DIPUTACIÓ DE VALÈNCIA

Protecció de Dades i Seguretat de la Informació

Boletín protección de datos

Boletín del Departamento de protección de datos y Seguridad de la Información de la Diputación Provincial de Valencia

Boletín N.º 10| Abril 2021

ANÁLISIS, GESTIÓN Y COMUNICACIÓN DE LAS BRECHAS DE SEGURIDAD EN EL CONTEXTO DEL RGPD

Í N D I C E

IDENTIFICACIÓN, GESTIÓN Y COMUNICACIÓN DE LAS BRECHAS DE SEGURIDAD EN EL CONTEXTO DEL RGPD.

Os invitamos a trasladarnos aquellas temáticas que resulten de vuestro interés para los próximos boletines informativos. Estas peticiones deberán dirigirse a:

Diputación de Valencia

Dpto. de Protección de Datos y Seguridad de la Información

Pl. de Manises, 4 46003 Valencia

email: dpdssi@dival.es

SUSCRIPCIONES

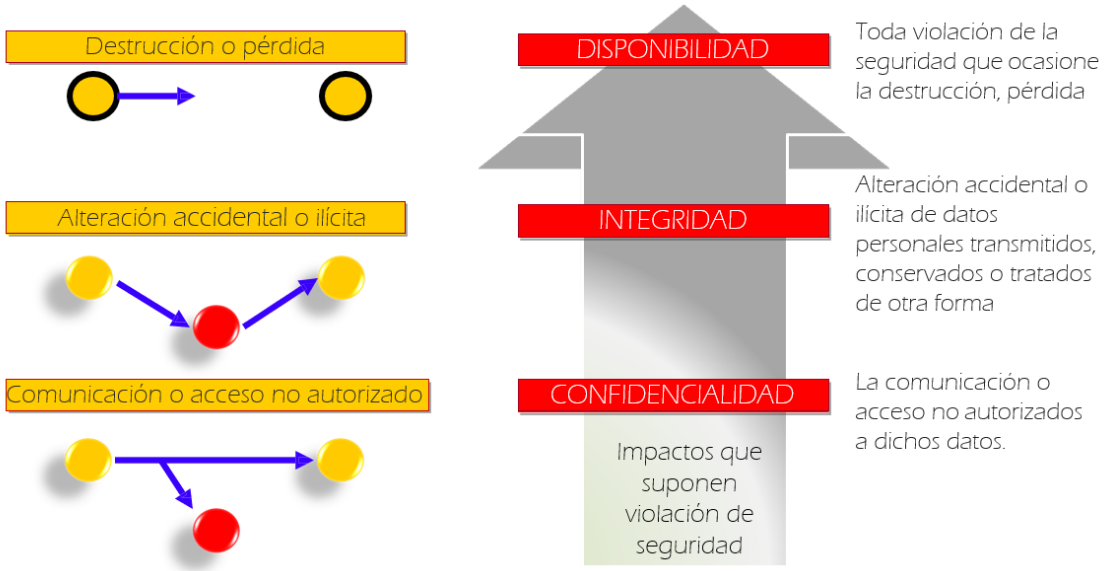
Si deseas suscribirse a nuestro Boletín informativo accede al siguiente enlace

INTRODUCCIÓN

Una "violación de seguridad" -también denominada "brecha de seguridad"- es un incidente de seguridad que afecta a datos de carácter personal. Este incidente puede tener un origen accidental o intencionado y, además, puede afectar a datos tratados digitalmente o en formato papel. En general, se trata de un suceso que ocasiona la destrucción, pérdida, alteración, comunicación o acceso no autorizado a datos personales, como podemos comprobar más adelante.

El Reglamento General de Protección de Datos (RGPD) define 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"*, y obliga a que, aquellas violaciones de seguridad que puedan suponer un riesgo para los derechos y libertades de las personas físicas, sean notificadas a la autoridad de control competente -en nuestro caso, se trata de la Agencia Española de Protección de Datos (AEPD)-. En determinados casos, los de riesgo alto para los derechos y libertades de los interesados, se deberá notificar también a estos últimos.

Es evidente que cualquier organización que trate datos personales se encuentra expuesta a sufrir una brecha de seguridad que podrá repercutir en la privacidad de los interesados, por lo que se debe implementar un procedimiento para la adecuada gestión de las mismas. Esto permitirá responder de forma rápida, ordenada y eficaz, minimizando las consecuencias sobre la propia organización y terceras partes implicadas, las cuales afectan a la confidencialidad, integridad o disponibilidad de los datos:



EN LA DIPUTACIÓN DE VALENCIA, LA GESTIÓN DE LAS BRECHAS DE SEGURIDAD HABRÁ DE REGIRSE POR EL PROCEDIMIENTO INTERNO VIGENTE EN CADA MOMENTO.

IDENTIFICACIÓN

La detección de un incidente que pueda afectar a la seguridad de información y suponer una brecha de seguridad de los datos personales es de vital importancia, ya que el RGPD establece que se deben notificar a la autoridad de control competente las brechas de seguridad que puedan suponer un riesgo para los derechos y libertades de las personas físicas, sin dilación indebida y, a más tardar, 72 horas después de que se haya tenido constancia de ella. En determinados casos se deberá notificar también a los afectados, sin dilación indebida.

Esta labor de detección e identificación recaerá, en numerosas ocasiones, en los usuarios de los sistemas de información. **Cualquier suceso que suponga o pudiera suponer un incidente de seguridad deberá ser comunicado inmediatamente para valorar si puede catalogarse como "brecha de seguridad de los datos personales".** Por ejemplo, deberán comunicarse inmediatamente eventos como:


La pérdida de contraseñas de acceso a los Sistemas de Información.


La pérdida o robo de soportes informáticos o documentos en papel con datos de carácter personal.


La presencia de archivos con caracteres inusuales.


La recepción de correos electrónicos con archivos adjuntos sospechosos.


El comportamiento extraño de dispositivos.


La imposibilidad de acceder a ciertos archivos


Ataques a la red


La infección de los sistemas de información por virus u otros elementos dañinos


La pérdida de datos por un mal uso de las aplicaciones

Los distintos momentos de atención que requieren las brechas de seguridad se suceden desde la identificación de la incidencia hasta su cierre, pasando por el debido análisis previo y, en su caso, respuestas y/o comunicaciones correspondientes.

En la figura siguiente, extraída de la *Guía para la gestión y notificación de brechas de seguridad de la AEPD*, podemos apreciar las fases más importantes en las que podemos dividir la gestión de este tipo de incidentes:

La identificación de un incidente de seguridad puede producirse a través de fuentes internas a la organización o fuentes externas. Estas últimas serían los avisos que podemos recibir de terceros (proveedores, técnicos, etc.).

En este sentido, además de cumplir todos los protocolos de seguridad y prestar atención a las anomalías que puedan surgir en el trabajo con sistemas de información, hay que estar pendientes de las alertas que suelen difundir en casos de riesgo los distintos organismos públicos como el Instituto Nacional de Ciberseguridad (INCIBE), el Centro Criptológico Nacional (CCN), Fuerzas y Cuerpos de Seguridad del Estado, o los medios de comunicación.

Una vez identificado el incidente de seguridad, la actuación que procede es un análisis que permita **conocer más detalles sobre lo acontecido** una identificación y clasificación más precisa del mismo.

Además de las respuestas reaccionarias al incidente, es muy importante que, según el caso, se proceda a la notificación o comunicación de la brecha de seguridad a la autoridad de control. Pasamos a revisarlo en los apartados siguientes.

"UNA VEZ IDENTIFICADO EL INCIDENTE DE SEGURIDAD, SE RECABARÁ MÁS DETALLES PARA DECIDIR QUÉ MEDIDAS TOMAR Y PARA VALORAR LA NECESIDAD DE NOTIFICAR A LA AUTORIDAD DE CONTROL Y, EN SU CASO, A LOS AFECTADOS."

ANÁLISIS

EL ROL DEL DPD

Dado que el **Delegado de Protección de Datos (DPD)** desarrolla un papel muy relevante, en este caso de liderazgo, es importante que sea consultado tan pronto se haya detectado el incidente, lo que implicará que el usuario que lo detecte deba comunicarlo sin dilación. La actuación del DPD tendrá especial relevancia en esta fase de comunicación puesto que, entre las funciones que la normativa le atribuye, está la de actuar como punto de contacto entre el Responsable del tratamiento -la Diputación de Valencia- y la autoridad de control -la AEPD-.

La **información útil al DPD** para decidir qué medidas tomar y para valorar la necesidad de notificar a la autoridad de control y afectados, al menos será la siguiente:

- **Medio por el que se ha materializado** o ha ocurrido, por ejemplo: la pérdida de un dispositivo con datos personales, el robo de documentación que alberga información de carácter personal, la publicación de datos personales por error, el envío a un destinatario equivocado, un ransomware que ha cifrado un dispositivo, la intrusión no autorizada en un sistema de información con datos personales, un empleado que ha sido víctima de phishing, etc**.**
- **Origen de la brecha:** si ha sido interna o externa y su intencionalidad.
- **Categorías de datos:** si son datos básicos como credenciales o datos de contacto o si bien son categorías especiales, como puedan ser datos de salud.
- **Volumen de datos afectados**: tanto en número de ficheros o registros afectados como en número de personas cuyos datos constaran en aquellos.
- **Categorías de afectados:** empleados, ciudadanos, diputados, etc. Es importante identificar si podría haber afectado a algún colectivo vulnerable.
- **Información temporal:** cuándo se inició, cuándo se ha detectado y cuándo ha quedado resuelta.

En todo caso, es preciso que cualquier brecha de la seguridad, hechos relacionados, efectos y medidas adoptadas, se registre y justifique documentalmente, de modo que permita en el futuro a la autoridad de control verificar el cumplimiento de la normativa.

COMUNICACIÓN

Con independencia de las notificaciones internas que se deban efectuar para gestionar un incidente de seguridad, el RGPD establece que, en caso de brecha de la seguridad de los datos personales, el responsable del tratamiento -la Diputación de Valencia- deberá valorar el riesgo, tal y como se muestra en la siguiente imagen, a modo de resúmen, y en función de ello, determinar si se requiere notificar a la autoridad de control y en su caso, a los interesados.

Directrices sobre la notificación de las violaciones de la seguridad de los datos personales de acuerdo con el Reglamento 2016/679.
GRUPO DE TRABAJO SOBRE PROTECCIÓN DE DATOS DEL ARTÍCULO 29

Según proceda, las brechas de seguridad deberán ser comunicadas a:

LA AUTORIDAD DE CONTROL COMPETENTE -AEPD-

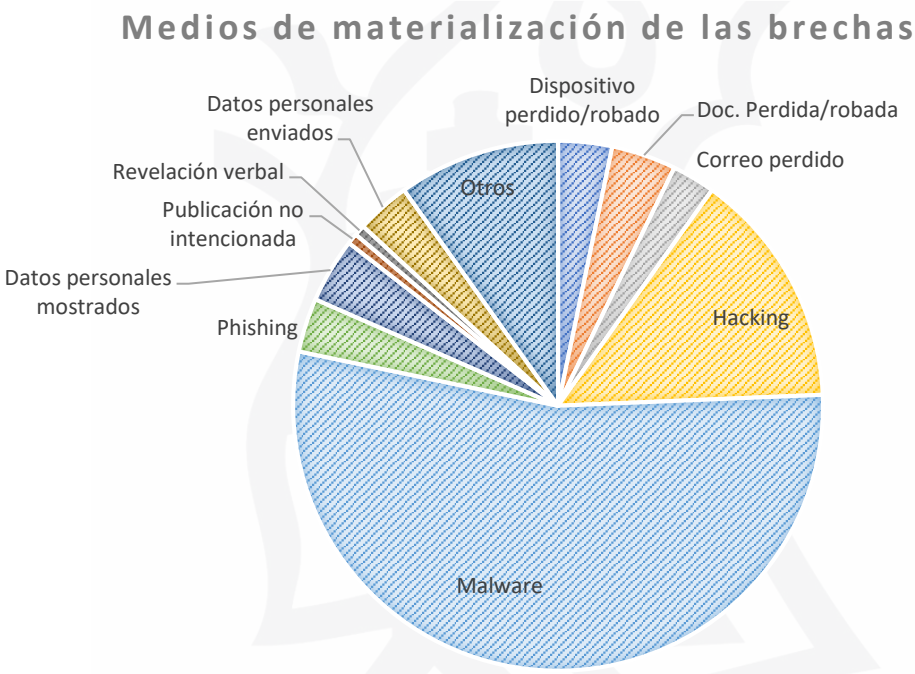
La comunicación deberá efectuarse sin dilación indebida y, a más tardar, 72 horas después de haber tenido constancia de ella, a menos que sea improbable que dicha brecha de la seguridad constituya un riesgo para los derechos y las libertades de las personas físicas. Si en el momento de la notificación, no fuese posible facilitar toda la información, podrá facilitarse posteriormente, de manera gradual en distintas fases. La primera notificación se realizará en las primeras 72h, y al menos se realizará una comunicación final o de cierre cuando se disponga de toda la información relativa al incidente. La notificación a la AEPD se realizará a través del formulario destinado a tal efecto publicado en la Sede Electrónica de la Agencia**.**

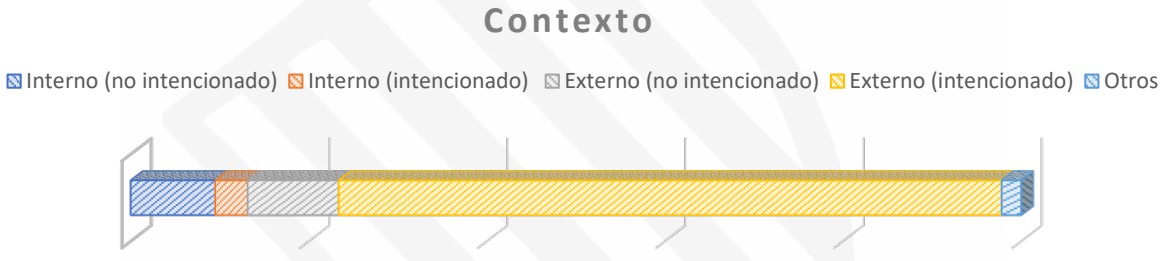
LOS AFECTADOS

El RGPD también establece los casos en los que una brecha de seguridad se debe comunicar a los afectados, en concreto, cuando sea probable que la brecha de la seguridad de los datos personales entrañe un **alto riesgo** para los derechos y libertades de las personas físicas. En este caso, la comunicación deberá efectuarse **sin dilación indebida.** La notificación, preferentemente, se deberá realizar de forma directa al afectado, ya sea por teléfono, correo electrónico, SMS, a través de correo postal, o a través de cualquier otro medio dirigido al afectado que se considere adecuado.

TENDENCIAS ACTUALES

La Agencia Española de Protección de Datos (AEPD) publica, mensualmente, un informe que resume las características principales de las notificaciones de brechas de seguridad recibidas. En su último informe, publicado en el mes de marzo, se señala que durante el mes de febrero se experimentó un **incremento sustancial en las notificaciones recibidas** respecto al mes anterior, debido a un incidente de seguridad de tipo *ransomware* en un encargado de tratamiento. El informe recoge las notificaciones de brechas de seguridad de los datos personales recibidas durante febrero de 2021, siendo un total de **146 notificaciones**. En el mes de enero, el número de brechas notificadas a la AEPD fue de 88.





"EN FEBRERO DE 2021, LA AEPD RECIBIÓ 146 NOTIFICACIONES DE BRECHAS DE SEGURIDAD, UN NÚMERO SUSTANCIALMENTE SUPERIOR A LAS NOTIFICADAS EN ENERO (88). LA MAYORÍA DE BRECHAS FUERON PROVOCADAS, DE MANERA INTENCIONADA, POR UN AGENTE EXTERNO A LAS ORGANIZACIONES, SIENDO EL MALWARE EL MEDIO DE MATERIALIZACIÓN MÁS HABITUAL."

MATERIAL COMPLEMENTARIO

- Web de la Agencia Española de Protección de Datos (AEPD). Apartado dedicado a "Brechas de seguridad". Consulta este enlace.
- Directrices sobre la notificación de las violaciones de la seguridad de los datos personales de acuerdo con el RGPD (Grupo de Trabajo del Artículo 29). Consulta este enlace.
- Guía para la gestión y notificación de brechas de seguridad (AEPD). Consulta este enlace.
- Formulario de notificación de brechas de seguridad de la Sede Electrónica (AEPD). Consulta enlace.
- Brechas de seguridad de datos personales: qué son y cómo actuar (Blog AEPD). Consulta este enlace.
- Brechas de seguridad: el correo electrónico y las plataformas de productividad online (Blog AEPD). Consulta este enlace.
- Brechas de seguridad: El Top 5 de las medidas técnicas a tener en cuenta (Blog AEPD). Consulta este enlace.
- Brechas de seguridad: comunicación a los interesados (Blog AEPD). Consulta este enlace.
- Brechas de seguridad: protégete ante el ransomware. Consulta este enlace.

NOTICIAS

- **El reciente ciberataque contra el Servicio de Empleo Público Estatal (SEPE) ha puesto de manifiesto las vulnerabilidades a las que se enfrentan a diario los organismos del Estado ante las amenazas cibernéticas.**

  El número de ciberataques *'ransomware'* en España creció un 160% en el último trimestre de 2020. Sin embargo, la administración pública española no es más vulnerable que la de los países de nuestro entorno europeo. Seguir leyendo a través de este enlace.

- **Las brechas de seguridad también ocurren en las compañías tecnológicas más grandes del mundo.**

  Archivos con datos personales de 533 millones de usuarios de Facebook aparecieron en un pequeño foro de hackeo. Los datos incluyen el número de teléfono, nombre completo, número de identificación en Facebook, localización actual y anterior, fecha de nacimiento, correo electrónico, fecha de creación, estado sentimental y biografía. La particularidad de la brecha es que incluye cientos de millones de números de teléfono vinculados a sus propietarios, entre ellos 10,8 millones de españoles y de otros países latinoamericanos. Facebook dice que los datos pertenecen a una brecha parcheada en 2019, con lo que la información filtrada tiene al menos un par de años. Consulta la noticia en este enlace.

- **Hackean miles de cámaras de seguridad: acceden a cárceles, hospitales y a fábricas de Tesla.**

  En marzo han sido afectadas más de 150.000 cámaras, a las cuales los hackers han tenido acceso debido a una brecha de seguridad. Consulta la noticia en este enlace.