multas administrativas y su cuantía se impondrán, en función de las circunstancias de cada caso individual, teniendo en cuenta:

- La naturaleza, gravedad, duración o intencionalidad
- **Medidas tomadas para paliar los daños y perjuicios**
- Infracciones anteriores, beneficios obtenidos o pérdidas evitadas
- Grado de cooperación con la autoridad de control
- Categorías de los datos afectados
- **Si se notificó la infracción o no** *(beneficio de notificar)*
- Adhesión a códigos de conducta o certificación

Las sanciones pueden llegar hasta **20 millones € o 4 % del volumen de negocio total anual global** (ejercicio financiero anterior).

economistas
Colegio de Valencia

QUICKSAND

CASOS PRACTICOS REALES

LEGISLACION PROTECCION DE DATOS = CLIENTE CABREADO

LEGISLACION PROTECCION DE DATOS = SENTIDO COMÚN

www.elmundo.es/cataluna/2018/05/03/5aeab9a622601db1078b45fa.html

EM ‹ España | Cataluña | Noticias Elecciones catalanas

CATALUÑA

Hacienda embarga 110.000 euros a Òmnium y ANC por una sanción de la Agencia de Protección de Datos

EFE | Barcelona 3 MAY. 2018 | 09:43

noticiasdenavarra.com
Diario de Noticias de Navarra. Noticias de última hora locales, nacionales, e internacionales.

Tribunal Superior de Justicia de Navarra

Salud repercute la multa de 125.000 euros a los trabajadores que violaron un historial

tiene previsto iniciar el procedimiento antes de junio

La historia clínica, perteneciente a una mujer fallecida, fue vista por 419 sanitarios en 2.825 ocasiones

m. gonzález - Jueves, 26 de Abril de 2012 - Actualizado a las 05:09h

La consejera de Salud, Marta Vera, con el director gerente del SNS-O, Ángel Sanz Barea.

El departamento de Salud tiene previsto iniciar antes de junio el proceso para repercutir en los trabajadores que entraron de forma inadecuada a una historia clínica la sanción de 125.000 euros que le impuso el Tribunal Superior de Justicia de Navarra por el "acceso masivo e ilegítimo" a los datos de la paciente.

pamplona. La sentencia, una de las primeras resoluciones dictadas en la Comunidad Foral sobre la materia, recoge que se produjeron 2.825 accesos realizados por 419 usuarios al historial, que incluía fotografías de la paciente. Los trabajadores pertenecían a 55 servicios de diferentes centros, hospitalarios, de salud, ambulatorios, etcétera, cuando la mujer solo estuvo ingresada en un hospital y en cuatro servicios y en uno de ellos, Urgencias, lo hizo de forma breve.

Antes de iniciar el proceso para que los trabajadores se hagan cargo de la indemnización impuesta al Servicio Navarro de Salud-Osasunbidea al haberse producido "un funcionamiento anormal en el sistema sanitario público navarro en la medida en que ha permitido accesos ilegítimos a la historia clínica", el SNS-O deberá pagar los 120.000 euros, según explicó su director gerente, Ángel Sanz Barea, en el transcurso de la inauguración del Foro sobre Protección de Datos. "Todavía no se ha ejecutado la sanción a la que nos han condenado y hasta que no se haga no podemos iniciar las acciones para repercutirla en los trabajadores infractores. Estamos en la tramitación para hacer efectiva la sentencia y cuando lo hagamos ya podremos iniciar las acciones oportunas. Hasta que no paguemos, no podemos hacerlo", explicó.

Algunos de los expertos asistentes al acto cuestionaron que Salud pueda hacer pagar la indemnización a los trabajadores. "Legalmente no está previsto, quien debiera pagar es el Servicio Navarro de Salud. Lo que puede hacer éste es adoptar las medidas disciplinarias que considere oportunas contra las personas que accedieron de forma indebida a la historia clínica", aseguró Emilio Aced, subdirector del Registro de la Agencia de Protección de Datos de la Comunidad de Madrid.

Sanz Barea, sin embargo, manifestó su confianza en la legalidad de la medida. "Nosotros iniciaremos el expediente y, por supuesto, no haremos nada que no se pueda hacer, pero, por la información que nos han transmitido, en estas circunstancias podemos transmitir a los trabajadores esa responsabilidad", precisó.

De hecho, no es la primera ocasión en que la Administración repercute las indemnizaciones a los infractores, con independencia de la sanción administrativa que se les haya impuesto como consecuencia de su acción. Este tipo de infracciones están consideradas como graves y pueden acarrear una sanción de hasta quince días de suspensión de empleo y sueldo. "Adoptar medidas disciplinarias sería ejemplarizante. Suspender a una persona de empleo y sueldo tiene un coste económico", defendió la secretaria general de la Agencia Española de Protección de Datos, María José Blanco Antón.

Tecnologia | Martes 15 de Abril de 2008

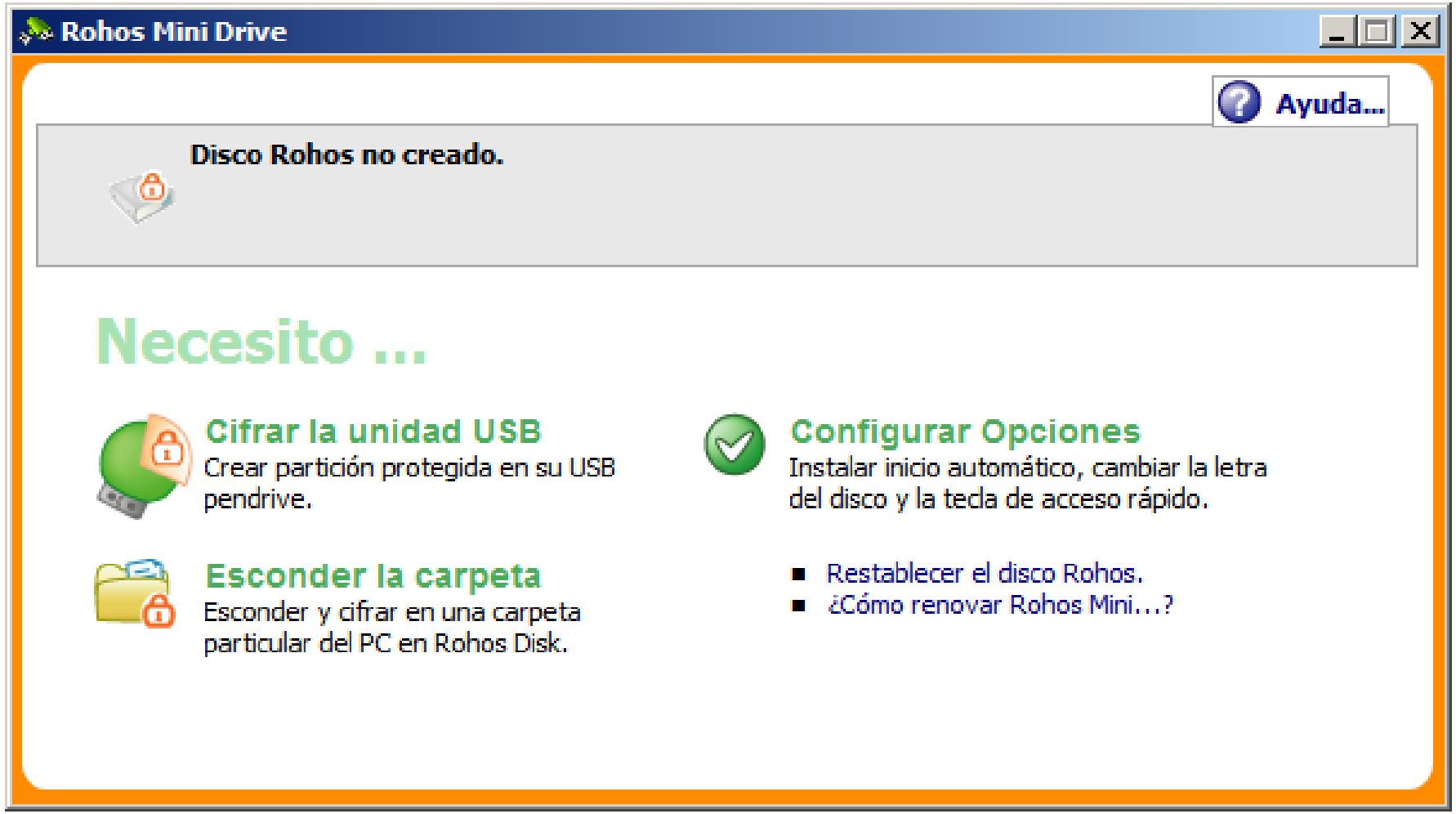
Datos de empresas en peligro por el uso indiscriminado de pendrives

Publique su comentario

Las unidades flash USB se pueden convertir en un instrumento propicio para la fuga de información de las compañías a través de los empleados

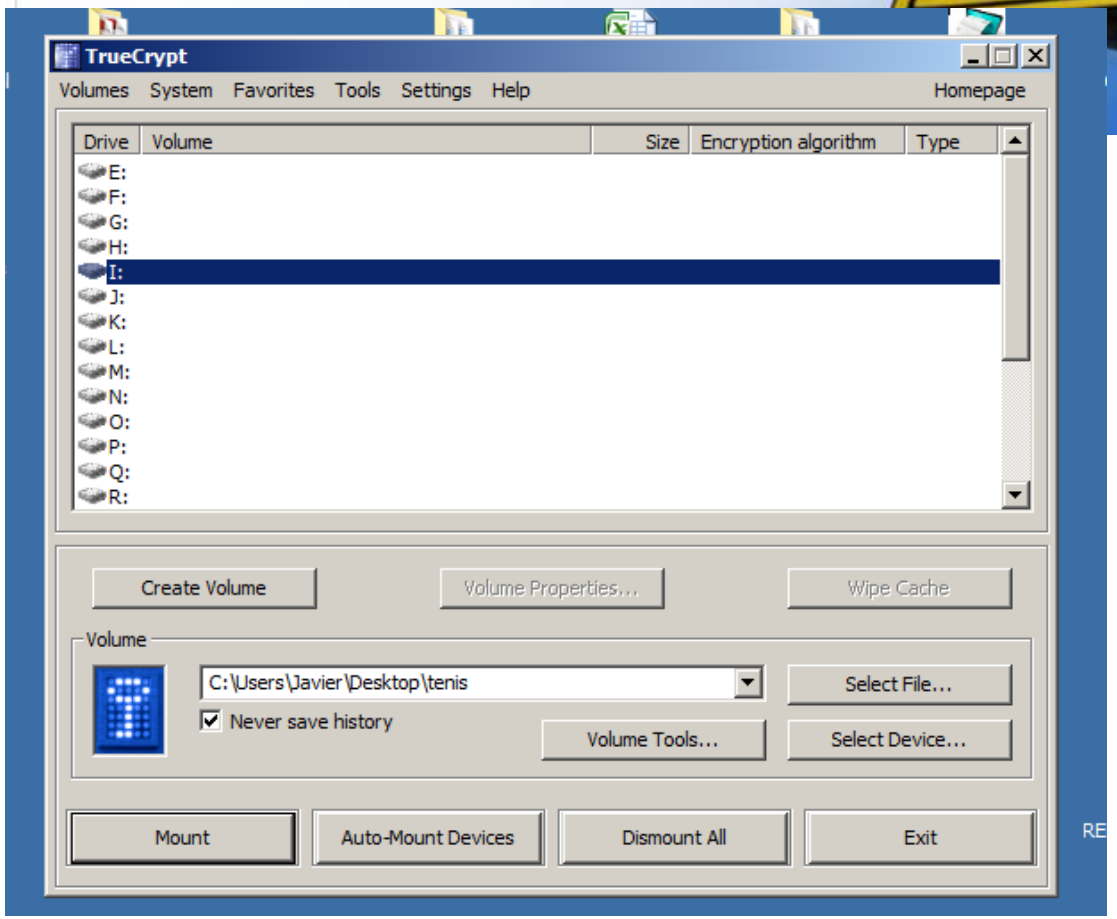
La información digital de las empresas y organizaciones en general está en riesgo debido al uso de unidades flash USB, también conocidas como "pendrives". El empleo de estos dispositivos de almacenamiento es más del doble que las expectativas que tienen las compañías, de acuerdo a un relevamiento privado.

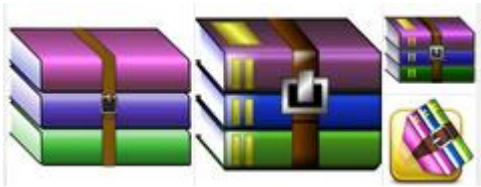
El tema es de gran importancia para las organizaciones, porque los archivos personales almacenados en unidades flash incluyen registros de clientes, información financiera, planes de negocio y código fuente.


Rohos Mini Drive
Ayuda...
Disco Rohos no creado.
Necesito ...
Cifrar la unidad USB
Crear partición protegida en su USB pendrive.
Configurar Opciones
Instalar inicio automático, cambiar la letra del disco y la tecla de acceso rápido.
Esconder la carpeta
Esconder y cifrar en una carpeta particular del PC en Rohos Disk.
Restablecer el disco Rohos.
¿Cómo renovar Rohos Mini...?

Por término medio, se roba un equipo portátil 53 segundos.[1]

Mantenga protegidos sus datos privados, aunque le roben o pierda su equipo portátil.





La venganza de los `ex´ Cómo reforzar la frontera `usuario´ y `contraseña´

Los sabotajes incluyen el robo, la manipulación y el borrado de información
Chris Hondros mauricio ascione

Rosario Sepúlveda Domingo , 21-02-10

Resentidos, despechados como los amantes. El sentimiento que provoca la comunicación de un despido no dista mucho del que produce el conocimiento de cualquier noticia traumática. «Se han descrito cinco fases en estos procesos: negación, ira, negociación, depresión y aceptación. De ahí que, al enterarte que te han despedido, lo ideal es alejarte de la empresa sin actuar ni comprometerte a nada. Intenta mantener la sangre fría, porque todas las reacciones que brotan de un `calentón´ son erróneas», aconseja el psicólogo Marcos Chicot, autor del libro `¡Me han despedido!´.

Sin embargo, no todo el mundo termina por aceptar el trago de verse en la calle y, acomodados en ese sentimiento de ira sobre el que alerta Chicot, urden o improvisan una venganza contra su antigua empresa. «Cada vez hay más casos en los que los sistemas de información y los datos de las compañías son objeto de robo o manipulación por parte de ex empleados», confirma Marc Martínez, socio del área de Information Technology Risk Advisory de Ernst & Young, que ha publicado el informe `2009 Global Information Security Survey´.

Basado en entrevistas a ejecutivos de 1.900 organizaciones de 60 países, el estudio desvela que las represalias por parte de antiguos empleados, así como la escasez de presupuesto para acometer un buen plan de seguridad, suponen los mayores quebraderos de cabeza de los directivos que gestionan la seguridad de la información en las empresas.

El Gabinete Profesional de Peritos Judiciales también advierte un aumento exponencial de sabotajes informáticos como respuesta al despido desde que empezó la crisis. Manel Cruz, su gerente, estima que, en el último año, han cursado un 60% más de estos casos. «Lo más habitual es sacar información de la compañía o bien borrarla. En el 80 o 90% de las ocasiones, sin embargo, la información borrada se recupera, siempre y cuando la máquina no se haya tocado tras el sabotaje».

¿Sabemos usar contraseñas seguras?

NoguerolesJavier

J4v13r_N0gu3r0l3$

SANCIÓN

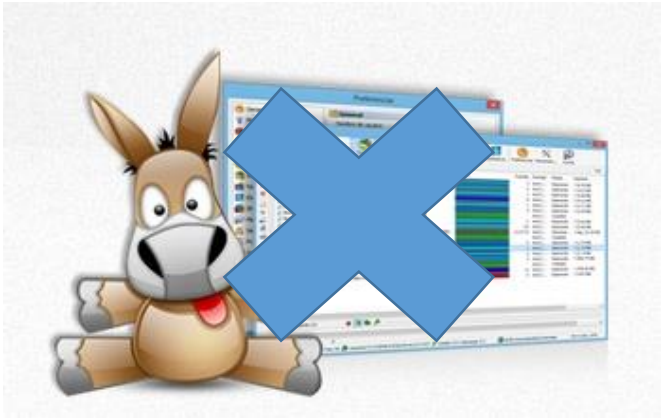
Multan con 6.000 euros a un gimnasio por difundir en la red datos bancarios de clientes

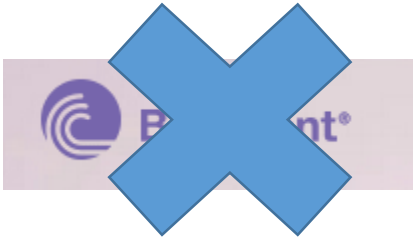
La Agencia de Protección rebaja la sanción inicial, de 120.000 euros, al no constar intencionalidad en la divulgación en internet de esas informaciones personales

MARÍA LÓPEZ

No disponer de los perceptivos sistemas de seguridad informáticos para la privacidad de información puede salir muy caro. La Agencia Española de Protección de Datos ha sancionado con 6.000 euros a una cadena de gimnasios con establecimientos en Vigo y Ourense por difundir datos personales de sus clientes en internet, entre los que se incluyen números de cuentas bancarias.

Inicialmente, la agencia había impuesto dos multas de 60.101,21 millones de euros a la empresa, pero más tarde comprobó que "no constaba intencionalidad ni reincidencia en la conducta, consistente en vulnerar las





Expediente

La Agencia de Datos multa a la federación de ciclismo por publicar sanciones de corredores

La AEPD considera que la institución ciclista de la Comunitat cometió una infracción grave al divulgar los nombres en internet

NOTICIAS RELACIONADAS

* "No lo hicimos para perjudicar a los ciclistas" . Comunitat Valenciana

RAMÓN FERRANDO VALENCIA La Agencia Española de Protección de Datos (AEPD) ha impuesto una multa a la Federación de Ciclismo de la Comunitat Valenciana por publicar en su página web las sanciones a los corredores. La AEPD inició el expediente tras recibir una denuncia de la Real Federación Española de Ciclismo (RFEC) y concluyó que la divulgación en internet de los nombres de los corredores supone una infracción grave. La Federación de Ciclismo de la Comunitat Valenciana (FCCV) acaba de pagar la sanción y la ha recurrido. El presidente de la federación valenciana, Amadeo Olmos, insistió ayer en que en la relación que colgaron en la web no se detallaba si los ciclistas habían sido sancionados por dopaje o por cualquier infracción como correr enganchados de un coche.

SOCIEDAD

Multa de 2.000 euros por difundir la foto de una menor en la ofrenda

Una sentencia condena a Turismo Valencia por publicitar en 100.000 ejemplares una fotografía de la niña durante la ofrenda

03.03.11 - 00:29 - A. RALLO | VALENCIA.

El padre de una menor cobrará 2.000 euros de indemnización porque Turismo Valencia difundió una imagen de su hija durante la ofrenda a la Virgen de los Desamparados en unos folletos para promocionar la ciudad. El Ayuntamiento de Valencia, a quien también se le exigían responsabilidades, ha quedado absuelto, según una sentencia a la que ha tenido acceso LAS PROVINCIAS.

El fondo del asunto es velar por uno de los derechos fundamentales: el de la propia imagen. La colisión en este caso, tal y como muestra la sentencia, se produce entre el derecho anterior y el de libertad de información. Pero, además, hay que añadir la circunstancia de que se trata de una menor, con la «especial protección» de la que gozan en el ordenamiento jurídico con la finalidad de «proteger el interés superior del menor».

La resolución del juzgado de primera instancia número 10 recuerda que para la captación, reproducción o publicación de una fotografía de un menor será necesaria su autorización (si tiene la suficiente edad o madurez para concederla) o la de sus padres o representantes legales. Y, en cualquier caso, será ineficaz si con ese visto bueno «se menoscaba su reputación». Como no existió la correspondiente, la sentencia determina que se trata «de una intromisión ilegítima».

LOS HECHOS

Fotografía. Se trata de un primer plano de la menor vestida de fallera en la Ofrenda a la Virgen.

Ejemplares. Turismo Valencia difundió más de 100.000 ejemplares para promocionar la ciudad y sus fiestas. Más de la mitad eran en lenguas extranjeras.

Indemnización. El padre reclamaba 6.000 euros. Finalmente, serán unos 2.000 euros. La entidad no pidió permiso ni para captar ni difundir la imagen.

La parte demandada alegó que la Ofrenda es un acto público y de importancia central dentro de las Fallas. Pero el magistrado considera que esa circunstancia no permite concluir que cualquiera pueda captar una imagen «y proceder después a difundirla en publicaciones sin su consentimiento». Además, la fotografía, tal y como explica la sentencia, no identifica sin más la ofrenda o el interés de ese acto. «Este puede quedar plasmado en imágenes de carácter mucho más general», apunta.

Un plano muy cercano

La fotografía, que ha sido motivo de la demanda, consiste en una instantánea en la que la menor es el motivo principal de la misma: «aparece en un plano muy cercano, de cintura para arriba, con sus rasgos perfectamente identificables».

Sanción por instalar cookies de Google Analytics (y otras)

Procedimiento sancionador abierto por incumplir la normativa de *cookies*

AVISO: Sanciones ya impuestas: 3.000€ y 500€.

La Ley de Cookies sí se aplica.

La AEPD acaba de notificar a Santiago A. J., mi cliente, que se inicia un procedimiento sancionador contra una empresa que no cumple la Ley de Cookies (disculpad que no ponga los datos identificativos reales). La sanción por el incumplimiento leve (art. 38.4.g LSSI) de la Ley de Cookies (art. 22.2 LSSI) es de hasta 30.000 (art 39.1.c LSSI). La sanción podría ser de hasta 150.000€ (art. 39.b LSSI) si el incumplimiento fuera significativo (art. 38.3.i LSSI), pero no es el caso.

Sanción de 60.000 euros a una hotelera por manejo indebido de un currículo

Protección de Datos calificó de falta grave usar datos de un buscador de empleo sin su permiso

NOTICIAS RELACIONADAS

La privacidad en internet, a debate. Mallorca

FELIPE ARMENDÁRIZ. PALMA. La Agencia Española de Protección de Datos (AEPD), el organismo oficial dedicado a velar por la protección de datos y los derechos de los ciudadanos en dicha materia, sancionó hace algún tiempo a una cadena hotelera mallorquina por uso indebido del currículo de un aspirante a recepcionista.

El perjudicado lo había entregado a otro hotel de otra empresa y desde allí se remitió a la cadena expedientada, que contactó con el trabajador.

La AEPD abrió un expediente en 2004 tras tener conocimiento de que el grupo hotelero había usado datos del

VALENCIA

Usaba el correo de la Politécnica para vender 'tuppersex' estando de baja

La UPV ha abierto un expediente informativo y ha prohibido el uso de medios informáticos a la trabajadora

13.04.12 - 16:22 - EFE | VALENCIA

La Universidad Politécnica de Valencia ha abierto un expediente informativo y ha prohibido el uso de medios informáticos a una trabajadora que, estando de baja por enfermedad, utilizaba su correo electrónico para anunciar reuniones de " tapersex", en las que se ofrecían productos y juguetes relacionados con la práctica sexual.

En declaraciones a la Agencia EFE, el vicerrector de Cultura, Comunicación e Imagen Institucional de la Universidad Politécnica Joan Bautista Peiró, ha comentado que la empleada en cuestión se encontraba de baja laboral por problemas psicológicos.

La afectada, perteneciente a la plantilla de Administración y Servicios de esta centro, recurrió a su correo electrónico y al listado de sus compañeros para, desde su puesto de trabajo, enviar convocatorias de reuniones de "tapersex", en las que se ofrecían distintos productos y juguetes relacionados con el sexo.

El "tapersex", cuya denominación procede del termino inglés "tuppersex", consiste en una reunión informal de personas, principalmente mujeres, que conocen y adquieren productos, artilugios y juguetes eróticos que les ofrece un comercial.

Tanto el Jefe del Personal como el gerente de la UPV se han dirigido a esta trabajadora para prohibirle que haga uso privado de su correo electrónico universitario, al tiempo que le han abierto un expediente informativo, según ha señalado el vicerrector de Cultura.

ECD EL CONFIDENCIAL DIGITAL

22 de enero del 2013

Multa de la Agencia de Protección de Datos por enviar un correo electrónico masivo con las direcciones accesibles y no como destinatario oculto

Aviso a 'navegantes'. La Agencia Española de Protección de Datos ha determinado que la Fundación Santa María la Real vulneró el derecho a la privacidad de los receptores de un correo electrónico informativo por enviarlo sin ocultar sus direcciones de email. Les han impuesto una multa.

Se trata de una sanción que **sirve como aviso ante una práctica bastante extendida**: un correo electrónico enviado a cientos o miles de direcciones, en el que no se ha procedido a **ocultar los emails de los receptores.**

El organismo denunciado, **Fundación Santa María la Real**, es una escuela de **restauración y conservación** del patrimonio, con sede en el Monasterio que lleva su mismo nombre situado en Aguilar de Campoo, provincia de Palencia.

Con motivo de la cercanía de la **Feria del Libro de Madrid**, la institución decidió enviar un correo electrónico a todos aquellos **clientes que figuraban en su base de datos** tras haber comprado alguno de los artículos que ofrece. En el caso del denunciante, una colección de DVD`s.

Este mail fue enviado a 1.**000 direcciones de correo electrónico**, pero por un **"error involuntario"** de la persona que operaba con el ordenador, tal y como reconoce la propia fundación, **se envío sin ocultar la dirección** de los destinatarios, de forma que todos los que lo recibían podían comprobar las direcciones del resto de receptores.

"Desde ahora, y como ya lo hicimos en dichas alegaciones previas, **admitimos el error** y por tanto reconocemos voluntariamente nuestra responsabilidad a efectos de la graduación de la sanción (…) que se ha tipificado como GRAVE con **escala de 40.000 € a 300.000 €** y que nos parece, sea dicho con todo el respeto, a**bsolutamente desproporcionada**" indicó la fundación en su carta de respuesta a la AEPD.

Finalmente, la **Agencia Española de Protección de Datos**, tras estudiar el **expediente**, ha impuesto a la fundación una multa de **2.000 euros**, considerando una infracción del artículo 10 de la Ley de Protección de Datos.

COMUNIDAD VALENCIANA

Justicia recoge de un contenedor de los juzgados de Valencia documentos judiciales con datos personales

JUAN NIETO | Valencia 26 ABR. 2018 | 12:07

Responsable de la Ciudad de la Jutsicia este miércoles retirando los expedientes de la basura. / J. N.

Denunciadas cuatro clínicas, una en Zaragoza, por divulgar datos de mujeres que abortaron

Efe. Madrid/Zaragoza | Actualizada 16/12/2014 a las 19:34

Estos centros habrían tirado a contenedores de basura informes y residuos sanitarios.

Etiquetas

- Zaragoza

La **Asociación Española de Abogados Cristianos** ha presentado una **denuncia** ante la Agencia Española de Protección de Datos contra varios centros dedicados a la **práctica de abortos**, uno en Zaragoza, por tirar presuntamente a los contenedores de basura informes de mujeres que habían abortado.

Entre estos centros, ha informado este martes la Asociación en una nota de prensa, se encuentran **tres madrileños**, la Clínica Dator-Partner Line, la Clínica Ginecológica Callao, la Clínica El Bosque, así como la Clínica AMEC, de **Zaragoza**.

La organización anuncia que "en los próximos días" se van a interponer también las correspondientes **querellas** ante las **consejerías de Sanidad** que tienen convenios con estos centros.

Además de las **historias clínicas y la información médica** relacionada con las mujeres que abortaron, se encontraron "**residuos sanitarios humanos** e instrumentales que tienen una normativa de tratamiento muy estricta y que presuntamente se estaba ignorando".

Por este motivo, la Asociación Española de Abogados Cristianos iniciará asimismo las preceptivas denuncias ante la **Policía Sanitaria Mortuoria**.

"Se trata de un trabajo de recopilación sin precedentes del que se derivarían **responsabilidades administrativas**, civiles y penales", manifiesta la organización en la nota de prensa.

El trabajo de investigación y recopilación de pruebas ha sido realizado por la asociación **La Vida Importa,** quien afirma que "altas instancias del Ministerio del Interior tenían conocimiento de estos hechos desde hace meses, sin que hasta ahora se haya llevado a cabo ninguna actuación, por lo que se está estudiando interponer una **querella por omisión del deber de perseguir delitos**".

En la **documentación hallada en los contenedores** se encuentran "historias clínicas con nombres, apellidos, dirección, DNI, abortos previos, citaciones, datos de quirófano, revisiones y hasta fotocopias de libros de familia".

La Asociación Española de Abogados Cristianos considera estas **infracciones "muy graves"** al haber "tirado", presuntamente, en contenedores de basura

CincoDías

Legal

Protección de datos >

La AEPD multa a una empresa por dar datos "excesivos" en la negociación de un ERTE

- **La sanción, de 15.000 euros, se impone incluso sin intencionalidad**
- **Los sindicatos presentaron una reclamación contra la compañía**

PEDRO DEL ROSAL

Ir a comentarios

Madrid | 27 ABR 2018 - 16:01 CEST

La Agencia Española de Protección de Datos (AEPD) ha impuesto una **sanción de 15.000 euros a una empresa por** proporcionar datos excesivos **de sus empleados durante el proceso de negociación colectiva** de un Expediente de Regulación Temporal (ERTE). En una de las reuniones de la comisión negociadora, los representantes de la compañía entregaron a los sindicatos unas memorias USB que contenían dos archivos relativos al personal afectado por el ERTE y al personal no afectado.

Ninguno de los trabajadores incluidos en dichos ficheros había sido consultado para ello, y **tampoco se les había solicitado consentimiento alguno para la cesión de sus datos**, por lo que tres de los representantes de los

La protección de datos en Whatsapp

Crear grupos de WhatsApp sin consentimiento de sus miembros y compartir información en ellos puede acarrear infracciones graves en materia de protección de datos

Gabinete

5 Marzo, 2018 2:53 pm

Cerca de 200 afectados

Sanción al Gobierno de Navarra por crear un grupo de Whatsapp con información privada de ciudadanos

La Agencia de Protección de Datos considera infracción grave la creación de un chat sin consentimiento de los participantes para avisar de revisiones médicas

La Agencia Española de Protección de Datos ha dictado una resolución en la que califica de infracción grave la creación de un grupo de whatsapp por parte del departamento de Educación del Gobierno navarro. En él incluyó a ciudadanos que no habían dado su consentimiento.

AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS

1/20

Procedimiento Nº AP/00050/2017

CONSUMO

Multan a una tienda de Worten en Sevilla por vender un disco duro con datos de su plantilla

Sevilla Directo - 10/08/2016 13:16:50

La multa de 10.000 euros llega tras una denuncia de Facua. La asociación alertó a la AEPD de que el aparato comprado contenía abundante información personal y profesional de los empleados de la cadena.

La Agencia Española de Protección de Datos (AEPD) ha multado a Worten con 10.000 euros tras haber vendido a un cliente como producto nuevo un disco duro ya usado, y en cuyo interior además se encontraban almacenados datos personales de todos los empleados de la empresa.

Andrés C.G., socio de FACUA Sevilla, había adquirido en una de las tiendas que la cadena tenía en la capital andaluza (cerró a principios de 2015) un disco duro teóricamente nuevo pero que en realidad ya había sido usado. Un fraude cometido por Worten que, sin embargo, destapó una segunda, e igualmente grave, infracción: al encender el aparato, el usuario advirtió que estaba lleno de datos personales y profesionales de los empleados de la cadena.

PUBLICADA EN

LA PROVINCIA

DISTRITOS

Bellavista – La Palmera
Casco Antiguo
Cerro – Amate
Este – Alcosa – Torreblanca
Los Remedios
Macarena
Nervión
Norte
San Pablo – Santa Justa
Sur
Triana
Cartuja. Barrio tecnológico
La Provincia

SEGURIDAD INFORMÁTICA

Una vulnerabilidad permite ver la información de clientes de 1.600 gimnasios

Una brecha de seguridad en una aplicación móvil para clientes de gimnasios permitiría acceder a diversa información de clientes de más de 1.600 establecimientos de 16 países, entre ellos España, ha denunciado hoy el experto en hacking ético y ciberseguridad Deepak Daswani.

EFEFUTURO MADRID | MIÉRCOLES 25.04.2018

Sobres con datos financieros visibles

Publicado:
Julio 29, 2010 – 7:30 am

Autor:
Por microgal

Categorías:
- General

Comentarios:
- Ninguno
- Feed RSS de Comentarios
- Post a comment
- URL para Trackbacks

En el procedimiento sancionador PS/00526/2007, instruido por la AGPD, a la entidad BANCO CETELEM, se trata de una denuncia en la que se declara que se ha recibido por correo ordinario dos cartas del banco Cetelem, que se han remitido en un sobre con "ventanilla", a través de la cual no solo se visualizan los datos de la denunciante como destinataria de las mismas, sino que se puede leer "he devuelto impagado el recibo"

En este caso ah quedado acreditado que la denunciada , como responsable del fichero, vulneró el deber de secreto que le incumbía al permitir que cualquier ajeno al afectado pudiera ver el contenido del escrito del interior, que explicita datos financieros que unidos a los datos de una identidad permiten obtener una evaluación de la persona destinataria.

En este caso la vulneración del deber de secreto efectuada por la entidad financiera es constitutiva de una infracción grave del art 10. Con una multa de 60.102 €

https://www.youtube.com/watch?v=_8b25ivMyOg&feature=youtu.be

Público

SOCIEDAD SUCESOS EDUCACIÓN SANIDAD IGUALDAD INMIGRACIÓN MEDI

› El 'agujero negro' de los datos personales afecta también a la Agencia Tributaria

MADRID, 20/05/2018 12:57 • Actualizado: 20/05/2018 12:57

PABLO ROMERO @pabloromero

Nadie sabe si el 25 de mayo será el día del fin del mundo, aunque para algunos lo parezca. A partir de ese día, sí o sí, va ser de aplicación directa el temido Reglamento General de Protección de Datos (RGPD, o GDPR según sus siglas en inglés). No obstante, quienes sí que van a notar un cambio radical en su actividad son los trabajadores de la Agencia Española de Protección de Datos (AEPD). Su directora, **Mar España**, lo tiene claro: con una fuerza laboral de 180 personas, de los que **sólo 15 son inspectores**, los próximos meses van a ser "todo un reto" para la propia Agencia.

¿Quién no ha notado una creciente avalancha de correos electrónicos y mensajes de empresas y servicios que se adaptan al RGPD? No es más que el esfuerzo de las miles de empresas que, pese a haber tenido dos años para adaptarse a la nueva normativa (en vigor desde 2016, pero directamente aplicable a partir del próximo jueves), han dejado para el final el cumplimiento de nuevos y más estrictos requisitos que deben cumplir en el territorio de los 28 países en donde se aplica esta norma: **más control de los datos para los ciudadanos, más transparencia en el uso de los mismos, mayores multas para quienes incumplan**.

¿Para qué implantar la LOPD en su organización?

Proporciona:

- Confianza
- Eficiencia
- Calidad

¿Cuáles son los beneficios de adecuarse a la LOPD?

- **Reducción riesgos de sanción** debido a infracciones por no tener debidamente implantada la LOPD

- **Diferenciación sobre la competencia** al tratar los datos de carácter personal manera adecuada.

- **Reducción fugas información** por la implantación de métodos y sistemas que eviten las fugas.

MUCHAS GRACIAS POR SU ATENCIÓN

Javier Nogueroles Olaizola

Email: jnogueroles@quicksand.es

www.quicksand.es

Móvil: 638963976