GRUPO DE TRABAJO SOBRE PROTECCIÓN DE DATOS DEL ARTÍCULO 29

18/ES

WP250rev.01

Directrices sobre la notificación de las violaciones de la seguridad de los datos personales de acuerdo con el Reglamento 2016/679

Adoptadas el 3 de octubre de 2017

Revisadas por última vez y adoptadas el 6 de febrero de 2018

EL GRUPO DE TRABAJO DE PROTECCIÓN DE LAS PERSONAS EN LO QUE RESPECTA AL TRATAMIENTO DE DATOS PERSONALES

creado por la Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995,

vistos los artículos 29 y 30 de dicha Directiva,

visto su Reglamento interno,

HA ADOPTADO LAS PRESENTES DIRECTRICES:

ÍNDICE

INTRODUCCIÓN

El Reglamento General de Protección de Datos (RGPD) introduce la obligación de que una violación de la seguridad de los datos personales (en lo sucesivo, «violación») se notifique a la autoridad de control nacional competente[1] (o, en el caso de una violación transfronteriza, a la autoridad principal) y, en determinados casos, de que se comunique a las personas cuyos datos personales se hayan visto afectados por la violación.

En la actualidad, algunas organizaciones, como los proveedores de servicios de comunicaciones electrónicas disponibles al público, están obligadas a notificar las violaciones (como se especifica en la Directiva 2009/136/CE y en el Reglamento (UE) n.º 611/2013)[2]. Algunos Estados miembros de la UE ya cuentan también con su propia obligación nacional de notificación de violaciones, que puede incluir la obligación de notificar las violaciones que afecten a categorías de responsables del tratamiento, además de a los proveedores de servicios de comunicaciones electrónicas disponibles al público (por ejemplo, en Alemania e Italia), o la obligación de notificar todas las violaciones que afecten a los datos personales (como en los Países Bajos). Otros Estados miembros pueden disponer de códigos de prácticas pertinentes (por ejemplo, Irlanda[3]). Mientras que, en la actualidad, varias autoridades de protección de datos de la UE alientan a los responsables del tratamiento a que informen de las violaciones, la Directiva 95/46/CE sobre protección de datos[4], sustituida por el RGPD, no contiene una obligación específica de notificación de violaciones y, por tanto, este requisito será nuevo para muchas organizaciones. En la actualidad, el RGPD obliga a todos los responsables del tratamiento a notificar una violación, a menos que sea improbable que esta constituya un riesgo para los derechos y las libertades de las personas[5]. Los encargados del tratamiento también desempeñan un papel importante y deben notificar cualquier violación a su responsable del tratamiento[6].

El Grupo de Trabajo del Artículo 29 (GT29) considera que el nuevo requisito de notificación tiene varias ventajas. A la hora de notificar a la autoridad de control, los responsables del tratamiento pueden obtener asesoramiento sobre la necesidad de informar a las personas afectadas. De hecho, la autoridad de control puede ordenar al responsable del tratamiento que informe a esas personas sobre la violación[7]. La comunicación de una violación a las personas permite que el responsable del tratamiento proporcione información sobre los riesgos que se presentan como resultado de la violación y las medidas que dichas personas pueden adoptar para protegerse de sus posibles consecuencias. Cualquier plan de respuesta en caso de violación debe centrarse en la protección de las

[1] Véase el artículo 4, apartado 21, del RGPD.

[2] Véase http://eur-lex.europa.eu/legal-content/ES/TXT/?uri=celex:32009L0136 y http://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX%3A32013R0611

[3] Véase https://www.dataprotection.ie/docs/Data_Security_Breach_Code_of_Practice/1082.htm

[4] Véase http://eur-lex.europa.eu/legal-content/ES/TXT/?uri=celex:31995L0046

[5] Los derechos consagrados en la Carta de los Derechos Fundamentales de la Unión Europea pueden consultarse en http://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX:12012P/TXT

[6] Véase el artículo 33, apartado 2. Este concepto es similar al del artículo 5 del Reglamento (UE) n.º 611/2013, que establece que un proveedor contratado para prestar parte de un servicio de comunicaciones electrónicas (sin tener una relación contractual directa con los abonados) está obligado a notificar al proveedor contratante en caso de violación de datos personales.

[7] Véanse el artículo 34, apartado 4, y el artículo 58, apartado 2, letra e).

personas y de sus datos personales. Por consiguiente, la notificación de las violaciones de la seguridad debe considerarse como una herramienta que mejora el cumplimiento respecto de la protección de los datos personales. Al mismo tiempo, cabe señalar que el hecho de no informar de una violación a una persona o a una autoridad de control podría significar que, de conformidad con el artículo 83, el responsable del tratamiento podría ser objeto de una sanción.

Por tanto, se anima a los responsables y a los encargados del tratamiento a que planifiquen de antemano y pongan en marcha procesos que permitan detectar y controlar con prontitud una violación, evaluar el riesgo para las personas[8] y, a continuación, determinar si es necesario notificar a la autoridad de control competente y comunicar la violación a las personas afectadas cuando proceda. La notificación a la autoridad de control debe formar parte de dicho plan de respuesta a los incidentes.

El RGPD contiene disposiciones sobre cuándo debe notificarse una violación y a quién, así como qué información debe proporcionarse en la notificación. La información requerida para la notificación puede facilitarse de manera gradual, pero, en cualquier caso, de producirse una violación los responsables del tratamiento deben actuar en tiempo oportuno.

En su Dictamen 03/2014 sobre la notificación de violación de datos personales[9], el GT29 proporcionó orientación a los responsables del tratamiento con el fin de ayudarles a decidir si, en caso de violación, debían notificarlo a los interesados. En el dictamen se examinó la obligación de los proveedores de servicios de comunicaciones electrónicas en relación con la Directiva 2002/58/CE y se ofrecieron ejemplos de diferentes sectores en el contexto del entonces proyecto de RGPD y se presentaron buenas prácticas para todos los responsables del tratamiento.

En las presentes Directrices se explican los requisitos de la obligación de notificación y comunicación de violaciones del RGPD y algunas de las medidas que los responsables y los encargados del tratamiento pueden adoptar para cumplir estas nuevas obligaciones. Asimismo, se aportan ejemplos de varios tipos de violaciones y a quiénes habría que notificarlas en diferentes situaciones.

I. Notificación de violación de la seguridad de los datos personales con arreglo al RGPD

A. Consideraciones básicas de seguridad

Uno de los requisitos del RGDP es que, mediante el uso de medidas técnicas y organizativas apropiadas, los datos personales se tratarán de manera que se garantice una seguridad adecuada de los datos personales, incluida la protección contra el tratamiento no autorizado o ilícito y contra su pérdida, destrucción o daño accidental[10].

Por consiguiente, el RGPD exige que los responsables y los encargados del tratamiento cuenten con las medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo que implica el tratamiento de los datos personales. Deben tener en cuenta el estado de la técnica, los costes de aplicación, y la naturaleza, el alcance, el contexto y los fines del tratamiento, así

[8] Esto puede garantizarse en virtud del requisito de seguimiento y revisión de una evaluación de impacto relativa a la protección de datos (EIPD), exigida para las operaciones de tratamiento que puedan entrañar un alto riesgo para los derechos y las libertades de las personas físicas (artículo 35, apartados 1 y 11).

[9] Véase el Dictamen 03/2014 sobre notificación de violación de datos personales http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp213_es.pdf

[10] Artículo 5, apartado 1, letra f), y artículo 32.

como riesgos de probabilidad y gravedad variables para los derechos y libertades de las personas físicas[11]. Además, el RGPD establece la adopción de todas las medidas de protección tecnológicas y organizativas apropiadas para determinar de inmediato si se ha producido una violación, lo cual determina a su vez si se cumple la obligación de notificación[12].

Por consiguiente, un elemento clave de cualquier política en materia de seguridad de los datos es poder, en la medida de lo posible, prevenir una violación y, cuando a pesar de todo se produzca, reaccionar de forma rápida.

B. ¿Qué es una violación de la seguridad de los datos personales?

1. Definición

Para subsanar una violación de seguridad, el responsable del tratamiento debe, en primer lugar, ser capaz de reconocerla. En el artículo 4, apartado 12, del RGPD se define una «violación de la seguridad de los datos personales» como:

> «toda violación de la seguridad que ocasione 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».

El concepto de «destrucción» de los datos personales debe estar muy claro: es cuando los datos ya no existen, o ya no existen en una forma que sea de utilidad para el responsable del tratamiento. El concepto de «daño» también debe estar relativamente claro: cuando los datos personales han sido alterados, corrompidos o dejan de estar completos. La «pérdida» de datos personales debe interpretarse en el sentido de que los datos pueden seguir existiendo, pero el responsable del tratamiento ha perdido el control o el acceso a ellos, o ya no obran en su poder. Por último, el tratamiento no autorizado o ilícito puede incluir la divulgación de datos personales a (o el acceso por parte de) destinatarios que no están autorizados a recibir (o acceder a) los datos, o cualquier otra forma de tratamiento que vulnere el RGPD.

Ejemplo

Un ejemplo de pérdida de datos personales puede incluir la pérdida o robo de un dispositivo que contenga una copia de la base de datos de los clientes de un responsable del tratamiento. Otro ejemplo de pérdida puede ser cuando la única copia de un conjunto de datos personales ha sido objeto de cifrado mediante un programa de secuestro o el responsable del tratamiento la ha cifrado utilizando una clave que ya no obra en su poder.

Lo que debe quedar claro es que una violación es un tipo de incidente de seguridad. Sin embargo, como se indica en el artículo 4, apartado 12, el RGPD solo se aplica en caso de violación de la seguridad de los *datos personales*. La consecuencia de tal violación es que el responsable del tratamiento no podrá garantizar el cumplimiento de los principios relativos al tratamiento de los datos personales, tal como se establece en el artículo 5 del RGPD. Esto pone de relieve la diferencia entre un incidente de seguridad y una violación de la seguridad de los datos personales, en esencia, aunque

[11] Artículo 32; véase también el considerando 83.

[12] Véase el considerando 87.

todas las violaciones de la seguridad de los datos personales son incidentes de seguridad, no todos los incidentes de seguridad son necesariamente violaciones de la seguridad de los datos personales[13].

A continuación se examinan los posibles efectos adversos de una violación de la seguridad en las personas.

2. Tipos de violaciones de la seguridad de los datos personales

En su Dictamen 03/2014 sobre la notificación de violación de datos personales, el GT29 explicó que las violaciones pueden clasificarse con arreglo a los siguientes tres conocidos principios de seguridad de la información[14]:

- «Violación de la confidencialidad»: cuando se produce una revelación no autorizada o accidental de los datos personales, o el acceso a los mismos.
- «Violación de la integridad»: cuando se produce una alteración no autorizada o accidental de los datos personales.
- «Violación de la disponibilidad»: cuando se produce una pérdida de acceso accidental o no autorizada[15] a los datos personales, o la destrucción de los mismos.

Asimismo, cabe señalar que, dependiendo de las circunstancias, una violación puede afectar a la confidencialidad, la integridad y la disponibilidad de los datos personales al mismo tiempo, así como a cualquier combinación de estos elementos.

Mientras que la determinación de la existencia de una violación de la confidencialidad o la integridad resulta relativamente clara, una violación de la disponibilidad puede ser menos obvia. Una violación se considerará siempre como una violación de la disponibilidad cuando se haya producido una pérdida o una destrucción permanente de los datos personales.

Ejemplo

Entre los ejemplos de pérdida de la disponibilidad se incluyen los casos en que los datos se hayan borrado accidentalmente o por una persona no autorizada o, en el ejemplo de los datos cifrados de forma segura, en los casos en que se haya perdido la clave de descifrado. En caso de que el responsable del tratamiento no pueda restaurar el acceso a los datos, por ejemplo, desde una copia de seguridad, esto se considera una pérdida permanente de la disponibilidad.

También puede ocurrir una pérdida de la disponibilidad cuando se haya producido una interrupción significativa del servicio normal de una organización, por ejemplo, cuando se haya producido un fallo

[13] Cabe señalar que un incidente de seguridad no se limita a modelos de amenaza en los que se ataca a una organización desde una fuente externa, sino que incluye incidentes de tratamiento interno que infringen los principios de seguridad.

[14] Véase el Dictamen 03/2014.

[15] Está bien establecido que el «acceso» es una parte fundamental de la «disponibilidad». Véase, por ejemplo, NIST SP800-53rev4, que define la «disponibilidad» como: «Garantizar el acceso oportuno y fiable a la información y su utilización», disponible en http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf. CNSSI-4009 también hace referencia al: «Acceso oportuno y fiable a los datos y a los servicios de información para los usuarios autorizados». Véase https://rmf.org/wp-content/uploads/2017/10/CNSSI-4009.pdf. ISO/IEC 27000:2016 también define «disponibilidad» como la «propiedad de ser accesible y utilizable cuando lo requiera una entidad autorizada». https://www.iso.org/obp/ui/#iso:std:iso-iec:27000:ed-4:v1:en

en el suministro eléctrico o un ataque de denegación de servicio que haga que los datos personales no estén disponibles

Cabe preguntarse si una pérdida temporal de la disponibilidad de los datos personales debe considerarse una violación de la seguridad y, en caso afirmativo, si debe notificarse. En el artículo 32 del RGPD, «seguridad del tratamiento», se explica que al aplicar medidas técnicas y organizativas para garantizar un nivel de seguridad adecuado al riesgo, debe tenerse en cuenta, entre otras cosas, «la capacidad de garantizar la confidencialidad, integridad, disponibilidad y resiliencia permanentes de los sistemas y servicios de tratamiento» y «la capacidad de restaurar la disponibilidad y el acceso a los datos personales de forma rápida en caso de incidente físico o técnico».

Por tanto, un incidente de seguridad que provoque la no disponibilidad de los datos personales durante un período de tiempo es también un tipo de violación, ya que la ausencia de acceso a los datos puede tener un impacto significativo en los derechos y las libertades de las personas físicas. Para que quede claro, el hecho de que los datos personales no estén disponibles debido a la realización de un mantenimiento planificado del sistema no constituye una «violación de la seguridad», tal como se define en el artículo 4, apartado 12.

Al igual que en el caso de pérdida o destrucción permanente de datos personales (o de cualquier otro tipo de violación), una violación que implique la pérdida temporal de la disponibilidad debe documentarse de conformidad con el artículo 33, apartado 5. Esto ayuda al responsable del tratamiento a demostrar la responsabilidad proactiva a la autoridad de control, que podría pedir ver dichos registros[16]. Sin embargo, dependiendo de las circunstancias de la violación, esta puede requerir, o no, la notificación a la autoridad de control y la comunicación a las personas afectadas. El responsable del tratamiento deberá evaluar la probabilidad y la gravedad del impacto de la ausencia de disponibilidad de los datos personales en los derechos y las libertades de las personas físicas. De conformidad con el artículo 33, el responsable del tratamiento deberá notificar la violación, a menos que sea improbable que esta constituya un riesgo para los derechos y las libertades de las personas. Por supuesto, esto deberá evaluarse caso por caso.

Ejemplos

En el contexto de un hospital, la no disponibilidad de los datos médicos críticos sobre los pacientes, aunque sea temporalmente, podría constituir un riesgo para los derechos y las libertades de las personas; por ejemplo, se pueden cancelar operaciones y ponerse en peligro vidas humanas.

Por el contrario, el hecho de que los sistemas de una empresa de medios de comunicación no estén disponibles durante varias horas (por ejemplo, debido a un fallo de alimentación), y dicha empresa no pueda enviar boletines informativos a sus suscriptores es poco probable que suponga un riesgo para los derechos y las libertades de las personas.

Cabe señalar que, si bien la pérdida de disponibilidad de los sistemas de un responsable del tratamiento puede ser solo temporal y no repercutir en las personas, es importante que el responsable del tratamiento considere todas las posibles consecuencias de una violación, ya que esta podría requerir notificación por otros motivos.

Ejemplo

La infección por un programa de secuestro (programa malicioso que cifra los datos del responsable del tratamiento hasta que se pague un rescate) podría provocar una pérdida temporal de disponibilidad

[16] Véase el artículo 33, apartado 5.

en el caso de que los datos se puedan restaurar desde la copia de seguridad. Sin embargo, se produjo una intrusión en la red, y podría ser necesaria una notificación si el incidente se califica de violación de la confidencialidad (es decir, si el atacante accede a los datos personales) y esto presenta un riesgo para los derechos y las libertades de las personas.

3. Las posibles consecuencias de la violación de la seguridad de los datos personales

Una violación puede tener una serie de efectos adversos considerables en las personas, susceptibles de ocasionar daños y perjuicios físicos, materiales o inmateriales. En el RGPD se explica que estos efectos pueden incluir la pérdida de control sobre sus datos personales, la restricción de sus derechos, la discriminación, la usurpación de identidad o fraude, las pérdidas financieras, la reversión no autorizada de la seudonimización, el daño para la reputación y la pérdida de confidencialidad de datos personales sujetos al secreto profesional. También puede incluir cualquier otro perjuicio económico o social significativo para esas personas[17].

Por consiguiente, el RGPD exige al responsable del tratamiento que notifique una violación a la autoridad de control competente, a menos que sea improbable que exista el riesgo de que se produzcan estos efectos adversos. Cuando sea probable que exista un alto riesgo de que se produzcan estos efectos adversos, el RGPD exige al responsable del tratamiento que comunique la violación de la seguridad a las personas afectadas tan pronto como sea razonablemente posible[18].

En el considerando 87 del RGPD se destaca la importancia de poder identificar una violación de la seguridad, evaluar el riesgo para las personas y, a continuación, notificarla en caso necesario:

«Debe verificarse si se ha aplicado toda la protección tecnológica adecuada y se han tomado las medidas organizativas oportunas para determinar de inmediato si se ha producido una violación de la seguridad de los datos personales y para informar sin dilación a la autoridad de control y al interesado. Debe verificarse que la notificación se ha realizado sin dilación indebida teniendo en cuenta, en particular, la naturaleza y gravedad de la violación de la seguridad de los datos personales y sus consecuencias y efectos adversos para el interesado. Dicha notificación puede resultar en una intervención de la autoridad de control de conformidad con las funciones y poderes que establece el presente Reglamento».

En la sección IV se examinan otras directrices sobre la evaluación del riesgo de efectos adversos para las personas.

Si los responsables del tratamiento no notifican una violación de la seguridad de los datos a la autoridad de control o a los interesados, o a ambos, aun cuando se cumplan los requisitos de los artículos 33 y 34, se presentará a la autoridad de control una elección que deberá incluir la consideración de todas las medidas correctivas de que disponga, entre las que se incluiría la posibilidad de la imposición de la multa administrativa apropiada[19], bien acompañada de una medida correctiva con arreglo al artículo 58, apartado 2, o bien sola. Cuando se opta por una multa administrativa, su valor puede ser de 10 000 000 EUR como máximo o, tratándose de una empresa, de una cuantía equivalente al 2 % como máximo del volumen de negocio total anual global con arreglo al artículo 83, apartado 4, letra a), del RGPD. Asimismo, es importante tener en cuenta que, en algunos

[17] Véanse también los considerandos 85 y 75.

[18] Véase también el considerando 86.

[19] Para más detalles, consulte las Directrices sobre la aplicación y la fijación de multas administrativas del GT29, disponible aquí: http://ec.europa.eu/newsroom/just/document.cfm?doc_id=47889

casos, el hecho de no notificar una violación de la seguridad de los datos puede revelar la ausencia de medidas de seguridad o su inadecuación. Las directrices del GT29 sobre multas administrativas establecen: «La comisión de varias infracciones distintas en un caso individual concreto permite a la autoridad de control aplicar las multas administrativas a un nivel que sea efectivo, proporcionado y disuasorio dentro de los límites de la infracción más grave». En ese caso, las autoridades de control también tendrán la posibilidad de imponer sanciones por no notificar o comunicar la violación (artículos 33 y 34), por una parte, y por la ausencia de medidas de seguridad (adecuadas) (artículo 32), por otra, ya que se trata de dos infracciones distintas.

II. **Artículo 33 - Notificación a la autoridad de control**

A. Cuándo notificar

1. Artículo 33, requisitos

El artículo 33, apartado 1, dispone:

> «En caso de violación de la seguridad de los datos personales, el responsable del tratamiento la notificará a la autoridad de control competente de conformidad con el artículo 55 sin dilación indebida y, de ser posible, a más tardar 72 horas después de que haya tenido constancia de ella, a menos que sea improbable que dicha violación de la seguridad constituya un riesgo para los derechos y las libertades de las personas físicas. Si la notificación a la autoridad de control no tiene lugar en el plazo de 72 horas, deberá ir acompañada de indicación de los motivos de la dilación».

El considerando 87 dice[20]:

> «Debe verificarse si se ha aplicado toda la protección tecnológica adecuada y se han tomado las medidas organizativas oportunas para determinar de inmediato si se ha producido una violación de la seguridad de los datos personales y para informar sin dilación a la autoridad de control y al interesado. Debe verificarse que la notificación se ha realizado sin dilación indebida teniendo en cuenta, en particular, la naturaleza y gravedad de la violación de la seguridad de los datos personales y sus consecuencias y efectos adversos para el interesado. Dicha notificación puede resultar en una intervención de la autoridad de control de conformidad con las funciones y poderes que establece el presente Reglamento».

2. ¿Cuándo «tiene constancia» un responsable del tratamiento?

Como se ha explicado anteriormente, el RGPD establece que, en caso de una violación, el responsable del tratamiento lo notificará sin dilación indebida y, de ser posible, a más tardar setenta y dos horas después de que haya tenido constancia de ella. Esto puede plantear la cuestión de cuándo puede considerarse que un responsable del tratamiento «tiene constancia» de una violación. El GT29 piensa que debe considerarse que un responsable del tratamiento «tiene constancia» cuando tenga un grado razonable de certeza de que se ha producido un suceso que compromete datos personales.

Sin embargo, como se ha indicado anteriormente, el RGPD requiere que el responsable del tratamiento aplique todas las medidas técnicas de protección y organización oportunas para determinar de inmediato si se ha producido una violación e informar sin dilación a la autoridad de control y a los interesados. Asimismo indica que debe verificarse que la notificación se ha realizado

[20] El considerando 85 también es importante.

sin dilación indebida teniendo en cuenta, en particular, la naturaleza y gravedad de la violación y sus consecuencias y efectos adversos para el interesado[21]. Esto obliga al responsable del tratamiento a garantizar que tendrá constancia de cualquier violación de forma rápida para que pueda tomar las medidas oportunas.

El momento exacto en que puede considerarse que un responsable del tratamiento «tiene constancia» de una violación concreta dependerá de las circunstancias de dicha violación. En algunos casos, estará relativamente claro desde el principio que se ha producido una violación, mientras que en otros puede llevar algún tiempo establecer si los datos personales se han visto comprometidos. No obstante, debe hacerse hincapié en la necesidad de actuar con rapidez para investigar un incidente a fin de determinar si, efectivamente, se ha violado la seguridad de los datos personales y, de ser así, para adoptar medidas correctivas y, en caso necesario, notificarlo.

Ejemplos

1. En caso de pérdida de una llave USB con datos personales no cifrados, a menudo no es posible determinar si personas no autorizadas han tenido acceso a dichos datos. No obstante, aunque el responsable del tratamiento no pueda determinar si se ha producido una violación de la confidencialidad, tal caso debe notificarse, ya que existe un grado razonable de certeza de que se ha producido una violación de la disponibilidad; el responsable del tratamiento «tendría constancia» cuando se dio cuenta de que la llave USB se había perdido.

2. Un tercero informa a un responsable del tratamiento de que ha recibido accidentalmente los datos personales de uno de sus clientes y proporciona pruebas de la comunicación no autorizada. Dado que se han presentado pruebas claras de la existencia de una violación de la confidencialidad al responsable del tratamiento, no cabe duda de que este «tiene constancia» de ella.

3. Un responsable del tratamiento detecta que ha habido una posible intrusión en su red. El responsable del tratamiento comprueba sus sistemas para determinar si los datos personales que se encuentran en ese sistema se han visto comprometidos y efectivamente es así. De nuevo, dado que ahora el responsable del tratamiento tiene pruebas claras de una violación, no cabe duda de que este «tiene constancia» de ella.

4. Un ciberdelincuente se pone en contacto con el responsable del tratamiento después de haber pirateado su sistema para pedir un rescate. En ese caso, tras comprobar su sistema para confirmar que ha sido objeto de un ataque, el responsable del tratamiento tiene pruebas claras de que se ha producido una violación y no cabe duda de que tiene constancia de ello.

Tras haber sido informado de una posible violación por una persona, un medio de comunicación u otra fuente, o cuando el propio responsable del tratamiento haya detectado un incidente de seguridad, este podrá iniciar un breve período de investigación para determinar si se ha producido o no una violación. Durante este período de investigación, no se puede considerar que el responsable del tratamiento «tenga constancia». Sin embargo, cabe esperar que la investigación inicial comience lo antes posible y establezca con un grado razonable de certeza si se ha producido una violación; a continuación, puede realizar una investigación más detallada.

Una vez que el responsable del tratamiento tenga constancia de una violación notificable, esta deberá notificarse sin dilación indebida y, de ser posible, en un plazo máximo de setenta y dos horas. Durante este período, el responsable del tratamiento deberá evaluar el posible riesgo para las personas a fin de determinar si se aplica el requisito de notificación, así como las medidas necesarias para hacer frente a

[21] Véase el considerando 87.

la violación. No obstante, es posible que un responsable del tratamiento ya disponga de una evaluación inicial del posible riesgo que podría derivarse de una violación en el marco de una evaluación de impacto relativa a la protección de datos (EIPD)[22] realizada antes de la operación de tratamiento en cuestión. Sin embargo, la EIPD puede ser más general en relación con las circunstancias específicas de cualquier violación real, por lo que en cualquier caso será necesario realizar una evaluación adicional que tenga en cuenta esas circunstancias. Para más detalles sobre la evaluación del riesgo, véase la sección IV.

En la mayoría de los casos, estas acciones preliminares deben realizarse poco después de la alerta inicial (es decir, cuando el responsable o el encargado del tratamiento sospechen que se ha producido un incidente de seguridad que pueda afectar a datos personales) – solo en casos excepcionales debe tardarse más tiempo.

Ejemplo

Una persona informa al responsable del tratamiento de que ha recibido un mensaje de correo electrónico de alguien que se hace pasar por el responsable del tratamiento y que contiene datos personales relativos a su uso (real) del servicio, lo cual indica que la seguridad del responsable del tratamiento se ha visto comprometida. El responsable del tratamiento lleva a cabo una breve investigación e identifica una intrusión en su red y pruebas de un acceso no autorizado a los datos personales. En este momento se consideraría que el responsable del tratamiento «tiene constancia» y la notificación a la autoridad de control es necesaria, a menos que sea improbable que esto presente un riesgo para los derechos y las libertades de las personas. El responsable del tratamiento deberá adoptar las medidas correctivas adecuadas para subsanar la violación.

Por tanto, el responsable del tratamiento debe disponer de procesos internos para poder detectar y subsanar una violación. Por ejemplo, para encontrar algunas irregularidades en el tratamiento de los datos, el responsable o el encargado del tratamiento pueden utilizar ciertas medidas técnicas, tales como analizadores de flujo de datos y de registro, a partir de los cuales es posible definir eventos y alertas mediante la correlación de cualquier dato de registro[23]. Es importante que, cuando se detecte una violación, se notifique al nivel de gestión apropiado para que se pueda abordar y, en su caso, notificar de conformidad con el artículo 33 y, en caso necesario, con el artículo 34. Tales medidas y mecanismos de información podrían detallarse en los planes de respuesta a incidentes o en los mecanismos de gobernanza del responsable del tratamiento. Esto ayudará al responsable del tratamiento a planificar de forma eficaz y a determinar quién, dentro de la organización, tiene la responsabilidad operativa de gestionar una violación y si se debe remitir un incidente a un nivel superior según proceda, así como la manera de hacerlo.

El responsable del tratamiento también debe haber establecido acuerdos con los encargados del tratamiento a los que recurra, los cuales tienen a su vez la obligación de notificar la violación al responsable del tratamiento del caso (véase a continuación).

Si bien corresponde a los responsables y a los encargados del tratamiento adoptar las medidas adecuadas para poder prevenir, reaccionar y hacer frente a una violación, en todos los casos deben adoptarse algunas medidas prácticas.

[22] Véanse las Directrices sobre la evaluación de impacto relativa a la protección de datos del GT29 en: http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611236

[23] Cabe señalar que los datos de registro que facilitan la verificabilidad de, por ejemplo, el almacenamiento, la modificación o la supresión de datos, también pueden considerarse datos personales relativos a la persona que inició la operación de tratamiento en cuestión.

- La información relativa a todos los sucesos relacionados con la seguridad debe dirigirse a la persona o personas responsables de hacer frente a los incidentes, determinar la existencia de una violación y evaluar el riesgo.
- Debe evaluarse el riesgo para las personas derivado de una violación (probabilidad de que no haya riesgo, de que haya riesgo o riesgo alto), y se debe informar a los departamentos pertinentes de la organización.
- En caso necesario debe hacerse la notificación a la autoridad de control y, en su caso, la comunicación de la violación a las personas afectadas.
- Al mismo tiempo, el responsable del tratamiento debe actuar para contener y recuperar la violación.
- La documentación de la violación debe realizarse a medida que esta se desarrolla.

Por consiguiente, debe quedar claro que el responsable del tratamiento está obligado a actuar a partir de cualquier alerta inicial y a determinar si se ha producido o no una violación. Este breve período permite que se realicen algunas investigaciones y que el responsable del tratamiento reúna pruebas y otros detalles pertinentes. No obstante, una vez que el responsable del tratamiento haya establecido con un grado razonable de certeza que se ha producido una violación, si se cumplen las condiciones del artículo 33, apartado 1, deberá notificarlo a las autoridades de control sin dilación indebida y, de ser posible, en un plazo máximo de setenta y dos horas[24]. Si un responsable del tratamiento no actúa de manera rápida y resulta evidente que se ha producido una violación, esto podría considerarse una falta de notificación de conformidad con el artículo 33.

El artículo 32 deja claro que el responsable y el encargado del tratamiento deben disponer de las medidas técnicas y organizativas adecuadas para garantizar un nivel adecuado de seguridad de los datos personales: la capacidad para detectar, abordar y notificar una violación en tiempo oportuno debe considerarse un elemento esencial de estas medidas.

3. Corresponsables del tratamiento

El artículo 26 se refiere a los corresponsables y especifica que estos determinarán sus responsabilidades respectivas en el cumplimiento del RGPD[25]. Ello incluirá determinar cuál de las partes tendrá la responsabilidad del cumplimiento de las obligaciones previstas en los artículos 33 y 34. El GT29 recomienda que los acuerdos contractuales entre los corresponsables del tratamiento incluyan disposiciones que determinen qué responsable asumirá la dirección o será responsable del cumplimiento de las obligaciones de notificación de violaciones impuestas por el GDPR.

4. Obligaciones del encargado del tratamiento

El responsable del tratamiento conserva la responsabilidad general de la protección de los datos personales, pero el encargado del tratamiento desempeña un papel importante para que el responsable del tratamiento pueda cumplir sus obligaciones; y esto incluye la notificación de violaciones. En efecto, el artículo 28, apartado 3, especifica que el tratamiento por parte de un encargado se regirá por un contrato u otro acto jurídico. El artículo 28, apartado 3, letra f), dispone que el contrato u otro acto jurídico estipulará que el encargado del tratamiento «ayudará al responsable a garantizar el cumplimiento de las obligaciones establecidas en los artículos 32 a 36, teniendo en cuenta la naturaleza del tratamiento y la información a disposición del encargado».

[24] Véase el Reglamento n.º 1182/71 por el que se determinan las normas aplicables a los plazos, fechas y términos, disponible en: https://eur-lex.europa.eu/legal-content/ES/TXT/HTML/?uri=CELEX:31971R1182&from=ES

[25] Véase también el considerando 79.

El artículo 33, apartado 2, establece claramente que si el responsable del tratamiento recurre a un encargado y este tiene conocimiento de una violación de la seguridad de los datos personales que está tratando por cuenta del responsable, deberá notificarlo «sin dilación indebida». Cabe señalar que no es necesario que el encargado del tratamiento evalúe la probabilidad de riesgo derivado de una violación antes de notificarlo al responsable del tratamiento; corresponde al responsable del tratamiento realizar dicha evaluación cuando tenga conocimiento de la violación. El encargado del tratamiento solo tiene que determinar si se ha producido una violación y notificarlo al responsable del tratamiento. El responsable del tratamiento recurre al encargando del tratamiento para lograr sus objetivos; por tanto, en principio, el responsable del tratamiento debe considerar que «tiene constancia» una vez que el encargado del tratamiento le haya informado de la violación. La obligación del encargado del tratamiento de notificar a su responsable del tratamiento permite a este poner remedio a la violación y determinar si está obligado o no a notificarla a la autoridad de control de conformidad con el artículo 33, apartado 1, y a las personas afectadas de conformidad con el artículo 34, apartado 1. El responsable del tratamiento puede querer investigar también la violación, ya que es posible que el encargado del tratamiento no esté en condiciones de conocer todos los hechos pertinentes relacionados con el asunto, por ejemplo, si el responsable del tratamiento sigue conservando una copia o una copia de seguridad de los datos personales que el encargado ha destruido o perdido. Esto puede afectar a si el responsable del tratamiento debe o no notificar.

El RGPD no establece un plazo explícito dentro del cual el encargado del tratamiento deba alertar al responsable del tratamiento, excepto que debe hacerlo «sin dilación indebida». Por tanto, el GT29 recomienda que el encargado del tratamiento lo notifique sin demora al responsable del tratamiento, y facilite más información sobre la violación 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 setenta y dos horas.

Como ya se ha explicado, el contrato entre el responsable y el encargado del tratamiento 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 del tratamiento que, a su vez, apoyen la obligación del responsable del tratamiento de informar a la autoridad de control en un plazo de setenta y dos horas.

En caso de que el encargado del tratamiento preste servicios a varios responsables del tratamiento afectados por el mismo incidente, el encargado del tratamiento deberá comunicar los detalles del incidente a cada uno de ellos.

Un encargado del tratamiento podría efectuar una notificación en nombre del responsable del tratamiento si este le hubiera concedido la autorización adecuada y esto formara parte de los acuerdos contractuales formalizados entre el responsable y el encargado del tratamiento. Dicha notificación debe efectuarse con arreglo a lo dispuesto en los artículos 33 y 34. No obstante, es importante señalar que la responsabilidad legal de notificar recae en el responsable del tratamiento.

B. Facilitar información a la autoridad de control

1. Información que debe facilitarse

Cuando un responsable del tratamiento notifica una violación a la autoridad de control, el artículo 33, apartado 3, establece que, como mínimo, debe:

> «a) describir la naturaleza de la violación de la seguridad de los datos personales, inclusive, cuando sea posible, las categorías y el número aproximado de interesados afectados, y las categorías y el número aproximado de registros de datos personales afectados;
>
> b) comunicar el nombre y los datos de contacto del delegado de protección de datos o de otro punto de contacto en el que pueda obtenerse más información;

c) describir las posibles consecuencias de la violación de la seguridad de los datos personales;

d) 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».

El RGPD no define categorías de interesados ni de registros de datos personales. Sin embargo, el GT29 sugiere categorías de interesados para referirse a los distintos tipos de personas cuyos datos personales se han visto afectados por una violación: dependiendo de los descriptores utilizados, se podría incluir, entre otros, a los niños y otros grupos vulnerables, a las personas con discapacidad, a los empleados o a los clientes. Del mismo modo, las categorías de registros de datos personales pueden referirse a los diferentes tipos de registros que el responsable del tratamiento puede tratar, como datos sanitarios, expedientes educativos, información sobre asistencia social, datos financieros, números de cuentas bancarias, números de pasaporte, etc.

El considerando 85 deja claro que uno de los objetivos de la notificación es limitar los daños y perjuicios ocasionados a las personas. Por consiguiente, si los tipos de interesados o los tipos de datos personales indican un riesgo de que se produzcan daños y perjuicios particulares como consecuencia de una violación (por ejemplo, usurpación de identidad, fraude, pérdida financiera, amenaza al secreto profesional), es importante que la notificación indique estas categorías. De este modo, se vincula al requisito de describir las posibles consecuencias de la violación.

El hecho de no disponer de información precisa (por ejemplo, el número exacto de interesados afectados) no debe constituir un obstáculo para la notificación de las violaciones en tiempo oportuno. El RGPD permite cálculos aproximados del número de personas y del número de registros de datos personales afectados. La atención debe centrarse en abordar los efectos adversos de la violación y no en proporcionar cifras precisas. Así pues, cuando ha quedado claro que se ha producido una violación, pero aún no se conoce el alcance de la misma, una notificación gradual (véase a continuación) es una forma segura de cumplir las obligaciones de notificación.

El artículo 33, apartado 3, establece que el responsable del tratamiento «deberá como mínimo» facilitar esta información con una notificación, de modo que el responsable del tratamiento pueda, en caso necesario, optar por proporcionar más detalles. Diferentes tipos de violaciones (confidencialidad, integridad o disponibilidad) pueden requerir que se proporcione más información para explicar plenamente las circunstancias de cada caso.

Ejemplo

Como parte de su notificación a la autoridad de control, un responsable del tratamiento puede considerar útil identificar a su encargado del tratamiento si este es la causa principal de una violación, en particular si ello ha dado lugar a un incidente que afecta a los registros de datos personales de muchos otros responsables del tratamiento que recurren al mismo encargado del tratamiento.

En cualquier caso, la autoridad de control podrá solicitar más detalles en el marco de su investigación de una violación.

2. Notificación gradual

Dependiendo de la naturaleza de la violación, puede ser necesario que el responsable del tratamiento siga investigando para establecer todos los hechos pertinentes relacionados con el incidente. Así, el artículo 33, apartado 4, dispone:

«Si no fuera posible facilitar la información simultáneamente, y en la medida en que no lo sea, la información se facilitará de manera gradual sin dilación indebida».

Esto significa que el RGPD reconoce que los responsables del tratamiento no siempre dispondrán de toda la información necesaria sobre una violación en un plazo de setenta y dos horas a partir del momento en que tengan constancia de la misma, ya que es posible que no siempre se disponga de detalles completos y exhaustivos del incidente durante este período inicial. Como tal, permite una notificación gradual. Es más probable que esto ocurra en el caso de violaciones más complejas, como algunos tipos de incidentes de ciberseguridad en los que, por ejemplo, puede ser necesaria una investigación forense pormenorizada para determinar plenamente la naturaleza de la violación y en qué medida se han visto comprometidos los datos personales. Por consiguiente, en muchos casos el responsable del tratamiento tendrá que investigar más a fondo y hacer un seguimiento con información adicional en una fase posterior. Esto es admisible, siempre que el responsable del tratamiento justifique el retraso, de conformidad con el artículo 33, apartado 1. El GT29 recomienda que cuando el responsable del tratamiento contacte la primera vez con la autoridad de control para efectuar la notificación, también le indique si no dispone aún de toda la información requerida y que, con posterioridad, proporcionará más detalles. La autoridad de control debe estar de acuerdo en cómo y cuándo debe facilitarse la información adicional. Ello no impide que el responsable del tratamiento facilite más información en cualquier otra fase si tiene conocimiento de detalles adicionales pertinentes sobre la violación que deban facilitarse a la autoridad de control.

El objetivo del requisito de notificación es alentar a los responsables del tratamiento a que actúen con prontitud en caso de violación, contenerla y, si es posible, recuperar los datos personales comprometidos, así como recabar el asesoramiento pertinente de la autoridad de control. El hecho de notificar a la autoridad de control dentro de las primeras setenta y dos horas puede permitir que el responsable del tratamiento se asegure de que las decisiones sobre si debe o no notificar a las personas sean correctas.

Sin embargo, el propósito de la notificación a la autoridad de control no es únicamente obtener orientación sobre si se debe notificar a las personas afectadas. En algunos casos será obvio que, debido a la naturaleza de la violación y a la gravedad del riesgo, el responsable del tratamiento deberá notificarlo sin dilación 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[26], el responsable del tratamiento debe actuar sin dilación indebida para contener la violación y comunicarla a las personas afectadas (véase la sección III). En circunstancias excepcionales, esto podría ocurrir incluso antes de la notificación a la autoridad de control. En términos más generales, la notificación de la autoridad de control no puede servir de justificación para no comunicar la violación al interesado cuando sea necesario.

También debe quedar claro que, después de efectuar una notificación inicial, un responsable del tratamiento puede informar a la autoridad de control si en una investigación de seguimiento se descubren pruebas de que se había contenido el incidente de seguridad y de que no se había producido realmente ninguna violación. Esta información podría entonces añadirse a la ya facilitada a la autoridad de control y, por consiguiente, registrar el incidente como una no violación. No hay sanciones por informar sobre un incidente que, en última instancia, resulta no ser una violación.

Ejemplo

Un responsable del tratamiento notifica a la autoridad de control dentro de las setenta y dos horas siguientes a la detección de una violación que ha perdido una llave USB que contiene una copia de los datos personales de algunos de sus clientes. Con posterioridad, la llave USB se encuentra mal archivada dentro de las instalaciones del responsable del tratamiento y se recupera. El responsable del tratamiento informa a la autoridad de control y solicita que se modifique la notificación.

[26] Véase el artículo 9.

Cabe señalar que ya existe un enfoque gradual de la notificación en virtud de las obligaciones existentes de la Directiva 2002/58/CE, el Reglamento (UE) n.º 611/2013 y otros incidentes autodeclarados.

3. Retraso en la notificación

El artículo 33, apartado 1, establece claramente que si la notificación a la autoridad de control no tiene lugar en el plazo de setenta y dos horas, deberá ir acompañada de indicación de los motivos de la dilación. Esto, junto con el concepto de notificación gradual, reconoce que un responsable del tratamiento no siempre puede notificar una violación dentro de ese plazo, y que puede permitirse una notificación con retraso.

Esta situación podría darse cuando, por ejemplo, un responsable del tratamiento experimenta violaciones de la confidencialidad múltiples y similares en un corto período de tiempo, que afectan de la misma manera a un gran número de interesados. Un responsable del tratamiento podría tener constancia de una violación y, en el momento de iniciar su investigación y antes de la notificación, detectar otras violaciones similares y que tienen causas diferentes. Dependiendo de las circunstancias, el responsable del tratamiento puede tardar algún tiempo en determinar el alcance de las violaciones y, en lugar de notificar cada una de ellas de forma individual organiza una notificación pertinente que incluya varias violaciones muy similares, con posibles causas diferentes. Esto podría dar lugar a que la notificación a la autoridad de control se retrase más de setenta y dos horas después de que el responsable del tratamiento tenga constancia por primera vez de estas violaciones.

En sentido estricto, cada violación individual es un incidente notificable. No obstante, para evitar una carga excesiva, el responsable del tratamiento podrá presentar una notificación «agrupada» que incluya todas estas violaciones, siempre que afecten al mismo tipo de datos personales y cuya violación de la seguridad se haya producido de la misma manera, en un período de tiempo relativamente corto. Si se produce una serie de violaciones de la seguridad que afecten a diferentes tipos de datos personales y que se hayan producido de manera diferente, la notificación deberá realizarse de la forma habitual, notificándose cada violación de conformidad con el artículo 33.

Aunque el RGPD permite, hasta cierto punto, retrasar las notificaciones, esto no debería considerarse como algo que deba ocurrir con regularidad. Cabe señalar que las notificaciones agrupadas también pueden hacerse en caso de que se produzcan violaciones múltiples similares notificadas dentro del plazo de setenta y dos horas.

C. Violaciones transfronterizas y en establecimientos no pertenecientes a la UE

1. Violaciones transfronterizas

En caso de tratamiento transfronterizo[27] de datos personales, una violación puede afectar a interesados de más de un Estado miembro. El artículo 33, apartado 1, deja claro que, cuando se haya producido una violación, el responsable del tratamiento debe notificarlo a la autoridad de control competente de conformidad con el artículo 55 del RGPD[28]. El artículo 55, apartado 1, dice:

> «Cada autoridad de control será competente para desempeñar las funciones que se le asignen y ejercer los poderes que se le confieran de conformidad con el presente Reglamento en el territorio de su Estado miembro».

[27] Véase el artículo 4, apartado 23.

[28] Véase también el considerando 122.

El artículo 56, apartado 1, establece:

> «Sin perjuicio de lo dispuesto en el artículo 55, la autoridad de control del establecimiento principal o del único establecimiento del responsable o del encargado del tratamiento será competente para actuar como autoridad de control principal para el tratamiento transfronterizo realizado por parte de dicho responsable o encargado con arreglo al procedimiento establecido en el artículo 60».

El artículo 56, apartado 6, dispone:

> «La autoridad de control principal será el único interlocutor del responsable o del encargado en relación con el tratamiento transfronterizo realizado por dicho responsable o encargado».

Esto significa que siempre que se produzca una violación en el contexto de un tratamiento transfronterizo y la notificación sea obligatoria, el responsable del tratamiento deberá notificarlo a la autoridad de control principal[29]. Por tanto, a la hora de elaborar su plan de respuesta a las violaciones, el responsable del tratamiento debe evaluar qué autoridad de control es la autoridad de control principal a la que deberá presentar las notificaciones[30]. Esto permitirá al responsable del tratamiento responder con rapidez ante una violación y cumplir sus obligaciones en relación con el artículo 33. Debe quedar claro que, en caso de que se produzca una violación que implique un tratamiento transfronterizo, esta debe notificarse a la autoridad de control principal, que no está necesariamente en el lugar en el que se encuentran los interesados afectados o en el que se ha producido la violación. Cuando se notifique a la autoridad principal, el responsable del tratamiento debe indicar, en su caso, si la violación afecta a establecimientos situados en otros Estados miembros y en qué Estados miembros es probable que los interesados se hayan visto afectados por la violación. Si el responsable del tratamiento tiene alguna duda para determinar la autoridad de control principal, como mínimo deberá notificarlo a la autoridad de control local donde se haya producido la violación.

2. Violaciones en establecimientos no pertenecientes a la UE

El artículo 3 se refiere al ámbito territorial del RGPD, incluso cuando se aplica a un responsable o un encargado del tratamiento que no esté establecido en la UE. En concreto, el artículo 3, apartado 2, dispone[31]:

> «El presente Reglamento se aplica al tratamiento de datos personales de interesados que residan en la Unión por parte de un responsable o encargado no establecido en la Unión, cuando las actividades de tratamiento estén relacionadas con:
>
> a) la oferta de bienes o servicios a dichos interesados en la Unión, independientemente de si a estos se les requiere su pago, o
>
> b) el control de su comportamiento, en la medida en que este tenga lugar en la Unión».

También es pertinente el artículo 3, apartado 3, y dispone[32]:

---

[29] Véanse las Directrices para determinar la autoridad de control principal de un responsable o un encargado del tratamiento del GT29, disponibles en http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611235

[30] En la siguiente dirección puede encontrarse una lista de los datos de contacto de todas las autoridades nacionales europeas de protección de datos: http://ec.europa.eu/justice/data-protection/bodies/authorities/index_en.htm

[31] Véanse también los considerandos 23 y 24.

«El presente Reglamento se aplica al tratamiento de datos personales por parte de un responsable que no esté establecido en la Unión sino en un lugar en que el Derecho de los Estados miembros sea de aplicación en virtud del Derecho internacional público».

Cuando un responsable del tratamiento que no está establecido en la UE esté sujeto a lo dispuesto en el artículo 3, apartados 2 o 3, y tenga conocimiento de una violación, seguirá estando obligado a cumplir las obligaciones de notificación previstas en los artículos 33 y 34. El artículo 27 exige que el responsable del tratamiento (y el encargado) designe a un representante en la UE cuando sea de aplicación el artículo 3, apartado 2. En tales casos, el GT29 recomienda que se notifique a la autoridad de control del Estado miembro en el que esté establecido el representante del responsable del tratamiento en la UE[33]. Del mismo modo, cuando un encargado del tratamiento esté sujeto a lo dispuesto en el artículo 3, apartado 2, este se someterá a las obligaciones de los encargados del tratamiento, en particular a la obligación de notificar una violación al responsable del tratamiento con arreglo al artículo 33, apartado 2.

D. Condiciones en que no se requiere notificación

El artículo 33, apartado 1, deja claro que las violaciones cuando «sea improbable que dicha violación de la seguridad constituya un riesgo para los derechos y las libertades de las personas físicas» no requieren notificación a la autoridad de control. Un ejemplo podría ser cuando los datos personales ya están disponibles al público y su comunicación no constituye un riesgo probable para la persona. Esto contrasta con los actuales requisitos de notificación de violaciones para los proveedores de servicios de comunicaciones electrónicas disponibles al público de la Directiva 2009/136/CE, que establecen que todas las violaciones pertinentes deben notificarse a la autoridad competente.

En su Dictamen 03/2014 sobre la notificación de violaciones de datos personales[34], el GT29 explicó que una violación de la confidencialidad de los datos personales codificados con un algoritmo de última generación sigue siendo una violación de la seguridad de los datos personales y debe notificarse. Sin embargo, si la confidencialidad de la clave está intacta, es decir, si la clave no se ha visto comprometida en ninguna violación de la seguridad y ha sido generada de forma que ninguna persona que no esté autorizada a acceder a ella pueda determinarla con los medios técnicos disponibles, los datos son, en principio, ininteligibles. Por tanto, es poco probable que la violación afecte negativamente a las personas y, por consiguiente, no requeriría su comunicación a dichas personas[35]. No obstante, incluso cuando los datos estén cifrados, una pérdida o alteración puede tener consecuencias negativas para los interesados cuando el responsable del tratamiento no disponga de copias de seguridad adecuadas. En ese caso, sería necesario comunicárselo a los interesados, aun cuando los propios datos estuvieran sujetos a medidas de cifrado adecuadas.

El GT29 también explicó que este sería el caso si, para datos personales como las contraseñas, cifradas de forma segura con un «hash salado», el valor de hash se calculara mediante una función hash con clave criptográfica de tecnología avanzada, la clave utilizada para aplicar el algoritmo hash a los datos no se viera comprometida en ningún caso y se hubiera generado de forma que no pudiera

---

[32] Véase también el considerando 25.

[33] Véanse el considerando 80 y el artículo 27.

[34] Dictamen 03/2014 sobre notificación de violación de datos personales http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp213_es.pdf

[35] Véase también el artículo 4, apartados 1 y 2, del Reglamento (UE) n.º 611/2013.

determinarse con los medios tecnológicos disponibles por ninguna persona que no tenga autorización para acceder a ella.

Por consiguiente, si los datos personales se han hecho esencialmente ininteligibles para las partes no autorizadas y si los datos son una copia o existe una copia de seguridad, puede que no sea necesario notificar a la autoridad de control una violación de la confidencialidad que implique datos personales debidamente cifrados. Esto se debe a que es improbable que dicha violación constituya un riesgo para los derechos y las libertades de las personas. Naturalmente, esto implica que tampoco sería necesario informar a la persona, ya que es probable que no haya un riesgo alto. No obstante, hay que tener en cuenta que aunque la notificación puede no ser necesaria inicialmente si no existe probabilidad de riesgo para los derechos y las libertades de las personas, esto puede cambiar con el tiempo y habría que reevaluar el riesgo. Por ejemplo, si con posterioridad se descubre que la clave se ha visto comprometida, o se descubre una vulnerabilidad en el software de cifrado, es posible que la notificación sea necesaria.

Asimismo, debe tenerse en cuenta que si se produce una violación en la que no haya copias de seguridad de los datos personales cifrados, entonces se habrá producido una violación de la disponibilidad, lo cual podría suponer un riesgo para las personas y, por consiguiente, podría requerir notificación. Del mismo modo, cuando se produce una violación que implique la pérdida de datos personales cifrados, incluso en caso de que exista una copia de seguridad de los datos personales, todavía puede ser notificable, dependiendo del tiempo que se tarde en restaurar los datos de dicha copia de seguridad y del efecto que la falta de disponibilidad tenga en las personas. Como establece el artículo 32, apartado 1, letra c), un factor de seguridad importante es «la capacidad de restaurar la disponibilidad y el acceso a los datos personales de forma rápida en caso de incidente físico o técnico».

Ejemplo

Una violación que no requeriría notificación a la autoridad de control sería la pérdida de un dispositivo móvil cifrado de forma segura, utilizado por el responsable del tratamiento y su personal. Siempre que la clave de cifrado permanezca bajo la custodia segura del responsable del tratamiento y no se trate de la única copia de los datos personales, estos serán inaccesibles para un atacante. Esto significa que es poco probable que la violación constituya un riesgo para los derechos y las libertades de los interesados en cuestión. Si más tarde se pone de manifiesto que la clave de cifrado estaba comprometida o que el software o el algoritmo de cifrado es vulnerable, entonces el riesgo para los derechos y las libertades de las personas físicas cambiará y, por tanto, la notificación podría ser necesaria.

No obstante, el incumplimiento de lo dispuesto en el artículo 33 se producirá cuando el responsable del tratamiento no lo notifique a la autoridad de control en una situación en la que los datos no hayan sido cifrados realmente de forma segura. Por tanto, al seleccionar el software de cifrado, los controladores deben sopesar cuidadosamente la calidad y la correcta aplicación del cifrado ofrecido, entender cuál es el nivel de protección que realmente proporciona y si es apropiado para los riesgos que se presentan. Los responsables del tratamiento también deben estar familiarizados con los detalles específicos relativos al funcionamiento de su producto de cifrado. Por ejemplo, un dispositivo puede cifrarse una vez que se apaga, pero no mientras está en modo de espera. Algunos productos que utilizan cifrado tienen «claves por defecto» que los clientes deben cambiar para que sean efectivas. Los expertos en seguridad también pueden considerar que, en la actualidad, el cifrado es adecuado, pero puede quedar obsoleto en unos pocos años, lo cual significa que surgiría la duda de si ese producto cifra suficientemente los datos y proporciona un nivel adecuado de protección.

III. **Artículo 34 – Comunicación al interesado**

A. Informar a las personas

En algunos casos, además de notificar a la autoridad de control, el responsable del tratamiento también está obligado a comunicar una violación a las personas afectadas.

El artículo 34, apartado 1, establece:

> «Cuando sea probable que la violación de la seguridad de los datos personales entrañe un alto riesgo para los derechos y libertades de las personas físicas, el responsable del tratamiento la comunicará al interesado sin dilación indebida».

Los responsables del tratamiento deben recordar que la notificación a la autoridad de control es obligatoria a menos que sea improbable que exista un riesgo para los derechos y las libertades de las personas como consecuencia de una violación. Además, cuando exista la probabilidad de un alto riesgo para los derechos y las libertades de las personas como consecuencia de una violación, también se debe informar a las personas. Por tanto, el umbral para la comunicación a las personas es más elevado que para la notificación a las autoridades de control y, por tanto, no se exigirá la comunicación de todas las violaciones a las personas, protegiéndolas así de un exceso de notificaciones.

El RGPD establece que la comunicación de una violación a las personas debe hacerse «sin dilación indebida», lo cual significa lo antes posible. El objetivo principal de la notificación a las personas es proporcionarles información específica sobre las medidas que deben adoptar para protegerse[36]. Como ya se ha señalado, dependiendo de la naturaleza de la violación y del riesgo que entrañe, una comunicación rápida ayudará a las personas a adoptar medidas para protegerse de sus consecuencias negativas.

En el anexo B de las presentes Directrices figura una lista no exhaustiva de ejemplos en los que es probable que una violación entrañe un alto riesgo para las personas y, por tanto, de casos en los que un responsable del tratamiento tendrá que notificar una violación a las personas afectadas.

B. Información que debe facilitarse

A la hora de notificar a las personas, el artículo 34, apartado 2, especifica que:

> «La comunicación al interesado contemplada en el apartado 1 del presente artículo 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)».

Según esta disposición, el responsable del tratamiento debe facilitar, como mínimo, la siguiente información:

- una descripción de la naturaleza de la violación;
- el nombre y los datos de contacto del delegado de protección de datos o de otro punto de contacto;
- una descripción de las posibles consecuencias de la violación; y

[36] Véase también el considerando 86.

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

Como ejemplo de las medidas adoptadas para subsanar la violación y mitigar sus posibles efectos adversos, el responsable del tratamiento podría indicar que, tras haberla notificado a la autoridad de control pertinente, ha recibido asesoramiento sobre el modo de gestionarla y de reducir su impacto. El responsable del tratamiento también debe, cuando proceda, asesorar de manera específica a las personas para que se protejan de las posibles consecuencias adversas de la violación, como establecer nuevas contraseñas si sus credenciales de acceso se han visto comprometidas. De nuevo, un responsable del tratamiento puede decidir proporcionar más información de la que se requiere aquí.

C. Contactar con las personas

En principio, la violación en cuestión debe comunicarse directamente a los interesados afectados, a menos que ello suponga un esfuerzo desproporcionado. En ese caso, se optará por una comunicación pública o una medida semejante por la que se informe de manera igualmente efectiva a los interesados [artículo 34, apartado 3, letra c)].

Para comunicar una violación a los interesados se deben utilizar mensajes específicos y no se deben enviar junto con otra información, como actualizaciones periódicas, boletines informativos o mensajes normalizados. Esto ayuda a que la comunicación de la violación sea clara y transparente.

Ejemplos de métodos de comunicación transparentes son la mensajería directa (por ejemplo, correo electrónico, SMS, mensajes directos), los anuncios web destacados, las comunicaciones postales y los anuncios prominentes en medios de comunicación impresos. Una notificación que se limite únicamente a un comunicado de prensa o a un blog corporativo no sería un medio eficaz para comunicar una violación a una persona. El GT29 recomienda que los responsables del tratamiento elijan un medio que aumente al máximo la posibilidad de comunicar la información a todas las personas afectadas de forma adecuada. Dependiendo de las circunstancias, esto puede implicar que el responsable del tratamiento emplee varios métodos de comunicación, en lugar de utilizar un solo canal de contacto.

Es posible que los responsables del tratamiento también tengan que asegurarse de que la comunicación esté accesible en formatos alternativos apropiados y en los idiomas pertinentes con el fin de garantizar que las personas puedan comprender la información que se les proporciona. Por ejemplo, cuando se comunique una violación a una persona, el lenguaje utilizado previamente durante el curso normal de las actividades con el destinatario será, en general, apropiado. Sin embargo, si la violación afecta a interesados con los que el responsable del tratamiento no haya interactuado con anterioridad o, particularmente a aquellos que residan en un Estado miembro diferente o en otro tercer país distinto de aquel en que el responsable del tratamiento esté establecido, la comunicación en la lengua nacional local podría ser aceptable, teniendo en cuenta los recursos necesarios. La clave es ayudar a los interesados a comprender la naturaleza de la violación y las medidas que pueden adoptar para protegerse.

Los responsables del tratamiento son los más indicados para determinar cuál es el canal de contacto más apropiado para comunicar una violación a las personas, en particular si interactúan con sus clientes con frecuencia. Sin embargo, es evidente que un responsable del tratamiento debe evitar utilizar un canal de contacto que la violación haya comprometido, ya que este canal también podrían utilizarlo los atacantes que se hacen pasar por él.

Al mismo tiempo, el considerando 86 explica que:

«Dichas comunicaciones a los interesados deben realizarse tan pronto como sea razonablemente posible y en estrecha cooperación con la autoridad de control, siguiendo sus orientaciones o las de

otras autoridades competentes, como las autoridades policiales. Así, por ejemplo, la necesidad de mitigar un riesgo de daños y perjuicios inmediatos justificaría una rápida comunicación con los interesados, mientras que cabe justificar que la comunicación lleve más tiempo por la necesidad de aplicar medidas adecuadas para impedir violaciones de la seguridad de los datos personales continuas o similares».

Por consiguiente, los responsables del tratamiento tal vez deseen ponerse en contacto con la autoridad de control y consultarla no solo para pedir asesoramiento sobre la información a los interesados en relación con una violación de conformidad con el artículo 34, sino también sobre la adecuación de los mensajes que deben enviarse a las personas, así como la forma más adecuada de ponerse en contacto con ellas.

A este respecto está el consejo del considerado 88 de que la notificación de una violación debe «tener en cuenta los intereses legítimos de las autoridades policiales en caso de que una comunicación prematura pueda obstaculizar innecesariamente la investigación de las circunstancias de una violación de la seguridad de los datos personales». Ello puede significar que, en determinadas circunstancias, cuando esté justificado, y con el asesoramiento de las autoridades policiales, el responsable del tratamiento podrá retrasar la comunicación de la violación a las personas afectadas hasta el momento en que no perjudique dichas investigaciones. No obstante, los interesados deberán ser informados sin dilación una vez transcurrido este plazo.

Cuando no sea posible que el responsable del tratamiento comunique una violación a una persona porque los datos almacenados sean insuficientes para ponerse en contacto con ella, en esa circunstancia concreta, el responsable del tratamiento deberá informar a la persona tan pronto como sea razonablemente posible (por ejemplo, cuando una persona ejerza su derecho de acceso a los datos personales con arreglo al artículo 15 y facilite al responsable del tratamiento la información adicional necesaria para ponerse en contacto con ella).

D. Condiciones en que no se requiere comunicación

El artículo 34, apartado 3, establece tres condiciones que, si se cumplen, no requieren notificación a las personas en caso de violación. Estas condiciones son:

- Que el responsable del tratamiento haya adoptado medidas de protección técnicas y organizativas apropiadas para proteger los datos personales antes de la violación, en particular aquellas que los hagan ininteligibles para cualquier persona que no esté autorizada a acceder a ellos. Por ejemplo, esto podría incluir la protección de datos personales con un cifrado de tecnología avanzada o mediante tokenización.
- Que, inmediatamente después de una violación, el responsable del tratamiento haya tomado medidas que garanticen que ya no exista la probabilidad de que se concretice el alto riesgo para los derechos y libertades de la persona. Por ejemplo, dependiendo de las circunstancias del caso, el responsable del tratamiento podría haber identificado inmediatamente a la persona que accedió a los datos personales y tomar medidas contra ella, antes de que pudiera hacer nada con ellos. Es preciso prestar la debida atención a las posibles consecuencias de cualquier violación de la confidencialidad, de nuevo, en función de la naturaleza de los datos en cuestión.
- Que suponga un esfuerzo desproporcionado[37] ponerse en contacto con las personas, quizás cuando sus datos de contacto se hayan perdido como resultado de la violación o, de entrada, no se conozcan. Por ejemplo, el almacén de una oficina de estadística se ha inundado y los

[37] Véanse las Directrices sobre transparencia del GT29, que examinarán la cuestión del esfuerzo desproporcionado, disponibles en http://ec.europa.eu/newsroom/just/document.cfm?doc_id=48850

documentos que contienen los datos personales solo estaban almacenados en papel. A cambio, el responsable del tratamiento debe hacer una comunicación pública o adoptar una medida semejante por la que se informe de manera igualmente efectiva a los interesados. En caso de esfuerzo desproporcionado, también podrían preverse disposiciones técnicas para que la información sobre la violación esté disponible a petición del interesado, lo cual podría resultar útil para las personas que puedan verse afectadas por una violación, pero con las que el responsable del tratamiento no pueda ponerse en contacto de otro modo.

De conformidad con el principio de obligación de rendir cuentas, los responsables del tratamiento deben poder demostrar a las autoridades de control que cumplen una o varias de estas condiciones[38]. Hay que tener en cuenta que, si bien la notificación puede no ser necesaria inicialmente si no existe un riesgo para los derechos y las libertades de las personas, esto puede cambiar con el tiempo y habría que reevaluar el riesgo.

Si un responsable del tratamiento decide no comunicar una violación a la persona, el artículo 34, apartado 4, explica que la autoridad de control puede exigirle que lo haga si considera que dicha violación puede entrañar un alto riesgo para las personas. Por otra parte, puede considerar que se han cumplido las condiciones del artículo 34, apartado 3, en cuyo caso no se requiere notificación. Si la autoridad de control determina que la decisión de no notificar a los interesados no está bien fundamentada, podrá considerar la posibilidad de hacer uso de las facultades y sanciones de que dispone.

IV. **Evaluación del riesgo y riesgo alto**

A. El riesgo como desencadenante de la notificación

Aunque el RGPD introduce la obligación de notificar una violación, no es obligatorio hacerlo en todas las circunstancias:

- La notificación a la autoridad de control competente es obligatoria a menos que sea improbable que una violación constituya un riesgo para los derechos y las libertades de las personas.
- La comunicación de una violación a la persona solo se realizará cuando sea probable que entrañe un alto riesgo para sus derechos y libertades.

Esto significa que, 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. Hay dos razones importantes para ello: en primer lugar, conocer la probabilidad y la gravedad potencial del impacto en la persona ayudará al responsable del tratamiento a adoptar medidas eficaces para contener y poner remedio a la violación; en segundo lugar, le ayudará a determinar si la notificación a la autoridad de control es necesaria y, en su caso, a las personas afectadas.

Como se ha explicado anteriormente, la notificación de una violación es obligatoria a menos que sea improbable que constituya un riesgo para los derechos y las libertades de las personas, y el factor clave que exige la comunicación de una violación a los interesados es cuando sea probable que entrañe un *alto* riesgo para los derechos y las libertades de las personas. Este riesgo existe cuando la violación puede dar lugar a daños y perjuicios físicos, materiales o inmateriales para las personas cuyos datos han sido violados. Ejemplos de tales daños y perjuicios son la discriminación, la

[38] Véase el artículo 5, apartado 2.

usurpación de identidad o el fraude, la pérdida financiera y el daño para la reputación. 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[39].

B. Factores a tener en cuenta a la hora de evaluar el riesgo

Los considerandos 75 y 76 del RGPD señalan que, en general, al evaluar el riesgo, debe tenerse en cuenta tanto la probabilidad como la gravedad del riesgo para los derechos y las libertades de los interesados. Además, se señala que el riesgo debe evaluarse sobre la base de una valoración objetiva.

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[40]. 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.

Ejemplo

Una EIPD indica que el uso propuesto de un determinado programa informático de seguridad con el fin de proteger los datos personales es una medida apropiada para garantizar un nivel de seguridad adecuado al riesgo que, de otro modo, entrañaría el tratamiento para las personas. Sin embargo, si posteriormente se tiene conocimiento de una vulnerabilidad, esto cambiaría la idoneidad del programa informático respecto de la contención del riesgo para los datos personales protegidos, por lo que habría que volver a evaluarla como parte de una EIPD continua.

Con posterioridad, se explota una vulnerabilidad del producto y se produce una violación. El responsable del tratamiento debe evaluar las circunstancias específicas de la violación, los datos afectados y el nivel potencial de impacto en las personas, así como la probabilidad de que este riesgo se materialice.

Por consiguiente, 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. Por tanto, el GT29 recomienda que la evaluación tenga en cuenta los siguientes criterios[41]:

- El tipo de violación

[39] Véanse los considerandos 75 y 85.

[40] Véanse las Directrices sobre la evaluación de impacto relativa a la protección de datos del GT29 en: http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611236

[41] En el artículo 3, apartado 2, del Reglamento (UE) n.º 611/2013 se proporcionan orientaciones sobre los factores que deben tenerse en cuenta respecto de la notificación de las violaciones de la seguridad de datos personales en el sector de los servicios de comunicaciones electrónicas, las cuales pueden ser útiles en el contexto de la notificación en el marco del Reglamento RGPD. Véase https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2013:173:0002:0008:eS:PDF

El tipo de violación que se haya producido puede afectar al nivel de riesgo que presente para las personas. Por ejemplo, una violación de la confidencialidad por la que se haya revelado información médica a partes no autorizadas podría tener para una persona un conjunto de consecuencias diferente que las que podría tener una violación en la que los datos médicos de una persona se hayan perdido y ya no estén disponibles.

- La naturaleza, el carácter sensible y el volumen de datos personales

Por supuesto, al evaluar el riesgo, un factor clave es el tipo y la sensibilidad de los datos personales que se hayan visto comprometidos a causa de la violación. Por lo general, cuanto más sensibles sean los datos, mayor será el riesgo de daño para las personas afectadas, pero también deben tenerse en cuenta otros datos personales que ya puedan estar disponibles sobre el interesado. Por ejemplo, es poco probable que la divulgación del nombre y la dirección de una persona cause daños y perjuicios sustanciales en circunstancias normales. Sin embargo, si se revela el nombre y la dirección de un padre adoptivo a un padre biológico, las consecuencias podrían ser muy graves tanto para el padre adoptivo como para el niño.

Las violaciones que implican datos relativos a la salud, documentos de identidad o datos financieros como detalles de tarjetas de crédito, pueden causar daño por sí mismas, pero juntas podrían utilizarse con fines de usurpación de identidad. Una combinación de datos personales suele ser más delicada que un único dato personal.

Algunos tipos de datos personales pueden parecer al principio relativamente inocuos, sin embargo, la información que esos datos puedan revelar sobre la persona afectada debe examinarse cuidadosamente. Una lista de clientes que aceptan entregas regulares puede no ser especialmente sensible, pero los mismos datos sobre los clientes que han solicitado que se interrumpan sus entregas durante las vacaciones serían una información útil para los delincuentes.

Del mismo modo, una pequeña cantidad de datos personales muy sensibles puede tener un impacto elevado en una persona, y una gran variedad de detalles puede revelar una mayor diversidad de información sobre esa persona. Asimismo, una violación que afecte a un gran volumen de datos personales sobre muchos interesados puede tener efectos para el correspondiente gran número de personas.

- Facilidad de identificación de las personas

Un factor importante a tener en cuenta es lo fácil que será para una parte que tenga acceso a datos personales comprometidos identificar a personas específicas, o comparar los datos con otra información para identificar a esas personas. Dependiendo de las circunstancias, la identificación podría ser posible directamente a partir de los datos personales violados sin necesidad de realizar una investigación especial para descubrir la identidad de la persona, o cotejar los datos personales con los de una persona en particular podría ser extremadamente difícil, pero esto aún sería posible en determinadas condiciones. La identificación sería posible de forma directa o indirecta a partir de los datos violados, pero también podría depender del contexto específico de la violación y el acceso público a datos personales relacionados. Esto puede ser más relevante para las violaciones de la confidencialidad y la disponibilidad.

Como se ha indicado anteriormente, los datos personales protegidos mediante un nivel adecuado de cifrado serán ininteligibles para personas no autorizadas que no dispongan de la clave de descifrado. Además, una «seudonimización» correctamente realizada (definida en el artículo 4, apartado 5, como «el tratamiento de datos personales de manera tal que ya no puedan atribuirse a un interesado sin utilizar información adicional, siempre que dicha información adicional figure por separado y esté sujeta a medidas técnicas y organizativas destinadas a garantizar que los datos personales no se atribuyan a una persona física identificada o identificable») también puede reducir la probabilidad de

identificación de personas en caso de una violación. Sin embargo, no se puede considerar que las técnicas de seudonimización por sí solas hagan que los datos sean ininteligibles.

- Gravedad de las consecuencias para las personas.

Dependiendo de la naturaleza de los datos personales implicados en una violación, por ejemplo, si se trata de categorías especiales de datos, los posibles daños y perjuicios que se derivan para las personas pueden ser especialmente graves, en particular cuando la violación podría dar lugar a una usurpación de identidad o fraude, daño físico, sufrimiento psicológico, humillación o daño para la reputación. Si la violación se refiere a datos personales de personas vulnerables, estas podrían correr un mayor riesgo de sufrir daños.

El hecho de que el responsable del tratamiento tenga constancia de que los datos personales están en manos de personas cuyas intenciones se desconocen o son posiblemente maliciosas puede influir en el nivel de riesgo potencial. Puede producirse una violación de la confidencialidad por la que se revelen datos personales a un tercero, tal como se define en el artículo 4, apartado 10, o a otro destinatario por error. Esto puede ocurrir, por ejemplo, cuando los datos personales se envían accidentalmente al departamento equivocado de una organización, o a una organización proveedora habitualmente utilizada. El responsable del tratamiento podrá pedir al destinatario que devuelva o destruya de forma segura los datos que haya recibido. En ambos casos, dado que el responsable del tratamiento mantiene una relación permanente con ellos, y puede conocer sus procedimientos, historia y otros detalles relevantes, el destinatario puede considerarse «de confianza». En otras palabras, el responsable del tratamiento puede tener un cierto grado de garantía con el destinatario, de modo que puede esperar razonablemente que no lea ni acceda a los datos enviados por error y que cumpla con sus instrucciones de devolverlos. Incluso si se ha accedido a los datos, el responsable del tratamiento todavía puede confiar en que el destinatario no hará nada con ellos, los devolverá rápidamente al responsable del tratamiento y cooperará para su recuperación. En tales casos, esto puede tenerse en cuenta en la evaluación del riesgo que el responsable del tratamiento lleve a cabo tras el incumplimiento: el hecho de que se confíe en el destinatario puede eliminar la gravedad de las consecuencias del incumplimiento, pero no significa que dicho incumplimiento no se haya producido. Sin embargo, esto puede eliminar también la probabilidad de riesgo para las personas, por lo que ya no es necesario notificarlo a la autoridad de control ni a las personas afectadas. De nuevo, esto dependerá de cada caso particular. No obstante, el responsable del tratamiento debe conservar la información relativa a esta violación como parte de la obligación general de llevar registros de las violaciones (véase la sección V, más adelante).

También se debe tener en cuenta la permanencia de las consecuencias para las personas cuando se considere que el impacto es mayor si los efectos son a largo plazo.

- Características particulares de la persona

Una violación puede afectar a los datos personales de niños u otras personas vulnerables que, como consecuencia de ello, pueden verse expuestos a un mayor peligro. Puede haber otros factores relativos al individuo susceptibles de afectar el nivel de impacto que dicha violación puede tener en ellos.

- Características particulares del responsable del tratamiento

La naturaleza y el papel del responsable del tratamiento y sus actividades pueden afectar al nivel de riesgo que una violación podría tener para las personas. Por ejemplo, una organización médica tratará categorías especiales de datos personales, lo cual significa que si se violan sus datos personales la amenaza para las personas es mayor que si se tratara de la lista de distribución de un periódico.

- El número de personas afectadas

Una violación puede afectar solo a una persona, a unas pocas o a varias miles, o incluso a muchas más. En general, cuanto mayor sea el número de personas afectadas, mayor puede ser su impacto. Sin embargo, una violación puede tener un impacto grave incluso en una sola persona, dependiendo de la naturaleza de los datos personales y del contexto en el que se hayan visto comprometidos. De nuevo, la clave es tener en cuenta la probabilidad y la gravedad del impacto en los afectados.

- Consideraciones generales

Por tanto, a la hora de evaluar el riesgo que puede entrañar una violación, el responsable del tratamiento debe tener en cuenta una combinación de la gravedad del impacto potencial en los derechos y las libertades de las personas y la probabilidad de que este se produzca. Evidentemente, cuando las consecuencias de una violación son más graves, el riesgo es más elevado y, del mismo modo, cuando la probabilidad de que se produzcan es mayor, el riesgo también aumenta. En caso de duda, el responsable del tratamiento debe pecar por exceso de precaución y notificar. En el anexo B se proporcionan algunos ejemplos útiles de diferentes tipos de violaciones que implican riesgo o riesgo alto para las personas.

La Agencia de Seguridad de las Redes y de la Información de la Unión Europea (ENISA) ha elaborado una serie de recomendaciones para una metodología de evaluación de la gravedad de una violación, que los responsables y los encargados del tratamiento pueden considerar útil a la hora de diseñar su plan de respuesta de gestión de violaciones[42].

V. **Responsabilidad proactiva y llevanza de registros**

A. Documentación de las violaciones

Independientemente de si una violación debe notificarse o no a la autoridad de control, el responsable del tratamiento debe conservar la documentación de todas las violaciones, como se explica en el artículo 33, apartado 5:

> «El responsable del tratamiento documentará cualquier violación de la seguridad de los datos personales, incluidos los hechos relacionados con ella, sus efectos y las medidas correctivas adoptadas. Dicha documentación permitirá a la autoridad de control verificar el cumplimiento de lo dispuesto en el presente artículo».

Esto está ligado al principio de responsabilidad proactiva del RGPD contenido en el artículo 5, apartado 2. La finalidad de registrar las violaciones no notificables, así como las notificables, también está relacionada con las obligaciones del responsable del tratamiento con arreglo al artículo 24, y las autoridades de control pueden solicitar ver dichos registros. Por consiguiente, se alienta a los controladores a que establezcan un registro interno de violaciones, independientemente de si están obligados a notificarlas o no[43].

[42] ENISA, *Recommendations for a methodology of the assessment of severity of personal data breaches*, https://www.enisa.europa.eu/publications/dbn-severity

[43] El responsable del tratamiento podrá optar por documentar las violaciones como parte de su registro de actividades de tratamiento, que se lleva de conformidad con el artículo 30. No se requiere un registro separado, siempre que la información relativa a la violación sea claramente identificable como tal y pueda extraerse previa solicitud.

Si bien corresponde al responsable del tratamiento determinar el método y la estructura que debe utilizarse para documentar una violación existen, por lo que respecta a la información que se puede registrar, elementos clave que deben incluirse en todos los casos. Como exige el artículo 33, apartado 5, el responsable del tratamiento debe registrar los detalles relativos a la violación, que deben incluir sus causas, lo sucedido y los datos personales afectados. También debe incluir los efectos y las consecuencias de la violación, así como las medidas correctivas adoptadas por el responsable del tratamiento.

El RGPD no especifica un período para conservar esta documentación. Cuando dichos registros contengan datos personales, corresponderá al responsable del tratamiento determinar el período de conservación adecuado de conformidad con los principios relativos al tratamiento de datos personales[44] y cumplir una base jurídica para el tratamiento[45]. Deberá conservar la documentación de conformidad con el artículo 33, apartado 5, en la medida en que pueda exigírsele que presente pruebas del cumplimiento de dicho artículo a la autoridad de control o, en general, con el principio de la obligación de responsabilidad proactiva. Evidentemente, si los registros no contienen datos personales, entonces no se aplica el principio de limitación del plazo de conservación[46] del RGPD.

Además de estos detalles, el GT29 recomienda que el responsable del tratamiento documente también su razonamiento de las decisiones adoptadas en respuesta a una violación. En particular, si no se notifica una violación, debe documentarse la justificación de dicha decisión. Esto debe incluir las razones por las que el responsable del tratamiento considera que es improbable que la violación constituya un riesgo para los derechos y las libertades de las personas[47]. En cambio, si el responsable del tratamiento considera que se cumple alguna de las condiciones del artículo 34, apartado 3, debe estar en disposición de aportar pruebas adecuadas de ello.

Cuando el responsable del tratamiento notifique una violación a la autoridad de control, pero lo haga con retraso, el responsable del tratamiento deberá poder justificar dicho retraso; la documentación relativa a esta cuestión podría ayudar a demostrar que el retraso en la comunicación está justificado y no es excesivo.

Cuando el responsable del tratamiento comunique una violación a las personas afectadas, deberá ser transparente al respecto y comunicar de manera eficaz y en tiempo oportuno. En consecuencia, conservar pruebas de dicha comunicación ayudaría al responsable del tratamiento a demostrar la responsabilidad proactiva y el cumplimiento.

Para facilitar el cumplimiento de los artículos 33 y 34, sería ventajoso tanto para los responsables como para los encargados del tratamiento disponer de un procedimiento de notificación documentado, en el que se establezca el proceso que debe seguirse una vez detectada una violación, incluida la forma de contener, gestionar y subsanar el incidente, así como de evaluar el riesgo y notificar la violación. A este respecto, para demostrar el cumplimiento del RGPD también podría ser útil demostrar que se ha informado a los empleados sobre la existencia de dichos procedimientos y mecanismos y que estos saben cómo reaccionar ante las violaciones.

Cabe señalar que no documentar de forma adecuada una violación puede dar lugar a que la autoridad de control ejerza las facultades que le confiere el artículo 58 o imponga una multa administrativa de conformidad con el artículo 83.

---

[44] Véase el artículo 5.

[45] Véanse los artículos 6 y 9.

[46] Véase el artículo 5, apartado 1, letra e).

[47] Véase el considerando 85.

B. Función del delegado de protección de datos

El responsable o el encargado del tratamiento podrán tener un delegado de protección de datos (DPD)[48], bien en virtud de lo dispuesto en el artículo 37, bien de forma voluntaria como buena práctica. El artículo 39 del RGPD establece una serie de tareas obligatorias para el DPD, pero no impide que el responsable del tratamiento le asigne, si procede, otras tareas.

De especial importancia para la notificación de violaciones, las tareas obligatorias del DPD incluyen, entre otras, proporcionar asesoramiento e información en materia de protección de datos al responsable o al encargado del tratamiento, supervisar el cumplimiento del RGPD y asesorar en relación con las EIPD. Además, el DPD debe cooperar con la autoridad de control y actuar como punto contacto con dicha autoridad y con los interesados. Asimismo, cabe señalar que, a la hora de notificar la violación a las autoridades de control, el artículo 33, apartado 3, letra b), exige que el responsable del tratamiento facilite el nombre y los datos de contacto de su DPD u otro punto de contacto.

Por lo que se refiere a la documentación de las violaciones, es posible que el responsable o el encargado del tratamiento deseen obtener la opinión de su DPD sobre su estructura, configuración y administración. Además, podría encomendarse al DPD la función de mantener dichos registros.

Estos factores significan que el DPD debe desempeñar un papel clave a la hora de ayudar a prevenir una violación o a prepararse proporcionando asesoramiento y supervisión del cumplimiento, así como durante una violación (es decir, cuando se notifica a la autoridad de control) y durante cualquier investigación posterior por parte de la autoridad de control. En este sentido, el GT29 recomienda que el DPD sea informado con rapidez de la existencia de una violación y que participe en todo el proceso de gestión y de notificación de la misma.

VI. Obligaciones de notificación en virtud de otros instrumentos jurídicos

Los responsables del tratamiento deben ser conscientes de los requisitos de notificación y comunicación de violaciones en virtud del RGPD, pero también de cualquier obligación de notificar incidentes de seguridad en virtud de otra legislación asociada aplicable y de si ello puede requerir, al mismo tiempo, la notificación de una violación de la seguridad de los datos personales a la autoridad de control. Estos requisitos pueden variar de un Estado miembro a otro, pero entre los ejemplos de requisitos de notificación que figuran en otros instrumentos jurídicos y la forma en que estos se interrelacionan con el RGPD cabe citar los siguientes:

- el Reglamento (UE) n.º 910/2014 relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior (Reglamento eIDAS)[49];

El artículo 19, apartado 2, del Reglamento eIDAS establece que los prestadores de servicios de confianza notifiquen a su órgano de supervisión cualquier violación de la seguridad o pérdida de la integridad que tenga un impacto significativo en el servicio de confianza prestado o en los datos personales correspondientes. Cuando proceda, es decir, cuando dicha violación o pérdida constituya también una violación de la seguridad de los datos personales según el RGPD, el proveedor de servicios de confianza también debe notificarlo a la autoridad de control.

[48] Véanse las Directrices sobre los DPD del GT en: http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612048

[49] Véase https://eur-lex.europa.eu/legal-content/ES/TXT/?qid=1533896164443&uri=CELEX:32014R0910

- Directiva (UE) 2016/1148 relativa a las medidas destinadas a garantizar un elevado nivel común de seguridad de las redes y sistemas de información en la Unión (Directiva RSI)[50].

Los artículos 14 y 16 de la Directiva RSI exigen que los operadores de servicios esenciales y los proveedores de servicios digitales notifiquen los incidentes de seguridad a su autoridad competente. Como se reconoce en el considerando 63 de la Directiva RSI[51], los incidentes de seguridad pueden incluir a menudo un riesgo para los datos personales. Aunque la Directiva RSI dispone que las autoridades competentes y las autoridades de supervisión cooperen e intercambien información en ese contexto, sigue siendo cierto que, cuando estos incidentes constituyan violaciones de datos personales, o se conviertan en ellas, con arreglo al RGPD, se exigirá a dichos operadores o proveedores que los notifiquen a la autoridad de control de manera independiente de los requisitos de notificación de incidentes de la Directiva RSI.

Ejemplo

Un proveedor de servicios en la nube que notifique una violación con arreglo a la Directiva RSI, también puede tener que notificarla a un responsable del tratamiento si también se produce una violación de la seguridad de los datos personales. Del mismo modo, un proveedor de servicios de confianza que notifique en virtud del Reglamento eIDAS también puede estar obligado a notificar las violaciones que se produzcan a la autoridad de protección de datos pertinente.

- Directiva 2009/136/CE (Directiva sobre derechos de los ciudadanos) y Reglamento (UE) n.º 611/2013 (Reglamento de notificación de violaciones de datos personales).

Los proveedores de servicios de comunicaciones electrónicas disponibles al público en el contexto de la Directiva 2002/58/CE[52] deben notificar las violaciones a las autoridades nacionales competentes.

Los responsables del tratamiento también deben estar informados de cualquier obligación adicional de notificación legal, médica o profesional en el marco de otros regímenes aplicables.

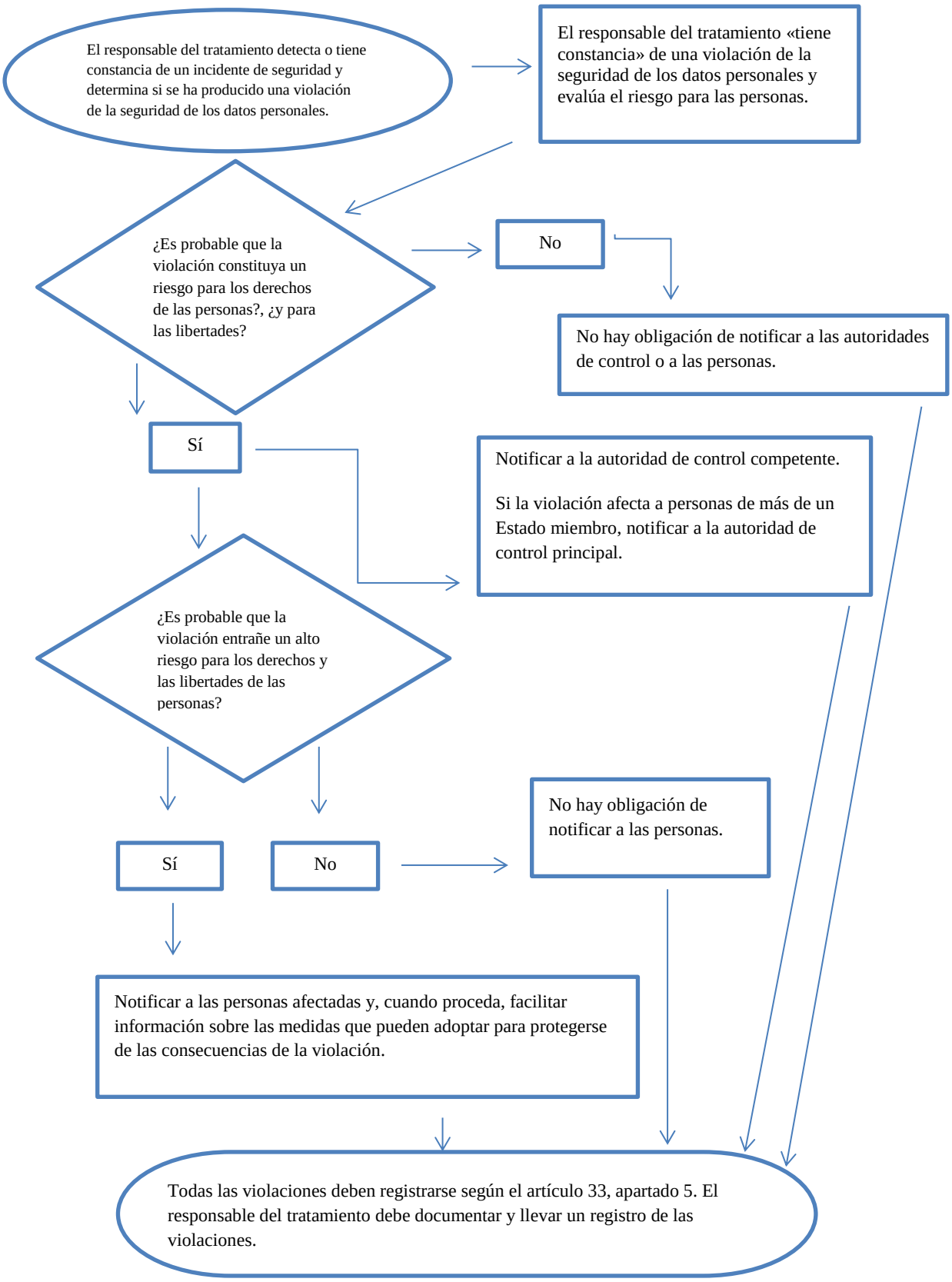
[50] Véase https://eur-lex.europa.eu/legal-content/ES/TXT/?qid=1533896016917&uri=CELEX:32016L1148

51 Considerando 63: *«En numerosas ocasiones los datos de carácter personal se ven comprometidos a raíz de incidentes. En este contexto, las autoridades competentes y las autoridades responsables de la protección de datos han de cooperar e intercambiar la información sobre todos los asuntos pertinentes ante las violaciones de datos personales derivadas de incidentes.»*

[52] El 10 de enero de 2017, la Comisión Europea propuso un Reglamento sobre la privacidad y las comunicaciones electrónicas que sustituirá a la Directiva 2009/136/CE y eliminará los requisitos de notificación. No obstante, hasta que el Parlamento Europeo apruebe esta propuesta, los requisitos de notificación existentes siguen en vigor, véase https://ec.europa.eu/digital-single-market/en/news/proposal-regulation-privacy-and-electronic-communications

VII. **Anexo**

A. Diagrama de flujo que muestra los requisitos de notificación



B. Ejemplos de violaciones de la seguridad de los datos personales y a quién deben notificarse

Los siguientes ejemplos no exhaustivos ayudarán a los responsables del tratamiento a determinar si deben notificar en diferentes situaciones de violación de la seguridad de los datos personales. Estos ejemplos también pueden ayudar a distinguir entre riesgo y riesgo alto para los derechos y las libertades de las personas.

Ejemplo	**¿Notificar a la autoridad de control?**	**¿Notificar al interesado?**	**Notas/recomendaciones**
i. Un responsable del tratamiento guardó una copia de seguridad de un archivo de datos personales cifrados en una llave USB. La llave desaparece durante un robo.	No.	No.	Puede ser una violación no notificable siempre y cuando los datos estén cifrados con un algoritmo de tecnología avanzada, existan copias de seguridad de los datos, la clave única no esté comprometida y los datos puedan restaurarse a tiempo. Sin embargo, si se compromete posteriormente, la notificación es obligatoria.
ii. Un responsable del tratamiento mantiene un servicio en línea. Como resultado de un ciberataque al servicio, se roban datos personales de individuos. El responsable del tratamiento tiene clientes en un único Estado miembro.	Sí, informe a la autoridad de control si existe la probabilidad de que haya consecuencias para las personas.	Sí, informe a las personas en función de la naturaleza de los datos personales afectados y de si la gravedad de las posibles consecuencias para las personas es alta.	
iii. Un breve fallo de alimentación que dura varios minutos en el centro de llamadas de un responsable del tratamiento, por lo que los clientes no pueden llamarle y acceder a sus registros.	No.	No.	No es una violación notificable, pero el incidente debe registrarse según el artículo 33, apartado 5. El responsable del tratamiento debe llevar los registros adecuados.
iv. Un controlador sufre el ataque de un programa de secuestro que provoca el cifrado	Sí, informe a la autoridad de control si existe la probabilidad de que haya	Sí, informe a las personas en función de la naturaleza de los datos personales	Si se dispone de una copia de seguridad y los datos pueden restaurarse a tiempo, no sería

de todos los datos. No hay copias de seguridad disponibles y los datos no se pueden restaurar. En la investigación se pone de manifiesto que la única funcionalidad del software de rescate era cifrar los datos, y que no había otro programa malicioso presente en el sistema.	consecuencias para las personas, ya que se trata de una pérdida de disponibilidad.	afectados y del posible efecto de la falta de disponibilidad de los datos, así como de otras posibles consecuencias.	necesario informar de ello a la autoridad control o a las personas, ya que no se habría producido una pérdida permanente de disponibilidad o de confidencialidad. No obstante, si las autoridades de control han tenido conocimiento del incidente por otros medios, podrán considerar la posibilidad de llevar a cabo una investigación para evaluar el cumplimiento de los requisitos de seguridad más amplios del artículo 32.
v. Una persona llama por teléfono al centro de llamadas de un banco para informar de una violación de la seguridad de los datos. La persona ha recibido un extracto mensual de otra persona. El responsable del tratamiento lleva a cabo una breve investigación (es decir, finalizada en un plazo de veinticuatro horas) y establece con un grado de confianza razonable que se ha producido una violación de la seguridad de los datos personales y si existe un fallo sistémico que podría implicar que otras personas pueden o podrían estar afectadas.	Sí.	Solo se notifica a las personas afectadas si existe un alto riesgo y es evidente que otras personas no se vieron afectadas.	Si tras una investigación más detallada se determina que más personas están afectadas, debe informarse a la autoridad de control y el responsable del tratamiento adopta la medida adicional de notificar la violación a otras personas si existe un alto riesgo para ellas.
vi. Un responsable del tratamiento gestiona un mercado en línea y	Sí, informe a la autoridad de control principal si se trata de	Sí, ya que podría dar lugar a un riesgo alto.	El responsable del tratamiento debe tomar medidas, por ejemplo,

tiene clientes en varios Estados miembros. El mercado sufre un ciberataque y el atacante publica en línea los nombres de usuario, contraseñas e historial de compras.	un tratamiento transfronterizo.		forzando el restablecimiento de las contraseñas de las cuentas afectadas, así como otras medidas para mitigar el riesgo. El responsable del tratamiento debe considerar también cualquier otra obligación de notificación, por ejemplo, en virtud de la Directiva RSI como proveedor de servicios digitales.
vii. Una empresa de alojamiento de páginas web que actúa como encargado del tratamiento de datos identifica un error en el código que controla la autorización de los usuarios. El efecto del fallo significa que cualquier usuario puede acceder a los detalles de la cuenta de cualquier otro usuario.	En tanto que encargado del tratamiento, la empresa de alojamiento de páginas web debe notificarlo a sus clientes afectados (los responsables del tratamiento) sin dilación indebida. Suponiendo que la empresa de alojamiento de páginas web haya llevado a cabo su propia investigación, los responsables del tratamiento afectados deben estar razonablemente seguros de si todos ellos han sufrido una violación y, por tanto, es probable que se considere que «tienen constancia» una vez que la empresa de alojamiento (el encargado del tratamiento) se lo haya notificado. En tal caso, el responsable del tratamiento deberá notificarlo a la autoridad de control.	Si no existe la probabilidad de un alto riesgo para las personas, no es necesario que se les notifique.	La empresa de alojamiento de páginas webs (el encargado del tratamiento) debe considerar también cualquier otra obligación de notificación (por ejemplo, en virtud de la Directiva RSI como proveedor de servicios digitales). Si no hay pruebas de que se esté explotando esta vulnerabilidad con ninguno de sus responsables del tratamiento, es posible que no se haya producido una violación notificable, pero es probable que deba registrarse o que se trate de un caso de incumplimiento con arreglo al artículo 32.

viii. Los registros médicos de un hospital no están disponibles en un período de treinta horas debido a un ciberataque.	Sí, el hospital está obligado a notificarlo, ya que puede existir un alto riesgo para el bienestar y la privacidad del paciente.	Sí, informe a las personas afectadas.	
ix. Los datos personales de un gran número de estudiantes se envían erróneamente a la lista de correo equivocada con más de mil destinatarios.	Sí, informe a la autoridad de control.	Sí, informe a las personas en función del alcance y el tipo de datos personales de que se trate y de la gravedad de las posibles consecuencias.	
x. Se envía un correo electrónico de mercadotecnia directa a los destinatarios en los campos «Para:» o «Cc.:», permitiendo así que cada destinatario vea las direcciones de correo electrónico de los otros destinatarios.	Sí, la notificación a la autoridad de control puede ser obligatoria si están afectadas un gran número de personas, si se revelan datos sensibles (por ejemplo, una lista de correo de un psicoterapeuta) o si otros factores presentan altos riesgos (por ejemplo, el correo contiene las contraseñas iniciales).	Sí, informe a las personas en función del alcance y el tipo de datos personales de que se trate y de la gravedad de las posibles consecuencias.	Puede que la notificación no sea necesaria si no se revelan datos sensibles y si solo se revela un número pequeño de direcciones de correo electrónico.