Guía para la notificación de brechas de datos personales

v. mayo de 2021

RESUMEN EJECUTIVO

El presente documento tiene por objetivo guiar a los responsables de los tratamientos de datos personales en el cumplimiento de sus obligaciones de notificación a las Autoridades de Control competentes de las brechas de datos personales y de la comunicación a las personas que se han visto afectadas por ésta.

Esta guía actualiza la ya publicada por la AEPD en junio de 2018, simultáneamente a la entrada en vigor del RGPD, cuyo objetivo fue proporcionar un instrumento que ayudase a los responsables en el cumplimiento de sus obligaciones en lo referente a las brechas de datos personales.

Esta nueva versión incluye la experiencia recogida en los primeros años de aplicación de las obligaciones recogidas en los artículos 33 y 34 del RGPD, tanto a nivel nacional, como con relación a los criterios establecidos por el Comité Europeo de Protección de Datos (CEPD).

El principal propósito de esta actualización es permitir cumplir de forma eficaz y eficiente con los objetivos últimos de la notificación de brechas de datos personales. Estos son: la protección efectiva de los derechos y libertades de los interesados, la creación de un entorno más resiliente basado en el conocimiento de las vulnerabilidades en los tratamientos y la garantía de una seguridad jurídica al disponer los responsables de un medio para demostrar diligencia.

Esta guía está orientada a proporcionar directrices generales en la notificación de brechas de datos personales y en la comunicación a los interesados, precisando plazos y aspectos concretos sobre el procedimiento para notificar y el contenido de las notificaciones. La información proporcionada permite al responsable conocer con precisión el alcance de sus obligaciones y facilitar su cumplimiento.

La guía se centra en los casos en que la brecha tenga o pueda tener incidencia en el ámbito del RGPD, es decir, en aquellos casos en los que la brecha de datos personales pueda afectar a los derechos y libertades fundamentales de las personas. En el apartado final se destacan las cuestiones específicas de la notificación de brechas de datos personales acuerdo con la Ley General de Telecomunicaciones.

Palabras clave: RGPD, LOPDGDD, notificación, comunicación, afectados, vulneración, sede, formulario, solicitante, DPD, responsable, brecha, seguridad.

ÍNDICE

I. 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[1] de las Comunidades Autónomas donde exista Autoridad de Control Autonómica.

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"[2]. No obstante, deben entenderse con el mismo significado las expresiones "violación de la seguridad de los datos personales", "brecha de seguridad de los datos personales", "brecha de seguridad", "quiebra de seguridad" y "quiebra de seguridad de los datos personales" utilizadas en otros textos y procedimientos, algunos anteriores al RGPD.

En junio de 2018 la AEPD publicó la "Guía para la Gestión y Notificación de Brechas de Seguridad" elaborada en colaboración con varias instituciones. Fue un instrumento pionero en Europa destinado a ayudar a responsables y encargados en el cumplimiento de sus nuevas obligaciones en lo referente a las brechas de datos personales. Dicha guía rápidamente se convirtió en una referencia útil entre responsables y encargados de toda la Unión Europea.

Tras varios años de aplicación del RGPD, conviene aprovechar la experiencia adquirida por la AEPD, otras Autoridades de Control y el Comité Europeo de Protección de Datos para renovar la guía y, de esta forma, proporcionar a responsables y encargados directrices más precisas que faciliten y simplifiquen aún más el cumplimiento de las obligaciones establecidas en los artículos 33 y 34, relativas a la gestión y notificación de brechas de datos personales.

En esta actualización se pretende, además, concretar algunos plazos que el RGPD deja abiertos, como son los plazos para notificar una brecha de datos personales de manera gradual a la Autoridad de Control, plazos para comunicar una brecha de datos personales a los interesados, o plazos para que los encargados informen a los responsables sobre una brecha. En el texto se precisará el alcance, contenido y plazos de las notificaciones por parte de la Autoridad de Control, lo que permitirá optimizar los recursos que los responsables de tratamiento deban dedicar a esas notificaciones.

El principal propósito de la actualización de esta guía es permitir cumplir de forma más eficaz y eficiente con los objetivos últimos de la notificación de brechas de datos personales. Estos son: la protección efectiva de los derechos y libertades de los interesados mediante la

[1] Así como otras entidades en el ámbito de las competencias concretas de cada Autoridad de Control Autonómica.
[2] Para evitar una repetición excesiva de términos en algunos párrafos.

comunicación de brechas de datos, la creación de un entorno más resiliente basado en el conocimiento de las vulnerabilidades en los tratamientos, y dotar de seguridad jurídica a los responsables de tratamiento al disponer de un medio para demostrar diligencia.

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[3].

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.

Los ejemplos incluidos en esta guía se circunscriben a las circunstancias y situaciones específicas que se describen en cada caso, debiendo entenderse en ese sentido como ejemplos para aclarar conceptos concretos y como tal deben ser considerados. Estos ejemplos no constituyen en ningún caso reglas de aplicación general que pueden utilizarse en cualquier circunstancia.

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.

[3] Al tratarse de una Directiva, es necesaria su trasposición para que sea aplicable en España. A fecha de publicación de esta guía el Proyecto de Ley Orgánica Proyecto de Ley Orgánica de protección de datos personales tratados para fines de prevención, detección, investigación y enjuiciamiento de infracciones penales y de ejecución de sanciones penales, en tramitación en las Cortes Generales, traspone estas condiciones en los artículos 38 y 39.

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

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

II. BRECHAS DE DATOS PERSONALES

A. ¿QUÉ ES UNA BRECHA DE DATOS PERSONALES? ¿QUÉ NO LO ES?

El RGPD define, de un modo amplio, las "*brechas de datos personales*" como "*todas aquellas violaciones*[4] *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 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 ejemplo, el mero hecho de recibir correos electrónicos con malware o sospechosos de malware sin haberlo ejecutado, detectar un sistema infectado con un virus, o sufrir un intento de ciberataque sin que se llegue a materializar, no puede ser considerado en sí mismo como una brecha de datos personales cuando no puedan producir consecuencias sobre los derechos y libertades de las personas. No obstante, deben ser gestionadas como incidentes de seguridad, incluyendo la necesidad de determinar si han llegado a afectar a datos personales. En base al principio de responsabilidad proactiva, ante cualquier suceso que pueda tener consecuencias para los derechos y libertades de los interesados el responsable de tratamiento ha de reaccionar y mitigar dichas consecuencias

En las Directrices 01/2021 sobre ejemplos relativos a la notificación de brechas de datos personales adoptadas por el Comité Europeo de Protección de Datos el 14 de enero de 2021 se pueden encontrar algunos ejemplos de brechas de datos personales.

Un incidente de seguridad que **no ha afectado a datos personales o tratamientos de datos personales no** es una **brecha de datos personales**, dado que no podría producir daños sobre los derechos y libertades de las personas físicas cuyos datos son objeto del tratamiento, independientemente de otros perjuicios que pueda producir al responsable o encargado del tratamiento.

B. PROCESO DE GESTIÓN DE INCIDENTES

En todo tratamiento debe determinarse el riesgo que para los derechos y libertades puede suponer que se materialice una brecha de datos personales, es decir un tratamiento no legítimo o accidental sobre los datos. Esta es una tarea previa a la materialización de una

[4] brechas

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.

Además, se hace referencia a la necesidad de gestionar los posibles errores, debilidades, vulnerabilidades o ataques que se pudieran derivar de las distintas medidas técnicas y organizativas que implementan estrategias de protección de datos por defecto, desde el diseño u otras garantías (los sistemas de garantías) como:

- La seudonimización y el cifrado de datos personales ya señalados
- Procesos de anonimización
- Procesos de desvinculación de datos
- Ejecución de la eliminación de datos
- Tratamientos federados
- Paneles de preferencias

La gestión de incidentes es un proceso que, con mayor o menor grado de madurez, ya debe formar parte de la cultura de responsables y encargados de tratamientos[5]. Esta gestión de incidentes debe actualizarse, si no lo está ya, e incorporar los procedimientos para responder a las obligaciones que se desprenden del RGPD. Concretamente para el caso de esta guía, de los artículos 33 y 34 en cuanto a la notificación de la brecha a la Autoridad de Control y la comunicación a los afectados.

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

[5] Guía de Seguridad de las TIC CCN-STIC 817 – CCN-CERT
Incident Handling Management – ENISA

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.

No existe un modelo estándar de registro de incidentes. Cada organización debe utilizar el que considere más conveniente y que se integre en sus sistemas de gestión. En cualquier caso, mediante la herramienta FACILITA-EMPRENDE, disponible en la web de esta Agencia, se puede obtener un modelo de registro de incidentes para empresas dentro del ámbito de aplicación de la herramienta, que puede hacerse extensivo a otras organizaciones.

Como parte del proceso de gestión de incidentes se debe incorporar un procedimiento de notificación de brechas de datos personales que concrete todos los aspectos fundamentales que son necesarios para la correcta aplicación del RGPD. Por ejemplo, se ha de definir cuál es la Autoridad de Control a la que se debe notificar, qué sucesos motivarán la ejecución del procedimiento, qué persona debe realizar la notificación a la Autoridad de Control, aprovisionar los medios técnicos o de cualquier índole necesarios para notificar, asegurar el cumplimiento de los plazos, y en su caso establecer el procedimiento de autorizaciones que se requiera para notificar conforme a las instrucciones del responsable de tratamiento.

De la misma manera, se debe establecer un procedimiento para la comunicación a los afectados en el que se concreten aspectos como quién realizará la comunicación, cómo se comunicará a los afectados, los canales y medios con los que se realizará la comunicación y en general los detalles que permitan comunicar de forma efectiva.

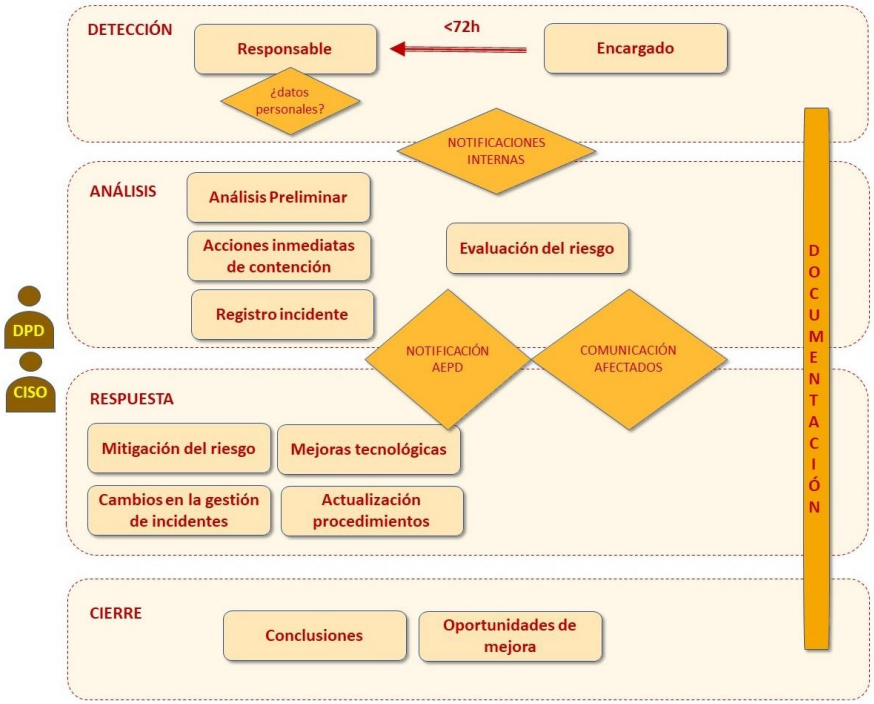


Figura 1- Proceso de gestión de brechas de datos personales.

Ambos procedimientos han de estar definidos antes de que se materialice una brecha. Pueden considerase como procedimientos independientes, o bien un procedimiento único que cubra ambos aspectos, o, lo que es más recomendable, estar integrado dentro de los procedimientos de gestión de incidentes de seguridad de la organización.

C. FIGURAS IMPLICADAS

Detectada una brecha de datos personales en la organización, y a efectos de una correcta y eficaz gestión, será necesaria la colaboración y actuación de distintas figuras. Para que cada una de las personas implicadas pueda actuar de forma efectiva, previamente deben haberse establecidos los procedimientos y articulado los medios necesarios.

A continuación, se expone brevemente las funciones y responsabilidades de las figuras implicadas:

Responsable de tratamiento[6]: 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.

Igualmente, podrá contar con el asesoramiento de expertos en materia de seguridad, como el CISO[7] de la organización, o los servicios informáticos propios o que pueda tener subcontratados. Así mismo, podrá delegar la gestión de la brecha de datos personales en los encargados de tratamiento, como por ejemplo servicios informáticos ajenos.

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[8]: 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.

El encargado de tratamiento tiene la obligación de 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.

---

[6] RGPD art.4.7 «responsable del tratamiento» o «responsable»: la persona física o jurídica, autoridad pública, servicio u otro organismo que, solo o junto con otros, determine los fines y medios del tratamiento; si el Derecho de la Unión o de los Estados miembros determina los fines y medios del tratamiento, el responsable del tratamiento o los criterios específicos para su nombramiento podrá establecerlos el Derecho de la Unión o de los Estados miembros;

[7] Chief Information Security Officer

[8] RGPD art.4.8 «encargado del tratamiento» o «encargado»: la persona física o jurídica, autoridad pública, servicio u otro organismo que trate datos personales por cuenta del responsable del tratamiento;

La información al responsable de tratamiento debe incluir los detalles necesarios para que el responsable pueda cumplir con sus obligaciones, en particular la de evaluar el riesgo de la brecha de datos personales y en su caso notificarla a la Autoridad de Control y/o comunicar a los afectados.

Delegado de protección de datos (DPD)[9]:

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 RGPD encomienda al DPD la función de informar y asesorar al responsable o encargado de las obligaciones que les incumben, incluidas las relativas a la gestión y notificación de las brechas de datos personales, así como cooperar con la Autoridad de Control y actuar como punto de contacto de la Autoridad de Control para cuestiones relativas al tratamiento.

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.

El responsable de tratamiento, y encargado de tratamiento en su caso, debe dotar al DPD de los medios necesarios y la información para el ejercicio de sus funciones.

No obstante, la responsabilidad recae ineludiblemente en el responsable y encargado de tratamiento respecto de las obligaciones de cada uno de ellos.

[9] RGPD art 39.2 el delegado de protección de datos desempeñará sus funciones prestando la debida atención a los riesgos asociados a las operaciones de tratamiento, teniendo en cuenta la naturaleza, el alcance, el contexto y fines del tratamiento.

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

D. DIAGRAMA DE FLUJO DEL PROCESO DE BRECHAS DE DATOS PERSONALES

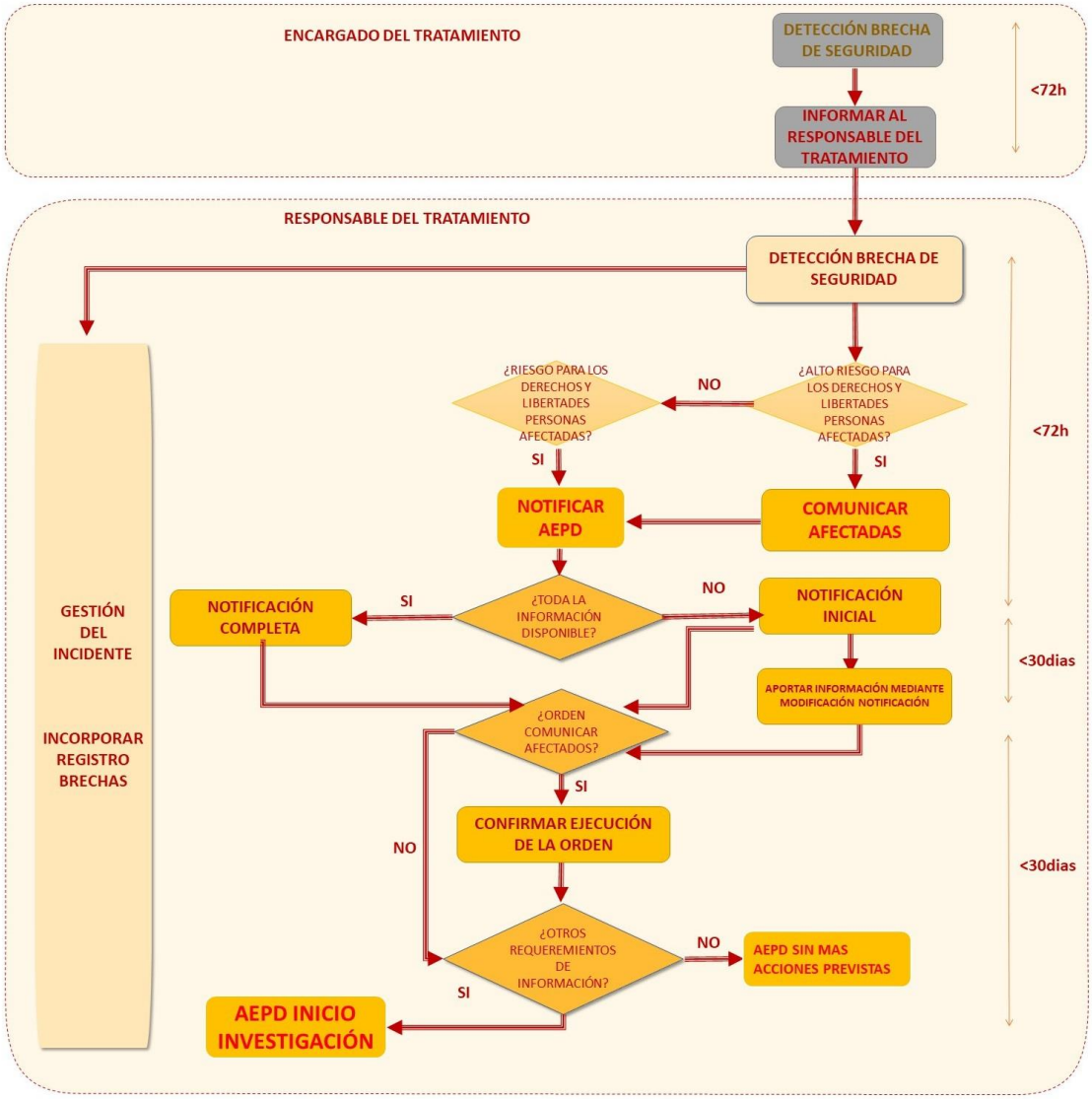


Figura 2- Diagrama resumen de notificación a la AEPD.

III. MARCO NORMATIVO

Sin perjuicio de otras obligaciones normativas que puedan afectar a los responsables, esta guía se refiere únicamente a brechas de datos personales. A continuación, se incluye una relación con las normas, guías y recomendaciones que contemplan la obligación de la gestión y notificación de brechas de datos personales en la fecha de publicación de esta guía.

A. EUROPEO

- 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) - Artículos 33 y 34.
- DIRECTIVA (UE) 2016/680 DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 27 de abril de 2016 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 y por la que se deroga la Decisión Marco 2008/977/JAI del Consejo. – Artículos 30 y 31.

B. NACIONAL

- Real Decreto 43/2021, de 26 de enero, por el que se desarrolla el Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información.
- Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información (NIS).
- Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (LOPDGDD)
- Real Decreto 704/2011, de 20 de mayo, por el que se aprueba el Reglamento de Protección de las Infraestructuras Críticas.
- Ley 8/2011, de 28 de abril, por la que se establecen medidas para la protección de las infraestructuras críticas.
- Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica - Artículos 24, 36 y Disposición Adicional cuarta.

C. SECTORIAL

- Ley 9/2014, de 9 de mayo, General de Telecomunicaciones - Artículos 41 y 44
- REGLAMENTO (UE) 611/2013 de la Comisión, de 24 de junio de 2013, relativo a las medidas aplicables a la notificación de casos de brechas de datos personales en el marco de la Directiva 2002/58/CE del Parlamento Europeo y del Consejo sobre la privacidad y las comunicaciones electrónicas.
- Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico, que regula la Gestión de incidentes de ciberseguridad que afecten a la red de Internet. Disposición adicional novena.

D. GUÍAS Y ESTÁNDARES

- Guidelines 01/2021 on Examples regarding Data Breach Notification[10] adoptadas el 14 de enero de 2021.
- Directrices sobre notificación de brechas de datos personales de acuerdo con el Reglamento 2016/679 (WP250), adoptadas el 3 de octubre de 2017 por el Grupo de Trabajo del Artículo 29 y refrendado en la primera reunión del Comité Europeo de Protección de Datos.
- UNE-EN ISO/IEC 27001:2017. Tecnología de la información. Técnicas de seguridad. Sistemas de Gestión de la Seguridad de la Información. Requisitos.
- UNE-EN ISO/IEC 27002:2017. Tecnología de la Información. Técnicas de seguridad. Código de prácticas para los controles de seguridad de la información
- ISO/IEC 29100:2011 Information technology – Security Techniques – Privacy framework
- Guía Nacional de notificación y gestión de ciberincidentes. DSN.
- Guía CCN-STIC 817 de Gestión de ciberincidentes en el ámbito del ENS. CCN-CERT

[10] A fecha de publicación de esta guía el documento sigue en fase de consulta pública.

IV. 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.

A. CUÁNDO NOTIFICAR

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. En su caso, debe realizarse sin dilación y a más tardar en las 72 horas[11] siguientes, computando también las horas trascurridas durante fines de semana y festivos.

El criterio para determinar si un incidente ha producido "una brecha de datos personales" se recoge en el propio RGPD: "toda violación 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 es obligatorio notificar todas las brechas de datos personales, dado que el RGPD prevé una excepción a esta obligación cuando, conforme al principio de responsabilidad proactiva, el responsable pueda garantizar que es improbable[12] que la brecha de datos personales entrañe un riesgo[13] para los derechos y las libertades de las personas físicas.

Factores para evaluar el riesgo de una brecha:
Tipo de brecha de datos personales
Naturaleza, carácter sensible y el volumen de datos personales
Facilidad de identificación de las personas
Gravedad de las consecuencias para los derechos y libertades de las personas
Características particulares del responsable de tratamiento
Número de personas afectadas
Consideraciones generales

En el anexo B de las directrices WP250 se pueden encontrar algunos ejemplos sobre la valoración de la necesidad de notificar a la Autoridad de Control. En las Directrices 01/2021 sobre ejemplos relativos a la notificación de brechas de datos personales se expone una colección muy completa de ejemplos.

[11] Véase el Reglamento n.º 1182/71 por el que se determinan las normas aplicables a los plazos, fechas y términos

[12] WP250: Cuando la violación se refiera a datos personales que revelen el origen étnico o racial, las opiniones políticas, la religión o las creencias filosóficas, la militancia en un sindicato, o que incluyan datos genéticos, datos relativos a la salud o datos sobre la vida sexual, o las condenas e infracciones penales o medidas de seguridad conexas, se considerará probable que tales daños y perjuicios se produzcan.

[13] WP250: … inmediatamente después de tener conocimiento de una violación, es de vital importancia que el responsable del tratamiento no trate solo de contener el incidente, sino que también evalúe el riesgo que podría derivarse del mismo.

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[14]. 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[15] 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, salvo en algunos supuestos, expuestos y determinados en esta guía. El lenguaje será claro y sencillo, de forma concisa y transparente. Puede obtener más detalle sobre esta obligación en el apartado VI *"Comunicación de una brecha de datos personales a los interesados"*.

La notificación de una brecha de datos personales a la Autoridad de Control conforme al artículo 33 del RGPD, además de una obligación, es un ejercicio de responsabilidad proactiva. Por contra, si lo que se desea es denunciar o reclamar ante una posible vulneración de la normativa de protección de datos por parte de un tercero, empleado, exempleado u otros, o desea comunicar una brecha de datos personales de la que ha sido conocedor o afectado, el canal a utilizar es el formulario para presentación de reclamaciones de la Sede Electrónica de la Agencia.

El parámetro determinante para **notificar** una brecha de datos personales a la **Autoridad de Control** o **comunicarla a los afectados** es el nivel de riesgo. No cualquier tipo de riesgo o un riesgo para la organización, sino específicamente el **riesgo para los derechos y libertades de las personas físicas** afectadas por la brecha.

B. PLAZOS PARA NOTIFICAR

El RGPD establece que el responsable de tratamiento notificará las brechas de datos personales a la Autoridad de Control sin dilación indebida y a más tardar dentro de las 72 horas desde que se tenga constancia de la brecha de datos personales.

El plazo de 72 horas[16] 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. Para la notificación del encargado al responsable, el RGPD no establece un plazo de tiempo concreto y se limita a indicar que debe realizarse sin dilación indebida.

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

[14] WP250: No es necesario que el encargado del tratamiento evalúe la probabilidad de riesgo derivado de la brecha de seguridad antes de informar al responsable del tratamiento, sino que esta evaluación le corresponde al responsable de tratamiento.
[15] WP250: Cabe señalar que la evaluación del riesgo para los derechos y las libertades de las personas como resultado de una violación tiene un enfoque diferente del riesgo considerado en una EIPD. En la EIPD se consideran tanto los riesgos de que el tratamiento de datos se lleve a cabo según lo previsto, como los riesgos en caso de que se produzca una violación. A la hora de considerar una posible violación, en términos generales, se examina la probabilidad de que esto ocurra y los daños y perjuicios que podrían derivarse para el interesado; en otras palabras, se trata de la evaluación de un acontecimiento hipotético. En caso de violación real, el hecho ya se ha producido, por lo que la atención se centra exclusivamente en el riesgo derivado del impacto de la violación en las personas.
[16] Véase el Reglamento n.º 1182/71 por el que se determinan las normas aplicables a los plazos, fechas y términos.

responsables y encargados deben concretar este plazo, incluso reflejarlo en el contrato de encargo de tratamiento[17]. En cualquier caso, dicho plazo debería establecerse en función del riesgo de los tratamientos llevados a cabo por el encargado de tratamiento[18], 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.

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. 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 en esta guía deben entenderse como días hábiles[19].

C. AUTORIDAD DE CONTROL A LA QUE SE DEBE NOTIFICAR

Con carácter general, en el ámbito privado[20], 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[21] 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.

Los responsables de tratamiento con establecimiento principal en otro Estado Miembro de la Unión Europea, o que no tengan un establecimiento en la Unión pero hayan nombrado un representante en otro Estado Miembro, deberán notificar a la Autoridad de Control de dicho Estado Miembro. En tal caso, los establecimientos no principales situados en España que hayan sufrido una brecha de datos personales han de incorporar en su procedimiento de gestión de brechas los mecanismos adecuados para que el establecimiento principal

[17] WP250: En contrato entre el responsable y el encargado debe especificar el modo en que deben cumplirse los requisitos expresados en el artículo 33, apartado 2, además de otras disposiciones del RGPD. Esto puede incluir requisitos de notificación temprana por parte del encargado de tratamiento que a su vez apoyen la obligación del responsable del tratamiento de informar a la autoridad de control en un plazo de 72h.

[18] WP250: El GT29 recomienda que el encargado del tratamiento lo notifique sin demora al responsable de tratamiento, u facilite más información de forma gradual, a medida que lleguen más detalles. Esto es importante para ayudar al responsable del tratamiento a cumplir el requisito de notificación a la autoridad de control en un plazo de 72h.

[19] Disposición adicional tercera de la LOPDGDD.

[20] A excepción de las entidades en el ámbito de las competencias concretas de cada Autoridad de Control Autonómica.

[21] Establecimiento desde el que se determinen los fines y medios del tratamiento de datos personales.

pueda realizar la notificación correspondiente ante la Autoridad de Control del Estado Miembro competente.

En el ámbito público, con carácter general las AAPP deben notificar las brechas de datos personales a la Agencia Española de Protección de Datos a excepción del caso de las Comunidades Autónomas de Andalucía, Cataluña y País Vasco, cuando las brechas de datos personales se produzcan en entidades del sector público bajo su competencia, la Autoridad de Control a la que notificar será:

- En el caso de Cataluña: la Autoridad Catalana de Protección de Datos (https://apdcat.gencat.cat/es/inici/) a través de su sede electrónica.
- En el caso del País Vasco: la Agencia Vasca de Protección de Datos mediante el correo electrónico avpd@avpd.eus
- En el caso de Andalucía: el Consejo de Transparencia y Protección de Datos de Andalucía a través de su ventanilla electrónica (https://www.ctpdandalucia.es/ventanilla-electronica)

En todos los casos en los que la Autoridad de Control competente no es la AEPD, deberán observarse las recomendaciones y directrices específicas de cada autoridad.

Autoridad Competente	Sector	Ámbito
Agencia Española de Protección de Datos	Privado	Su único establecimiento está en España El establecimiento principal está en España Sin establecimientos en la UE, tiene representante en España Si no está en los casos anteriores, y la brecha cuenta con afectados en España
	Público	Todo el territorio nacional (Ámbito Estatal, Autonómico y Local) excepto lo que sea competencia de las Autoridades Autonómicas de Cataluña, País Vasco o Andalucía
Autoridad Catalana de Protección de Datos	Público	Comunidad Autónoma de Cataluña y Administración Local
Agencia Vasca de Protección de Datos	Público	Comunidad Autónoma del País Vasco y Administración Local
Consejo de Transparencia y Protección de Datos de Andalucía	Público	Comunidad Autónoma de Andalucía y Administración Local

D. QUIÉN DEBE NOTIFICAR

Cuando un responsable de tratamiento tenga la constancia de que una brecha de datos personales pueda suponer un riesgo para los derechos y libertades de las personas físicas, deberá notificar ante la correspondiente autoridad competente de Protección de Datos.

La notificación de una brecha de datos personales a la Autoridad de Control conforme al artículo 33 del RGPD corresponde al responsable del tratamiento. El responsable puede autorizar una persona física, representante o entidad que ejerza su representación para que realice la notificación de la brecha de datos personales ante la Autoridad de Control.

El encargado del tratamiento que ha sido objeto de la brecha de datos personales únicamente podrá notificar en nombre del responsable si así lo tiene establecido en un contrato o vínculo legal de similar índole. En todo caso, el responsable de tratamiento debe ser previamente informado sobre la ocurrencia de la brecha de datos personales y todos los detalles relevantes como establece el artículo 33.2 del RGPD.

En su caso, el encargado de tratamiento deberá realizar una notificación de brecha de datos personales por cada responsable de tratamiento afectado, dado que una brecha en un encargado de tratamiento puede afectar de forma muy distinta a varios responsables de tratamiento.

Únicamente en casos de brechas de datos personales ocurridas en un encargado de tratamiento y que hayan afectado por igual a los derechos y libertades de los interesados[22] de diferentes responsables de tratamiento a los que presta servicio, el encargado podrá realizar una única notificación de brecha de datos personales relacionando a todos los responsables cuyos tratamientos se han visto afectados[23].

En el caso de grandes empresas y organizaciones, si previamente no estaba previsto dentro del proceso de gestión de incidentes, es conveniente formalizar un procedimiento de notificación, en el que se establezca el proceso a seguir para notificar las brechas de datos personales a las Autoridades de Control y, en su caso, comunicar a los afectados. Dicho procedimiento debe describir la manera en la que se comunica, e identificar al representante dentro de la organización que actuará como punto único a efectos de notificación ante la Autoridad de Control. Este rol podrá ser desempeñado por el Delegado de Protección de Datos en el caso de que lo hubiera. La organización debe hacer los esfuerzos necesarios para que dicho procedimiento sea conocido por todos aquellos que deban participar.

En caso de empresas pequeñas y con tratamientos de bajo riesgo la persona que realice la notificación, cuando sea necesaria, podrá ser el administrador único, apoderado, o la persona física o jurídica que éste designe como representante legal o para ser el punto de contacto con la Autoridad de Control.

El procedimiento de notificaciones de brechas de datos personales tiene como finalidad establecer un criterio común para todos los tratamientos de datos personales que consten en el registro de actividades de tratamiento de una organización y garantizar que se dispone de los medios para notificar en plazo.

La notificación de brechas de datos personales no es un trámite dirigido a terceros ajenos al responsable de tratamiento, ni a ciudadanos o afectados por una brecha de datos personales. Para ello se disponen de otros procedimientos en la misma Sede Electrónica para poner en conocimiento de la AEPD posibles vulneraciones de la normativa de protección de datos, en particular de posibles incumplimientos del RGPD y/o LOPDGDD.

En el caso de que el responsable haga uso de encargados de tratamiento, ha de quedar claramente definido en el **contrato de encargo** quién ha de realizar las **notificaciones** o

[22] Mismas categorías de datos, mismas categorías de interesados, mismas medidas de seguridad previas, mismas acciones tomadas, etc.

[23] En la Sede Electrónica de la AEPD el formulario permite a un encargado notificar una brecha que afecte hasta a 10 responsables de tratamiento por igual.

comunicaciones. La elección, en aras de la **responsabilidad proactiva**, debe considerar el mejor modo de defender los **derechos y libertades de los interesados**.

El responsable ha de tener **diligencia** en seleccionar encargados de tratamiento que sean capaces de darle el adecuado soporte en la gestión de las brechas de datos.

E. QUÉ SE DEBE 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."

Para facilitar el cumplimiento de estos requisitos en el contenido de las notificaciones de brechas de datos personales, la AEPD ha elaborado un formulario en línea y lo pone a disposición de los responsables de tratamiento a través de su Sede Electrónica.

El formulario pretende dar certidumbre a los responsables de tratamiento respecto a la información que se debe facilitar a la AEPD para notificar una brecha de datos personales, evitando el exceso de información o notificaciones sin la información suficiente. Esto permite a los responsables de tratamiento optimizar los esfuerzos dedicados a la notificación de brecha de datos personales, evitando malgastar recursos en generar notificaciones con información excesiva e innecesaria en muchos casos. Hay que tener en cuenta que una notificación que resultase defectuosa podría incurrir en una vulneración de la normativa de protección de datos.

Notificar la brecha mediante el formulario en sede electrónica no requiere que se adjunte documentación adicional sobre la misma. En su caso, la AEPD requerirá al responsable toda aquella información adicional necesaria y el responsable la podrá remitir como respuesta a esos requerimientos junto con la información adicional que considere relevante.

Notificación brecha de datos personales:
Sobre el tratamiento y el responsable
Intencionalidad y origen
Tipología
Categorías de datos y perfil de los afectados
Consecuencias
Resumen de la brecha
Implicaciones transfronterizas
Información temporal y medios de detección
Medidas de seguridad preventivas
Acciones tomadas
Comunicación a los afectados

En el apartado VI de esta guía se muestra información detallada sobre el modelo de formulario, con aclaraciones y ejemplos para cumplimentarlo correctamente. A efectos exclusivamente informativos o de referencia, se proporciona un enlace al modelo en formato PDF[24].

F. CÓMO SE DEBE NOTIFICAR

El artículo 14.2 de la Ley 39/2015 de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas (en adelante LPACAP), establece la obligación de relacionarse con las Administraciones Públicas a través de medios electrónicos para las personas jurídicas, las entidades sin personalidad jurídica, así como quienes representen a los sujetos obligados a relacionarse electrónicamente con la Administración, entre otros.

En estos casos, si la Autoridad de Control competente es la AEPD, esta autoridad considera aceptable realizarla de forma telemática en el formulario de Notificación de brechas de datos personales de la Sede Electrónica de la Agencia. Para acceder al formulario es necesario disponer de un certificado electrónico reconocido, como el incorporado en el DNIe o los certificados de persona física o de representante expedidos por la Fábrica Nacional de Moneda y Timbre (FNMT).

Por tanto, el formulario de notificaciones de brechas de datos personales de la AEPD está exclusivamente dirigido a responsables de tratamiento, quienes tienen la obligación de notificar sus brechas de datos personales, a través de una persona física autorizada, representante o entidad que ejerza su representación.

Para acceder al formulario de notificación de brechas de datos personales es necesario estar en posesión de un certificado electrónico reconocido o sistemas Cl@ve permanente y PIN24H. Cuando el certificado electrónico utilizado sea un certificado electrónico de representación del responsable de tratamiento, quedará dicha representación automáticamente acreditada. Si no se dispone de un certificado de representación, podrá

[24] Este formulario en PDF únicamente puede ser utilizado para notificar una brecha de datos personales por aquellos responsables que no estén obligados a relacionarse con la Administración Pública por medios electrónicos.

adjuntarse opcionalmente un documento acreditativo de la representación o la AEPD podrá requerir a posteriori que se acredite dicha representación o la autorización del responsable para notificar la brecha de datos personales.

La acreditación de la representación del responsable por parte del solicitante, de ser necesaria, se llevará a cabo conforme al artículo 32.3 del Real Decreto 203/2021 de 30 de marzo en el que se aprueba el Reglamento de actuación y funcionamiento del sector público por medios electrónicos.

Las **notificaciones de brechas de datos personales** a la AEPD por los sujetos obligados en el artículo 14.2 de la Ley 39/2015 se deben realizar de forma **electrónica,** preferentemente usando el formulario de notificación de brechas de datos personales de la Sede Electrónica para garantizar una correcta ejecución de las obligaciones del artículo 33.3 del RGPD.

Quienes tienen la obligación de notificar, tienen también la **obligación de prever los medios** formales y materiales necesarios para poder notificar por esta vía en forma y plazo.

G. OBLIGACIONES DEL RESPONSABLE TRAS NOTIFICAR UNA BRECHA DE DATOS PERSONALES

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[25] 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.

La AEPD remite sus notificaciones y comunicaciones electrónicas a través del servicio compartido de gestión de Notificaciones *Notific@,* que envía las notificaciones a los sistemas *Carpeta Ciudadana* y *Dirección Electrónica Habilitada* del Ministerio de Política Territorial y Función Pública.

De acuerdo con lo previsto por el art. 43 de la citada LPACAP, se cumplirá la obligación de notificar con la puesta a disposición de la notificación en la sede electrónica o en la Dirección Electrónica Habilitada (DEH) única del responsable de tratamiento identificado en el formulario de notificación de brecha de datos personales. Se entiende que la notificación ha sido rechazada cuando hayan transcurrido diez días desde su puesta a disposición sin que se acceda a su contenido.

Una vez se realiza el envío, se entenderá que la notificación ha surtido efectos en la fecha de comparecencia en la que el responsable recoge la notificación. En caso de no recoger la notificación se entenderá igualmente que ha surtido efectos en la fecha en la que expire la notificación.

Para el caso de entidades de ámbito público, las comunicaciones y/o notificaciones también se dirigirán a la DEH de la entidad responsable de tratamiento identificada en el formulario de notificación.

Tras notificar una brecha de datos personales, el responsable de tratamiento puede recibir por parte de la AEPD diversas comunicaciones o notificaciones electrónicas, por ejemplo:

[25] Únicamente se utilizará notificación postal cuando el responsable de tratamiento no esté obligado a relacionarse con la Administración por medios electrónicos.

- **Comunicación** con información relativa al registro de la brecha de datos personales notificada.
- **Notificación** con un requerimiento de información adicional sobre la brecha de datos personales o el tratamiento de datos personales en cuestión en virtud de las funciones y potestades de esta Agencia a las que refiere el artículo 47 de la LOPDGDD así como el artículo 58 del RGPD.
- **Notificación** con una **orden para comunicar a los afectados** la brecha de datos personales en virtud del artículo 34.4 al considerar que el riesgo para los afectados es alto, en virtud de las funciones y potestades de esta Agencia a las que refiere el artículo 47 de la LOPDGDD así como el artículo 58 del RGPD.

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 confirmación a la AEPD deberá incluir los siguientes detalles:

- Contenido de la comunicación a los afectados.
- Fecha o periodo en el que se ha ejecutado la comunicación.
- Número de sujetos comunicados.
- Medio utilizado para comunicar a los afectados.
- Justificación para optar por una comunicación pública de las establecidas en el art. 34.3.c) del RGPD en su caso.

V. COMUNICACIÓN A LOS AFECTADOS

Los interesados afectados son las personas físicas cuyos datos personales se han visto afectados por una brecha comprometiendo la confidencialidad, integridad y/o disponibilidad de esos datos, y quienes pueden sufrir las consecuencias.

En todo caso, el proceso de gestión de brechas de datos personales establecido en la organización deberá incluir un procedimiento para llevar a cabo la comunicación de la brecha de datos personales a los interesados afectados, concretando la información contenida en los siguientes apartados, inclusive estableciendo los plazos concretos adecuados.

A. CUÁNDO COMUNICAR

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[26] la brecha de datos personales a los afectados sin dilación indebida.

Por tanto, tan pronto como el responsable de tratamiento tenga constancia de la brecha de datos personales deberá valorar el riesgo para las personas afectadas y determinar la necesidad de comunicar la brecha a los afectados. En caso de que el riesgo se determine como alto, la comunicación a los afectados deberá realizarse a la mayor brevedad posible.

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. Por ejemplo, mediante 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.

La herramienta Comunica-Brecha RGPD ofrece ayuda a los responsables de tratamiento para la toma de decisiones en cuanto a la obligación de comunicar una brecha de datos

[26] WP250: En algunos casos será obvio que, debido a la naturaleza de la brecha y a la gravedad del riesgo, el responsable de tratamiento deberá notificarlo sin dilación indebida a las personas afectadas. Por ejemplo, si existe una amenaza inmediata de usurpación de identidad, o si se revelan en línea categorías especiales de datos personales, el responsable del tratamiento debe actuar sin dilación indebida para contener la brecha y comunicarla a las personas afectadas.

personales a los afectados, quienes en cualquier caso deben documentar las decisiones adoptadas.

Si el responsable todavía no ha comunicado al afectado la brecha de datos personales considerando el alto riesgo potencial, la Autoridad de Control podrá exigirle:

- Realizar la comunicación a los afectados
- Que demuestre que cumple alguna de las condiciones anteriormente mencionadas para que la comunicación a los afectados no sea obligada.

En el anexo B de las directrices WP250 se pueden encontrar algunos ejemplos sobre la valoración de la necesidad de comunicar la brecha de datos personales a las personas afectadas. También en las Directrices 01/2021, sobre ejemplos relativos a la notificación de brechas de datos personales, se incluyen una serie de casos sobre cómo valorar la existencia de esa obligación.

B. PLAZOS PARA COMUNICAR

El RGPD no establece un plazo concreto para la comunicación a los afectados[27], pero sí indica que deberá realizarse sin dilación indebida.

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 particular, 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.

Cuando la comunicación a las personas afectadas se produzca como consecuencia de una orden emitida por la Agencia Española de Protección de Datos, 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.

C. QUIÉN DEBE COMUNICAR

La comunicación de una brecha de datos personales a las personas afectadas conforme al artículo 34 del RGPD corresponde al responsable del tratamiento. El responsable puede encomendar a un tercero en virtud de un contrato o vínculo legal, que actuará como encargado de tratamiento, para que realice la comunicación de la brecha de datos personales a los afectados.

El encargado del tratamiento que ha sido objeto de la brecha de datos personales únicamente podrá comunicar la brecha a los afectados si así lo tiene establecido en un contrato o vínculo legal con el responsable de tratamiento.

En todo caso, el responsable de tratamiento debe ser previamente informado sobre la ocurrencia de la brecha de datos personales y sobre todos los detalles relevantes como establece el artículo 33.2 del RGPD, pues le corresponde decidir sobre la necesidad de comunicar la brecha de datos personales a los afectados.

[27] WP250: En circunstancias excepcionales, esto podría ocurrir incluso antes de la notificación a la autoridad de control.

D. CÓMO Y QUÉ SE DEBE COMUNICAR

Conforme al artículo 34.2 del RGPD, la comunicación al interesado "describirá en un lenguaje claro y sencillo la naturaleza de la violación de la seguridad de los datos personales y contendrá como mínimo la información y las medidas a que se refiere el artículo 33, apartado 3, letras b), c) y d)".

Por tanto, 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.

Cuando la comunicación a los afectados suponga un esfuerzo desproporcionado con relación a los riesgos para los derechos y libertades que están sufriendo los interesados, se podrá realizar una comunicación indirecta a través de avisos públicos. Esto podrían ser, por ejemplo, sitios web como blogs corporativos, o comunicados de prensa. Estas técnicas podrían emplearse, también, cuando no sea posible contactar con las personas afectadas (por ejemplo, porque ha habido pérdida de datos e imposibilidad para recuperarlos, o se desconocen los datos de contacto, o estos no están actualizados) y esté debidamente justificado.

En tal caso, el aviso público ocupará un lugar destacado, de forma que en ningún caso pueda pasar desapercibidos.

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.

La **comunicación a los afectados** debe realizarse en un **lenguaje claro y sencillo**, respetar el **contenido mínimo** establecido en el art. 34 del RGPD y dirigirse específicamente a **aquellas personas para las que exista un riesgo alto de que sus derechos y libertades pueden verse dañados**.

VI. CONTENIDO DE LAS NOTIFICACIONES DE BRECHAS DE DATOS PERSONALES A LA AEPD

En los siguientes apartados se detalla la información relevante para la notificación de brechas de datos personales en el formulario de la AEPD.

A. CARÁCTER DE LA NOTIFICACIÓN

A través del formulario en la Sede Electrónica de la AEPD se puede realizar dos tipos de notificaciones de brecha de datos personales:

- **Nueva notificación de brecha de datos personales:** Notificar una brecha de datos personales de la que no se ha informado previamente a la AEPD. Puede ser una notificación COMPLETA cuando en el momento de la notificación se disponga de toda la información necesaria, o una notificación INICIAL cuando en el momento de la notificación no se disponga de toda la información necesaria y se tenga previsto aportar información adicional.

- **Modificación de una brecha de datos personales ya notificada:** Cuando se haya notificado previamente una brecha de datos personales de manera inicial, en el plazo 30 días se podrá realizar una modificación sobre esta información para completar la notificación de la brecha de datos personales. Para ello, se debe facilitar el número de registro de la notificación que se desea modificar y la fecha en la que se realizó. De forma general, está prevista una única modificación de una notificación de brecha de datos personales realizada previamente, y dentro del plazo de 30 días desde la notificación inicial.

B. INFORMACIÓN GENERAL SOBRE EL TRATAMIENTO

Se trata de información de carácter general sobre el tratamiento de datos personales que se ha visto afectado por la brecha de datos personales y el responsable de tratamiento que permite estimar el riesgo inherente al tratamiento, y que el responsable de tratamiento debe conocer a priori:

Sobre el tratamiento:

- Duración del tratamiento, permitiendo distinguir entre tratamientos puntuales y tratamientos de larga duración.
- Número total de personas cuyos datos forman parte del tratamiento afectado por la brecha de datos personales[28], aunque no necesariamente todos se hayan visto afectados por la brecha de datos personales.
- Ámbito geográfico del tratamiento, si se realiza sobre personas de la misma localidad, provincia, si es a nivel nacional y/o de otro Estado Miembro, o a nivel mundial.

C. INTENCIONALIDAD Y ORIGEN

Intencionalidad del incidente que ha causado la brecha:

- Intencionado – Ejemplo: Ataque de un ciberdelincuente de diverso tipo, robo de un dispositivo.

[28] Se indicará el número total de personas sobre las que se tratan datos personales para el tratamiento específico en cuestión, aunque el número de personas afectadas por la brecha de datos personales sea menor.

- Accidental o fortuito – Ejemplo: Envío de datos personales por error a destinatario incorrecto, pérdida de dispositivo, publicación no intencionada.

Origen o ámbito del incidente:

- Interno: Personal o sistemas bajo el control del responsable de tratamiento – Ejemplo: envío de datos personales a encargado de tratamiento incorrecto o extravío de dispositivo.
- Interno: Personal o sistemas bajo el control del encargado de tratamiento – Ejemplo: envío de documentación a destinatarios incorrectos, incidencia técnica en sistemas de información.
- Externo: Otros, ajenos al responsable y encargado de tratamiento – Ejemplo: ciberataque o robo de dispositivos.

Sucesos que han originado la brecha de datos personales: Independientemente de las consecuencias y tipología de la brecha de datos personales, es necesario identificar el suceso que desencadena el incidente para determinar las causas, evaluar las consecuencias de la brecha y tomar medidas que impidan un suceso similar.

En el formulario de notificaciones de brechas de datos personales se consideran los sucesos de la tabla que se muestra a continuación. En la misma tabla se indica la dimensión de seguridad potencialmente afectada en cada uno de los casos. No se pretende significar que cada uno de estos sucesos suponga automáticamente la afectación de las dimensiones marcadas, sino que potencialmente podría verse afectada y el responsable de tratamiento es quien debe determinar si efectivamente así ha sido. Para más detalle sobre el significado de cada una de estas dimensiones, consulte el siguiente apartado.

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 / secuestro 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 en Internet	X	X	X
Incidencia técnica	X	X	X
Modificación no autorizada de datos			X
Datos personales mostrados al individuo incorrecto	X		

Ejemplo: En un ciberincidente de ransomware que afecta a los datos personales de los clientes de una organización la dimensión de seguridad afectada sería la disponibilidad. Sin embargo, si no se puede descartar que se haya producido también una exfiltración de información, también se vería afectada la confidencialidad de los datos.

Ejemplo: En el caso de una brecha de datos personales causada por una incidencia técnica en un sistema, potencialmente se podría ver afectada cualquiera de las dimensiones de la seguridad. Es necesario determinar con certeza en función de las circunstancias concretas qué dimensión/es se han visto realmente afectadas.

D. TIPOLOGÍA

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. 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: En brechas de confidencialidad 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: En brechas de confidencialidad 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. Por ejemplo, incluye casos de cifrado de datos personales o de los sistemas de información causado por malware de tipo ransomware, pérdida de documentación en papel con datos personales o la imposibilidad de acceder a un almacenamiento de datos (acceso físico o lógico).

Para el responsable del 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. Para ello, los responsables de tratamiento deben establecer estrategias y procedimientos de recuperación ante situaciones de este tipo, incluyendo procedimientos de copia de seguridad, recuperación ante incidentes y estrategias de gobernanza de los datos.

Ejemplo: En brechas de disponibilidad causadas por malware tipo ransomware en las que el responsable de tratamiento 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 de disponibilidad 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 organización la información relativa a los datos bancarios de los empleados que se utilizan para el pago de las nóminas, o un alumno modifica las calificaciones en la base de datos de un centro educativo.

Cuando se producen brechas de datos personales de integridad el responsable 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 el responsable 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: Los responsables podrán 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.

E. CATEGORÍAS DE DATOS Y PERFIL DE 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.

En cuanto a las categorías de datos personales afectadas, en la notificación a la AEPD se consideran las siguientes:

Categorías de datos	Significado
Datos básicos	Nombre, apellidos o la fecha de nacimiento de los afectados
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 ubicación de la persona en un determinado momento o durante un periodo de tiempo)	Datos de posicionamiento, coordenadas o direcciones habituales (no residencia) de los afectados
Medios de pago (números de tarjeta o cuenta bancaria)	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

Habitualmente, las organizaciones realizan tratamientos de datos personales de distintas características en función del perfil de las personas físicas. Las organizaciones no realizan los mismos tratamientos a los datos personales de sus clientes que a los de sus empleados, ni siquiera tratarán las mismas categorías de datos personales. El nivel de riesgo para los derechos y libertades de las personas afectadas puede ser distinto en función del perfil, y requerir distintas medidas de mitigación.

Si se determina que el riesgo de una brecha de datos personales es, por ejemplo, alto para los empleados, pero bajo para los clientes, el responsable de tratamiento podría optar por comunicar la brecha de datos personales de acuerdo con el art.34 el RGPD únicamente a sus empleados, por ser quienes pueden sufrir las consecuencias con severidad alta.

> *Ejemplo: sea un ciberincidente en el que se hayan visto comprometidas las credenciales de acceso de un empleado. Esto ha permitido, además del acceso a los datos del empleado, el borrado de información básica de una decena de clientes que, sin embargo, es recuperable de una copia de respaldo. El responsable se encuentra ante una brecha de datos personales que afecta a la disponibilidad[29] de datos básicos de clientes y confidencialidad de datos del empleado. Los riesgos son distintos para cada uno de estos perfiles y se ha de dar una respuesta distinta a cada uno de ellos.*

En cuanto a los perfiles de las personas físicas afectadas, se pueden considerar los siguientes:

Perfiles de las personas físicas afectadas
Clientes / ciudadanos
Estudiantes / alumnos
Usuarios
Pacientes
Suscriptores / potenciales clientes
Afiliados / asociados
Fuerzas y Cuerpos de Seguridad del Estado
Empleados
Otros

Un aspecto importante a tener en cuenta como agravante del riesgo potencial es si el tratamiento que ha sufrido la brecha de datos personales se realiza sobre datos de personas

[29] Cuando el responsable puede garantizar que la confidencialidad de los datos de los clientes no se ha visto afectada.

que pertenecen a un colectivo especialmente vulnerable. Estos son: menores de edad, supervivientes de violencia de género, de acoso o situaciones similares. Este aspecto es particularmente importante en brechas que afectan a la confidencialidad, y cuando los datos afectados o las circunstancias de la brecha de datos personales permiten identificar a las personas como pertenecientes a dichos colectivos.

> *Ejemplo: Una brecha de datos personales resulta en la exfiltración de una base de datos con datos identificativos y de contacto de 500 personas. A priori, los datos exfiltrados no permiten identificar a las personas como pertenecientes a ningún colectivo concreto, pero si la organización afectada por la brecha es una entidad colaboradora de adopción internacional, presumiblemente se pueden haber filtrado datos de menores o de personas en situación de vulnerabilidad. Las características del responsable de tratamiento deben ser consideradas para valorar el riesgo para las personas afectadas.*

> *Ejemplo: Una brecha de datos personales producida por el robo de los ordenadores portátiles en un organismo de una Administración Pública tendrá mayor riesgo si realiza tratamientos de datos sobre minorías en riesgo de exclusión y no ha adoptado medidas de seguridad acordes, como en este caso pueda ser el cifrado de los dispositivos, en lugar de contar únicamente con acceso por contraseña al dispositivo.*

El responsable de tratamiento debe determinar, al menos de forma aproximada, el número de personas cuyos datos personales se han visto afectados por la brecha de datos personales. Es necesario indicar un número mayor que 0.

El **número de personas afectadas** se refiere al número de **personas físicas** cuyos **derechos o libertades** podrían verse **dañados** como consecuencia de una **brecha de datos personales**, por ejemplo, por el **tratamiento ilícito o no autorizado** que se pueda producir de sus datos personales, la **imposibilidad de acceder a un servicio** o en definitiva la **pérdida de control** sobre sus datos personales.

No contabilizan personas jurídicas (u otras organizaciones) que también podrían haberse visto afectadas, en tanto que el concepto de dato personal atañe exclusivamente a personas físicas.

Si tiene la certeza de que los datos personales de un tratamiento pueden haberse visto afectados, pero desconoce el número exacto de afectados, se indicará aproximadamente o en último extremo el número total de personas sobre las que se tratan datos.

F. 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[30], 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

[30] Especialmente graves cuando afecta a derechos fundamentales

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[31] 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

En el caso de una brecha de datos personales la severidad para las personas afectadas debe evaluarse con una metodología similar a la empleada en la gestión de riesgo. Sin embargo, se trata de una evaluación mucho más específica en función de las circunstancias concretas de la brecha de datos personales que se ha producido y la efectividad de las medidas tomadas para reducir o eliminar el riesgo[32].

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:

[31] WP250: al evaluar el riesgo para las personas derivado de una violación, el responsable del tratamiento debe tener en cuenta las circunstancias específicas de la violación, incluida la gravedad del impacto potencial y la probabilidad de que esto ocurra.

[32] WP250: Cabe señalar que la evaluación del riesgo para los derechos y las libertades de las personas como resultado de una violación tiene un enfoque diferente del riesgo considerado en una EIPD. En la EIPD se consideran tanto los riesgos de que el tratamiento de datos se lleve a cabo según lo previsto, como los riesgos en caso de que se produzca una violación. A la hora de considerar una posible violación, en términos generales, se examina la probabilidad de que esto ocurra y los daños y perjuicios que podrían derivarse para el interesado; en otras palabras, se trata de la evaluación de un acontecimiento hipotético. En caso de violación real, el hecho ya se ha producido, por lo que la atención se centra exclusivamente en el riesgo derivado del impacto de la violación en las personas.

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.)

En cuanto a la probabilidad, no se trata de determinar la probabilidad de que la brecha de datos personales se materialice, porque obviamente en esta situación la brecha ya se habría materializado, sino determinar si existe 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 para evitar que el daño se materialice.

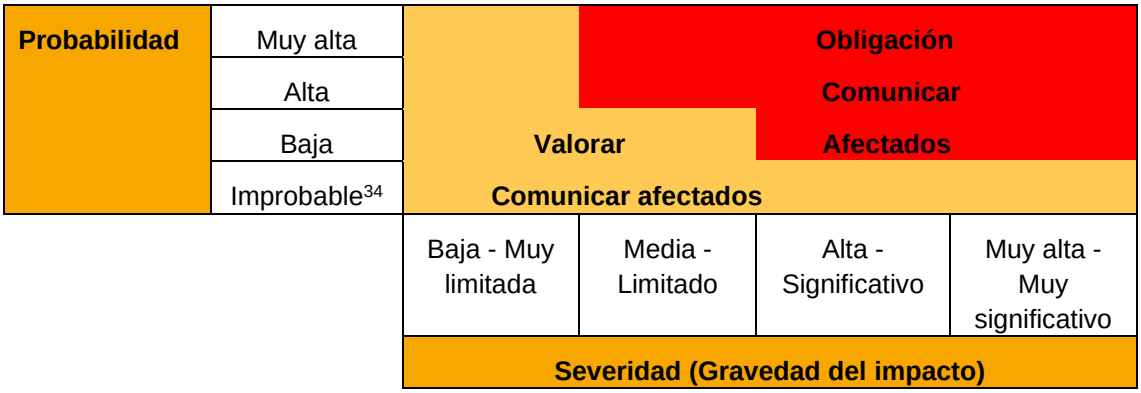
Puede ocurrir que el responsable de tratamiento ya tenga conocimiento de que se ha materializado un daño concreto sobre una persona afectada, en cuyo caso ya no sería necesario determinar un nivel de probabilidad porque se tiene la certeza de que ya ha ocurrido.

En caso de no haberse materializado el daño, se deberá estimar esta probabilidad. 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 las personas afectadas conforme al artículo 34 del RGPD, excepto si puede garantizar que no existe probabilidad de que se materialice el daño[33].

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.

[33] Artículo 34.3.b del RGPD: "el responsable de 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 a que se refiere el apartado 1"



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.

G. RESUMEN DE LA BRECHA

En este apartado se debe describir de forma sucinta y concisa los hechos acontecidos y las medidas adoptadas para mitigar los efectos sobre las personas físicas afectadas. No se deben incluir datos personales, ni aportar información contradictoria a lo reflejado a lo largo del cuestionario. La notificación deberá ajustarse a la longitud prevista en el formulario, evitando fórmulas tipo: “En documento adjunto”, “Ver adjunto” o similares.

En este apartado puede aportarse información que se considere relevante y no se recoja en el resto de los apartados del formulario. Algunos ejemplos son:

- Indicar medidas concretas adoptadas para mitigar el riesgo sobre las personas afectadas no recogidas en el apartado de acciones tomadas.
- En caso de que un ciberincidente sea el causante de la brecha de datos personales y esté siendo tratado por un CERT o lo haya sido, se puede indicar el CERT y el número de ticket.
- Indicar el número de afectados en España cuando no coincida con el número de total de afectados.
- Indicar si hay diferencias sustanciales en el riesgo para las personas según su perfil.
- Si la brecha está vinculada a un servicio que se presta bajo una denominación comercial distinta a la razón social del responsable, indicar tanto el servicio como la denominación comercial.
- Cuando se notifique como encargado y en nombre de varios responsables, especificar el número total de personas afectadas y el número de personas afectadas por cada responsable.

H. IMPLICACIONES TRANSFRONTERIZAS

Es necesario indicar las implicaciones transfronterizas de la brecha de datos personales en caso de haberse producido. Se debe indicar si hay afectados en otros estados miembro

[34] El responsable puede garantizar que no existe probabilidad

de la Unión Europea, el número aproximado de afectados en cada Estado miembro, utilizando los criterios ya expuestos en el apartado E de esta Guía, y si el responsable ha notificado o tiene previsto notificar a la Autoridad de Control de algún otro Estado miembro.

I. INFORMACIÓN TEMPORAL DE LA BRECHA Y MEDIOS DE DETECCIÓN

La notificación a la Autoridad de Control y a los afectados, en su caso, debe realizarse sin dilación indebida, y en el caso de la notificación a la autoridad de control se establece un plazo máximo de 72 horas. Los plazos de detección y resolución de una brecha de datos personales junto con los medios de detección son relevantes para determinar el nivel de riesgo para los derechos y libertades de las personas afectadas.

A tal efecto en el formulario de notificaciones de brechas de datos personales se recoge la siguiente información:

- Fecha de detección: fecha en la que el responsable de tratamiento tiene constancia de que un incidente ha afectado a datos personales, y es la fecha que establece el inicio de los plazos de notificación a la Autoridad de Control y a los afectados.
- Si la fecha en la que se está realizando la notificación de brecha de datos personales está fuera del plazo de 72 horas respecto a la fecha de detección, deberá indicarse también el motivo. Se consideran los siguientes supuestos[35]:
    - Plazo de 72 horas expirado fuera de la jornada laboral, fin de semana o períodos de vacaciones.
    - Problemas en medios técnicos.
    - Inicialmente no se consideró susceptible de notificación a la Autoridad de control.
    - Demora en el procedimiento de gestión de brechas.
    - No interferir en una investigación policial o judicial en curso.
- Medios de detección de la brecha: medio por el cual el responsable de tratamiento ha tenido constancia de la brecha de datos personales. Se consideran los siguientes supuestos:
    - Medios de detección propios del encargado o responsables.
    - A través de la comunicación de algún afectado.
    - Medios de comunicación: Se considera este caso cuando el responsable tiene constancia de los hechos a través de la publicación en medios de comunicación.
    - Detectado por un empleado del encargado o responsable.
    - Tercero ajeno al tratamiento: Se considera en este caso cuando se tiene constancia de la brecha mediante la comunicación realizada por un investigador de seguridad, un CERT o cualquier tercero ajeno al tratamiento de datos personales.

[35] Los supuestos listados no eximen de la responsabilidad en que se pueda incurrir al notificar fuera de plazo.

- Fecha de inicio de la brecha: De conocerla, se debe indicar la fecha de inicio del incidente que provoca la brecha de datos personales. Puede indicar una fecha exacta o estimada.

J. 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. No se pretende cubrir la totalidad, ni el detalle, de las medidas de seguridad aplicadas en el tratamiento de datos, sino aportar información básica de las medidas aplicadas.

- Medidas de seguridad con las que contaba el tratamiento antes de la brecha: Se consideran las siguientes opciones:
    - 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.
- Indicar si la brecha de datos personales pudiera haberse evitado adoptando alguna medida de seguridad adicional.
- Indicar si el origen de la brecha es debido a un fallo, deficiencia o incumplimiento de alguna de las medidas de seguridad implementadas.
- Indicar la disponibilidad de un análisis de riesgos o evaluación de impacto en protección de datos documentado que justifique las medidas adoptadas.

K. ACCIONES TOMADAS

El artículo 33 del RGPD establece que la notificación de la brecha de datos personales a la Autoridad de Control debe incluir las medidas adoptadas o propuestas para poner remedio a la brecha y mitigar los posibles efectos negativos. A tal efecto el responsable de tratamiento deberá indicar la siguiente información:

- Si se ha actualizado el registro de incidentes con los detalles relativos a la brecha de datos personales.
- Identificar de entre las medidas consideradas en el apartado anterior cuáles han sido mejoradas y/o adoptadas como nuevas medidas de seguridad.
- Si se han establecido mejoras en los procedimientos y políticas de seguridad tras la brecha.
- Si se han denunciado los hechos ante las Autoridades policiales y/o judiciales competentes por considerarlo constitutivo de delito, o se pretende hacerlo. No es necesario adjuntar a la notificación de brecha de datos personales una copia de la denuncia, en su caso, se le podría requerir al responsable con posterioridad.

- Si el responsable de tratamiento considera que se han tomado todas las acciones posibles y ha dado por resuelta la brecha. En tal caso se deberá indicar también la fecha en la que se dio por resuelta la brecha de datos personales.

En caso de que el riesgo para las personas afectadas haya quedado mitigado con acciones más concretas que las consideradas en este apartado se indicarán brevemente en el resumen del incidente.

L. COMUNICACIÓN A LOS AFECTADOS

La notificación de la brecha de datos personales a la Autoridad de Control debe contener información sobre la decisión tomada por el responsable de tratamiento respecto de la comunicación de la brecha de datos personales a los afectados conforme al artículo 34 del RGPD.

En concreto, en la notificación de brecha de datos personales a la AEPD se solicita la siguiente información:

- Si el responsable de tratamiento ha comunicado la brecha de datos personales a las personas afectadas conforme al artículo 34 del RGPD deberá indicar la fecha en la que ha realizado la comunicación, el número de personas comunicadas y el medio utilizado para la comunicación.
- Si el responsable de tratamiento no ha comunicado la brecha de datos personales a las personas afectadas en el momento de la notificación de brecha de datos personales, pero tiene decidido hacerlo sin dilación indebida, deberá indicar igualmente la fecha en la que tiene prevista hacer la comunicación, el número de personas que tiene previsto informar y el medio que se utilizará para la comunicación a los afectados.
- Si el responsable de tratamiento no ha comunicado ni comunicará la brecha de datos personales a las personas afectadas, deberá indicar los motivos para no hacerlo. Se consideran las siguientes posibilidades[36]:
    - No existe un riesgo alto para los derechos y libertades de los afectados.
    - No hay ninguna acción que el afectado pueda llevar a cabo para mitigar los daños que le causará la brecha.
    - El daño reputacional para la organización sería muy elevado.
    - La comunicación supone un esfuerzo desproporcionado.
    - Para no interferir en una investigación policial/judicial en curso.
- Cuando el responsable de tratamiento no haya tomado una decisión al respecto en el momento de notificar la brecha de datos personales a la AEPD, podrá también indicarlo. Esta opción únicamente es válida en el caso de nuevas notificaciones, cuando el responsable tenga previsto aportar notificaciones adicionales con posterioridad y todavía no se haya identificado el riesgo como alto. En notificaciones completas, cuando el responsable de tratamiento no tenga previsto aportar más información y la brecha de datos personales se haya dado por resuelta, o si el riesgo ya ha sido evaluado como alto, el responsable de tratamiento debería haber adoptado una decisión respecto a la notificación de la brecha de datos personales a los afectados.

[36] Los supuestos listados no eximen de la responsabilidad en que se pueda incurrir.

Para ayudar en la toma de la decisión de comunicar o no a los afectados la AEPD pone a disposición de los responsables la herramienta Comunica-RGPD que asesora al responsable sobre que acción se debe tomar al consignar las características de la brecha de datos personales sufrida.

M. IDENTIFICACIÓN DE LOS INTERVINIENTES

En la notificación de brecha de datos personales a la AEPD se deberán facilitar los datos de los siguientes intervinientes:

- **Solicitante**: persona física que rellena el formulario de notificación. Tiene que estar en posesión de un certificado electrónico reconocido o sistemas Cl@ve permanente y PIN24H, siendo el único interviniente que se autentica con un certificado digital en la sede.
- **Entidad representada**: Si el solicitante utiliza un certificado electrónico de representación (de persona jurídica, para administradores únicos o de entidad sin personalidad jurídica), se recogen los datos de la entidad a la que representa el solicitante. Queda autenticada tanto la entidad como su representación por parte del solicitante. Si la entidad representada es el responsable de tratamiento queda acreditada la representación del responsable. En caso de que la entidad representada no sea el responsable de tratamiento, sino otra entidad que notifica en su nombre, se podrá adjuntar a la notificación un documento acreditativo de representación del responsable de tratamiento. La AEPD podría requerir a posteriori esta acreditación.
- **Delegado de Protección de Datos o Persona de Contacto**: En cumplimiento de lo estipulado en el artículo 33.3.b del RGPD, se recogen los datos del Delegado de Protección de Datos. En caso de no tenerlo designado, se recogen los datos de la persona de contacto a efectos de protección de datos.
- **Responsable de tratamiento**[37]: Es el sujeto obligado a notificar las brechas de datos personales, en virtud del RGPD u otra norma. Además de los datos identificativos y de contacto del responsable de tratamiento, en el formulario se solicitará la siguiente información:
    - Sector de actividad del responsable de tratamiento.
    - Tipo de organización: Autónomo o microempresa, PYME, Gran empresa o multinacional, u otros.
    - Ámbito público o privado[38].
- **Encargado de tratamiento**: En su caso, se solicitan los datos identificativos y de contacto del encargado de tratamiento, así como si se trata de una organización del ámbito público o privado.

N. DOCUMENTACIÓN ADJUNTA A LA NOTIFICACIÓN

De forma general no es necesario adjuntar ningún tipo de documentación adicional a la notificación de brecha de datos personales.

Si la notificación se realiza mediante el formulario de notificación de brechas de datos personales de la Sede Electrónica de la Agencia utilizando un certificado electrónico de

[37] Cuando un encargado notifique en nombre de varios responsables de tratamiento, deberá proporcionar la información correspondiente a todos los responsables de tratamiento afectados.
[38] En caso de entidades que puedan ejercer funciones públicas y privadas, definir el ámbito con relación al tratamiento afectado por la brecha.

representante del responsable de tratamiento, no será necesaria adjuntar documentación acreditativa de dicha circunstancia. En otro caso, será necesario adjuntar la documentación acreditativa de haber sido designado por el responsable de tratamiento para notificar sus brechas de datos personales a la Agencia, o en su caso la autorización para notificar una brecha de datos personales concreta o la acreditativa de representación del responsable de tratamiento

Si la Agencia considera que el responsable de tratamiento debe aportar documentación adicional para esclarecer los hechos, ésta le será requerida con posterioridad.

En cualquier caso, en la documentación adjunta a la notificación de brecha de datos personales nunca se deben incluir los datos personales que han sido objeto de la brecha. De igual forma, estos datos no deben ser incluidos en los registros de incidentes que han de llevar responsables y encargados. Tampoco se deben anexar formularios o documentos “adhoc” que reproduzcan la información consignada en la Sede Electrónica de la AEPD.

VII. RÉGIMEN SANCIONADOR RELATIVO A LAS OBLIGACIONES DEL ARTÍCULO 33 Y 34

Las notificaciones de brechas de datos personales ante la Autoridad de Control es parte de la responsabilidad proactiva de los responsables, o encargados en su caso, demostrando diligencia en los tratamientos de datos. La notificación de brecha no implica la imposición de una sanción. Al contrario, una notificación, y en su caso comunicación, realizada en tiempo y forma, es una evidencia de la diligencia de la organización a la hora de ejecutar eficazmente la obligación de responsabilidad proactiva del RGPD. Sin embargo, el no cumplir con las obligaciones de notificación y comunicación a los interesados sí está tipificado como infracción.

El artículo 58 del RGPD establece los poderes de investigación, correctivos y de autorización y consultivos de la Autoridad de Control competente.

En referencia a las brechas de datos personales hay que destacar los siguientes poderes correctivos establecidos en artículo 58.2 del RGPD:

- "e) Ordenar al responsable del tratamiento que comunique al interesado las violaciones de seguridad de los datos;"
- "i) Imponer una multa administrativa con arreglo al artículo 83, además o en lugar de las medidas mencionadas en el presente apartado, según las circunstancias de cada caso particular;"

El artículo 83 del RGPD prevé multas administrativas de hasta 10.000.000 € o hasta el 2% del volumen de negocio total global anual del ejercicio financiero anterior para responsables y encargados para las infracciones de las obligaciones establecidas, entre otros, en los artículos 32 (Seguridad del tratamiento), 33 (Notificación a la Autoridad de Control) y 34 (Comunicación al interesado) del RGPD.

Asimismo, el incumplimiento de las resoluciones de la Autoridad de Control en virtud del artículo 58 del RGPD como lo es una orden para comunicar una brecha de datos personales a los interesados, puede comportar sanciones de hasta 20.000.000 € o hasta el 4% del volumen de negocio total global anual del ejercicio financiero anterior.

El Título IX de la LOPDGDD viene a precisar el régimen sancionador establecido en el RGPD. En el artículo 70 se establece que además de responsables y encargados, cuando no estén establecidos en el territorio de la Unión Europea, estarán sujetos al régimen sancionador del RGPD sus representantes.

El mismo artículo 70 de la LOPDGDD excluye a los Delegados de Protección de Datos de la aplicación del régimen sancionador.

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

- "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"

- "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."

Por último, 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."

VIII. ESPECIFICIDADES DE LOS SUJETOS OBLIGADOS EN LA LGT

Otros sujetos obligados a notificar incidentes de seguridad a los equipos de respuesta a incidentes de seguridad informática (CSIRT) designados son los operadores de servicios esenciales y proveedores de servicios digitales[39]. Además, los prestadores de servicios de la Sociedad de la Información[40] pueden notificar voluntariamente a equipos de respuesta a emergencias informáticas (CERT) competentes, y en cualquier caso están obligados a prestar colaboración con éstos para la resolución de incidentes de ciberseguridad que tengan efectos significativos en la continuidad de los servicios que prestan.

No obstante, la obligación exigible a los operadores de servicios de telecomunicaciones electrónicas disponibles al público o que exploten redes públicas de comunicaciones electrónicas continúa rigiéndose por lo previsto en el artículo 41 y concordantes de la Ley 9/2014, de 9 de mayo, General de Telecomunicaciones (LGT).

En efecto, el artículo 95 del RGPD establece que el RGPD no impone obligaciones adicionales en el marco de la prestación de servicios públicos de comunicaciones electrónicas de redes públicas de telecomunicación de la Unión en ámbitos en que dichos servicios estén sujetos a las obligaciones específicas con el mismo objetivo establecidas en la Directiva 2002/58/CE.

Por tanto, debe interpretarse que las obligaciones previstas en la LGT, como norma de transposición de la citada Directiva, se mantienen vigentes.

Aunque la regulación de la LGT y del RGPD presenta elementos comunes, también incluye elementos diferenciales como los siguientes:

- Ausencia del plazo máximo de 72 horas para la notificación en la LGT.
- No contempla la obligación del encargado de tratamiento de notificar las brechas de datos personales al responsable en la LGT.
- Diferencias en el contenido mínimo de la notificación (omisión de las categorías y número aproximado de interesados afectados y de registros o datos personales en la LGT).
- La tipificación de las infracciones a la obligación de notificar como graves y leves en la LGT.
- El régimen sancionador (multas de hasta 50.000 euros o de hasta 2.000.000 de euros por infracciones leves o graves, respectivamente, en la LGT).
- La competencia para declarar las infracciones en caso de incumplimiento de la obligación de notificar a la Administración de telecomunicaciones y no a la AEPD.

[39] Artículos 19 y 20 del Real Decreto-ley 12/2018, de 7 de septiembre, de Seguridad de las redes y sistemas de información

[40] Disposición adicional novena Ley 34/2002 de Servicios de la Sociedad de la Información y de Comercio Electrónico

IX. RECURSOS A DISPOSICIÓN DEL RESPONSABLE

A continuación, se relacionan un conjunto de recursos de diversas fuentes a disposición de responsable y encargados de tratamiento como ayuda para la implementación de la responsabilidad proactiva en la gestión de brechas de datos personales.

Herramientas:

Micro-site de brechas de datos personales

Comunica-RGPD

Facilita - Emprende

Plantilla de formulario de notificación de brechas de datos personales AEPD[41]

Vídeos:

¿Sabrías reaccionar a un incidente?

Cómo prevenir la fuga de información

¿Cómo identificar una fuga de información? Monitoriza y analiza el tráfico

¿Sabes para qué sirve cada documento de tu plan de continuidad?

Continuidad de negocio en circunstancias adversas

Respuesta jurídica a ataques

Cinco medidas técnicas para evitar las brechas de seguridad

Recursos formativos:

https://www.incibe.es/protege-tu-empresa

https://www.incibe.es/protege-tu-empresa/juego-rol-pyme-seguridad

https://www.incibe.es/sites/default/files/contenidos/JuegoRol/juegorol_cuestionarioincialrespuestaincidentes.pdf

Guía de fuga de información

Ciberseguridad en la identidad digital y la reputación online

[41] Disponible a efectos informativos cuando se publique el nuevo formulario de notificación de brechas en la Sede Electrónica de la Agencia.