PROCEDIMIENTO DE BRECHAS DE SEGURIDAD

CONTROL DE REVISIONES			
EDICIÓN	**FECHA DE REVISIÓN**	**Descripción**	**FECHA DE APROBACIÓN**
1	20/4/2025	Creación de nuevo documento	25/4/2025

Tabla de contenido

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 (Reglamento General de Protección de Datos, (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 el caso de España, la Autoridad de Control a la que hay que notificar es la Agencia Española de Protección de Datos (AEPD), tanto para el sector privado como para el público, excepción de los organismos públicos de las Comunidades Autónomas donde exista Autoridad de Control Autonómica. Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos y garantía de derechos digitales (LOPDGDD). 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. En la versión original del RGPD en inglés, así como en las directrices del Comité Europeo de Protección de Datos, la expresión utilizada es “personal data breach”, sin embargo, la versión en español utiliza “violación de la seguridad de los datos personales”. A lo largo de esta guía se utilizará prioritariamente la expresión “brecha de datos personales” y ocasionalmente simplemente “brecha”.

Los artículos 33 y 34 del RGPD 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. Este proceso de gestión de brechas vendría a completar el proceso de gestión de incidentes de la organización. De esta forma el proceso de gestión de brechas se suma a las políticas de información ya existentes en una organización y es una parte necesaria para mantener la actividad de cualquier entidad. Este proceso se constituye en una de las medidas organizativas más importantes a la hora de salvaguardar los derechos y libertades de los interesados a través de medidas de seguridad de los tratamientos. Cualquier organización que trate datos personales se encuentra expuesta a sufrir una brecha de datos personales que pueda repercutir en los derechos y libertades de las personas físicas, y por tanto está obligada a preverlas y gestionarlas adecuadamente. Análogamente al RGPD, la Directiva (UE) 2016/680 relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por parte de las autoridades competentes para fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, y a la libre circulación de dichos datos, establece en sus artículos 30 y 31 las condiciones para la notificación de una brecha de datos personales a la Autoridad de Control y a las personas afectadas.

Las notificaciones de brechas de datos personales ante la Autoridad de Control son parte de la responsabilidad proactiva de los responsables, o encargados en su caso, demostrando diligencia en los tratamientos de datos. 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 organización 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 y comunicación a los interesados sí está tipificado como infracción.

En ningún caso una notificación de brecha de datos personales es el cauce para interponer reclamaciones contra una persona física o jurídica, ni tendrán la consideración de denuncias. La notificación de brechas de datos personales es una tarea y una obligación del responsable del tratamiento.

2. BRECHAS DE DATOS PERSONALES

A. ¿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 sujetas a los artículos 33 y 34 del RGPD 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.

Por lo tanto, no todos los incidentes de seguridad son necesariamente brechas de datos personales y no solo los ciber incidentes 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.

B. PROCESO DE GESTIÓN DE INCIDENTES

Esta es una tarea previa a la materialización de una brecha de datos personales, y forma parte de la preparación de la organización para afrontar las brechas que pueda sufrir. Una vez establecido el nivel de riesgo, y aunque este sea escaso, se deben establecer, las medidas de para minimizar dicho riesgo, tal y como se establece en los artículos 24 (p.ej. políticas de protección de datos), 25 (medidas de protección de datos por defecto y desde el diseño), 32 (medidas de seguridad) y 35 (evaluaciones de impacto para la protección de datos), entre otros. El RGPD contempla tanto medidas preventivas para evitar o disminuir el riesgo como correctivas para reaccionar ante la materialización del riesgo.

En particular, el artículo 32.1 enumera específicamente un conjunto no exhaustivo de medidas de seguridad que se podrían contemplar para gestionar el riesgo mediante medidas de seguridad en un tratamiento, como son:

- Medidas orientadas a garantizar la confidencialidad, integridad y disponibilidad.
- Medidas para garantizar la resiliencia de los sistemas y servicios de tratamiento, y para dotar de capacidad de restaurar la disponibilidad y el acceso a los datos personales de forma rápida en caso de incidente físico o técnico.

- La seudonimización y el cifrado de datos personales.
- Los procesos de verificación, evaluación y valoración regulares de las medidas de seguridad.

De este conjunto de medidas se desprende la necesidad de evaluar el impacto 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.

El responsable ha de ser diligente en la implementación de medidas para la detección de un incidente y su clasificación como brecha de datos personales. Estas medidas podrían incorporar procedimientos, recursos y medios de detección y gestión, ya sean propios o a través de terceros, así como garantías de que los anteriores funcionan correctamente. Las medidas deben permitir reaccionar lo antes posible a la brecha de datos personales y evaluar el riesgo para los derechos y libertades de las personas físicas. Los encargados del tratamiento deberán informar sin dilación de las brechas que sufran a los responsables para que estos evalúen el riesgo y ejerzan sus obligaciones.

Una vez detectada y evaluada la brecha de datos personales, durante su resolución se debe documentar el proceso con toda la información que se vaya recopilando. Esta documentación será adjuntada al registro de incidentes que deben mantener los responsables de los tratamientos. La información relativa a las decisiones tomadas sobre la notificación a la autoridad competentes y la comunicación a los afectados (incluida una copia de la comunicación de realizarse) debe recogerse también en este registro de forma detallada.

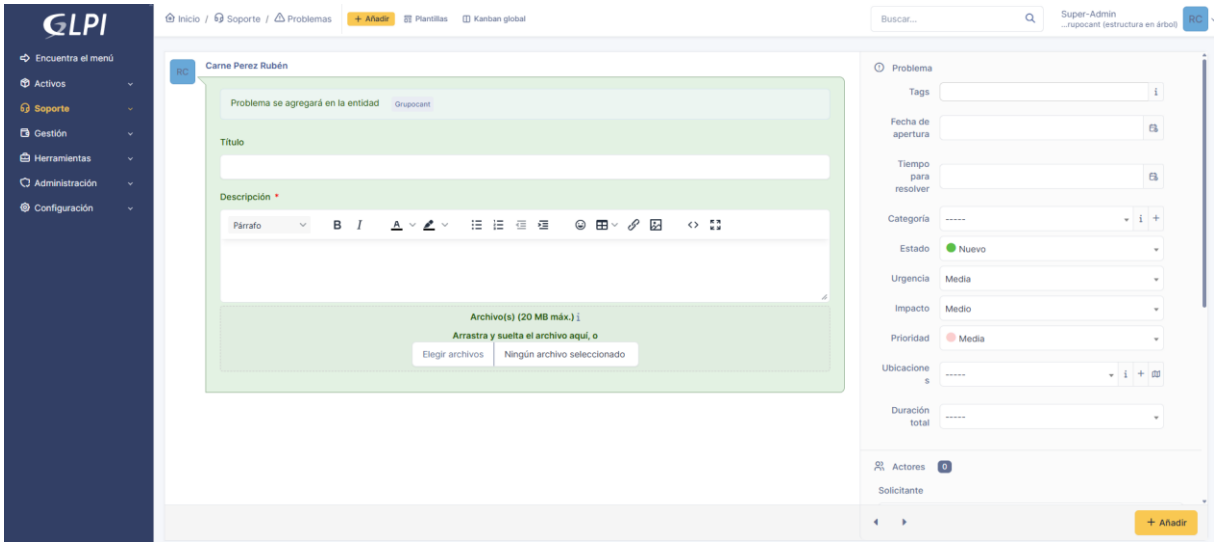
B.1 Registro de incidentes en la herramienta corporativa de ticketing

La organización utilizará su herramienta corporativa de ticketing GLPI como sistema oficial de registro y gestión de incidentes y brechas de seguridad.

Toda brecha o posible brecha de datos personales deberá registrarse sin dilación en dicha herramienta, mediante la apertura de un ticket específico que incluya, como mínimo:

- Fecha y hora de detección.
- Persona que reporta.
- Descripción detallada del incidente.
- Sistemas, servicios y datos afectados.
- Evaluación preliminar del impacto en datos personales.
- Valoración inicial del riesgo para los interesados.
- Acciones de contención y mitigación.
- Análisis posterior y medidas adoptadas.
- Decisiones relativas a la notificación a la Autoridad de Control.
- Decisiones relativas a la comunicación a los afectados.

El ticket generado en la herramienta constituye el registro documental exigido por el artículo 33.5 del RGPD, y deberá mantenerse actualizado durante todo el ciclo de gestión de la brecha. Permanecerá accesible para auditorías internas, externas o requerimientos de la Autoridad de Control.



C. ROLES IMPLICADOS EN LA GESTIÓN DE BRECHAS

- **Responsable de tratamiento**: le corresponde aplicar las medidas técnicas y organizativas apropiadas a fin de garantizar y poder demostrar que el tratamiento es conforme al RGPD. En su caso, 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. El responsable de tratamiento deberá contar con el asesoramiento del delegado de protección de datos cuando haya sido designado, o, en su defecto, podrá contar con el asesoramiento de equipos internos o externos expertos en protección de datos.
  El responsable puede delegar en el encargado la gestión de la brecha de datos personales, tanto en lo relativo a la respuesta como en lo relativo a la notificación, documentándose dicha delegación de funciones en el contexto de la relación contractual establecida. No obstante, el responsable debe asegurarse de que se están tomando las acciones de respuesta, notificación y comunicación oportunas, dado que la delegación de funciones no implica delegación de responsabilidad.
- **Encargado del tratamiento:** le corresponde 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. Aunque el RGPD no especifica un plazo concreto para que los encargados informen a los responsables, sí indica que la información debe enviarse sin dilación indebida.

- **Delegado de protección de datos**: En los casos en los que se haya designado un DPD (porque lo exija el RGPD o porque lo haya decidido el responsable), éste ocupará un papel muy relevante en el proceso de gestión de brechas. El DPD por tanto deberá informar y asesorar al responsable/encargado del tratamiento respecto de:
  - la implantación de un proceso de gestión de brechas de datos personales en la organización,
  - la evaluación del riesgo y las consecuencias que puede suponer para los derechos y libertades de las personas una brecha de datos personales,

- las acciones adecuadas que se deben tomar para mitigar los efectos de la brecha de datos personales sobre las personas afectadas,
- la necesidad de notificar la brecha de datos personales a la Autoridad de Control y en su caso a los interesados afectados,
- en el caso de encargados de tratamiento, la necesidad de notificar la brecha de datos personales al responsable.

El DPD actuará como punto de contacto con la Autoridad de Control en el proceso de notificación por parte del responsable de las brechas de datos personales, así como las respuestas a los requerimientos realizados por dicha Autoridad respecto a las mismas, siempre de acuerdo con el proceso de gestión de brechas implantado en la organización.

Figura	Funciones y responsabilidades
Responsable	• Implantación del proceso de gestión de brechas • Evaluación de las consecuencias para los derechos y libertades de las personas • Notificar la brecha de datos personales a la Autoridad de Control • Comunicar la brecha de datos personales a las personas afectadas
Encargado	• 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 • Ejecutar las labores de notificación o comunicación de la brecha que tenga asignadas por contrato
Delegado de protección de datos	• Informar y asesorar al responsable/encargado del tratamiento sobre sus obligaciones y responsabilidades con relación a las brechas de datos personales • Cooperar con la Autoridad de Control en las cuestiones relativas a la gestión de la brecha de datos personales • Actuar como punto de contacto con la Autoridad de Control, en particular, en el proceso de notificación de la brecha de datos personales

3. NOTIFICACIÓN A LA AUTORIDAD DE CONTROL

Con independencia de la necesidad de notificar a la Autoridad de Control sobre una brecha de datos personales, el artículo 33.5 del RGPD establece la obligación del responsable de tratamiento de documentar cualquier brecha, incluidos los hechos relacionados con la brecha, sus efectos y las medidas correctivas adoptadas.

Conforme al artículo 33 del RGPD, tan pronto como el responsable del tratamiento tenga conocimiento de que se ha producido una brecha de datos personales debe efectuar la correspondiente notificación a la Autoridad de Control competente, cuando sea probable que la brecha constituya un riesgo para los derechos y libertades de las personas.

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. El responsable debe documentar la brecha y evaluar tanto la necesidad de notificar ante la Autoridad de Control como la necesidad de comunicar a los afectados. El encargado podrá realizar la notificación de brecha de datos personales en nombre de los responsables involucrados cuando así lo tengan estipulado en un contrato o vínculo legal.

Cuando la brecha de datos personales entrañe un alto riesgo para los derechos y libertades de las personas afectadas, además de la notificación a la Autoridad de Control, se deberá comunicar a los afectados la brecha de datos personales sin dilación indebida. El lenguaje será claro y sencillo, de forma concisa y transparente.

4. PLAZOS PARA NOTIFICAR

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.

Para garantizar que no se produce una dilación indebida en la notificación del encargado al responsable, los procedimientos de gestión de brechas de datos personales de responsables y encargados deben concretar este plazo, incluso reflejarlo en el contrato de encargo de tratamiento.

En cualquier caso, dicho plazo debería establecerse en función del riesgo de los tratamientos llevados a cabo por el encargado de tratamiento18, y no debería ser superior a las 72 horas que el RGPD establece para la notificación de las brechas de datos personales a la Autoridad de Control.

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.

5. AUTORIDAD DE CONTROL A LA QUE SE DEBE NOTIFICAR

Con carácter general, en el ámbito privado, los responsables del tratamiento afectado por la brecha deberán notificar a la Agencia Española de Protección de Datos:

- Cuando su único establecimiento esté localizado en España.
- Si tienen varios establecimientos en la Unión Europea, únicamente cuando el establecimiento principal esté localizado en España.
- Si no tienen establecimiento principal en la Unión Europea, sólo en el caso de que hayan designado un representante en España.
- Si no tienen establecimiento ni representante en la Unión Europea, en el caso de que la brecha de datos personales cuente con afectados en España.

QUÉ NOTIFICAR

El artículo 33 del RGPD establece que la notificación de brechas de datos personales a la Autoridad de Control deberá como mínimo:

- "Describir la naturaleza de la violación de la seguridad de los datos personales, inclusive, cuando sea posible, las categorías y 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 del 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."

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

personales notificada. Para ello deberá prever los medios técnicos necesarios para poder acceder de forma rápida y ágil a estas comunicaciones.

6. COMUNICACIÓN 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 comunicará la brecha de datos personales a los afectados sin dilación indebida.

Existen 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.
- No será necesaria la comunicación a los afectados cuando:
- El responsable ha tomado medidas técnicas y organizativas adecuadas que evitan los riesgos anteriores, minimizan los daños a los derechos y libertades y/o los hacen reversibles.
- El responsable ha tomado con posterioridad a la brecha de datos personales las medidas de protección que mitiguen total o parcialmente el posible impacto para los afectados y garanticen que ya no hay posibilidad de que el alto riesgo para sus derechos y libertades se materialice.
- La comunicación a las personas afectadas se realizará en un lenguaje claro y sencillo, con el siguiente contenido mínimo:
- Datos de contacto del Delegado de Protección de Datos, o en su caso, del punto de contacto en el que pueda obtenerse más información.
- Descripción general del incidente y momento en que se ha producido.
- Las posibles consecuencias de la brecha de datos personales.
- Descripción de los datos e información personal afectados.
- Resumen de las medidas implantadas hasta el momento para controlar los posibles daños.
- Otras informaciones útiles a los afectados para que puedan proteger sus datos o prevenir posibles daños.

La comunicación preferentemente se deberá realizar de forma directa al afectado, ya sea por teléfono, correo electrónico, SMS, a través de correo postal, o a través de cualquier otro medio dirigido al afectado que el responsable considere adecuado.

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.

7. TIPOLOGÍA DE LAS BRECHAS

Uno de los parámetros más importantes a la hora de evaluar el nivel de riesgo de 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. Estas dimensiones son la confidencialidad, disponibilidad e integridad. Es importante considerar que una misma brecha de datos personales puede afectar a más de una dimensión dependiendo de las circunstancias particulares en cada caso.

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

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.

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.

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.

Ante una brecha de datos personales, el responsable de tratamiento debe ser capaz de determinar con precisión las categorías de datos personales afectadas, el número de personas afectadas y su perfil. Estos tres parámetros son fundamentales para poder determinar el nivel de riesgo para los afectados por la brecha de datos personales.

Categorías de datos	Categorías de datos
Datos básicos	Número de teléfono, email o dirección física de las personas
Datos de contacto	Número de teléfono, email o dirección física de las personas
Imágenes (foto/video)	Imágenes individuales o colectivas de las personas afectada
Documento identificativo	NIF, NIE, pasaporte, número de Seguridad Social o cualquier otro identificador a nivel nacional o extra nacional
Datos económicos o financieros	Datos referidos a nóminas, extractos bancarios, estudios económicos o cualquier otra información que pueda revelar información económica de los afectados
Datos de localización	Datos de posicionamiento, coordenadas o direcciones habituales (no residencia) de los afectados
Medios de pago	Información de los afectados referido a métodos de pago como números de tarjeta, cuentas bancarias, métodos de pago online como Paypal, bitcoins, etc.
Credenciales de acceso o identificación	Nombres de usuarios, contraseñas ya estén en claro, hasheadas o cifradas y datos como tarjetas de coordenadas o segundos factores de autenticación
Datos de perfiles	Perfiles de usuarios en redes o datos de perfilado psicosocial o que permitan realizar perfilados de personas físicas
Sobre la vida sexual	Datos relativos a la salud sexual, hábitos, orientación o tendencias sexuales, así como información que permita inferirlo

Religión o creencias	Religión que profesan los afectados, así como información sobre posturas religiosas, agnósticas o ateas
Origen racial o étnico	Información que refleje o permitan establecer el origen racial o la pertenencia a una determinada etnia de las personas
Datos de salud de empleados	Información sobre la salud que un responsable trate sobre sus empleados o personas con las que mantiene una relación laboral, como puedan ser partes de baja o informes sanitarios
Datos de salud de pacientes	Referido a la información que los responsables del sector sanitario dispongan de las personas
Opinión política	Información que refleje o permita averiguar la opinión o tendencias políticas de las personas
Datos genéticos	Características genéticas heredadas o adquiridas de una persona física que proporcionen una información única sobre la fisiología o la salud de esa persona, obtenidos en particular del análisis de una muestra biológica
Datos sobre condenas e infracciones penales	Certificados de antecedentes penales o los certificados de delitos de naturaleza sexual
Datos biométricos	Características físicas, fisiológicas o conductuales de una persona física, que permita su identificación
Datos sobre afiliación sindical	Informan sobre la pertenencia o afiliación de una persona a un sindicato

8. CONSECUENCIAS

El Considerando 85 del RGPD indica que las brechas de datos personales pueden entrañar daños y perjuicios físicos, materiales o inmateriales para las personas físicas, como pérdida de control sobre sus datos personales o restricción de sus derechos, discriminación, usurpación de identidad, pérdidas financieras, reversión no autorizada de la seudonimización, daño a la reputación, pérdida de confidencialidad de datos sujetos a secreto profesional, o cualquier otro perjuicio económico o social significativo para la persona en cuestión.

Cuando sucede una brecha de datos personales es necesario que el responsable determine de forma rigurosa cuáles son las posibles consecuencias, cómo pueden afectar a los derechos y libertades de las personas afectadas, es decir el nivel de severidad con el que se podrían materializar dichas consecuencias y la probabilidad de que se materialicen.

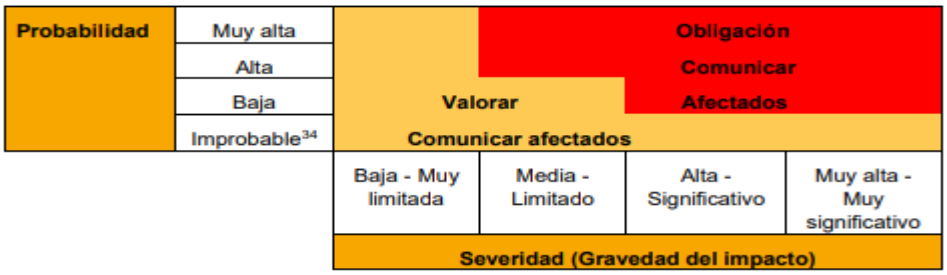
Con estos datos el responsable podrá determinar el nivel de riesgo para los derechos y libertades de las personas físicas y en función del riesgo tomar las opciones oportunas con el objetivo de protegerlos. Es importante destacar que se trata de determinar el nivel de riesgo para las personas físicas cuyos datos se han visto afectados por la brecha de datos personales, y no debe confundirse con otros tipos de riesgos o el riesgo para el responsable de tratamiento o alguno de sus encargados de tratamiento.

Para determinar todos estos factores el responsable de tratamiento debe apoyarse irremediablemente en el trabajo previo de gestión de riesgos de los tratamientos que lleva a cabo y sobre los que se ha producido la brecha de datos personales.

Consecuencias para los afectados
Imposibilidad de ejercer algún derecho o acceso a un servicio
Usurpación de la identidad
Víctima de campañas de phishing/spamming
Pérdidas financieras
Daños reputacionales
Pérdida de confidencialidad de datos afectados por secreto profesional
Daños psicológicos o físicos
Pérdida de control sobre sus datos personales

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 afectados
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
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
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.)
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.)



El responsable deberá comunicar una brecha de datos personales a las personas afectadas conforme al artículo 34 del RGPD cuando **no pueda garantizar** que es improbable que pueda dañar, reversible o irreversiblemente, derechos fundamentales o libertades públicas de las personas.

9. MEDIDAS DE SEGURIDAD ANTES DEL INCIDENTE

El responsable de tratamiento debe determinar si las medidas de seguridad disponibles antes de la brecha de datos personales eran adecuadas al nivel de riesgo. En caso necesario debe introducir medidas de seguridad adicionales o corregir fallos o deficiencias en las medidas de seguridad adoptadas.

- **Medidas de seguridad con las que contaba el tratamiento antes de la brecha**:
  - Políticas y formación en protección de datos y seguridad de la información.
  - Sistemas actualizados.
  - Registro de incidentes.
  - Auditorías periódicas.
  - Control de acceso físico y lógico.
  - Diferentes niveles de acceso a los datos.
  - Copias de seguridad / Plan de recuperación.
  - Anonimización.