DIPUTACIÓ DE VALÈNCIA

Protecció de Dades i Seguretat de la Informació

Cuadernos DivalData

Cuadernos dirigidos a delegados,
responsables y especialistas en protección
de datos personales

Cuaderno nº 20 | Febrero 2022

GESTIÓN Y NOTIFICACIÓN DE BRECHAS DE SEGURIDAD: NOVEDADES Y REPASO

DIPUTACIÓ DE VALÈNCIA
Protecció de Dades i Seguretat de la Informació

Í N D I C E

GESTIÓN Y NOTIFICACIÓN DE BRECHAS DE SEGURIDAD: NOVEDADES Y REPASO

	Página
Introducción	**2**
La gestión "de siempre" ante las brechas de seguridad	**4**
Las novedades que trae la guía editada en 2021	**7**
Material complementario y noticias	**10**

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: dpdsi@dival.es

SUSCRIPCIONES

Si deseas suscribirte a nuestra publicación accede al siguiente

enlace

"BRECHA ES EL TÉRMINO QUE UTILIZAMOS DE MANERA MÁS COMÚN PARA DENOMINAR LA VIOLACIÓN DE SEGURIDAD QUE AFECTA A DATOS DE CARÁCTER PERSONAL."

INTRODUCCIÓN

El Reglamento (UE) 2016/679 –Reglamento General de Protección de Datos o RGPD– trata las "violaciones de seguridad" en sus considerandos 85-88, así como en los artículos 4.12, 33 y 34 de su texto.

Una "violación de seguridad de los datos personales" viene definida como "toda violación de la seguridad 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 autorizados a dichos datos".

La consecuencia de esta violación es que el responsable del tratamiento no es capaz de garantizar más la observancia de los principios relativos al tratamiento de datos personales con arreglo al artículo 5 del RGPD. Hay que diferenciar, pues, cualquier otro acontecimiento relacionado con la seguridad de la información de una "violación de datos personales": mientras que todas las violaciones de datos personales son accidentes de seguridad, no todos los accidentes de seguridad son violaciones de datos personales.

"Brecha", definida por la Real Academia de la Lengua como "resquicio por donde algo empieza a perder su seguridad", es el término que utilizamos de manera más común, también en consonancia con el inglés *data breach*, para denominar la violación de seguridad que afecta a datos de carácter personal.

Esta situación puede tener un origen accidental o intencionado y además puede afectar a datos tratados digitalmente o en formato papel. Como responsable de tratamiento, la Diputación de Valencia debe estar preparado para posibilidades como estas.

La Agencia Española de Protección de Datos (AEPD) ha publicado, en junio de 2021, una nueva edición *Guía para la gestión y notificación de brechas de seguridad.*

"LA GUÍA DE JUNIO DE 2021 ACTUALIZA A LA ANTERIOR COMO INSTRUMENTO DE AYUDA A LOS RESPONSABLES EN EL CUMPLIMIENTO DE SUS OBLIGACIONES EN LO REFERENTE A LAS BRECHAS DE DATOS PERSONALES".

En junio de 2018 la AEPD publicó la primera guía dedicada a este tema, que fue un instrumento pionero en la Unión Europea, destinado a ayudar a responsables y encargados en el cumplimiento de sus nuevas obligaciones en lo referente a las brechas de datos personales.

La guía de junio de 2021 actualiza a la anterior como instrumento de ayuda a los responsables en el cumplimiento de sus obligaciones en lo referente a las brechas de datos personales. Esta actualización dice aprovechar la experiencia adquirida por la AEPD, otras Autoridades de Control y el Comité Europeo de Protección de Datos.

Su texto nos recuerda, una vez más, que cualquier organización que trate datos personales se encuentra expuesta a sufrir una brecha de datos personales que pueda repercutir en los derechos y libertades de las personas físicas, y por tanto está obligada a preverlas y gestionarlas adecuadamente.

Según la AEPD, el proceso de gestión de brechas se suma a las políticas de información ya existentes en una organización y es una parte necesaria para mantener la actividad de cualquier entidad. Este proceso se constituye en una de las medidas organizativas más importantes a la hora de salvaguardar los derechos y libertades de los interesados a través de medidas de seguridad de los tratamientos

La finalidad última de la notificación y comunicación de brechas de datos personales es la protección efectiva de los derechos fundamentales y libertades de las personas físicas afectadas por la brecha.

Las organizaciones que sufran una brecha de datos personales deben focalizar sus esfuerzos en evitar y mitigar las posibles consecuencias sobre los derechos fundamentales y libertades públicas de las personas afectadas.

EL INCIDENTE (TÉCNICO O 'HUMANO') DEBERÁ SER INMEDIATAMENTE COMUNICADO AL SERVICIO DE PROTECCIÓN DE DATOS Y SEGURIDAD DE LA INFORMACIÓN DE LA DIPUTACIÓN DE VALENCIA.

LA GESTIÓN "DE SIEMPRE" ANTE LAS BRECHAS DE SEGURIDAD

Una de las principales obligaciones ante el evento de una brecha de seguridad es su comunicación a la AEPD cuando se cumpla una serie de condiciones.

Cabe recordar que no todos los incidentes de seguridad son necesariamente brechas de datos personales y no solo los ciberincidentes pueden ser brechas de datos personales. A su vez, no toda acción que suponga una vulneración de la normativa de protección de datos puede ser considerada una brecha de datos personales.

Por tanto, es necesario establecer un criterio para diferenciar cuándo el incidente se concibe como una brecha o violación de la seguridad de los datos de carácter personal. Para ello es necesario conocer qué ha ocurrido y de qué forma las medidas de seguridad han funcionado o paliado los hechos para establecer si realmente se ha producido o no una violación de la seguridad de los datos.

Así, el proceso de gestión y notificación de incidentes se compone de las siguientes fases.

FASE 1: DETECCIÓN Y ALERTA

Cualquier empleado, proveedor u otra persona, puede informar a la Diputación de la existencia de un incidente/s que pudiera/n afectar a la seguridad de los datos de carácter personal.

Si la brecha de datos personales es detectada por el encargado del tratamiento (p.ej., nuestro proveedor), éste deberá remitir al responsable (p.ej., nosotros) toda la información necesaria para que pueda cumplir con sus obligaciones en tiempo y forma.

El incidente de seguridad deberá ser comunicado, inmediatamente, a este Servicio: **dpdssi@dival.es**

FASE 2: REGISTRO DEL INCIDENTE

Para la correcta documentación del incidente, incluyendo las decisiones a tomar sobre la notificación

"LA CONTENCIÓN DEL INCIDENTE SUPONDRÁ LA TOMA DE DECISIONES RÁPIDAS Y ADOPCIÓN DE MEDIDAS, TÉCNICAS Y ORGANIZATIVAS".

a la AEPD y la comunicación a los afectados, serán necesarios al menos la siguiente información:

- Fecha y hora de la detección.
- Detección [empleado, colaborador, 3º de confianza, externo].
- Naturaleza del evento de seguridad de los datos personales.
- Descripción breve.
- Sistema afectado.
- Unidad organizativa o unidades organizativas potencialmente afectadas.

En la medida de lo posible, y aunque sea información imprecisa o sin verificar, para poder evaluar la severidad del incidente, se recogerá además la siguiente información:

- Tipo y número aproximado por categoría de interesados afectados [menores, empleados, directivos, afiliados a sindicatos, etc.].
- Categorías y número aproximado de registros de datos personales afectados [DNI, nombre y apellidos, direcciones, matrículas, credenciales, etc.].
- Nivel de certeza de los hechos conocidos: [Sin evidencias / Indicios de evidencia / Evidencias contrastables].

FASE 3: ACTUACIONES DE CONTENCIÓN Y RECUPERACIÓN FRENTE A LOS INCIDENTES

La contención del incidente supondrá la toma de decisiones rápidas y adopción de medidas, técnicas y organizativas, como puede ser cerrar un sistema, aislarlo de la red, deshabilitar ciertas funciones, etc. Una vez aplicadas de las medidas, se debe verificar el correcto funcionamiento de éstas, confirmando su idoneidad para la eliminación del incidente.

Se debe considerar también si las medidas aplicadas son de carácter temporal o si forman parte de una solución definitiva, y el sistema y/o la información afectada ha vuelto de nuevo de modo efectivo a su estado original.

RECUERDA:

UN INCIDENTE DE SEGURIDAD QUE NO HA AFECTADO A DATOS PERSONALES O TRATAMIENTOS DE DATOS PERSONALES NO ES UNA BRECHA DE DATOS PERSONALES, DADO QUE NO PODRÍA PRODUCIR DAÑOS SOBRE LOS DERECHOS Y LIBERTADES DE LAS PERSONAS FÍSICAS CUYOS DATOS SON OBJETO DEL TRATAMIENTO, INDEPENDIENTEMENTE DE OTROS PERJUICIOS QUE PUEDA PRODUCIR AL RESPONSABLE O ENCARGADO DEL TRATAMIENTO.

Solucionado el incidente o la brecha de seguridad, y verificada la eficacia de las medidas adoptadas, se restablecerá el servicio en su totalidad, confirmando su funcionamiento normal y evitando en la medida de lo posible que sucedan nuevos incidentes basados en la misma causa. Esto será crucial para categorizar con carácter final la severidad del incidente de seguridad en protección de datos personales, y poder así valorar si estamos ante una brecha de seguridad.

FASE 4: VALORACIÓN DE LOS INCIDENTES Y BRECHAS DE SEGURIDAD

Uno de los parámetros más importantes a la hora de evaluar una brecha de datos personales es determinar con exactitud su tipología, es decir determinar a qué dimensión/es de seguridad de los datos personales ha afectado la brecha:

- Afecta a la **confidencialidad** cuando produce una revelación no autorizada o accidental de los datos personales, o su acceso (por ejemplo: envío de correo electrónico a una pluralidad de destinatarios sin uso de copia oculta);
- Afecta a la **disponibilidad** cuando produce una pérdida de acceso accidental o no autorizada a los datos personales, o su destrucción (por ejemplo: las llamadas situaciones de “pantallas en negro”);
- Afecta a la **integridad** cuando produce una alteración no autorizada o accidental de los datos personales (por ejemplo, descubrir que han sido modificados ficheros guardados).

Los factores a tener en cuenta para evaluar el riesgo de la brecha son:

- Tipo de brecha de datos personales.
- Facilidad de identificar a los interesados afectados.
- Naturaleza de la brecha.
- Categorías especiales de datos personales.
- Volumen de datos afectados.
- Gravedad de los daños ocasionados.
- Características de la entidad responsable.
- Número de interesados afectados.

"LA NOTIFICACIÓN A LA AEPD SE REALIZARÁ ANTES DE LAS 72 HORAS DESDE QUE SE HAYA TENIDO CONSTANCIA DE ELLA Y UNA VEZ SE HA VALORADO LA OBLIGACIÓN DE TENERLA QUE HACER POR LOS RIESGOS QUE SUPONE".

FASE 5: NOTIFICACIONES

El responsable de tratamiento debe valorar la severidad o gravedad de impacto de una brecha para los derechos y libertades de los afectados en relación con la probabilidad de producirse, y notificar en su caso a la AEPD cuando se den las condiciones estipuladas. En muchos casos, el responsable también deberá comunicar la brecha a las propias personas afectadas (sin plazo concreto, pero "sin dilación indebida").

La notificación a la AEPD se realizará antes de las 72 horas desde que se haya tenido constancia de ella y una vez se ha valorado la obligación de tenerla que hacer por los riesgos que supone.

FASES FINALES

El asunto estará en **seguimiento** hasta constatar que la brecha ha sido definitivamente resuelta y que el riesgo para los afectados no ha sido eliminado o reducido a niveles de riesgo residual aceptable. Acto seguido, se tratará de sacar **lecciones aprendidas**: solventar posibles deficiencias en la gestión de incidentes o incorporar mejoras que permitan una mejor respuesta en las siguientes ejecuciones.

LAS NOVEDADES QUE TRAE LA GUÍA EDITADA EN 2021

El motivo principal de la actualización de la Guía consiste en facilitar y agilizar el procedimiento de gestión y notificación de las brechas de seguridad por parte de los responsables y encargados del tratamiento.

En la nueva Guía se incluye información más específica para la gestión integral de una brecha de seguridad de datos personales de modo más eficaz y eficiente, los procedimientos obligatorios de gestión de la brecha de seguridad y los canales de notificación ante la Autoridad competente.

"NOTIFICAR EN TIEMPO Y FORMA ES UNA EVIDENCIA DE LA DILIGENCIA DE LA ORGANIZACIÓN".

SOBRE LAS NOTIFICACIONES

Las notificaciones de brechas de datos personales a la AEPD se deben realizar de forma electrónica, usando el formulario de notificación de brechas de datos personales de la Sede Electrónica con lo que se pretende garantizar una correcta ejecución de las obligaciones del artículo 33.3 del RGPD.

La notificación a la autoridad de control de una brecha que afecta a datos personales forma parte de la responsabilidad proactiva establecida en el RGPD, y el hecho de notificarla no implica necesariamente la apertura de un procedimiento administrativo. De hecho, notificar en tiempo y forma es una evidencia de la diligencia de la organización, mientras que no cumplir con esa obligación si está tipificado como infracción.

Una vez notificada una brecha de datos personales a la Autoridad de Control, el responsable de tratamiento ha de estar preparado para recibir y atender los posibles requerimientos, órdenes o comunicaciones que la AEPD pueda realizarle electrónicamente en relación con la brecha de datos personales notificada. Por ejemplo:

- **Comunicación** con información relativa al registro de la brecha de datos personales notificada.
- **Notificación** con un requerimiento de información adicional sobre la brecha de datos personales o el tratamiento de datos personales en cuestión.
- Notificación con una **orden para comunicar a los afectados** la brecha de datos personales en virtud del artículo 34.4 al considerar que el riesgo para los afectados es alto.

La AEPD remitiría sus comunicaciones y/o notificaciones a la Dirección Electrónica Habilitada (DEH) de la Diputación de Valencia, como entidad responsable de tratamiento identificada en el formulario de notificación.

"SE INCLUYE UN LISTADO DE MOTIVOS DE DEMORA EN LA NOTIFICACIÓN EN EL PLAZO ORDINARIO, QUE EN CUALQUIER CASO DEBERÁN ACOMPAÑARSE DE LA OPORTUNA JUSTIFICACIÓN EN EL MOMENTO DE LA NOTIFICACIÓN".

En cuanto a las comunicaciones a los interesados, que deberán realizarse en su caso –con el contenido mínimo establecido en el art. 34 del RGPD– de forma directa a los afectados, se recoge que pueden ser por medio de teléfono, correo electrónico, SMS, correo postal, o a través de cualquier otro medio dirigido al afectado que el responsable considere adecuado.

SOBRE LOS PLAZOS

Se trata de una de las principales novedades en comparación con la versión anterior es en cuanto a los plazos.

Si bien se mantiene el plazo de 72 horas para notificar la brecha de datos personales que constituya un riesgo para los derechos y libertades de los interesados, en esta versión se incluye un listado de motivos de demora en la notificación en el plazo ordinario, que en cualquier caso deberán acompañarse de la oportuna justificación en el momento de la notificación, a saber:

- el plazo de 72 horas expira fuera del horario de la jornada laboral, día inhábil o periodo de vacaciones;
- incidencia técnica;
- inicialmente no se consideró necesario notificar la brecha de seguridad;
- demora en el proceso de gestión; o
- interferencia en una investigación policial o judicial en curso.

Además, se establece un máximo de 30 días para modificar la notificación inicial, así como el plazo máximo de 30 días para confirmar la ejecución de una orden emitida por la AEPD.

VALORACIÓN DE LAS BRECHAS

La nueva Guía reitera, en un lenguaje claro y sencillo, los criterios a tener en cuenta a la hora de determinar la procedencia o no de la notificación de la brecha y, en su caso, la comunicación a los propios afectados.

Si bien, se trata de una valoración que se realizaría desde el Servicio de Protección de Datos y Seguridad de la información, con los datos que pueden ser facilitados con toda la urgencia que requiere estas situaciones.

MATERIAL COMPLEMENTARIO

- Guía para la Gestión y Notificación de Brechas de Datos Personales (AEPD). Consulta este enlace.
- *Guidelines 01/2021 on Examples regarding Data Breach Notification* (EDPB). Consulta en este enlace.
- Herramienta Comunica-Brecha RGPD (AEPD). Consulta este enlace.
- "Brechas de seguridad: comunicación a los interesados" (AEPD). Consulta este enlace.
- Consultas frecuentes (FAQS) de la Sede Electrónica de la AEPD. Consulta este enlace.

NOTICIAS

- **Las 5 claves para navegar seguro en el Día Europeo de la Protección de Datos.**

  ¿Qué hacer para evitar una brecha de datos en una industria asolada por este problema?

  Consulta los consejos en este enlace.

- **Exponer datos en grupos de WhatsApp, incluso con permisos previos, es ilegal.**

  Un ayuntamiento ha sido sancionado por crear un grupo de 'desconocidos' y no garantizar la confidencialidad de datos como móvil, foto o nombre. La opción era implantar una lista de difusión, que es unidireccional.

  Consulta la noticia en este enlace.

- **Espectacular aumento de las sanciones en la UE por Protección de Datos**

  Durante 2021 el importe las multas impuestas por las diferentes autoridades de control europeas por incumplimiento del Reglamento General de Protección de Datos (RGPD), ha superado los 1.000 millones de euros, frente a los poco más de 170 millones de 2020.

  Consulta la noticia en este enlace.

- **La privacidad de los datos, un imperativo para el 91% de las empresas españolas.**

  La inversión en soluciones que preserven la privacidad de los datos sigue creciendo a medida que las empresas ven incrementado su retorno de la inversión. Preservar la privacidad ya se ha convertido en una de las principales prioridades para el 91% de las empresas españolas.

  Consulta la noticia en este enlace.