PROCEDIMIENTO DE VIOLACIONES DE SEGURIDAD DE LOS DATOS PERSONALES

CONTROL DE VERSIONES.

Versión	Fecha	Control
1	01/09/2025	Elaboración del Procedimiento

ÍNDICE

1. OBJETO

El presente documento constituye una normativa interna de obligado cumplimiento para todo el personal de la Entidad. El objeto de este documento es desarrollar el procedimiento establecido por parte de Grupo Cooperativo Solventia (en adelante, la Entidad), en relación con la gestión de incidentes de seguridad, que puedan afectar a la confidencialidad, integridad o disponibilidad de los datos de carácter personal, así como la notificación - en caso de concebirse como brecha o violación de seguridad - a la Autoridad de Control en protección de datos estatal (Agencia Española de Protección de Datos) o, en su caso, autonómica y la comunicación a las personas físicas afectadas.

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.

Las notificaciones de brechas de datos personales ante la Autoridad de Control son parte de la responsabilidad proactiva de la Entidad. La notificación de brechas realizada de acuerdo con el RGPD no implica necesariamente la imposición de una sanción. Al contrario, una notificación y comunicación en tiempo y forma, en el caso de que la Autoridad de Control inicie actuaciones previas de investigación, es una evidencia de la diligencia de la Entidad a la hora de ejecutar eficazmente la obligación de responsabilidad proactiva requerida por el RGPD. Sin embargo, el no cumplir con las obligaciones de notificación a la Autoridad y comunicación a los interesados sí está tipificado como infracción.

Específicamente en relación con las brechas de datos personales, el artículo 73 de la LOPDGDD establece como **infracciones *graves***, *entre otras:*

• *"f) La falta de adopción de aquellas medidas técnicas y organizativas que resulten apropiadas para garantizar un nivel de seguridad adecuado al riesgo del tratamiento, en los términos exigidos por el artículo 32.1 del Reglamento (UE) 2016/679."*

• *"g) El quebrantamiento, como consecuencia de la falta de la debida diligencia, de las medidas técnicas y organizativas que se hubiesen implantado conforme a lo exigido por el artículo 32.1 del Reglamento (UE) 2016/679."*

• *"q) El incumplimiento del deber del encargado del tratamiento de notificar al responsable del tratamiento las violaciones de seguridad de las que tuviera conocimiento."*

• *"r) 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."*

• *"s) 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"*

Por otra parte, el artículo 74 de la LOPDGDD establece ***como infracciones leves****:*

• *"m) 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."*

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

• "ñ) 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."

2. ALCANCE

Este procedimiento es de aplicación a todas las Entidades del Grupo Cooperativo Solventia, así como a sus filiales.

3. MARCO NORMATIVO, GUÍAS Y ACRÓNIMOS

Acrónimo	Concepto
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).
LOPD-GDD	Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y Garantía de los Derechos Digitales
AEPD	Guía de la Agencia Española de Protección de Datos para la gestión y notificación de brechas de seguridad.
TC	Tribunal Constitucional.
TS	Tribunal Supremo.
SAN	Sentencia de la Audiencia Nacional.

4. ROLES Y RESPONSABILIDADES

En el contexto del presente procedimiento, se definen las siguientes responsabilidades, sin perjuicio de los roles y responsabilidades establecidos en el documento correspondiente:

- **Responsable del tratamiento**: deberá aplicar las medidas técnicas y organizativas apropiadas a fin de garantizar y poder demostrar que el tratamiento es conforme al RGPD:
  - deberá implantar el proceso de gestión de brechas.
  - deberá garantizar que se notifica la brecha de datos personales a la autoridad competente sin dilación indebida, y también que se comunicará la brecha de datos personales a los afectados cuando sea necesario.
  - evaluar las consecuencias para los derechos y libertades de las personas.
  - deberá contar con el asesoramiento del Delegado de Protección de Datos (DPO) cuando haya sido designado, o, en su defecto, podrá contar con el asesoramiento de equipos internos o externos expertos en protección de datos, así como con expertos en materia de seguridad (Ej. CISO).
  - Puede delegar en el Encargado la gestión de la brecha de datos personales, tanto en lo relativo a la respuesta como a la notificación, documentándose dicha delegación de funciones. No obstante, debe asegurarse que se están tomando las acciones de respuesta, notificación y comunicación oportunas.

- **Encargado del 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.
  - 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 tenga asignadas por contrato.

- **Responsable de Riesgos Tecnológicos:** será el encargado de supervisar los incidentes relacionados con las TIC en materia de seguridad de los datos personales.

- **Responsable de Seguridad Informática junto a Unidad Tecnológica e Innovación[1]:** serán los encargados de la resolución efectiva de los incidentes que se produzcan y que estén relacionados con los sistemas automatizados de la Entidad.
  - Informar al DPO de los incidentes que puedan afectar a la seguridad de los datos de carácter personal.

- **Delegado de Protección de Datos**: Persona nombrada por la Entidad para supervisar y asesorar en materia de cumplimiento de la legislación en materia de protección de datos. Su rol dentro de este procedimiento debe ser:

  - el asesoramiento y apoyo a las tareas de valoración del incidente y las posibles consecuencias al afectado.
  - Actuar como portavoz único ante la Agencia Española de Protección de Datos y ser 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 realizado por la Entidad.
  - Asesorar sobre la evaluación del riesgo y las consecuencias que puede suponer para los derechos y libertades de las personas una brecha de datos personales.
  - Asesorar sobre la necesidad de notificar la brecha de datos personales a la Autoridad de Control y en su caso a los interesados afectados.
  - Supervisar las acciones de mejora para asegurar la eficacia de las medidas y la validez de las lecciones aprendidas.

- Los **empleados** tienen la responsabilidad de conocer y cumplir el presente procedimiento.

5. ¿QUÉ ES UNA BRECHA DE SEGURIDAD DE LOS DATOS PERSONALES?

El artículo 4.12 RGPD define, de un modo amplio, la "violación 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".

Por lo tanto, la violación de la seguridad de los datos personales puede producirse porque se ocasione:

- La destrucción. Que se produce cuando los datos ya no existen, o ya no existen en una forma que sea de utilidad para el Responsable del tratamiento.
- El daño. Cuando los datos personales han sido alterados, corrompidos o dejan de estar completos.
- La pérdida. Lo que significa que los datos pueden seguir existiendo, pero el Responsable del tratamiento ha perdido el control o el acceso a ellos, o ya no obran en su poder.
- El tratamiento no autorizado o ilícito. Lo que puede incluir la divulgación de datos personales a destinatarios que no estén autorizados a recibir los datos, o que cualquier otra forma de tratamiento que vulnere el RGPD.

[1] Aplica únicamente a Cajalmendralejo y su filial, Banco de Depósitos.

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 por un responsable o un encargado.
- Ocurran en tratamientos llevados a cabo por una persona física en el ámbito doméstico.

De este modo, tal y como manifiesta la AEPD en la Guía para la notificación de brechas de datos personales, "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 que la Entidad determine los parámetros a considerar para valorar cuándo el incidente se concibe como una brecha o violación de la seguridad de los datos de carácter personal.

6. FASES EN LA GESTIÓN Y NOTIFICACIÓN DE LAS BRECHAS DE SEGURIDAD

Tal como 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.

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, debe informar a la Entidad 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, éste deberá remitir al Responsable toda la información necesaria para que pueda cumplir con sus obligaciones en tiempo y forma.

Cuando la brecha de seguridad haya sido detectada por alguna de las Entidades que constituyen el Grupo Cooperativo Solventia o por alguna de sus filiales, deberán remitir de manera inmediata la información que dispusieran sobre el incidente de seguridad.

El incidente de seguridad deberá ser comunicado, inmediatamente, al Responsable de Seguridad Informática (inesr@cajalmendralejo.es), al DPO (dpo@cajalmendralejo.es) y al Responsable de Riesgos Tecnológicos (riesgostecnologicos@cajalmendralejo.es) por los canales habilitados.

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 realizada) debe recogerse también en este registro de forma detallada.

La información a registrar, mínimamente, será:

- Fecha y hora de la detección.
- Origen del incidente.
- Naturaleza del evento de seguridad de los datos personales.
- Descripción breve.
- Tipología del incidente.

- Categorización del incidente.

En la medida de lo posible, y aunque sea información imprecisa o sin verificar, deberá también solicitarse información relativa a poder evaluar la severidad del incidente. Por ese motivo, se recogerá además la siguiente información:

- Tipo y número aproximado por categoría de interesados afectados [menores, empleados, proveedores, etc.].
- Categorías y número aproximado de registros de datos personales afectados [DNI, nombre y apellidos, direcciones, credenciales, etc.].

Es necesario destacar que, es posible que durante el primer registro del incidente no se disponga de toda la información descrita, en cuyo caso deberá solicitarse más información y la investigación del incidente para poder cumplimentar, al menos, con información aproximada los campos requeridos.

Documentos relacionados:

- **Anexo I**: evaluación del incidente.
- **Anexo IV**: registro de incidentes.

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 de la Unidad Tecnológica e Innovación / Responsable de Seguridad Informática a los efectos de llevar a cabo las siguientes actuaciones:

Contención

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 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.

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. 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.

En las Entidades no cabeceras del Grupo las actuaciones de contención y recuperación de incidentes serán asumidas por el proveedor que cada Entidad tenga contratado para tales fines.

FASE 4: Valoración de los incidentes y brechas de seguridad

La valoración del incidente se realizará por parte del Responsable de Seguridad Informática y/o del DPO, junto con el Responsable de Riesgos Tecnológicos.

4.1. Tipología brecha de seguridad

Tal y como afirma la AEPD 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:	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.

La violación de seguridad de los datos personales podría producirse como consecuencia de una violación de las tres al mismo tiempo o de una combinación, de cualquier manera, de estas.

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.

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.
- 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.

- Por ejemplo, un tercero ha modificado en la base de datos de la Entidad la información relativa a los datos bancarios de los empleados que se utilizan para el pago de las nóminas. Cuando se producen brechas de datos personales de integridad la Entidad debe 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.

La AEPD establece la siguiente tabla en la que se indican las dimensiones de seguridad potencialmente afectadas en cada uno de los casos:

Suceso	Confidencialidad	Disponibilidad	Integridad
Revelación verbal no autorizada	X		
Documentación perdida, robada o depositada en localización insegura	X	X	
Correo postal perdido o abierto	X	X	
Eliminación incorrecta de datos personales en papel		X	
Datos personales enviados por error de forma electrónica o en papel	X		
Datos personales eliminados o destruidos		X	

Abuso de privilegios de acceso por parte de miembro (Ejemplo: empleado) para extraer, reenviar o copiar datos personales	X		
Datos personales residuales en dispositivos obsoletos	X		
Publicación no intencionada/autorizada	X		
Envío de correo electrónico a múltiples destinatarios sin copia oculta o en una lista de distribución visible	X		
Dispositivo perdido o robado	X	X	
Ciberincidente: Dispositivo ha sido cifrado/secuestrado de la información	X	X	
Ciberincidente: Suplantación de identidad (phishing)/compromiso de cuenta de usuario o administrador	X	X	X
Ciberincidente: Acceso no autorizado a datos personales en un sistema de información ya sea corporativo o de un servicio de internet	X	X	X
Incidencia técnica	X	X	X
Modificación no autorizada de datos			X
Datos personales mostrados al individuo incorrecto	X		

4.2. Criterios de valoración.

Inmediatamente después de tener conocimiento de una violación de seguridad, el Responsable del tratamiento debe evaluar el riesgo. Al evaluar el riesgo, debe tenerse en cuenta tanto la probabilidad como la gravedad del riesgo para los derechos y libertades de los interesados.

Para estimar, desde la perspectiva del afectado, qué riesgo supone para los derechos y libertades de las personas físicas, se establecerán criterios de valoración según los tipos de daños en las tres dimensiones de la seguridad. A continuación, se establecen los criterios de valoración del riesgo para los derechos y libertades:

Tipo de violación:

El tipo de violación que se haya producido puede afectar al nivel de riesgo que presente para las personas.

Un factor clave es el tipo y la sensibilidad de los datos personales que se hayan visto comprometidos a causa de la violación. Del mismo modo, una pequeña cantidad de datos personales muy sensibles puede tener un impacto elevado en una persona y una gran variedad de detalles puede revelar una mayor diversidad de información sobre esa persona.

Categorización del incidente:

- Crítico (afecta a datos valiosos, gran volumen y en poco tiempo).

- Muy Alto (Cuando dispone de capacidad para afectar a información valiosa, en cantidad apreciable).
- Alto (Cuando dispone de capacidad para afectar a información valiosa).
- Medio (Cuando dispone de capacidad para afectar a un volumen apreciable de información).
- Bajo (Escasa o nula capacidad para afectar a un volumen apreciable de información).

Naturaleza, sensibilidad y categorías de los datos personales afectados:

- Datos de escaso riesgo: datos de contacto, de educación, familiares, profesionales, biográficos
- Datos de comportamiento: localización, tráfico, hábitos y preferencias,
- Datos financieros: transacciones, posiciones, ingresos, cuentas, facturas,
- Datos sensibles: de salud, biométricos, datos relativos a la vida sexual, etc.

Categoría de interesados afectados: Su posición en la estructura organizativa de la Entidad y, en su consecuencia, sus privilegios de acceso a información sensible o confidencial.

- Clientes.
- Usuarios.
- Empleados.
- Proveedores.
- Potenciales clientes.
- Menores.
- Personas en riesgo de exclusión.
- Otros.

Datos legibles/ilegibles:
Los datos personales protegidos mediante un nivel adecuado de cifrado serán ininteligibles para personas no autorizadas que dispongan de la clave de descifrado. Datos protegidos mediante algún sistema de seudonimización (por ejemplo, cifrado o hash) también puede reducir la probabilidad de identificación de personas en caso de violación

Volumen de datos personales:
Expresados en cantidad (registros, ficheros, documentos) y/o en periodos de tiempo (una semana, un año, etc.)

Facilidad de identificación de individuos:
La facilidad con la que se puede deducir la identidad de los individuos a partir de los datos involucrados en la brecha.

Características especiales de los individuos:
Si afectan a individuos con características especiales o con necesidades especiales.

Número de individuos afectados:
Se refiere al número de personas físicas cuyos derechos o libertades podrían verse dañados como consecuencia de una brecha de datos personales. Dentro de una escala determinada, por ejemplo, más de 100 individuos.

Características especiales del responsable del tratamiento (de la entidad en sí):
En base a la actividad de la entidad.

El número y tipología de los sistemas afectados:
Se tendrá en cuenta el número de sistemas afectados, así como del tipo de sistemas.

El impacto:
El impacto que la brecha puede tener en la Entidad, desde los puntos de vista de la protección de la información, la prestación de los Servicios, la conformidad legal y/o la imagen pública. Va a estar relacionado con la categoría o criticidad de los servicios y personas afectados. En este aspecto diferenciamos entre los siguientes impactos:

- Bajo (perjuicio limitado)
- Medio (perjuicio grave)
- Alto (perjuicio muy grave)

Los requerimientos legales y regulatorios:
Notificación de la brecha a la autoridad de control y cualquier otra obligación de notificación, comunicación a Fuerzas y Cuerpos de Seguridad del Estado en caso de delito.

Severidad de las consecuencias para los individuos:

- De conformidad con la Guía de la AEPD, para determinar el nivel de severidad debe tenerse en cuenta el daño que se puede producir al materializarse las consecuencias identificadas, considerando los siguientes niveles:

Nivel de severidad	Consecuencias para los interesados
Baja	Las personas no se verán afectadas o pueden encontrar algunos inconvenientes muy limitados y reversibles que superarán sin ningún problema (tiempo de reingreso de información, molestias, irritaciones, etc.)
Media	Las personas pueden encontrar inconvenientes importantes, produciendo un daño limitado, que podrán superar a pesar de algunas dificultades (costos adicionales, denegación de acceso a servicios comerciales, miedo, falta de comprensión, estrés, dolencias físicas menores, etc.)
Alta	Las personas pueden enfrentar consecuencias significativas, que deberían poder superar, aunque con serias dificultades (malversación de fondos, listas negras de los bancos, daños a la propiedad, pérdida de empleo, citación judicial, empeoramiento de la salud, etc.). En general cuando las consecuencias afectan a derechos fundamentales, pero pueden revertirse
Muy Alta	Las personas pueden enfrentar consecuencias muy significativas, o incluso irreversibles, que no pueden superar (exclusión o marginación social, dificultades financieras tales como deudas considerables o incapacidad para trabajar, dolencias psicológicas o físicas a largo plazo, muerte, etc.). Daña derechos fundamentales y libertades públicas de forma irreversible

La AEPD indica que, en caso de no haberse materializado el daño, se deberá estimar esta probabilidad, es decir, la posibilidad de que las consecuencias se materialicen con un nivel de severidad alto o muy alto. Para determinarlo, se deberá tener en cuenta las medidas técnicas y organizativas aplicadas antes de que se produjera la brecha y las acciones tomadas a posteriori.

Será “improbable” cuando el responsable pueda garantizar que no puede materializarse el daño; y graduar en baja, alta y muy alta cuando exista cierta probabilidad de materialización del daño.

Cuando la severidad para las personas afectadas por la brecha de datos personales sea alta o muy alta, el responsable de tratamiento deberá comunicar la brecha de datos personales a los afectados, excepto si puede garantizar que no existe probabilidad de que se materialice el daño. Además, en situaciones de severidad media o daño limitado, cuando la probabilidad de que dicho daño se materialice sea alta o muy alta, también se deberá comunicar a los afectados.

Según la evaluación de riesgos realizada sobre la violación de la seguridad de los datos y, atendiendo a los criterios establecidos respecto a quién notificar, se establecen las pautas para la notificación a cada una de las partes interesadas con las que comunicarse.

La AEPD dispone de una herramienta Comunica-Brecha-RGPD y Asesora-Brecha RGPD para la toma de decisiones en cuanto a la obligación de comunicar una brecha de datos personales a los afectados y a las autoridades de control, respectivamente.

- **COMUNICA-BRECHA-RGPD:** Es un recurso de utilidad para que el Responsable del tratamiento de datos personales, pueda valorar la obligación de informar a las personas físicas afectadas por una brecha de seguridad de los datos personales, tal y como establece el artículo 34 del Reglamento General de Protección de Datos.

  Esta herramienta se basa en un breve formulario en el que se recaban detalles que permiten aplicar unos criterios básicos que pueden ser indicativos del riesgo asociado a una brecha de datos personales, en función de la información que ha sido facilitada, ofrece como respuesta tres posibles escenarios:

  - Que se debe notificar la brecha de datos personales a los afectados al apreciarse un riesgo alto,
  - Que no es necesario dicha comunicación,
  - O que no se puede determinar el nivel de riesgo.

  Se trata de una herramienta sencilla y gratuita. Una vez finalizada su ejecución, los datos aportados durante el desarrollo de la misma se eliminan, por lo que la Agencia Española de Protección de Datos en ningún caso puede conocer la información que haya sido aportada.

  Comunica-Brecha RGPD es una ayuda a la toma de decisiones, pero esta última corresponde ineludiblemente al responsable de tratamiento y en ningún caso su utilización representa el pronunciamiento de esta Agencia sobre la aplicación del art. 34 del RGPD para una brecha de seguridad concreta. La herramienta se encuentra disponible en el siguiente enlace: http://comunica.aepd.es/

- **ASESORA BRECHA:** Es un recurso de utilidad para que el Responsable del tratamiento de datos personales, pueda valorar la obligación de notificar sin dilación indebida a la Agencia Española de Protección de Datos una brecha de datos personales, tal y como establece el artículo 33 del Reglamento General de Protección de Datos.

  Esta herramienta asesora sobre quién tiene que notificar, qué situaciones corresponden con una brecha de datos personales y cuáles no, cuál es el organismo competente y si la brecha de datos personales debe ser notificada o no en función del riesgo.

  La mera obtención de los documentos que proporcionan las herramientas de la AEPD no supone, en ningún caso, el cumplimiento automático de las obligaciones que el RGPD y la LOPDGDD establecen para los responsables y encargados de los tratamientos de datos personales, en particular lo referido al principio de responsabilidad proactiva que el RGPD desarrolla. en su Capítulo IV. Se trata de documentos iniciales de ayuda orientados a facilitar la comprensión de dichas obligaciones y abordarlas, inicialmente, de forma adecuada.

  Sobre la base de los documentos obtenidos los responsables y encargados de los tratamientos de datos personales deberán llevar a cabo cuantas adaptaciones fueran necesarias de forma particularizada para cada tratamiento de datos personales; teniendo en cuenta los riesgos que para los derechos y libertades de las personas físicas pudieran derivar de dichos tratamientos en función de su naturaleza, su alcance, su contexto y sus finalidades (Considerando 76 y Artículo 35.1 del RGPD).

  Se trata de una herramienta sencilla y gratuita. Una vez finalizada su ejecución, los datos aportados durante el desarrollo de la misma se eliminan, por lo que la Agencia Española de Protección de Datos en ningún caso puede conocer la información que haya sido aportada.

  Asesora Brecha es una ayuda a la toma de decisiones, pero esta última corresponde ineludiblemente a la persona responsable de tratamiento y en ningún caso su utilización representa el pronunciamiento de esta Agencia sobre la aplicación del art. 33 del RGPD para una brecha de seguridad concreta.

La herramienta se encuentra disponible en el siguiente enlace: https://asesora.aepd.es/

4.3. Ejemplos prácticos para saber si notificar o no a la AEPD.

A continuación, se indican algunos ejemplos orientativos sobre la notificación de la violación de seguridad. No se trata de una lista exhaustiva, sino que algunos tendrán que notificarse a la AEPD y otros no, según la valoración del incidente.

A) Brecha de confidencialidad.

Tipo de violación	Escenario de riesgo	Consecuencias posibles para el interesado	Tipo de notificación requerida
Violación de la confidencialidad	La información filtrada o extraviada se encuentra cifrada o almacenada en formato ininteligible y, por tanto, no podrá ser procesable o utilizada para ninguna finalidad. El dispositivo extraviado es gestionable de forma remota y puede ser borrado. Sería reevaluado como evento o incidencia de privacidad.	No se generan daños al interesado al no poderse tratar los datos afectados.	• No se requiere notificación a la AEPD. • No se requiere notificación al interesado o interesados.
	La información filtrada o extraviada no se encuentra protegida y podrá ser tratable.	Daño reputacional que afecte a su honor o intimidad. (P.e. información relacionada con el ámbito familiar, la personalidad, aficiones, etc. que pueda afectar negativamente al afectado en el entorno familiar, social o laboral) (Alto riesgo)	• Se requiere notificación a la AEPD. • Se requiere notificación al interesado o interesados.
		Daños que impactan en la solvencia patrimonial del afectado. (P.e. información que permita la suplantación de identidad y la contratación o compra de productos en nombre del afectado o bien la sustracción de dinero, bienes o inmuebles). (Alto riesgo)	• Se requiere notificación a la AEPD. • Se requiere notificación al interesado o interesados.
		El afectado debe asumir consecuencias judiciales (P.e. información relativa	• Se requiere notificación a la AEPD.

Tipo de violación	Escenario de riesgo	Consecuencias posibles para el interesado	Tipo de notificación requerida
		a la investigación de posibles infracciones o estado de situación de la gestión del patrimonio) (Alto riesgo)	• Se requiere notificación al interesado o interesados.
		Daño a su estado de salud. (P.e. información relativa a su estado de salud o cualquier otra circunstancia personal que pueda afectar al interesado y causarle consecuencias negativas de carácter físico o psicológico como consecuencia de su revelación (Depresión, ansiedad, estrés, etc.) (Alto riesgo)	• Se requiere notificación a la AEPD. • Se requiere notificación al interesado o interesados.

B) Brecha de integridad.

Tipo de violación	Escenario de riesgo	Consecuencias posibles para el interesado	Tipo de notificación requerida
Violación de la integridad:	La información alterada o modificada dispone de copia de seguridad y se ha garantizado su restauración. Sería reevaluado como evento o incidencia de privacidad.	No se generan daños al interesado al no verse dañados los datos afectados tras aplicar las medidas de contención y recuperación.	• No se requiere notificación a la AEPD. • No se requiere notificación al interesado o interesados.
	La información alterada o modificada no dispone de copia de seguridad, pero se puede reconstruir si vuelve a ser procesada. Sería reevaluado como evento o incidencia de privacidad.	No se generan daños de integridad al interesado al poder volver al estado anterior al incidente. Debe valorarse si se producen daños en disponibilidad por el tiempo en el que los datos no están accesibles.	• No se requiere notificación a la AEPD por daños en integridad. Deberá evaluarse por daños en disponibilidad. • No se requiere notificación al interesado o interesados.
	La información alterada o modificada no dispone de copia o ha sido procesada de forma incorrecta alterando el resultado de los tratamientos	Daño reputacional que afecte a su honor o intimidad. (Alto riesgo)	• Se requiere notificación a la AEPD. • Se requiere notificación al interesado o interesados.

Tipo de violación	Escenario de riesgo	Consecuencias posibles para el interesado	Tipo de notificación requerida
	realizados sobre el interesado.	Daños que impactan en la solvencia patrimonial del afectado. (Alto riesgo)	• Se requiere notificación a la AEPD. • Se requiere notificación al interesado o interesados.
		El afectado debe asumir consecuencias judiciales (Sanciones, indemnizaciones, embargos, etc). (Alto riesgo)	• Se requiere notificación a la AEPD. • Se requiere notificación al interesado o interesados.
		Daño a su estado de salud. (Alto riesgo)	• Se requiere notificación a la AEPD. • Se requiere notificación al interesado o interesados.

C) Brecha de disponibilidad.

Tipo de violación	Escenario de riesgo	Consecuencias posibles para el interesado.	Tipo de notificación requerida.
Violación de la disponibilidad	La información no accesible dispone de copia de seguridad y existen planes de contingencia para la vuelta a la normalidad. La duración de la indisponibilidad no afecta a los tratamientos. Sería reevaluado como evento o incidencia de privacidad.	No se generan daños al interesado al no poderse tratar los datos afectados durante el tiempo que dura la indisponibilidad de los datos o los sistemas donde estos se procesan.	• No se requiere notificación a la AEPD. • No se requiere notificación al interesado o interesados.
	La información filtrada o extraviada no es recuperable o su restauración supone un tiempo de indisponibilidad que afecta seriamente al tratamiento necesario.	Daño reputacional que afecte a su honor o intimidad. (Alto riesgo)	• Se requiere notificación a la AEPD. • Se requiere notificación al interesado o interesados.
		Daños que impactan en la solvencia patrimonial del afectado. (Alto riesgo)	• Se requiere notificación a la AEPD.

Tipo de violación	Escenario de riesgo	Consecuencias posibles para el interesado.	Tipo de notificación requerida.
			• Se requiere notificación al interesado o interesados.
		El afectado debe asumir consecuencias judiciales (Sanciones, indemnizaciones, etc).	• Se requiere notificación a la AEPD. • Se requiere notificación al interesado o interesados.
		Daño a su estado de salud. (Alto riesgo)	• Se requiere notificación a la AEPD. • Se requiere notificación al interesado o interesados.

FASE 5: Notificación a las autoridades, interesados y otras partes interesadas

5.1. Notificación a la AEPD.

Cualquier entrada categorizada como "Violación de Seguridad de Datos Personales" será notificada a la Agencia Española de Protección de Datos (AEPD) por quien actúe en nombre y representación del Responsable del Tratamiento, sin perjuicio de que el Delegado de Protección de Datos (DPO) de la Entidad actúe como interlocutor con la Autoridad de Control en los supuestos que sea necesario.

No es obligatorio notificar todas las brechas de datos personales cuando conforme al principio de responsabilidad proactiva, el Responsable pueda garantizar que es improbable que la brecha de datos personales entrañe un riesgo para los derechos y libertades de las personas físicas.

La notificación se realizará sin dilación indebida y a más tardar dentro de las 72 horas después de que se haya tenido constancia de ella y una vez se ha valorado la obligación de tenerla que hacer por los riesgos que supone.

La AEPD indica que *"El plazo de 72 horas empieza a calcularse desde el instante en que el responsable de tratamiento tenga constancia de que el incidente de seguridad ha afectado a datos personales, incluyendo las horas trascurridas durante fines de semana y días festivos".*

Corresponde al Encargado de tratamiento notificar al Responsable de tratamiento sin dilación indebida de las brechas de datos personales de las que tenga constancia.

Además, el Encargado únicamente podría notificar en nombre del Responsable si así lo tiene establecido en contrato o vínculo legal de similar índole. En todo caso, el Responsable debe ser previamente informado sobre la ocurrencia de la brecha de datos personales y datos relevantes tal y como establece el artículo 33.2 del RGPD. En su caso, el Encargado debe realizar una notificación de brecha de datos personales por cada Responsable afectado, únicamente cuando hayan afectado por igual a los derechos y libertades de los interesados de diferentes Responsables, podrá realizar una única notificación relacionando a todos los Responsables cuyos tratamientos se han visto afectados.

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 decisión sobre la comunicación de la brecha a los afectados, se realizará una notificación de tipo "completa", dado que no está previsto que el Responsable de tratamiento tenga que aportar información adicional. Alternativamente, cuando en el momento de la notificación no fuese posible cumplir con la obligación de facilitar toda la información necesaria, el RGPD prevé que la información se facilitará de manera gradual, a la mayor brevedad y sin dilación indebida.

De forma general la Agencia Española de Protección de Datos prevé la posibilidad de realizar una notificación de tipo "inicial", antes de las 72 horas señaladas, rellenando el formulario con la información preliminar que se disponga, o en su caso las estimaciones preliminares sobre la brecha de datos personales.

Antes del plazo máximo de 30 días desde la notificación inicial, el Responsable de tratamiento deberá completar 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. Todos los plazos indicados en días deben entenderse como días hábiles.

En la notificación se deberá incluir, al menos, la siguiente información:

- Describir la naturaleza de la violación de la seguridad de los datos personales, inclusive, cuando sea posible, las categorías y el número aproximado de interesados afectados, y las categorías y el número aproximado de registros de datos personales afectados;
- Comunicar el nombre y los datos de contacto del delegado de protección de datos o de otro punto de contacto en el que pueda obtenerse más información;
- Describir las posibles consecuencias de la violación de la seguridad de los datos personales;
- Describir las medidas adoptadas o propuestas por el responsable del tratamiento para poner remedio a la violación de la seguridad de los datos personales, incluyendo, si procede, las medidas adoptadas para mitigar los posibles efectos negativos.
- Informará sobre la intención o no de notificar a los afectados. Este punto permitirá a la AEPD valorar si concurre alguna circunstancia que exime de la notificación al afectado o si, por el contrario, se corre un alto riesgo y debe notificarse al afectado.

La notificación se realizará de forma electrónica a través del apartado "Notificación de brechas de datos personales" que la AEPD tiene disponible en su página web:

https://sedeagpd.gob.es/sede-electronica-web/vistas/formBrechaSeguridad/procedimientoBrechaSeguridad.jsf

Se realiza la notificación mediante el formulario de notificación de brechas de datos personales de la sede electrónica de la AEPD utilizando el certificado electrónico del representante del Responsable de tratamiento, sin que sea necesario adjuntar documentación acreditativa de dicha circunstancia.

En el ANEXO II se adjunta el enlace del formulario de la AEPD para la comunicación de brechas de seguridad.

De forma general no es necesario adjuntar ningún tipo de documentación adicional a la notificación de brecha de datos personales. Si la AEPD considera que el Responsable del tratamiento debe aportar documentación adicional para esclarecer los hechos, ésta le será requerida con posterioridad.

A modo de contingencia, en caso de no estar disponible el servicio electrónico de la AEPD, se indican los números de teléfono de contacto de la AEPD, así como su ubicación física con los que poder contactar con la AEPD para poder contactar con la agencia y acordar el canal alternativo por el que realizar la notificación.

- Telf. +34 900 293 183
- Calle Jorge Juan, 6, 28001 Madrid

5.2. Notificación a los afectados

El artículo 34 del RGPD establece que cuando sea probable que la brecha de datos personales entrañe un alto riesgo para los derechos y libertades de las personas físicas, el Responsable de tratamiento deberá comunicar la brecha a los afectados sin dilación indebida.

La comunicación se realizará por el Departamento de Organización.

No será necesaria la notificación al afectado cuando:

- "el responsable del tratamiento ha adoptado medidas de protección técnicas y organizativas apropiadas y estas medidas se han aplicado a los datos personales afectados por la violación de la seguridad de los datos personales, en particular aquellas que hagan ininteligibles los datos personales para cualquier persona que no esté autorizada a acceder a ellos, como el cifrado" [art 34.3.a) RGPD].
- "el responsable del tratamiento ha 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 [art 34.3.b) RGPD]. Ejemplo, en casos de suplantación de identidad cuando se pueda garantizar el proceso de renovación de credenciales y fuerce a los interesados afectados a establecer una nueva contraseña. La AEPD cita como ejemplos la identificación y puesta en marcha inmediatamente de medidas como la revocación, cancelación o bloqueo de credenciales de acceso o certificados digitales comprometidos, o mediante el restablecimiento de los servicios y copias de seguridad de los datos de forma que no puedan comprometerse otros datos personales.
- "suponga un esfuerzo desproporcionado. En este 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" [art 34.3.c) RGPD]. El DPO deberá valorar si la notificación supone un esfuerzo desproporcionado y, por tanto, se empleará una comunicación pública o una medida semejante por la que se informe de manera igualmente efectiva a los interesados. En este caso, se deberá coordinar el medio de comunicación a utilizar y el contenido del mensaje con el Comité de Crisis de Riesgo Tecnológico.

La AEPD indica diversos factores a tener en consideración para decidir si se ha de realizar la comunicación a las personas afectadas:

- Cuáles son las obligaciones legales y contractuales.
- Qué riesgos comporta para los derechos y libertades de las personas la pérdida de confidencialidad, integridad o disponibilidad de sus datos personales, de los servicios asociados a dichos datos personales, así como del compromiso de la identidad o identificación de los interesados. En particular, los perjuicios a sus derechos fundamentales, los daños físicos, daños reputacionales, fraudes, etc.
- Hasta qué punto los daños producidos serán irreversibles, se puede evitar o mitigar los daños inmediatos y los posibles perjuicios posteriores.

En caso de decidir realizar la comunicación a los afectados, esta se realizará sin dilación indebida, una vez se haya notificado la violación a la AEPD.

La AEPD indica que "*Cualquier dilación en la comunicación a los afectados le resta efectividad, por lo que una comunicación a destiempo puede llegar a tener el mismo efecto que una comunicación no realizada. Por tanto, todo retraso en la comunicación inmediata a los interesados cuando esta sea necesaria ha de justificarse".*

En todo caso, si la comunicación se produce como consecuencia de una orden emitida por la AEPD, deberá materializarse la comunicación a los afectados sin dilación indebida y comunicar la confirmación de haber ejecutado la orden dentro del plazo de 30 días, salvo que se indique un plazo diferente en la orden.

No obstante, la AEPD indica que, si después del análisis correspondiente se concluye que es necesario comunicar a los interesados, pero se prevé que la comunicación a los interesados puede comprometer el resultado de una investigación en curso, la comunicación podría posponerse siempre bajo la supervisión de la Autoridad de Control.

La comunicación de una brecha de datos personales a las personas afectadas conforme al artículo 34 RGPD corresponde al Responsable del tratamiento. El Responsable puede en virtud de contrato o vinculo legal encargar a un tercero, que actuará como Encargado de tratamiento, para que realice la comunicación.

El Encargado de tratamiento que sea objeto de la brecha de datos personales únicamente puede efectuar la comunicación a los afectados si así lo tiene establecido en contrato o vinculo legal con el Responsable del tratamiento. Siendo el Responsable en todo caso informado previamente sobre la ocurrencia de la brecha y sobre todos los detalles, conforme al artículo 33.2 del RGPD.

La comunicación a los afectados describirá, en un lenguaje claro y sencillo, la naturaleza de la violación de seguridad y contendrá, al menos, la siguiente información, de conformidad con el artículo 33.3 letras b), c) y d) del RGPD:

- Nombre y los datos de contacto del delegado de protección de datos o de otro punto de contacto en el que pueda obtenerse más información
- Describir las posibles consecuencias de la violación de la seguridad de los datos personales.
- Describir las medidas adoptadas o propuestas por el responsable del tratamiento para poner remedio a la violación de la seguridad de los datos personales, incluyendo, si procede, las medidas adoptadas para mitigar los posibles efectos negativos.

Preferentemente, la comunicación deberá realizarse de forma directa al afectado, ya sea por teléfono, e-mail, sms, correo postal o cualquier otro medio dirigido al afectado que el Responsable considere adecuado. Cuando suponga un esfuerzo desproporcionado en relación a los riesgos para los derechos y libertades que están sufriendo los interesados, se puede realizar una comunicación indirecta a través de avisos públicos, por ejemplo en página web o bien cuando no fuera posible contactar con la persona afectada y estuviese debidamente justificado.

Téngase en cuenta, según señala la AEPD, que "*Una comunicación incompleta (sin el contenido mínimo), de difícil acceso o realizada a las personas incorrectas no es efectiva, por lo que una comunicación en estas condiciones podría llegar a considerarse una comunicación no realizada".*

Se adjunta un ejemplo en el ANEXO III.

5.3. Notificación a los empleados u otras partes interesadas

Cualquier incidente que suponga una violación o brecha de seguridad catalogada como "Crítica" será notificada a los empleados u otras personas, relacionadas o vinculadas con la actividad, por parte de la Entidad.

Con ello, se pretende que el personal de la Entidad sea conocedor de los hechos y pueda estar informado de primera mano.

La comunicación se realizará, de forma coordinada y simultánea, a la realizada a las personas afectadas. La comunicación describirá, en un lenguaje claro y sencillo, la naturaleza de la violación de seguridad, así como el posicionamiento corporativo en relación a la violación ocurrida.

De igual forma, se valorará el envío de una comunicación similar a otras entidades u otras partes interesadas que deban conocer lo sucedido y ser informados por la Entidad de la violación de seguridad acaecida, así como el posicionamiento corporativo en relación a la violación ocurrida.

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 Responsable de Riesgos Tecnológicos, el Responsable de Seguridad Informática, la unidad / departamento que efectúa el tratamiento y el Delegado de Protección de Datos no podrán cerrar el asunto, y deberán permanecer abierto.

Asimismo, la Entidad ha de estar preparada 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.

La AEPD indica en su Guía que:

- En caso de recibir un requerimiento de información adicional el Responsable de Tratamiento deberá atenderlo en el plazo indicado en el requerimiento y remitiendo la información a través de registro electrónico, indicando que se trata de un registro relacionado con un procedimiento en tramitación e indicando el tipo de documento "contestación a requerimiento".
- En caso de recibir una orden de comunicación a los afectados, el responsable de tratamiento dispondrá del plazo indicado en esa orden para confirmar a la Agencia su ejecución a través del registro electrónico.

Con carácter general el plazo para la confirmación será de 30 días, aunque podría acortarse en función del nivel de riesgo. La confirmación se debe realizar igualmente mediante registro electrónico, indicando que se trata de un registro relacionado con un procedimiento en tramitación, indicando el número de registro de salida de la orden de comunicar a los afectados e indicando el tipo de documento "contestación a requerimiento".

La violación de datos personales en tanto no se clasifique como "definitivamente resuelta", será tratada en las diferentes reuniones que se convoquen en relación a asuntos relacionados con la seguridad de la información.

ANEXO I. EVALUACIÓN DE INCIDENTE DE SEGURIDAD

<table>
<tr><th colspan="4">EVALUACIÓN DE INCIDENTE DE SEGURIDAD</th></tr>
<tr><td colspan="2">☐ Incidente detectado como Responsable de Tratamiento.</td><td colspan="2">☐ Incidente detectado como Encargado de Tratamiento.</td></tr>
<tr><td colspan="4">Persona que detecta el incidente</td></tr>
<tr><td>Nombre y apellidos:</td><td colspan="3"></td></tr>
<tr><td>Entidad:</td><td colspan="3"></td></tr>
<tr><td>Fecha y hora en que se produjo el incidente o, en su caso, cuándo se detectó.</td><td></td><td>Origen.</td><td>☐ Interna
☐ Externa.</td></tr>
<tr><td colspan="2">¿Se considera subsanado el incidente?</td><td colspan="2">☐ SI ☐ NO</td></tr>
<tr><td colspan="2">En caso de persistir, fecha estimada de subsanación</td><td colspan="2"></td></tr>
<tr><td colspan="4">Persona que comunica el incidente:</td></tr>
<tr><td>Nombre y apellidos:</td><td colspan="3"></td></tr>
<tr><td>Entidad:</td><td colspan="3"></td></tr>
<tr><td colspan="4">Tipología del incidente: Brecha de confidencialidad: Tiene lugar cuando partes que no están autorizadas, o no tienen un propósito legítimo para acceder a la información, acceden a ella. La severidad de la pérdida de confidencialidad varía según el alcance de la divulgación, es decir, el número potencial y el tipo de partes que pueden haber accedido ilegalmente a la información.

Brecha de integridad: se produce cuando se altera la información original y la sustitución de datos puede ser perjudicial para el individuo. La situación más grave ocurre cuando existen serias posibilidades de que los datos alterados se hayan utilizado de una manera que pueda dañar al individuo.

Brecha de disponibilidad: su consecuencia es que no se puede acceder a los datos originales cuando es necesario. Puede ser temporal (los datos son recuperables, pero tomará un periodo de tiempo y esto puede ser perjudicial para el individuo), o permanente (los datos no pueden recuperarse).</td></tr>
<tr><td>☐ Afecta a la confidencialidad.</td><td>☐ Afecta a la integridad.</td><td colspan="2">☐ Afecta a la disponibilidad.</td></tr>
<tr><td colspan="4">Categorización del incidente: Crítico (afecta a datos valiosos, gran volumen y en poco tiempo) / Muy Alto (Cuando dispone de capacidad para afectar a información valiosa, en cantidad apreciable) / Alto (Cuando dispone de capacidad para afectar a información valiosa) / Medio (Cuando dispone de capacidad para afectar a un volumen apreciable de información) / Bajo (Escasa o nula capacidad para afectar a un volumen apreciable de información).</td></tr>
</table>

☐ CRÍTICO.	☐ MUY ALTO.	☐ ALTO.	☐ MEDIO.	☐ BAJO.

Descripción detallada de los hechos y medidas inmediatas adoptadas para contener el incidente

Naturaleza, sensibilidad y categorías de datos personales afectados: *Datos de escaso riesgo: datos de contacto, de educación, familiares, profesionales, biográficos; Datos de comportamiento: localización, tráfico, hábitos y preferencias; Datos financieros: transacciones, posiciones, ingresos, cuentas, facturas; Datos sensibles: de salud, biométricos, datos relativos a la vida sexual, etc.*

☐ Datos básicos (nombre, apellidos, fecha de nacimiento).

☐ Credenciales de acceso/identificación (usuario y/o contraseña).

☐ DNI/NIE/Pasaporte o cualquier documento identificativo.

☐ Datos de contacto

☐ Datos económicos/financieros (sin medios de pago).

☐ Datos de medios de pago.

☐ Datos de localización

Otros:

Categoría de interesados afectados

Clientes

Usuarios

Empleados

Proveedores

Potenciales clientes

Menores

Personas en riesgo de exclusión

Otros:

Datos legibles/ilegibles: *Datos protegidos mediante algún sistema de seudonimización (por ejemplo, cifrado o hash)*

Número de individuos afectados: *Dentro de una escala determinada, por ejemplo, más de 100 individuos.*

Volumen de datos: *expresados en cantidad (registros, ficheros, documentos) y/o en periodos de tiempo (una semana, un año, etc.)*
Facilidad de identificación de individuos: *facilidad con la que se puede deducir la identidad de los individuos a partir de los datos involucrados en la brecha*
Severidad de las consecuencias para los individuos: *Baja: Las personas no se verán afectadas o pueden encontrar algunos inconvenientes que superarán sin ningún problema (tiempo de reingreso de información, molestias, irritaciones, etc.) / Media: Las personas pueden encontrar inconvenientes importantes, que podrán superar a pesar de algunas dificultades (costos adicionales, denegación de acceso a servicios comerciales, miedo, falta de comprensión, estrés, dolencias físicas menores, etc.) / Alta: Las personas pueden enfrentar consecuencias importantes, que deberían poder superar aunque con serias dificultades (malversación de fondos, listas negras de los bancos, daños a la propiedad, pérdida de empleo, citación judicial, empeoramiento de la salud, etc.) / Muy alta: Las personas pueden enfrentar consecuencias significativas, o incluso irreversibles, que no pueden superar (exclusión o marginación social, dificultades financieras tales como deudas considerables o incapacidad para trabajar, dolencias psicológicas o físicas a largo plazo, muerte, etc.).*
Características especiales de los individuos: *Si afectan a individuos con características especiales o con necesidades especiales.*
Características especiales del responsable del tratamiento: *En base a la actividad de la entidad.*
Número y tipología de los sistemas afectados.
El impacto sobre la Entidad, *desde punto de vista de la protección de la información, la prestación de los Servicios, la conformidad legal y/o la imagen pública. Va a estar relacionado con la categoría o criticidad de los servicios y personas afectados. En este aspecto diferenciamos entre los siguientes impactos: Bajo (perjuicio limitado), Medio (perjuicio grave) y Alto (perjuicio muy grave).*
Requerimientos legales y regulatorios: *Notificación de la brecha a la autoridad de control y cualquier otra obligación de notificación, comunicación a Fuerzas y Cuerpos de Seguridad del Estado en caso de delito.*
Valoración del incidente

<table>
<tr><td rowspan="5">Volumen: número de registros afectados.</td><td></td><td>Entre 1 y 100 registros (1).</td><td rowspan="12">▪ Se considerará una Brecha a <u>notificar a la Autoridad de Control</u> el incidente que cumpla simultáneamente con las siguientes circunstancias:
✓ Riesgo con valor cuantitativo en un umbral superior a 20 (más o menos).
✓ Coincidencia de dos circunstancias cualitativas marcadas en negrita.
▪ Se <u>comunicará como brecha al interesado</u> cuando el incidente analizado cumpla simultáneamente las siguientes circunstancias:
✓ Riesgo con valor cuantitativo superior a 40 (más o menos).
✓ Ante la coincidencia de dos circunstancias cualitativas marcadas en negrita.</td></tr>
<tr><td></td><td>Entre 101 y 1.000 registros (2).</td></tr>
<tr><td></td><td>Entre 1.001 y 100.000 registros (3).</td></tr>
<tr><td></td><td>Entre 100.001 y 1.000.000 registros (4).</td></tr>
<tr><td></td><td>Más de 1.000.000 registros (5).</td></tr>
<tr><td rowspan="2">Tipología de datos.</td><td></td><td>Datos no sensibles (x1).</td></tr>
<tr><td></td><td>Datos sensibles (x2).</td></tr>
<tr><td rowspan="5">Impacto (exposición)</td><td></td><td>Nulo (0).</td></tr>
<tr><td></td><td>Interno -dentro de la entidad, controlado- (4).</td></tr>
<tr><td></td><td>Externo -perímetro proveedor, atacante- (6).</td></tr>
<tr><td></td><td>Pública -accesible en internet- (8).</td></tr>
<tr><td></td><td>Desconocido (10).</td></tr>
<tr><td colspan="4">CÁLCULO DEL RIESGO: Se podrá determinar de la siguiente forma:
▪ Riesgo = P (Volumen) x Impacto (Tipología x Impacto).
▪ Ejemplo: Fuga masiva pública de datos sensibles con impacto desconocido: 5 x (2x10) = 100%.</td></tr>
<tr><td colspan="4">RIESGO = P (__) X IMPACTO (__ X __) = ____</td></tr>
<tr><td colspan="4">RESULTADO DE LA EVALUACIÓN</td></tr>
<tr><td colspan="4">Según los criterios establecidos en el Análisis del Incidente, ¿se considera éste como una Brecha de Seguridad a los efectos de aplicación de la normativa en materia de protección de datos o bien se considera un Incidente Interno?</td></tr>
<tr><td colspan="2">☐ BRECHA DE SEGURIDAD</td><td colspan="2">☐ INCIDENTE INTERNO</td></tr>
<tr><td colspan="4">En _____, a ____ de _____ de _____.
Persona que cumplimenta este Informe: _____</td></tr>
</table>

Firma: _____

ANEXO II. FORMULARIO DE NOTIFICACIÓN DE INCIDENTES DE SEGURIDAD DE DATOS PERSONALES

Formulario en pdf https://www.aepd.es/sites/default/files/2021-02/formulario-brechas.pdf

ANEXO III. EJEMPLO DE NOTIFICACIÓN DEL INCIDENTE A LOS INTERESADOS

Estimado cliente:

En cumplimiento de la normativa de protección de datos de carácter personal, [RESPONSABLE]., con NIF: _____, dirección _____, e-mail: protecciondedatos@cajalmendralejo.es : dpo@cajalmendralejo.es , actuando en calidad de Responsable de tratamiento de datos personales, le informamos de que con fecha _____, hemos detectado que se ha producido el siguiente incidente de seguridad:

- *Descripción del incidente indicando, en caso de actuar como encargado de tratamiento, los datos del responsable por cuenta del cual se actúa y cuándo se ha producido.*

Una vez estudiado el incidente, se ha detectado que éste puede haber puesto en riesgo sus datos personales, en concreto:

- *Descripción de las posibles consecuencias de la violación de la seguridad de los datos personales.*
- *Descripción de los datos e información personal de los afectados.*

No obstante, le informamos de que se han puesto en marcha las siguientes medidas para evitar y mitigar, efectos negativos sobre sus datos personales.

- *Descripción de las medidas adoptadas o propuestas por el responsable del tratamiento para poner remedio a la violación de la seguridad de los datos personales, incluyendo, si procede, las medidas adoptadas para mitigar los posibles efectos negativos.*

Igualmente, le informamos de que, tal y como establece la normativa vigente sobre protección de datos personales, hemos procedido a comunicar la brecha de seguridad a la Autoridad de Control (Agencia de Protección de Datos: www.aepd.es).

Estamos a su disposición para facilitarle cualquier información adicional.

Lamentando mucho las molestias ocasionadas, reciba un cordial saludo.

En _____ , a __ de _____ de _____.

ANEXO IV. REGISTRO DE INCIDENTES

N.º INCIDENTE REGISTRADO	Encargado del Tratamiento	Categoría (Incidente interno/Brecha de seguridad)	Fecha incidente	Fecha comunicación	Persona encargada de gestión y resolución	Tipología / Descripción	Fecha cierre	Otra información