AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS

Brechas en el RGPD

Andrés Calvo

Coordinación Unidad Tecnológica

AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS

«Del registro de incidencias a la gestión y notificación de brechas de seguridad»

Registro

Soporte documental de las acciones realizadas
Requisito del artículo 33.5 RGPD

antecedentes

Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico.

Disposición adicional novena. *Gestión de incidentes de ciberseguridad que afecten a la red de Internet.*

1. Los prestadores de servicios de la Sociedad de la Información, los registros de nombres de dominio y los agentes registradores que estén establecidos en España están obligados a prestar su colaboración con el CERT competente, en la resolución de incidentes de ciberseguridad que afecten a la red de Internet y actuar bajo las recomendaciones de seguridad indicadas o que sean establecidas en los códigos de conducta que de esta Ley se

antecedentes

Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal.

Artículo 90. *Registro de incidencias.*

Deberá existir un procedimiento de notificación y gestión de las incidencias que afecten a los datos de carácter personal y establecer un registro en el que se haga constar el tipo de incidencia, el momento en que se ha producido, o en su caso, detectado, la persona que realiza la notificación, a quién se le comunica, los efectos que se hubieran derivado de la misma y las medidas correctoras aplicadas.

antecedentes

Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica.

Disposición adicional cuarta. *Desarrollo del Esquema Nacional de Seguridad.*

1. Sin perjuicio de las propuestas que pueda acordar el Comité Sectorial de Administración Electrónica según lo establecido en el artículo 29, apartado 2, se desarrollarán las siguientes instrucciones técnicas de seguridad que serán de obligado cumplimiento por parte de las Administraciones públicas:

a) Informe del estado de la seguridad.
b) Notificación de incidentes de seguridad.

antecedentes

Ley 9/2014, de 9 de mayo, General de Telecomunicaciones.

Artículo 41. *Protección de los datos de carácter personal.*

1. Los operadores que exploten redes públicas de comunicaciones electrónicas o que presten servicios de comunicaciones electrónicas disponibles al público, incluidas las redes públicas de comunicaciones que den soporte a dispositivos de identificación y recopilación de datos, deberán adoptar las medidas técnicas y de gestión adecuadas para preservar la seguridad en la explotación de su red o en la prestación de sus servicios, con el fin de garantizar la protección de los datos de carácter personal. Dichas medidas incluirán, como

RGPD

REGLAMENTO (UE) 2016/679 DEL PARLAMENTO EUROPEO Y DEL CONSEJO

de 27 de abril de 2016

relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos)

El RGPD define, de un modo amplio, las "violaciones de seguridad de los datos personales" como "todas aquellas violaciones de la seguridad que ocasionen la destrucción, pérdida o alteración accidental o ilícita de datos personales transmitidos, conservados o tratados de otra forma, o la comunicación o acceso no autorizados a dichos datos."

I. DISPOSICIONES GENERALES

JEFATURA DEL ESTADO

12257 *Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información.*

Disposición adicional tercera. *Notificación de violaciones de seguridad de los datos personales a través de la plataforma común prevista en este real decreto-ley.*

La plataforma común para la notificación de incidentes prevista en este real decreto-ley podrá ser empleada para la notificación de vulneraciones de la seguridad de datos personales según el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE, en los términos que acuerden la Agencia Española de Protección de Datos y los órganos que gestionen dicha plataforma.

AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS

Responsabilidad activa

- Se integra en el principio de responsabilidad activa del RGPD:

GARANTIZAR Y ESTAR EN CONDICIONES DE DEMOSTRAR QUE EL TRATAMIENTO DE DATOS SE LLEVA A CABO DE CONFORMICAD CON EL RGPD

AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS

novedades

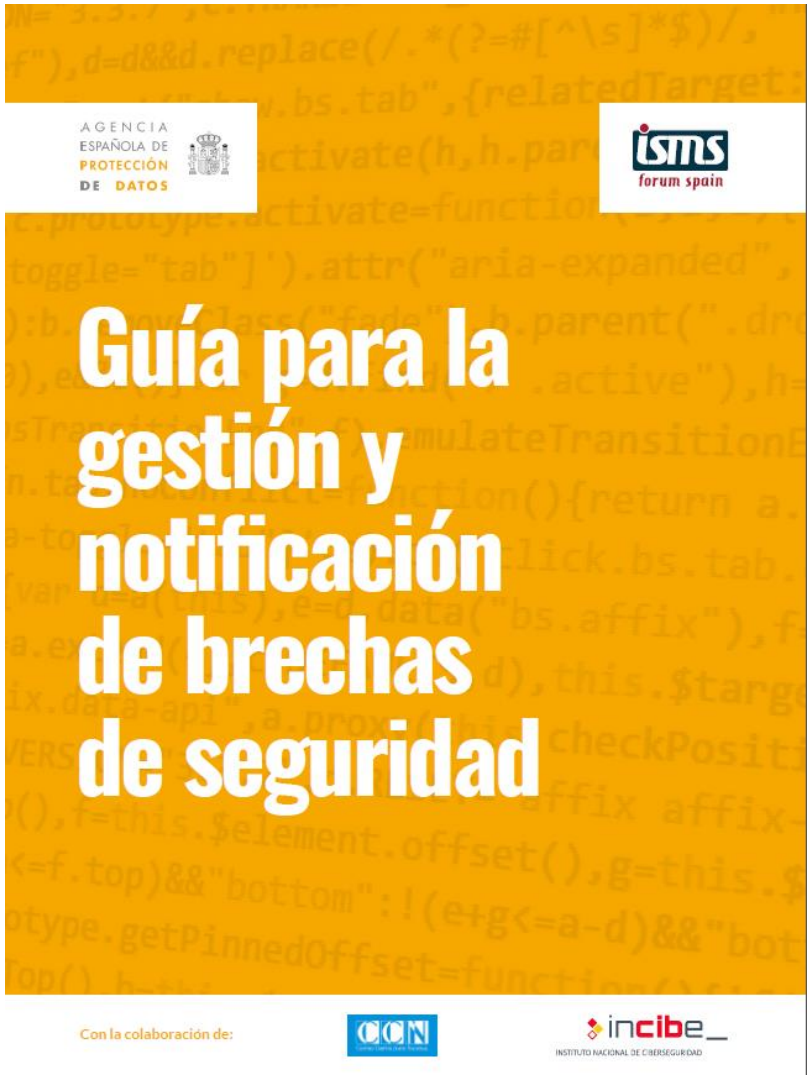
- Gestión y notificación aplica a cualquier tratamiento de datos personales
- Excepto: improbable que pueda afectar a los derechos y libertades de las personas
- A considerar: número afectados, tipos de datos, contenido de la notificación (Autoridad de control e interesados)
- Plazo de 72 horas
- Notificación a la autoridad de control y a los interesados o afectados.

Directrices sobre la notificación de las violaciones de la seguridad de los datos personales de acuerdo con el Reglamento 2016/679

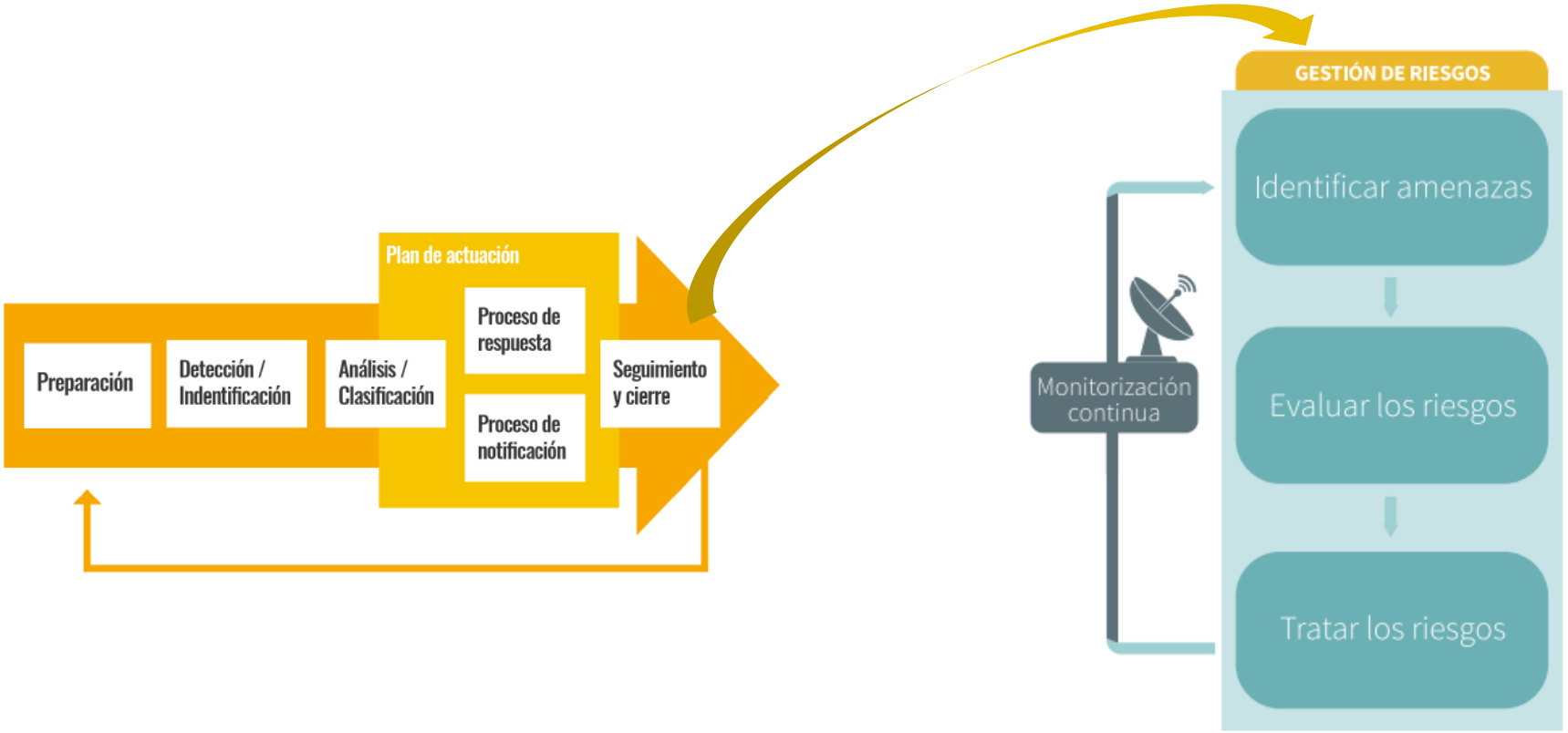
Adoptadas el 3 de octubre de 2017

Revisadas por última vez y adoptadas el 6 de febrero de 2018

AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS



contenido



INCIDENTES Y BRECHAS SON FUENTE DE INFORMACIÓN PARA LOS MAPAS DE RIESGOS

AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS

NOTIFICACIONES EN CIFRAS

DESDE EL 25 DE MAYO: 479 NOTIFICACIONES

- 32 SON NOTIFICACIONES ADICIONALES
- 477 EN TOTAL

AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS

NOTIFICACIONES EN CIFRAS

Tipo de organización:

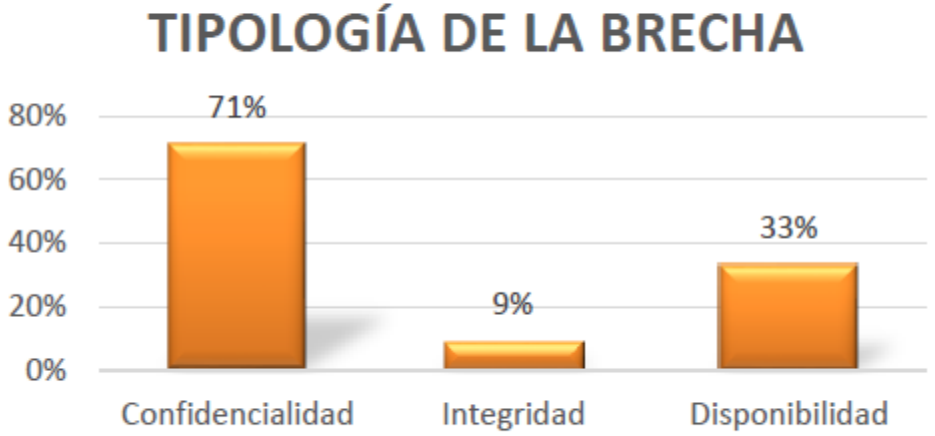
Descripción	%
Organizaciones privadas	89%
Organizaciones públicas	11%

AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS

NOTIFICACIONES EN CIFRAS

Tipología de la brecha:

Tipo	%
Confidencialidad	71%
Integridad	9%
Disponibilidad	33%



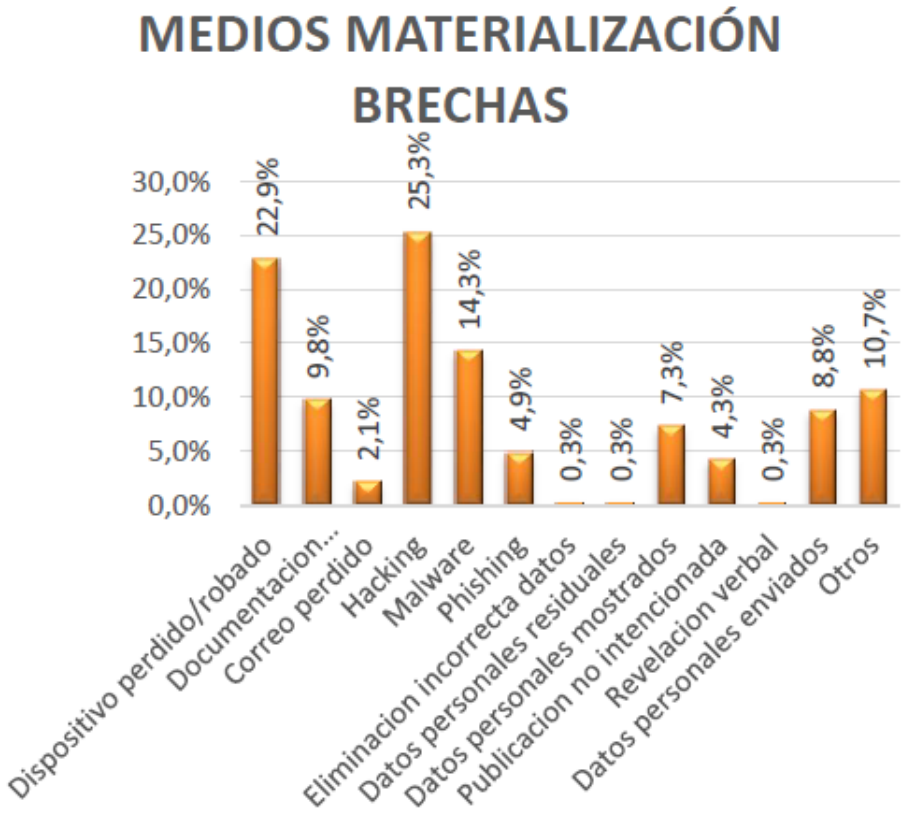
(existen brechas que afectan a más de una dimensión)

AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS

NOTIFICACIONES EN CIFRAS

Medios de materialización de las brechas:

Medios	%
Dispositivo perdido/robado	23%
Documentacion perdida/robada	10%
Correo perdido	2%
Hacking	25%
Malware	14%
Phishing	5%
Eliminacion incorrecta datos	0,3%
Datos personales residuales	0,3%
Datos personales mostrados	7%
Publicacion no intencionada	4%
Revelacion verbal	0,3%
Datos personales enviados	9%
Otros	14%

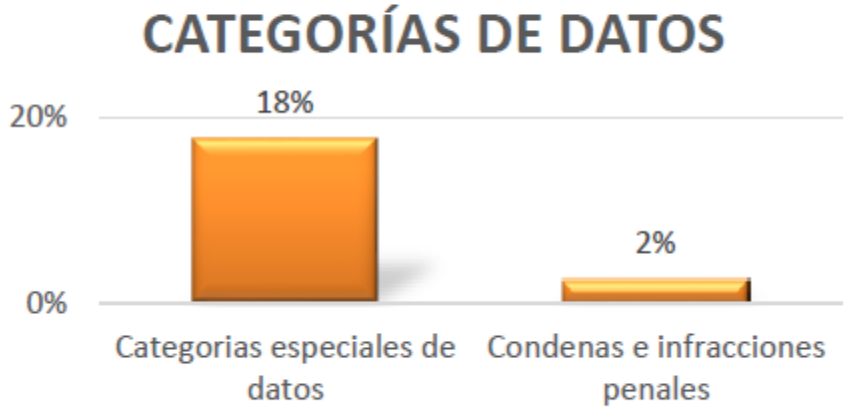


AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS

NOTIFICACIONES EN CIFRAS

Categorías de datos:

Categorías	%
Condenas o infr. penales	2%
Categorías Especiales	18%

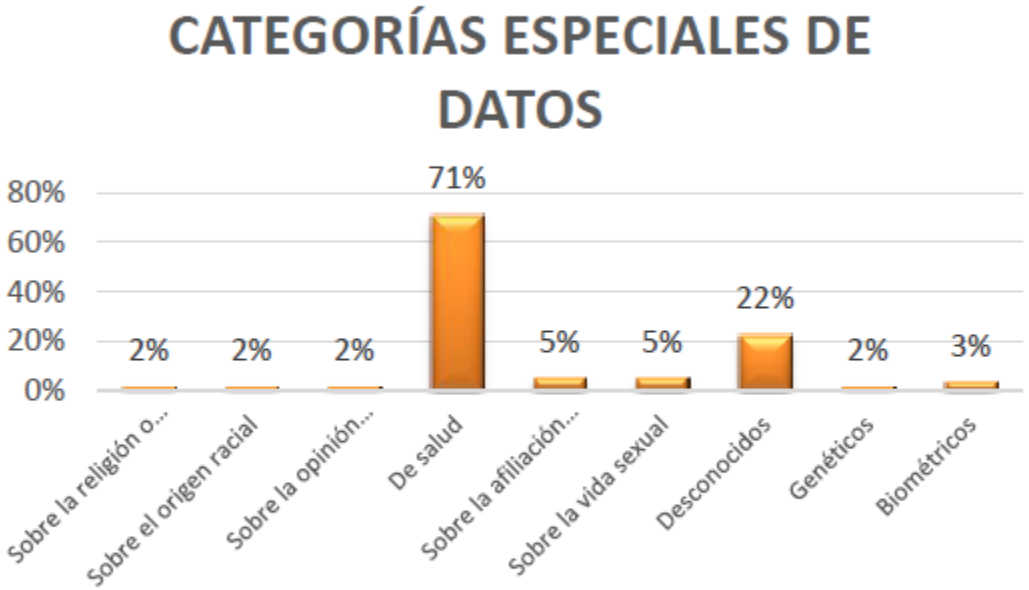


AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS

NOTIFICACIONES EN CIFRAS

Detalle categorías especiales[2]:

Medios	%
Sobre la religión o creencia	2%
Sobre el origen racial	2%
Sobre la opinión política	2%
De salud	71%
Sobre la afiliación sindical	5%
Sobre la vida sexual	5%
Desconocidos	26%
Genéticos	4%
Biométricos	7%



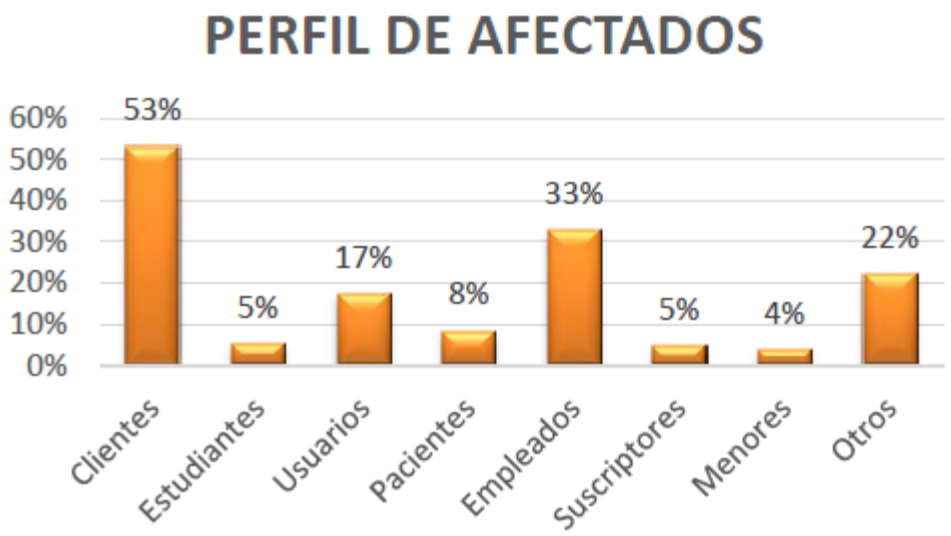
[2] Porcentajes con respecto al número de notificaciones que implican categorías especiales de datos.

AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS

NOTIFICACIONES EN CIFRAS

Perfiles de los afectados:

Afectados	%
Clientes	53%
Estudiantes	5%
Usuarios	17%
Pacientes	8%
Empleados	33%
Suscriptores	5%
Menores	4%
Otros	22%



AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS

NOTIFICACIONES EN CIFRAS

Notificaciones por Comunidades Autónomas:

Comunidad Autónoma	%
Andalucía	10,7%
Aragón	2,1%
Principado de Asturias	2,1%
Baleares	0,3%
Cantabria	0,6%
Castilla y León	2,4%
Castilla-La Mancha	1,2%
Cataluña	22,3%
Comunidad Valenciana	6,1%
Extremadura	0,9%
Galicia	6,7%
Comunidad de Madrid	38,7%
Región de Murcia	0,9%
Comunidad Foral de Navarra	0,6%
País Vasco	1,5%
La Rioja	0,3%
Canarias	2,4%
Ceuta	0,0%
Melilla	0,0%

AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS

RÉGIMEN SANCIONADOR
Medidas y Brechas de Seguridad

Luis de Salvador Carrasco

Subdirector Adjunto de Inspección

AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS

RÉGIMEN SANCIONADOR
Medidas y Brechas de Seguridad

Objetivo: Sostenibilidad, Confianza y Resiliencia

- Ajustado a un Modelo de Cumplimiento Orientado a Procesos
  - Política de Protección de Datos Art. R.a.24.2 RGPD
- Orientado a la rápida reparación de los intereses del sujeto
  - Traslado al DPD/responsable/organismos de resolución de conflictos/supervisión L.a.37/65
  - Medidas Provisionales L.a.69
- Orientado a la resolución de los problemas presentes y futuros de todos los sujetos.
  - Corregir el proceso
  - Apercibimiento/Sanción/Orden
- Orientación Paneuropea
  - Identificación de la Autoridad de Control competente
  - Establecimiento de criterios comunes
- Extensión de los sujetos sometidos L.a.70

AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS

RÉGIMEN SANCIONADOR
Medidas y Brechas de Seguridad

Régimen en la LOPDGDD

- Sanciones enumeradas en los artículos L.73-graves y L.74-leves
- Implica prescripción de 1 o 2 años (leves-graves)
- El L.a.73 se relaciona con el R.a.83.4 de sanciones (10ME – 2%vtn)
- El L.a.74 se relaciona con el R.a.83.4 y 5 pero sólo en sus aspectos formales.
- El R.a.83.4.a incluye el incumplimiento de las obligaciones relativas a los artículos R.a.33 y R.a.34, por lo que el rango sancionador no puede ser más de (0 … 10ME – 2%vtn).

AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS

RÉGIMEN SANCIONADOR
Medidas y Brechas de Seguridad

Grave L.a.73.f por no adoptar aquellas medidas técnicas y organizativas que resulte apropiadas para garantizar un nivel de seguridad adecuado al riesgo.

- Incluyendo aquellas para detectar y notificar las violaciones R.c.87
- Relacionado con la Política de Protección de Datos R.a.24
  - ⑩ Tendrá un apartado sobre seguridad que tendrá que estar integrado en la Política de Seguridad de la Información o SGSI.
- Implica un sistema de gestión de incidentes
- L.Da.1 Medidas de seguridad en el ámbito del sector público.
  - ⑩ ENS, pero con determinación del nivel de riesgo adaptado al R.a.32
- L.Da.18 Criterios de seguridad

•Leve 74. No documentar las violaciones.

- R.a.33.5
- Incluirá efectos, medidas adoptadas y hechos relacionadas.
- Implícitamente, un sistema de gestión de incidentes.

•Grave L.a.73.q Por incumplimiento de encargado de notificar al responsable.

- No se establece en la norma plazos de tiempo.

AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS

RÉGIMEN SANCIONADOR
Medidas y Brechas de Seguridad

- Grave L.a.73.r Por no comunicar a la AEPD la brecha, que puede resultar Leve L.a.74.m cuando esta notificación sea tardía, incompleta o defectuosa.
  - Se tendrá que informar de la naturaleza de la violación, volumen de datos e interesados, categorías de datos, posibles consecuencias, medidas adoptadas y propuestas y punto de contacto (DPD).
  - R.a.33.1 cuando no sea improbable que dicha violación de la seguridad constituya un riesgo para los derechos y las libertades de las personas físicas.
  - ➓Ver indicaciones Guía Brechas AEPD 6.2.3 y Anexo III.
  - ➓Modelo de comunicación en el Anexo II, con descripción de campos.
  - Plazo R.a.33.1 sin dilación indebida y, de ser posible, a más tardar 72 horas después de que haya tenido constancia de ella.
  - Para considerar la caracterización como leve se tendrá que documentar el motivo de la dilación Ra.33.1.
  - L.Da.9. Tratamiento de datos personales en relación con la notificación de incidentes de seguridad
  - La comunicación a la AEPD no es un hecho singular en el tiempo, sino que se puede/ha de extender según se incrementa lo información.
- Leve L.a.74.ñ Por falta de comunicación a los sujetos, que puede ser Grave L.a.73.s cuando esa comunicación haya sido requerida por la AEPD (R.58.2.e)
  - Si no es requerida, los criterios R.a.34.3 para realizarla son:
  - ➓a) el responsable ha adoptado medidas de protección a los datos personales afectados por la violación;
  - ➓b) el responsable ha tomado medidas ulteriores que garanticen que ya no existe un alto riesgo;
  - ➓c) suponga un esfuerzo desproporcionado, se optará por una comunicación pública o semejante e igualmente efectiva.
  - No hay un plazo concreto, tan solo que no haya dilación indebida R.a.34.1
  - Comunicación incluirá información sobre la naturaleza la violación y posibles consecuencias, medidas adoptadas y propuestas y punto de contacto (DPD). R.a.34.2
  - Será en un lenguaje claro y sencillo. R.a.34.2. Esto no significa información incompleta o edulcorada.

AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS

RÉGIMEN SANCIONADOR
Medidas y Brechas de Seguridad

•Graduación de la Sanción R.a.83.2

- La naturaleza, gravedad y duración, naturaleza, alcance, propósito, número de afectados, daños y perjuicios que hayan sufrido;
- La intencionalidad o negligencia;
- Medidas para paliar los daños y perjuicios;
- El grado de responsabilidad en virtud de R.a25 y 32;
- Toda infracción anterior
- El grado de cooperación con la AEPD para mitigar los efectos
- Las categorías de los datos
- Forma en que la AEPD tuvo conocimiento de la infracción,
- Cuando las medidas indicadas en el artículo 58, apartado 2 , hayan sido ordenadas previamente
- La adhesión a códigos de conducta R.a.40 o a mecanismos de certificación R.a.42
- Cualquier otro factor: beneficios financieros o pérdidas evitadas.

•Graduación de la Sanción L.a.76

- Carácter continuado de la infracción.
- Vinculación actividad del infractor con la realización de tratamientos de D.P.
- Los beneficios obtenidos como consecuencia de la comisión de la infracción.
- Posibilidad de que el afectado hubiera podido inducir a la comisión de la infracción.
- Fusión por absorción posterior a la infracción, no imputable a la entidad absorbente.
- Afectación de los derechos de menores
- No disponer del obligado DPD
- Sometimiento voluntario a mecanismos de resolución de conflictos.

AGENCIA
ESPAÑOLA DE
PROTECCIÓN
DE DATOS

www.aepd.es

@AEPD_es