La Rioja | Educación y Empleo
larioja.org

PROTOCOLO PARA LA GESTIÓN DE INCIDENTES DE SEGURIDAD Y NOTIFICACION DE BRECHAS DE DATOS PERSONALES

DELEGADA DE PROTECCION DE DATOS

Consejería de Educación y Empleo

PROTOCOLO PARA LA GESTIÓN DE INCIDENTES DE SEGURIDAD Y NOTIFICACION DE BRECHAS DE DATOS PERSONALES

1.- INTRODUCCIÓN

El Reglamento (UE) 2016/679, 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 (RGPD) establece en su **artículo 33** la obligación de notificar las brechas de los datos personales que puedan suponer un riesgo para los derechos y libertades de las personas físicas a la Autoridad de Control competente (en nuestro caso, Agencia Española de Protección de Datos (AEPD). Además, en su punto 5 establece la **obligación del responsable de tratamiento de documentar cualquier brecha**, incluidos los hechos relacionados con la misma, sus efectos y las medidas correctivas adoptadas.

Así mismo, en el **artículo 34 del RGPD** se establece la obligación del responsable de **comunicar las brechas de datos personales a los afectados**, personas físicas, cuando sea probable que entrañe un alto riesgo para sus derechos y libertades.

Estos preceptos exponen la necesidad de que las organizaciones integren dentro de sus políticas de información 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.

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.

El responsable de tratamiento está obligado a actuar a partir de cualquier alerta inicial de un incidente sobre los datos de carácter personal, independientemente de si los tratamientos se realizan de forma automatizada como si se realizan de forma manual, o si los incidentes son accidentales, tanto humanos como asociados a eventos naturales, o se han producido de forma intencionada.

Por otro lado, el artículo **33 del Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad** establece que las entidades del sector público notificarán al Centro Criptológico Nacional aquellos incidentes que tengan un impacto significativo en la seguridad de la información manejada y de los servicios prestados en relación con la categorización de sistemas recogidos en el Anexo I de este Real Decreto.

Así mismo, el artículo 25 del mismo texto normativo, referido a los Incidentes de seguridad, determina la exigencia de establecer un procedimiento de gestión de incidentes de seguridad de conformidad con lo dispuesto en el artículo 33 y de la Instrucción Técnica de Seguridad. Estos procedimientos cubrirán los mecanismos de detección, los criterios de clasificación, los procedimientos de análisis y resolución, así como los cauces de comunicación a las partes interesadas y el registro de las actuaciones. Este registro se empleará para la mejora continua de la seguridad del sistema.

Atendiendo a lo anterior, es precisa la existencia de un proceso de gestión de incidentes de seguridad, en el que, siguiendo las orientaciones de la AEPD, se incluyan los procesos para el cumplimiento de las obligaciones del RGPD cuando estos incidentes afecten a datos personales.

Este Protocolo pretende homogeneizar el proceso de gestión y de notificación de las brechas de datos de carácter personal y el de comunicación de violaciones de seguridad como apoyo para los responsables de tratamiento y responsables de la información y de los servicios.

El proceso marcará el itinerario de los pasos a seguir desde que surge la sospecha, las figuras implicadas, plazos y forma de notificación y, en su caso, de comunicación a las personas afectadas, documentación del proceso e inscripción en el registro de violaciones, en aras de una correcta y eficaz gestión.

2.- CONCEPTO DE INCIDENTE DE SEGURIDAD Y DE BRECHA DE DATOS PERSONALES

¿Qué es un incidente de seguridad de la información?

Se puede definir el **incidente de seguridad** como un suceso inesperado o no deseado con consecuencias en detrimento de la seguridad del sistema de información.

Sería, por tanto, un incidente de seguridad de la información un acceso, intento de acceso, uso, divulgación, modificación o destrucción no autorizada de información; un impedimento en la operación normal de las redes, sistemas o recursos informáticos; o una violación a una Política de Seguridad de la Información de la organización. En educación un incidente de seguridad

¿Qué es una brecha de datos personales?

El RGPD define, de un modo amplio, las ***"brechas de 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*".

No tendrán consideración de brecha de datos personales aquellos incidentes que no afecten a datos personales, es decir, a datos que no sean de personas físicas identificadas o identificables.

SI SUCEDE una brecha de seguridad: el responsable de tratamiento debe poner en marcha el plan de actuación, concretando tareas específicas que permitan resolver la brecha, minimizar sus consecuencias y evitar que vuelva a suceder en el futuro.
Además, cuando se sufre una brecha de seguridad se debe recabar una serie de información que será muy útil para decidir qué medidas tomar y qué acciones se emprenderán para cumplir los objetivos anteriores y para valorar la necesidad de notificar a la autoridad de control y afectados:

- Medio por el que se ha materializado la brecha, es decir, qué ha ocurrido: se ha perdido un dispositivo con datos personales, se ha producido un robo, se han publicado datos personales por error o se ha enviado a un destinatario equivocado, un ransomware ha cifrado un dispositivo, se ha producido una intrusión no autorizada en un sistema de información con datos personales, un empleado 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 registros afectados como en número de personas afectadas.
- Categorías de afectados: clientes, empleados, estudiantes, abonados, pacientes, etc. Es importante identificar si se trata de colectivos vulnerables.

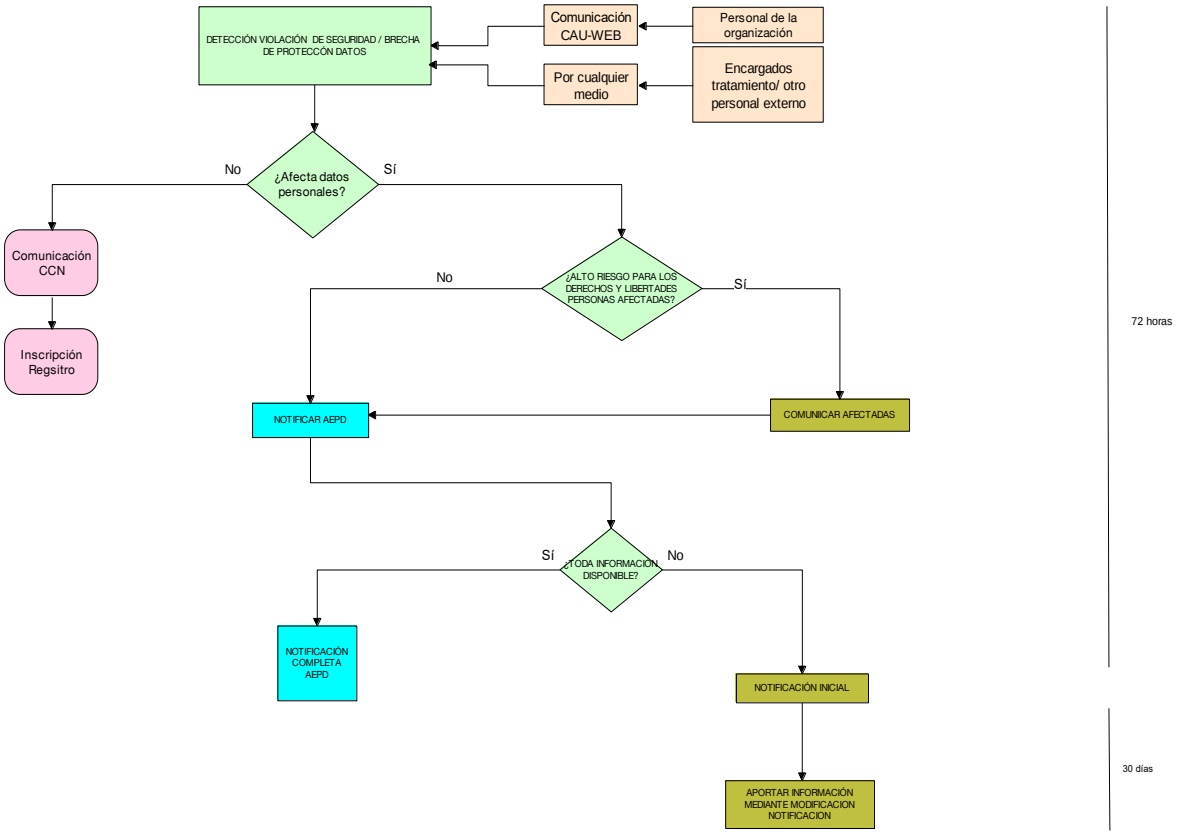
- Información temporal de la brecha: cuándo se inició, cuándo se ha detectado y cuándo se resolvió o resolverá la brecha de seguridad.

3.- FIGURAS IMPLICADAS

A continuación, se indican las principales funciones y responsabilidades que corresponden a los actores que intervienen en la gestión de un incidente o una brecha:

Figura	Funciones y responsabilidades
Responsable *de* tratamiento (RGPD) /Responsable de la información y Responsable del servicio (ENS) (Directores Generales, Secretarios Generales Técnicos y cargos asimilados en organismos públicos)	• Evaluación de las consecuencias para los derechos y libertades de las personas • Notificar la brecha de datos personales a la AEPD • Comunicar la brecha de datos personales a las personas afectadas
Encargado de tratamiento (RGPD) (Personas físicas o jurídicas que traten datos personales por cuenta del Responsable de Tratamiento)	• Informar al responsable de las brechas de datos personales que afecten a los tratamientos encargados • Ayudar al responsable en la gestión de la brecha de datos personales
Delegada de Protección de Datos **(de cada Consejería)**	• Informar y asesorar al responsable del tratamiento sobre sus obligaciones y responsabilidades con relación a las brechas de datos personales • Cooperar con la AEPD en las cuestiones relativas a la gestión de la brecha de datos personales • Actuar como punto de contacto con la AEPD, en particular, en el proceso de notificación de la brecha de datos personales
Responsable de seguridad	• Realizar el análisis preliminar de la incidencia, así como apertura, si se cree conveniente, de expediente con el CCN (Centro Criptológico Nacional). • Adoptar acciones inmediatas de contención •Documentar y registrar la incidencia

4.- PROCEDIMIENTO DE GESTION DE UNA BRECHA



A continuación, se describen los pasos a seguir en el supuesto en que se produzca una violación de seguridad:

1. Detección del incidente de seguridad

Cualquier persona de la organización que detecte cualquier anomalía que afecte o pueda afectar a la seguridad de los datos la comunicará de forma inmediata al máximo responsable de su unidad administrativa.

La anomalía puede ser detectada por la propia organización, por un encargado o por una persona ajena a la organización.

El responsable de la unidad realizará la notificación a través de la aplicación Cauweb (http://cauweb.larioja.org), describiendo la brecha con toda la información de la que se disponga, incluido la posible afectación a datos de carácter personal.

2. Análisis, clasificación, acciones inmediatas de contención y registro del incidente

Sin la menor dilación, el Responsable de Seguridad, junto con el Responsable de la Información/del Servicio, o persona en quien delegue:

- Clasificará la violación de seguridad de datos
- Realizará las acciones inmediatas de contención que resulten necesarias.
- Iniciará el proceso de registro y notificación del incidente de seguridad

En caso de que el incidente pueda afectar a datos de carácter personal, el Responsable de Seguridad de DGSD comunicará, **sin la menor dilación**, el resultado del análisis realizado respecto de la posible violación de seguridad de datos al Responsable de Tratamiento y al Delegado o Delegada de Protección de Datos (o a las personas en quiénes estos deleguen), para proceder a la constatación y calificación de la brecha a efectos de su notificación a la AEPD.

3. Incidentes y comunicación al CCN (Centro Criptológico Nacional)

El encargado de la notificación del incidente al Centro Criptológico Nacional será el Responsable de Seguridad de la Dirección General para la Sociedad Digital.

Se utilizará para ello la Guía CC-STIC 817 Esquema Nacional de seguridad- Gestión de Ciberincidentes.

https://www.boe.es/diario_boe/txt.php?id=BOE-A-2018-5370

https://www.ccn-cert.cni.es/series-ccn-stic/800-guia-esquema-nacional-de-seguridad/988-ccn-stic-817-gestion-de-ciberincidentes/file.html

4. Brecha de datos personales: Calificación de la violación y comunicación a la AEPD

El Responsable de tratamiento, asistido por el Responsable de Seguridad y la Delegada de Protección de datos, analizará la información con el fin de constatar:

- Si la violación afecta a datos de carácter personal. **Será esta constatación la que dé inicio al plazo para la notificación.**

- Si procede o no su notificación a la AEPD

- Si es precisa la comunicación a las personas afectadas

Determinación de la necesidad de notificación a la AEPD:

El parámetro determinante para notificar una brecha de datos personales a la AEPD es la **existencia de riesgo para los derechos y libertades** de las personas físicas afectadas.

No será necesario notificar las brechas en las que el responsable pueda garantizar que es improbable que exista un riesgo para los derechos y libertades de las personas físicas. La AEPD indica los siguientes factores para evaluar el riesgo de una brecha:

-Tipo de brecha de datos personales

-Naturaleza, carácter sensible y el volumen de datos personales

-Facilidad de identificación de las personas

-Gravedad de las consecuencias para los derechos y libertades de las personas

-Características particulares del responsable de tratamiento

-Número de personas afectadas

-Consideraciones generales

La AEPD facilita un recurso de utilidad para valorar la obligación de notificar sin dilación indebida a la AEPD una brecha de datos personales. Se trata de una ayuda a la toma de decisiones Asesora Brecha | AEPD, pero ésta última corresponde ineludiblemente al responsable del tratamiento.

Si se considera que ha de llevarse a cabo la notificación a la AEPD el Responsable de Tratamiento la notificará en un plazo no superior a 72 horas por medio de la siguiente dirección: Sede Electrónica - Agencia Española de Protección de Datos (sedeagpd.gob.es)

Dicho plazo se computa desde el momento en que el responsable de tratamiento tiene constancia de que el incidente ha afectado a datos personales, incluyendo las horas transcurridas durante fines de semana y días festivos. Si el plazo de 72 horas fuera rebasado, la notificación deberá ir acompañada de indicación de los motivos de la dilación.

El procedimiento que ofrece la AEPD permite realizar una notificación de forma gradual, de forma que si en las primeras 72 horas se dispone de toda la información se podrá realizar una única notificación completa; de no ser así se podrán llevar a cabo dos notificaciones, la "inicial" y la "completa" en un periodo máximo de 30 días entre las dos.

Se realizará una **notificación completa** de la incidencia cuando en el momento de la notificación se disponga de toda la información relevante para la gestión y resolución de la brecha de datos personales, incluida la comunicación de la brecha a los afectados.

Si no fuese posible facilitar toda la información necesaria esta se facilitará de manera gradual, a la mayor brevedad y sin dilación. En tal caso se realizará una **notificación de tipo "inicial",** antes de las 72 horas señaladas. Esta notificación se identifica como "**Inicial"** y tras su registro se informa por parte de la AEPD:

Esta notificación es INICIAL a los efectos de cumplimiento con el plazo de notificación establecido en el RGPD. En el plazo máximo de 30 días se notificará información adicional. En caso contrario, la autoridad de control considerará esta notificación como COMPLETA.

En este caso, la notificación se completará **antes del plazo máximo de 30 días** desde la notificación inicial. Se completará toda la información mediante una "modificación" de la notificación anterior, incluida la decisión tomada sobre la comunicación de la brecha de datos personales a los afectados, en caso de que no se haya hecho en la primera notificación.

El contenido de la notificación se puede consultar en el siguiente enlace formulario-brechas.pdf (aepd.es)

Se accede al formulario mediante certificado electrónico reconocido. La notificación debe realizarse por el Responsable de Tratamiento o persona en quien delegue. En caso de no realizarse directamente por

el Responsable de Tratamiento, deberá aportarse un documento acreditativo de la representación. Se adjunta como Anexo modelo de documento de representación.

Determinación de la necesidad de comunicación de la violación de seguridad de los datos a las personas interesadas

Cuando sea probable que la violación de la seguridad de los datos personales entrañe un alto riesgo para los derechos y libertades de las personas físicas, el Responsable de Tratamiento la comunicará al interesado, describiendo en lenguaje claro y sencillo:

- Naturaleza de la violación de la seguridad de los datos personales
- Datos de contacto del Delegado de Protección de Datos
- Posibles consecuencias de la violación de la seguridad de los datos personales.
- Resumen de las medidas adoptadas o propuestas para controlar los posibles daños
- Otras informaciones útiles a las personas afectadas para que puedan proteger sus datos o prevenir posibles daños.

El Responsable de Tratamiento lo comunicará a la persona afectada sin dilación indebida y preferentemente de forma directa al afectado, ya sea ya sea por teléfono, correo electrónico, SMS, a través de correo postal, o a través de cualquier otro medio que el responsable considere adecuado, y del que pueda dejar constancia.

Esta comunicación al interesado no será necesaria si se cumple alguna de las condiciones siguientes:

- La organización ha adoptado medidas de protección técnicas y organizativas apropiadas que hacen inteligibles los datos personales para cualquier persona que no esté autorizada a acceder a ellos (cifrado).
- Se han tomado medidas ulteriores que garanticen que ya no exista la probabilidad de que se concretice el alto riesgo para los derechos y libertades del interesado.
- Supone un esfuerzo desproporcionado, en cuyo caso, se optará en su lugar por una comunicación pública o una medida semejante por la que se informe de manera igualmente efectiva a los interesados. Se podrá realizar dicha comunicación a través de avisos públicos, sitio web, o comunicados de prensa. Estas técnicas podrían emplearse, también, cuando no sea posible contactar con las personas afectadas (por ejemplo, porque ha habido pérdida de datos e imposibilidad para recuperarlos, o se desconocen los datos de contacto, o estos no están actualizados) y esté debidamente justificado.

La AEPD ofrece la herramienta Comunica-Brecha RGPD COMUNICA BRECHA para ayudar a los responsables de tratamiento a la toma de decisiones en cuanto a la obligación de comunicar una a las personas afectadas, quienes en cualquier caso deberán documentarlas

Para más información se podrá consultar la Guía de notificación de brechas de datos personales de la AEPD, en la siguiente dirección:
https://www.aepd.es/es/documento/guia-brechas-seguridad.pdf

5. Infracciones asociadas al incumplimiento de la normativa relativa a la gestión de las brechas de datos personales.

La Ley orgánica 3/2018 establece en su artículo 70 los sujetos responsables que están sujetos al régimen sancionador establecido en el Reglamento (UE) 2016/679 y en la propia ley orgánica:

a) Los responsables de los tratamientos.
b) Los encargados de los tratamientos.
c) Los representantes de los responsables o encargados de los tratamientos no establecidos en el territorio de la Unión Europea.
d) Las entidades de certificación.
e) Las entidades acreditadas de supervisión de los códigos de conducta

El artículo 71 de la misma ley orgánica, establece que constituyen infracciones los actos y conductas a las que se refieren los apartados 4, 5 y 6 del artículo 83 del Reglamento (UE) 2016/679, así como las que resulten contrarias a dicha ley, que además establece distintos tipos de infracciones relacionadas con la incorrecta gestión de las brechas de datos personales:

Se consideran infracciones graves las siguientes:
• *El incumplimiento del deber del encargado del tratamiento de notificar al responsable del tratamiento las violaciones de seguridad de las que tuviera conocimiento*

• *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 Reglamento (UE) 2016/679*

• *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 Reglamento (UE) 2016/679 si el responsable del tratamiento hubiera sido requerido por la autoridad de protección de datos para llevar a cabo dicha notificación.*

Se consideran infracciones leves las siguientes:
• *La notificación incompleta, tardía 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 Reglamento (UE) 2016/679.*

• *El incumplimiento de la obligación de documentar cualquier violación de seguridad, exigida por el artículo 33.5 del Reglamento (UE) 2016/679.*

• *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 Reglamento (UE) 2016/679, salvo que resulte de aplicación lo previsto en el artículo 73 s) de esta ley orgánica.*