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 14 | Agosto 2021

DIRECTRICES PARA LA CORRECTA GESTIÓN DE LAS BRECHAS DE SEGURIDAD

DIPUTACIÓ DE VALÈNCIA
Protecció de Dades i Seguretat de la Informació

Í N D I C E

DIRECTRICES PARA LA CORRECTA GESTIÓN DE LAS BRECHAS DE SEGURIDAD

	Página
INTRODUCCIÓN	**2**
POLÍTICA CORPORATIVA	**3**
ROLES Y RESPONSABLES	**4**
TIPOS DE BRECHAS	**5**
FASES DE GESTIÓN	**8**
MATERIAL COMPLEMENTARIO Y NOTÍCIAS DE ACTUALIDAD	**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

"EL REGLAMENTO GENERAL DE PROTECCIÓN DE DATOS (RGPD) LAS LLAMA "VIOLACIONES DE SEGURIDAD" Y DEFINE POR PRODUCIRSE 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."

INTRODUCCIÓN

Una brecha de seguridad es un incidente de seguridad que afecta a datos personales, independientemente de si es la consecuencia de un accidente o de una acción intencionada y tanto si afecta a datos digitales o en formato papel.

El Reglamento General de Protección de Datos (RGPD) las llama "violaciones de seguridad de datos personales" y define por producirse 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 normativa en vigor desde 2018 obliga a notificar la violación de la seguridad de los datos personales a la autoridad de control competente tan pronto como se tenga conocimiento de que se ha producido, y a más tardar en un plazo de 72 horas; salvo que pueda demostrarse, atendiendo a su responsabilidad proactiva, que no existe riesgo para los derechos y libertades de las personas. La Ley Orgánica de Protección de Datos y de Garantías de Derechos Digitales no recoge explícitamente la obligación de notificar las brechas de seguridad a la AEPD, puesto que ya queda recogido en el RGPD, pero sí establece que dicho incumplimiento es una infracción muy grave.

Por otra parte, si la brecha pudiera derivarse un alto riesgo para los interesados, también habrá que comunicárselo a éstos, a fin de que tengan conocimiento y puedan tomar al respecto las medidas oportunas.

Las violaciones de seguridad o brechas de seguridad pueden afectar a diferentes dimensiones de la seguridad:

- Confidencialidad: revelación no autorizada o accidental de los datos personales, o su acceso
- Integridad: una alteración no autorizada o accidental de los datos personales
- Disponibilidad: revelación no autorizada o accidental de los datos personales, o su acceso.

Sobre estos aspectos profundizaremos a lo largo de los apartados siguientes.

"LA DIPUTACIÓN DE VALÈNCIA CUENTA CON UN PROCEDIMIENTO DE GESTIÓN DE INCIDENTES Y NOTIFICACIONES DE BRECHAS DE SEGURIDAD QUE PUEDE CONSULTARSE EN EL DEPARTAMENTO DE PROTECCIÓN DE DATOS Y SEGURIDAD DE LA INFORMACIÓN, PERO LAS NOCIONES BÁSICAS A ESTE RESPECTO SON NECESARIAS EN CADA UNO DE LOS CENTROS GESTORES DEL TRATAMIENTO DE DATOS DE NUESTRA CORPORACIÓN."

POLÍTICA CORPORATIVA

Para dar respuesta a los incidentes con la seguridad de la información, hemos de contar con los conocimientos necesarios sobre el modo de actuar. Aunque la respuesta dependerá mucho de la categoría de incidencia a la que nos enfrentemos, se tratará siempre de contener la situación evitando que el mal se expanda y agrave y, posteriormente, poner remedio al mismo tratando de garantizar la continuidad del servicio minimizando el riesgo para los derechos y libertades de los interesados. Hay que recordar que podría reclamarse responsabilidad patrimonial de la administración por los daños y perjuicios que el interesado haya podido sufrir, salvo que la Corporación pueda demostrar que ha cumplido fielmente con sus obligaciones.

En este sentido, los artículos 33 y 34 del RGPD exponen la necesidad de que las organizaciones integren dentro de sus políticas un proceso de gestión de brechas de datos personales que concrete cómo la organización va a dar cumplimiento a sus obligaciones con respecto a las brechas.

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. Así, es muy importante que todos los usuarios de la Corporación conozcan mínimamente de la gestión de incidentes y notificaciones de brechas de seguridad.

Cabe señalar que no tendrán consideración de violación o brecha de seguridad de datos personales, a los efectos de la obligación de notificación a la Autoridad de Control y comunicación a los afectados, aquellos incidentes que:

- No afecten a datos personales, es decir, a datos que no sean de personas físicas identificadas o identificables.
- No afecten a tratamientos de datos personales llevados a cabo en nuestra calidad de responsable o encargado de tratamiento.

De este modo, no todos los incidentes de seguridad son necesariamente brechas de datos personales y no sólo los incidentes que tengan lugar sobre los tratamientos automatizados pueden ser considerados brechas de datos personales, ya que también habría que considerar los tratamientos en papel.

"EL DELEGADO DE PROTECCIÓN DE DATOS ACTÚA COMO PORTAVOZ ÚNICO ANTE LA AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS Y SERÁ LA PERSONA QUE ATENDERÁ CUALQUIER CUESTIÓN, DUDA, DERECHO O DENUNCIA DE LOS INTERESADOS AFECTADOS POR EL INCIDENTE DE SEGURIDAD EN CUALQUIERA DE LOS TRATAMIENTOS DE DATOS PERSONALES"

ROLES Y RESPONSABILIDADES

Dependiendo de si actuamos como responsable o como encargado del tratamiento, tenemos impuestas unas u otras obligaciones ante la eventualidad de una brecha.

RESPONSABLE DEL TRATAMIENTO

Actuando en calidad de responsables del tratamiento, debemos aplicar las medidas técnicas y organizativas apropiadas a fin de garantizar y poder demostrar que el tratamiento es conforme al RGPD:

- valoración del incidente evaluando las consecuencias para los derechos y libertades de las personas;
- garantizar que se notifica la brecha de datos personales a la autoridad competente, cuando resulte necesario sin dilación indebida, y también que se comunicará la brecha de datos personales a los afectados cuando sea necesario;
- contar con el asesoramiento del Delegado de Protección de Datos y este Departamento de la Diputación;
- cumplir con las indicaciones de la Jefatura de este Departamento para cumplir el resto de obligaciones con respecto a las brechas.

ENCARGADO DEL TRATAMIENTO

Además de las anteriores, actuando como encargados del tratamiento tenemos la obligación de:

- informar al responsable de tratamiento sin dilación indebida de las brechas de datos personales que afecten a los tratamientos encargados (aportando la información necesaria para facilitar la evaluación del riesgo), sin perjuicio de las obligaciones adicionales que pueda haber adquirido en virtud del contrato de encargo de tratamiento;
- ayudar al responsable a garantizar el cumplimiento de las obligaciones establecidas en el RGPD, incluyendo la gestión, notificación y comunicación de las brechas de datos personales;
- ejecutar las labores de notificación o comunicación de la brecha que en su caso tenga asignadas por contrato.

Señalar que el Delegado de Protección de Datos actúa como portavoz único ante la Agencia Española de Protección de Datos y será la persona que atenderá cualquier cuestión, duda, derecho o denuncia de los interesados afectados por el incidente de seguridad en cualquiera de los tratamientos de datos personales.

"LA AEPD ESTABLECE 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"

TIPOS DE BRECHAS

Es imposible esperar una correcta gestión de las brechas de seguridad si no tenemos claro en qué aspectos pueden manifestarse como tal. Más aún, la propia AEPD establece que 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.

Por eso, pasamos a revisar los distintos tipos existentes de las mismas y algunos ejemplos de prevención y/o gestión.

CONFIDENCIALIDAD

Una brecha afecta a la confidencialidad cuando los datos personales de un tratamiento han podido ser accedidos por terceros sin permiso, incluyendo cuando los datos son exfiltrados. Esto incluye, por ejemplo, los casos de intrusión en sistema de información con acceso y/o exfiltración de datos personales, el envío de datos personales por error, la pérdida de dispositivos o documentación con datos personales, malware de tipo ransomware con exfiltración de datos, etc. Es importante saber si los datos personales afectados estaban (total o parcialmente) cifrados de forma segura, anonimizados o protegidos de forma que sean ininteligibles para quien haya tenido acceso a dichos datos o lo pueda tener en el futuro. Si es así, las consecuencias de la brecha de confidencialidad quedan en gran medida mitigadas, reduciendo o incluso anulando los riesgos derivados del incidente.

- Ejemplo: brechas causadas por pérdida o robo de dispositivos móviles cuyos elementos de almacenamiento están cifrados con un algoritmo no comprometido y el acceso al dispositivo protegido por una contraseña fuerte y difícilmente deducible, se puede considerar que los riesgos asociados a la pérdida de confidencialidad de los datos están apropiadamente mitigados.
- Ejemplo: brechas causadas por la exfiltración de un fichero de base de datos de usuarios conteniendo nombre de usuario, contraseña, datos de contacto y dirección:
- Si las contraseñas de los usuarios están protegidas con un algoritmo de hash considerado criptográficamente seguro, de forma que son ininteligibles para quien ha tenido acceso a la base de datos, el riesgo quedaría parcialmente mitigado. Si el algoritmo de hash no se considera

criptográficamente seguro (md5, sha1, …) la mitigación del riesgo no es efectiva.

- Si el fichero de base de datos exfiltrado estaba totalmente cifrado mediante un algoritmo criptográficamente seguro y la clave de cifrado no está comprometida, el riesgo queda mitigado de forma que en algunos casos se puede considerar que es prácticamente nulo

DISPONIBILIDAD

Una brecha afecta a la disponibilidad de los datos personales cuando han estado inaccesibles de forma temporal o permanente para quien legítimamente debe poder tratarlos o acceder a ellos. Esta situación puede ocurrir por sucesos que afecten a los datos personales en sí mismos o también por sucesos que afecten a los sistemas utilizados para su tratamiento. informar al responsable de tratamiento sin dilación indebida de las brechas de datos personales que afecten a los tratamientos encargados, sin perjuicio de las obligaciones adicionales que pueda haber adquirido en virtud del contrato de encargo de tratamiento.

Es importante determinar si la disponibilidad se ha podido recuperar o está en vías de recuperación, dado que recuperar los datos y los sistemas de tratamiento es la vía para mitigar el daño que pueden producir este tipo de brechas de datos personales.

- Ejemplo: brechas causadas por malware tipo ransomware en las que se pueda descartar con certeza la exfiltración de datos y se pueden reestablecer los datos personales y medios de tratamiento sin que afecte significativamente a los servicios prestados, se puede considerar que el riesgo se ha mitigado adecuadamente. En el caso de que la recuperación de los datos y/o tratamientos se prolongue en el tiempo afectando significativamente a los servicios prestados, por ejemplo, al no existir o no funcionar sistemas de respaldo de datos y procesos, se puede concluir que el riesgo no solo no ha quedado mitigado, sino que se está materializando y causando perjuicios de diversa consideración a los interesados. ejecutar las labores de notificación o comunicación de la brecha que tenga asignadas por contrato.
- Ejemplo: brechas causadas por malware tipo ransomware en las que se pueda descartar con certeza la exfiltración de datos y se pueden reestablecer los datos personales y medios de tratamiento sin que afecte significativamente a

"ES IMPORTANTE DETERMINAR SI LA DISPONIBILIDAD SE HA PODIDO RECUPERAR O ESTÁ EN VÍAS DE RECUPERACIÓN, DADO QUE RECUPERAR LOS DATOS Y LOS SISTEMAS DE TRATAMIENTO ES LA VÍA PARA MITIGAR EL DAÑO."

"CUANDO SE PRODUCEN BRECHAS DE DATOS PERSONALES DE INTEGRIDAD, HAY QUE DETERMINAR SI EL TRATAMIENTO DE LOS DATOS ALTERADOS ILEGÍTIMAMENTE PUEDE CAUSAR O HA CAUSADO ALGÚN DAÑO A LOS AFECTADOS Y EN SU CASO SI EL DAÑO SE PUEDE REVERTIR"

los servicios prestados, se puede considerar que el riesgo se ha mitigado adecuadamente.

- Ejemplo: En brechas causadas por la pérdida o destrucción accidental de datos personales, el riesgo se considerará mitigado cuando exista un plan de recuperación que incluya una copia actualizada y recuperable de los datos y se pueda reestablecer la prestación del servicio sin haber causado perjuicios a los interesados.

INTEGRIDAD

Una brecha afecta a la integridad cuando se han alterado los datos personales de forma ilegítima y el tratamiento de esos datos personales puede causar un daño a los afectados.

Uno de los posibles casos es que un tercero modifique en la base de datos de la organización la información relativa a los datos bancarios de los empleados que se utilizan para el pago de las nóminas, o un alumno modifica las calificaciones en la base de datos de su programa formativo. Cuando se producen brechas de datos personales de integridad, hay que determinar si el tratamiento de los datos alterados ilegítimamente puede causar o ha causado algún daño a los afectados y en su caso si el daño se puede revertir.

- Ejemplo: Para mitigar las brechas de integridad causadas por la modificación de ficheros se puede implementar herramientas de control de la integridad de los archivos que se basan en calcular el hash de cada fichero que se vigila y cuando es modificado, aunque sea un solo bit de alguno de estos archivos el sistema periódicamente vuelve a calcular el hash de cada uno y al compararlo detectará la modificación y emitirá un aviso.
- Ejemplo: Se podrá mitigar el riesgo de una brecha de integridad en las bases de datos contando con controles de acceso, alertas y registros ante modificaciones. Además, implementando sistemas que auditen de forma continua los accesos de lectura y escritura a estas bases de datos.

Afecta a:	Cuando produce una:
Confidencialidad	revelación no autorizada o accidental de los datos personales, o su acceso
Disponibilidad	pérdida de acceso accidental o no autorizada a los datos personales, o su destrucción
Integridad	una alteración no autorizada o accidental de los datos personales

"ANTES QUE NADA, 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."

FASES DE GESTIÓN

Antes que nada, tal como ya se ha referido, 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.

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

FASE 1: DETECCIÓN Y ALERTA

Comoquiera que se conozca la información sobre la existencia de una brecha de seguridad, posible o confirmada, esta circunstancia ha de comunicarse inmediatamente al Delegado de Protección de Datos.

FASE 2: REGISTRO DEL INCIDENTE

El incidente será registrado e irá documentándose el proceso con toda la información que se vaya recopilando. La información relativa a las decisiones tomadas sobre la notificación a la Autoridad de Control competente y la comunicación a los afectados (incluida una copia de la comunicación de realizarse) debe recogerse también en este registro de forma detallada.

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

Frente a los incidentes de seguridad, principalmente, los que afectan a los sistemas de información automatizados (informáticos o electrónicos) se precisará la intervención inmediata del Departamento de Protección de Datos y Seguridad de la Información, sin perjuicio de emprender directamente algunas medidas más inmediatas, todo ello a los efectos de llevar a cabo las siguientes actuaciones:

- **Contención:** 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.

- **Recuperación:** 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.

"EL DELEGADO DE PROTECCIÓN DE DATOS TOMARÁ LA DECISIÓN SOBRE LA PROCEDENCIA O NO DE COMUNICACIÓN A LA AGENCIA ESPAÑOLA DE PROPIEDAD DE DATOS. EL DPD TAMBIÉN VALORARÁ SI PROCEDE COMUNICAR SOBRE LA BRECHA A LOS INTERESADOS AFECTADOS."

FASE 4: VALORACIÓN DE LOS INCIDENTES Y BRECHAS DE SEGURIDAD

La valoración del incidente la realiza el Delegado de Protección de Datos atendiendo a la tipología de brecha de seguridad y una serie de criterios adicionales:

- Naturaleza, sensibilidad y categorías de los datos personales afectados.
- Datos legibles/ilegibles.
- Volumen de datos personales.
- Facilidad de identificación de individuos.
- Severidad de las consecuencias para los individuos (si la probabilidad de su materialización es baja, media o alta).
- Características especiales de los individuos.
- Número de individuos afectados.
- Características de la Diputación como responsable.
- El perfil de los usuarios afectados.
- El número y tipología de los sistemas afectados.
- El impacto.
- Los requerimientos legales y regulatorios.

A la vista de los anteriores, el Delegado de Protección de Datos tomará la decisión sobre la procedencia o no de comunicación a la Agencia Española de Propiedad de Datos. En su caso, la comunicación inicial, con todos los datos, se realizará en el plazo legal o contractual, así como será completada finalmente con información posterior en el plazo de 30 días.

En todo caso, el DPD también valorará si procede comunicar sobre la brecha a los interesados afectados.

FASE 6: SEGUIMIENTO

Mientras no se tenga constancia fehaciente que la violación de datos ha sido completamente resuelta y que el riesgo para los afectados no ha sido eliminado o reducido a niveles de riesgo residual aceptable, el asunto de la brecha permanecerá abierto, incluyendo porque podrán recibirse requerimientos, órdenes o comunicaciones por parte de la AEPD.

FASE 7: LECCIONES APRENDIDAS

Esta fase tiene por objetivo solventar posibles deficiencias en la gestión de incidentes o incorporar mejoras que permitan una mejor respuesta en las siguientes ejecuciones. Por ejemplo, depurar errores o actualizar información que se haya evidenciado obsoleta, revisar la eficacia del proceso de gestión y detectar nuevos mecanismos de control que puedan ser necesarios o mejorar los ya existentes.

MATERIAL COMPLEMENTARIO

- "Directrices sobre la notificación de las violaciones de la seguridad de los datos personales de acuerdo con el Reglamento 2016/679" (Grupo de Trabajo del Artículo 29). Consulta este enlace.
- "Guidelines 01/2021 on Examples regarding Data Breach Notification" (Comité Europeo de Protección de Datos). Consulta este enlace.
- "Brechas de seguridad: el correo electrónico y las plataformas de productividad online" (AEPD). Consulta este enlace.
- "Brechas de seguridad: El Top 5 de las medidas técnicas que debes tener en cuenta" (AEPD). Consulta este enlace.
- "Brechas de seguridad: comunicación a los interesados" (AEPD). Consulta este enlace.
- "Brechas de seguridad: protégete ante la pérdida o robo de un dispositivo portátil" (AEPD). Consulta este enlace.
- "Comunica-Brecha RGPD" (AEPD). Consulta en este enlace.

NOTICIAS

- **La Agencia Española de Protección de Datos (AEPD) publica una actualización de su *Guía para la notificación de brechas de datos personales*.**
  El documento que tiene como objetivo guiar a los responsables de los tratamientos de datos personales en su obligación de notificarlas a las autoridades de protección de datos y comunicárselo a las personas cuyos datos se hayan visto afectados.
  Esta guía actualiza la versión publicada en 2018, cuando comenzó a aplicarse el Reglamento General de Protección de Datos (RGPD), e incluye la experiencia recogida en este tiempo, tanto a nivel nacional como en relación con los criterios establecidos por el Comité Europeo de Protección de Datos.
  Consulta la guía en este enlace**.**

- **Una brecha de seguridad en el sistema de certificados COVID de Madrid llegaría a dejar al descubierto numerosas personas vacunadas.**
  Los datos personales de miles de madrileños, entre ellos los del Rey Felipe VI, el presidente del Gobierno, Pedro Sánchez, así como los de otros cargos públicos y personalidades habrían quedado al descubierto este miércoles durante varias horas a causa de una brecha de seguridad en los servidores de la Consejería de Sanidad de la Comunidad de Madrid. La Consejería ha reconocido la existencia de la brecha, pero niega que "cualquier ciudadano" pudiera acceder a la información. Sin embargo, fuentes de la noticia indican que "con una brecha de seguridad de este tipo, cualquiera persona con conocimientos de informática puede acceder a los datos personales del sistema". Consulta la noticia en este enlace.