Directrices 1/2021

sobre ejemplos de notificación de violaciones de la seguridad de los datos personales

Adoptadas el 14 de diciembre de 2021

Versión 2.0

Translations proofread by EDPB Members.
This language version has not yet been proofread.

Historial de versiones

Versión 2.0	14.12.2021	Adopción de las Directrices después de la consulta pública
Versión 1.0	14.1.2021	Adopción de las Directrices para la consulta pública

Índice

EL COMITÉ EUROPEO DE PROTECCIÓN DE DATOS

Visto el artículo 70, apartado 1, letra e), del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (en adelante, «el RGPD»),

Visto el Acuerdo EEE, y en particular su anexo XI y su protocolo 37, modificado por la Decisión del Comité Mixto del EEE n.º 154/2018, de 6 de julio de 2018[1],

Vistos los artículos 12 y 22 de su Reglamento interno,

Vista la Comunicación de la Comisión al Parlamento Europeo y al Consejo titulada «La protección de datos como pilar del empoderamiento de los ciudadanos y del enfoque de la UE para la transición digital: dos años de aplicación del Reglamento General de Protección de Datos»[2],

HA ADOPTADO LAS SIGUIENTES DIRECTRICES

1 INTRODUCCIÓN

1. El RGPD introduce, en determinados casos, la obligación de notificar una violación de la seguridad de los datos personales a la autoridad nacional de control competente (en lo sucesivo, «AC») y de comunicar dicha violación a las personas cuyos datos personales se hayan visto afectados (artículos 33 y 34).

2. El Grupo de Trabajo del artículo 29 ya elaboró una orientación *general* sobre la notificación de violaciones de la seguridad de los datos en octubre de 2017, en la que analizaba las secciones pertinentes del RGPD (Directrices sobre la notificación de las violaciones de la seguridad de los datos personales de acuerdo con el Reglamento 2016/679, WP 250) (en lo sucesivo, «las Directrices WP250»)[3]. Sin embargo, debido a su naturaleza y al momento en que se publicaron, estas Directrices no abordaban todas las cuestiones prácticas con suficiente detalle. Por lo tanto, ha surgido la necesidad de una orientación *práctica basada en casos concretos* que utilice la experiencia adquirida por las AC desde que se aplica el RGPD.

3. El presente documento tiene por objeto complementar las Directrices WP 250 y refleja las experiencias comunes de las AC del EEE desde la entrada en vigor del RGPD. Su objetivo es ayudar a los responsables del

[1] Las referencias a los «Estados miembros» en el presente documento deben entenderse como referencias a los «Estados miembros del EEE».

[2] COM(2020) 264 final de 24 de junio de 2020.

[3] G29 WP250 rev.1, 6 de febrero de 2018, Directrices sobre la notificación de las violaciones de la seguridad de los datos personales de acuerdo con el Reglamento 2016/679; aprobadas por el CEPD, https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612052.

tratamiento a decidir cómo tratar las violaciones de la seguridad de los datos personales y qué factores deben tenerse en cuenta durante la evaluación del riesgo.

4. Como parte de cualquier intento de abordar una violación, el responsable y el encargado del tratamiento deben poder reconocerla en primer lugar. El RGPD define la «violación de la seguridad de los datos personales» en su artículo 4, apartado 12, 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».

5. En su Dictamen 03/2014 sobre la notificación de violación de datos personales[4] y en sus Directrices WP 250, el Grupo de Trabajo del Artículo 29 explicó que las violaciones pueden clasificarse con arreglo a los siguientes tres conocidos principios de seguridad de la información:

   - «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 a los datos personales, o la destrucción de los mismos[5].

6. Una violación puede entrañar una serie de efectos adversos significativos para las personas, lo que puede dar lugar a daños físicos, materiales o inmateriales. El RGPD explica que esto puede 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 sujetos al secreto profesional. También puede incluir cualquier otro perjuicio económico o social significativo para esas personas. Una de las obligaciones más importantes del responsable del tratamiento es evaluar estos riesgos para los derechos y libertades de los interesados y aplicar las medidas técnicas y organizativas adecuadas para abordarlos.

7. En consecuencia, el RGPD exige que el responsable del tratamiento:

   - documente cualquier violación de la seguridad de los datos personales, incluidos los hechos relacionados con ella, sus efectos y las medidas correctivas adoptadas[6];
   - notifique a la autoridad de control la violación de la seguridad de los datos personales, a menos que sea improbable que dicha violación de la seguridad constituya un riesgo para los derechos y las libertades de las personas físicas[7];

---

[4] G29 WP213, 25 de marzo de 2014, Dictamen 03/2014 sobre la notificación de violación de datos personales, p. 5, https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/index_en.htm#maincontentSec4.

[5] Véanse las Directrices WP 250, p. 7. Debe tenerse en cuenta que una violación de la seguridad de los datos puede afectar a una o varias categorías simultáneamente o combinadas.

[6] Artículo 33, apartado 5, del RGPD.

[7] Artículo 33, apartado 1, del RGPD.

- notifique al interesado la violación de la seguridad de los datos personales, 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[8].

8. Las violaciones de la seguridad de los datos son problemas de por sí, pero también pueden ser síntomas de un régimen de seguridad de datos vulnerable y posiblemente obsoleto; también pueden indicar deficiencias del sistema que deben abordarse. Como verdad general, siempre es mejor prevenir las violaciones de la seguridad preparándose por anticipado, ya que varias de sus consecuencias son, por naturaleza, irreversibles. Antes de que un responsable del tratamiento pueda evaluar *plenamente* el riesgo derivado de una violación causada por algún tipo de ataque, debe identificarse la causa principal del problema, a fin de determinar si las vulnerabilidades que dieron lugar al incidente siguen presentes y, por tanto, es posible seguir aprovechándose de ellas. En muchos casos, el responsable del tratamiento puede determinar que el incidente puede dar lugar a un riesgo, por lo que debe notificarlo. En otros casos, no es necesario posponer la notificación hasta que se haya evaluado plenamente el riesgo y la repercusión de la violación, ya que la evaluación del riesgo completa puede producirse en paralelo a la notificación y la información así obtenida puede facilitarse a la AC por fases sin más dilación indebida[9].

9. La violación debe notificarse cuando el responsable del tratamiento considere que es probable que entrañe un riesgo para los derechos y libertades del interesado. Los responsables del tratamiento deben realizar esta evaluación en el momento en que tengan conocimiento de la violación. El responsable del tratamiento no debe esperar a un examen forense detallado y a medidas (tempranas) de mitigación antes de evaluar si es probable que la violación de datos entrañe un riesgo y, por tanto, debe notificarse.

10. Si un responsable del tratamiento autoevalúa el riesgo como improbable, pero resulta que el riesgo se materializa, la autoridad de control competente puede hacer uso de sus poderes correctivos y decidir aplicar sanciones.

11. Todos los responsables y encargados del tratamiento deben contar con planes y procedimientos para tratar posibles violaciones de la seguridad de los datos. Las organizaciones deben contar con jerarquías claras y personas responsables de determinados aspectos del proceso de recuperación.

12. La formación y la sensibilización sobre cuestiones de protección de datos para el personal del responsable y del encargado del tratamiento centradas en la gestión de las violaciones de la seguridad de los datos personales (identificación de un incidente de violación de la seguridad de los datos personales y nuevas medidas que deben adoptarse, etc.), también es esencial para los responsables y encargados del tratamiento. Esta formación debe repetirse periódicamente, dependiendo del tipo de actividad del tratamiento y del tamaño del responsable del tratamiento, y debe abordar las últimas tendencias y alertas procedentes de ciberataques u otros incidentes de seguridad.

13. El principio de responsabilidad proactiva y el concepto de la protección de datos desde el diseño podrían incorporar un análisis que contribuya a la propia «Guía sobre cómo tratar la violación de la seguridad de los datos personales» del responsable y del encargado del tratamiento que tenga por objeto establecer los hechos para cada aspecto del tratamiento en cada una de las fases principales de la operación. Esta guía redactada previamente proporcionaría una fuente de información mucho más rápida que permitiría a los responsables y encargados del tratamiento mitigar los riesgos y cumplir las obligaciones sin demoras

[8] Artículo 34, apartado 1, del RGPD.

[9] Artículo 33, apartado 4, del RGPD.

indebidas y garantizaría que, si se produjera una violación de la seguridad de los datos personales, las personas de la organización sabrían qué hacer y el incidente se gestionaría más rápidamente que si no existieran planes o medidas de mitigación.

14. Aunque los casos que se presentan a continuación son ficticios, se basan en casos típicos de la experiencia colectiva de las AC con las notificaciones de violaciones de la seguridad de los datos. Los análisis ofrecidos se refieren explícitamente a los casos examinados, pero con el objetivo de prestar asistencia a los responsables del tratamiento en la evaluación de sus propias violaciones de la seguridad de los datos. Cualquier modificación en las circunstancias de los casos que se describen a continuación puede dar lugar a niveles de riesgo diferentes o más significativos que, por tanto, requieren medidas diferentes o adicionales. Estas Directrices estructuran los casos en función de determinadas categorías de violaciones (por ejemplo, los ataques con programas de secuestro de archivos). A la hora de tratar una determinada categoría de violaciones, en cada caso se solicitan determinadas medidas de mitigación. Estas medidas no se repiten necesariamente en cada análisis de casos pertenecientes a la misma categoría de violaciones de la seguridad. Para los casos pertenecientes a la misma categoría, solo se establecen las diferencias. Por lo tanto, el lector debe leer todos los casos correspondientes a la categoría pertinente de una violación de la seguridad para identificar y distinguir las medidas correctas que deben adoptarse.

15. La documentación interna de una violación de la seguridad es una obligación independiente de los riesgos inherentes a dicha violación, y debe realizarse en todos y cada uno de los casos. Los casos que se presentan a continuación intentan aclarar si notificar o no la violación de la seguridad a la AC y comunicarla a los interesados afectados.

2 PROGRAMAS DE SECUESTRO

16. Una causa frecuente de una notificación de violación de la seguridad de los datos es un ataque con programas de secuestro sufrido por el responsable del tratamiento. En estos casos, un código malicioso cifra los datos personales y, posteriormente, el atacante pide al responsable del tratamiento un rescate a cambio del código de descifrado. Este tipo de ataque puede clasificarse normalmente como una violación de la disponibilidad, pero a menudo también puede producirse una violación de la confidencialidad.

2.1 CASO N.º 1: secuestro con copia de seguridad adecuada y sin exfiltración

Los sistemas informáticos de una pequeña empresa manufacturera fueron objeto a un ataque con programas de secuestro de archivos y los datos almacenados en dichos sistemas fueron cifrados. El responsable del tratamiento de datos utilizaba cifrado en reposo, por lo que todos los datos a los que accedió el programa de secuestro estaban almacenados en forma cifrada utilizando un algoritmo de cifrado de última generación. La clave de descifrado no se vio comprometida en el ataque, es decir, el atacante no pudo acceder a ella ni utilizarla indirectamente. En consecuencia, el atacante solo tuvo acceso a datos personales cifrados. En particular, ni el sistema de correo electrónico de la empresa ni los sistemas de clientes utilizados para acceder al mismo se vieron afectados. La empresa está utilizando los conocimientos especializados de una empresa externa de ciberseguridad para investigar el incidente. Se dispone de registros que permiten el seguimiento de todos los flujos de datos que salen de la empresa (incluido el correo electrónico de salida). Una vez analizados los registros y los datos recogidos por los sistemas de detección implantados por la empresa, una investigación interna apoyada por la empresa externa de ciberseguridad determinó *con certeza* que el autor solo cifró datos, sin exfiltrarlos. Los registros no muestran ningún flujo de datos de salida en el intervalo del ataque. Los datos personales afectados por la violación de la seguridad se refieren a clientes y empleados de la empresa, unas docenas de personas en total. Se disponía de una copia de seguridad y los datos se restablecieron unas horas después de que se produjera el ataque. La violación de la seguridad no ha tenido consecuencias para el funcionamiento cotidiano del responsable del tratamiento. No se produjeron retrasos en los pagos a los empleados ni en la tramitación de las solicitudes de los clientes.

17. En este caso, se obtuvieron los siguientes elementos a partir de la definición de «violación de la seguridad de los datos personales»: una violación de la seguridad dio lugar a una alteración ilícita y al acceso no autorizado a los datos personales almacenados.

2.1.1 CASO N.º 1: medidas previas y evaluación del riesgo

18. Al igual que ocurre con todos los riesgos que plantean agentes externos, la probabilidad de que un ataque con programas de secuestro de archivos tenga éxito puede reducirse drásticamente reforzando la seguridad del entorno de control de datos. La mayoría de estas violaciones pueden evitarse garantizando que se hayan adoptado las medidas de seguridad organizativas, físicas y tecnológicas adecuadas. Ejemplos de tales medidas son una gestión adecuada de los parches y el uso de un sistema adecuado de detección de programas maliciosos. Disponer de una copia de seguridad adecuada y separada ayudará a mitigar las consecuencias de un ataque exitoso en caso de que se produzca. Además, un programa de educación, formación y sensibilización de los empleados en materia de seguridad contribuirá a prevenir y reconocer este tipo de ataques. (En la sección 2.5 se incluye una lista de medidas recomendables). Entre esas medidas, una adecuada gestión de parches que garantice que los sistemas están actualizados y que se corrigen todas las vulnerabilidades conocidas de los sistemas instalados es una de las más importantes, ya que la mayoría de los ataques con programas de secuestro explotan vulnerabilidades bien conocidas.

19. Al evaluar los riesgos, el responsable del tratamiento debe investigar la violación de la seguridad y determinar el tipo de código malicioso para comprender las posibles consecuencias del ataque. Entre los riesgos que deben tenerse en cuenta se encuentra el riesgo de que los datos se hayan exfiltrado sin dejar rastro en los registros de los sistemas.

20. En este ejemplo, el atacante tuvo acceso a los datos personales y la confidencialidad de los textos codificados que contenían datos personales en forma cifrada se vio comprometida. Sin embargo, el violador no puede leer ni utilizar los datos que pudieran haberse exfiltrado, al menos por el momento. La técnica de cifrado utilizada por el responsable del tratamiento se ajusta al estado actual de la técnica. La clave de

descifrado no se vio comprometida y presumiblemente tampoco podía determinarse por otros medios. En consecuencia, los riesgos de confidencialidad para los derechos y libertades de las personas físicas se reducen a un mínimo, salvo que el progreso criptográfico haga que los datos cifrados sean inteligibles en el futuro.

21. El responsable del tratamiento debe considerar el riesgo para las personas debido a la violación de la seguridad[10]. En este caso, parece que los riesgos para los derechos y libertades de los interesados se derivan de la falta de disponibilidad de los datos personales, y la confidencialidad de los datos personales no se ve comprometida[11]. En este ejemplo, los efectos adversos de la violación de la seguridad se mitigaron poco después de que se produjera la violación de la seguridad. Disponer de un régimen de copia de seguridad[12] adecuado hace que los efectos de la violación de la seguridad sean menos graves y, en este caso, el responsable del tratamiento pudo hacer un uso eficaz de ella.

22. En cuanto a la gravedad de las consecuencias para los interesados, solo pudieron determinarse consecuencias menores, ya que los datos afectados se restablecieron en unas horas, la violación no tuvo consecuencias para el funcionamiento cotidiano del responsable del tratamiento y no tuvo ningún efecto significativo en los interesados (por ejemplo, pagos a los empleados o tramitación de solicitudes de clientes).

2.1.2 CASO N.º 1: mitigación y obligaciones

23. Sin una copia de seguridad, pocas medidas puede tomar el responsable del tratamiento para subsanar la pérdida de datos personales, y los datos deben recogerse de nuevo. Sin embargo, en este caso concreto, los efectos del ataque podrían controlarse de manera eficaz restableciendo todos los sistemas comprometidos a un estado limpio que se sabe que está como libre de códigos maliciosos, corrigiendo las vulnerabilidades y recuperando los datos afectados poco después del ataque. Sin una copia de seguridad, los datos se pierden y la gravedad puede aumentar debido a que los riesgos o las repercusiones para las personas también pueden hacerlo.

---

[10] Para las orientaciones sobre las operaciones de tratamiento «que pueden entrañar un alto riesgo», véase «Directrices sobre la evaluación de impacto relativa a la protección de datos (EIPD) y para determinar si el tratamiento "entraña probablemente un alto riesgo" a efectos del Reglamento (UE) 2016/679» del Grupo de Trabajo de Artículo 29, WP248 rev. 01, aprobadas por el CEPD, https://ec.europa.eu/newsroom/article29/items/611236, p. 9.

[11] Desde el punto de vista técnico, el cifrado de los datos implicará el «acceso» a los datos originales y, en el caso de los programas de secuestro, la supresión de los datos originales: es necesario acceder a los datos mediante un código malicioso para cifrarlos y eliminar los datos originales. Un atacante puede hacer una copia del original antes de la supresión, pero no siempre se extraerán los datos personales. A medida que avanza la investigación del responsable del tratamiento de datos, es posible que aparezca nueva información para modificar esta evaluación. El acceso que dé lugar a la destrucción, pérdida, alteración o comunicación no autorizada de los datos personales o a un riesgo para la seguridad del interesado, incluso sin interpretación de los datos, puede ser tan grave como el acceso con interpretación de los datos personales.

[12] Los procedimientos de copia de seguridad deben ser estructurados, coherentes y repetibles. Ejemplos de procedimientos complementarios son el método 3-2-1 y el método «abuelo-padre-hijo». Todo método debe probarse siempre en cuanto a la eficacia de la cobertura y el momento en que deben restablecerse los datos. Las pruebas también deben repetirse a intervalos y, especialmente, cuando se produzcan cambios en la operación de tratamiento o en sus circunstancias para garantizar la integridad del sistema.

24. La oportunidad de una recuperación eficaz de los datos a partir de la copia de seguridad disponible es una variable clave a la hora de analizar la violación. La especificación de un plazo adecuado para recuperar los datos comprometidos depende de las circunstancias únicas de la violación de que se trate. El RGPD establece que toda violación de la seguridad de los datos personales se notificará sin demora indebida y, cuando sea posible, en un plazo máximo de 72 horas. Por lo tanto, podría determinarse que en ningún caso es aconsejable superar el plazo de 72 horas, pero, cuando se trata de casos de alto nivel de riesgo, incluso el cumplimiento de este plazo puede considerarse insatisfactorio.

25. En este caso, tras una evaluación de impacto detallada y un proceso de respuesta a incidentes, el responsable del tratamiento determinó que era improbable que la violación diera lugar a un riesgo para los derechos y las libertades de las personas físicas, por lo que no es necesaria la comunicación a los interesados, ni la violación requiere una notificación a la AC. No obstante, como todas las violaciones de datos, debe documentarse de conformidad con el artículo 33, apartado 5. La organización también puede necesitar (o la AC puede pedirle posteriormente) actualizar y corregir su gestión organizativa y técnica de la seguridad de los datos personales y sus medidas y procedimientos de reducción de riesgos. En el marco de esta actualización y corrección, la organización debe investigar exhaustivamente la violación de la seguridad e identificar las causas y los métodos utilizados por el violador para evitar sucesos similares en el futuro.

Acciones necesarias en función de los riesgos detectados		
Documentación interna	Notificación a la AC	Comunicación a los interesados
✓	X	X

2.2 CASO N.º 2: secuestro sin una copia de seguridad adecuada

Uno de los ordenadores utilizados por una empresa agrícola fue objeto de un ataque con programas de secuestro y al atacante cifró sus datos. La empresa está utilizando los conocimientos especializados de una empresa externa de ciberseguridad para vigilar su red. Se dispone de registros que permiten el seguimiento de todos los flujos de datos que salen de la empresa (incluido el correo electrónico de salida). Tras analizar los registros y los datos, los demás sistemas de detección han recopilado la investigación interna asistida por la empresa de ciberseguridad y han determinado que el autor solo cifró los datos, sin exfiltrarlos. Los registros no muestran ningún flujo de datos de salida en el intervalo del ataque. Los datos personales afectados por la violación se refieren a los empleados y clientes de la empresa, unas pocas decenas de personas en total. No se han visto afectadas categorías especiales de datos. No se disponía de copias de seguridad en formato electrónico. La mayoría de los datos se recuperaron a partir de copias de seguridad en papel. La recuperación de los datos duró cinco días laborables y provocó retrasos menores en la entrega de pedidos a los clientes.

2.2.1 CASO N.º 2: medidas previas y evaluación del riesgo

26. El responsable del tratamiento debería haber adoptado las mismas medidas previas mencionadas en la parte 2.1 y en la sección 2.9. La principal diferencia con el caso anterior es la falta de copias de seguridad electrónicas y la falta de cifrado en reposo. Esto da lugar a diferencias críticas en las siguientes etapas.

27. Al evaluar los riesgos, el responsable del tratamiento debe investigar el método de infiltración y determinar el tipo de código malintencionado para comprender las posibles consecuencias del ataque. En este ejemplo, el programa de secuestro cifró los datos personales sin exfiltrarlos. Como resultado, parece que los riesgos para los derechos y libertades de los interesados se derivan de la falta de disponibilidad de los datos personales, y la confidencialidad de los datos personales no se ve comprometida. Un examen exhaustivo

de los registros del cortafuegos y sus implicaciones es esencial para determinar el riesgo. El responsable del tratamiento debe presentar las conclusiones objetivas de estas investigaciones previa solicitud.

28. El responsable del tratamiento de datos debe tener en cuenta que, si el ataque es más sofisticado, el programa malicioso tiene la funcionalidad de editar archivos de registro y eliminar el rastro. Por lo tanto, dado que los registros no se transmiten a un servidor de registro central ni se reproducen en él, incluso tras una investigación exhaustiva que determinara que los datos personales no fueron exfiltrados por el atacante, el responsable del tratamiento no puede afirmar que la ausencia de la anotación de registro demuestre la ausencia de exfiltración, por lo que no puede descartarse por completo la probabilidad de una violación de la confidencialidad.

29. El responsable del tratamiento debe evaluar los riesgos de esta violación de la seguridad[13] si el atacante tuvo acceso a los datos. Durante la evaluación del riesgo, el responsable del tratamiento también debe tener en cuenta la naturaleza, la sensibilidad, el volumen y el contexto de los datos personales afectados por la violación de la seguridad. En este caso, no se ven afectadas categorías especiales de datos personales, y la cantidad de datos vulnerados y el número de interesados afectados son bajos.

30. La recopilación de información exacta sobre el acceso no autorizado es fundamental para determinar el nivel de riesgo y prevenir un ataque nuevo o continuado. Si los datos se hubieran copiado de la base de datos, evidentemente habría sido un factor de riesgo creciente. Cuando no existan dudas sobre las características específicas del acceso ilegítimo, debe considerarse el peor escenario y el riesgo debe evaluarse en consecuencia.

31. La ausencia de una base de datos de seguridad puede considerarse un factor que incrementa el riesgo en función de la gravedad de las consecuencias para los interesados derivadas de la falta de disponibilidad de los datos.

2.2.2 CASO N.º 2: mitigación y obligaciones

32. Sin una copia de seguridad, pocas medidas puede tomar el responsable del tratamiento para subsanar la pérdida de datos personales, y los datos deben recogerse de nuevo, a menos que se disponga de otra fuente (por ejemplo, correos electrónicos de confirmación de pedidos). Sin una copia de seguridad, los datos pueden perderse y la gravedad dependerá de las consecuencias para las personas.

33. La recuperación de los datos no debe resultar excesivamente problemática[14] si los datos siguen estando disponibles en papel, pero, dada la falta de una base de datos de respaldo electrónica, se consideró necesaria una notificación a la AC, ya que la recuperación de los datos tardó algún tiempo y podría causar algunos retrasos en la entrega de los pedidos a los clientes y una cantidad considerable de metadatos (por ejemplo, registros, sellos de tiempo) podría no ser recuperable.

34. Informar a los interesados sobre la violación también puede depender del tiempo en que los datos personales no estén disponibles y de las dificultades que ello pueda causar en el funcionamiento del responsable del

[13] Para obtener orientación sobre las operaciones de tratamiento «que pueden entrañar un alto riesgo», véase la nota a pie de página 10.

[14] Esto dependerá de la complejidad y la estructura de los datos personales. En los escenarios más complejos, el restablecimiento de la integridad de los datos, la coherencia con los metadatos, la garantía de las relaciones correctas dentro de las estructuras de datos y la comprobación de la exactitud de los datos pueden requerir recursos y esfuerzos significativos.

tratamiento como consecuencia de ello (por ejemplo, retrasos en la transferencia de los pagos de los empleados). Dado que estos retrasos en los pagos y las entregas pueden dar lugar a pérdidas financieras para las personas cuyos datos se han visto comprometidos, también se podría argumentar que la violación de la seguridad puede entrañar un riesgo elevado. Asimismo, tal vez no sea posible evitar informar a los interesados si su contribución es necesaria para recuperar los datos cifrados.

35. Este caso sirve de ejemplo para un ataque con programas de secuestro con riesgo para los derechos y libertades de los interesados, pero que no alcanza un riesgo elevado. Deberá documentarse de conformidad con el artículo 33, apartado 5, y notificarse a la AC de conformidad con el artículo 33, apartado 1. La organización también puede necesitar (o la AC puede solicitarle) actualizar y corregir su gestión organizativa y técnica de la seguridad de los datos personales y sus medidas y procedimientos de reducción del riesgo.

Acciones necesarias en función de los riesgos detectados		
Documentación interna	Notificación a la AC	Comunicación a los interesados
✓	✓	X

2.3 CASO N.º 3: secuestro con copia de seguridad y sin exfiltración en un hospital

El sistema de información de un hospital/centro sanitario fue objeto de un ataque con programas de secuestro y el atacante cifró una parte significativa de sus datos. La empresa está utilizando los conocimientos especializados de una empresa externa de ciberseguridad para vigilar su red. Se dispone de registros que permiten el seguimiento de todos los flujos de datos que salen de la empresa (incluido el correo electrónico de salida). Tras analizar los registros y los datos, los demás sistemas de detección han recopilado la investigación interna asistida por la empresa de ciberseguridad y han determinado que el autor solo cifró los datos, sin exfiltrarlos. Los registros no muestran ningún flujo de datos de salida en el intervalo del ataque. Los datos personales afectados por la violación de la seguridad se refieren a los empleados y pacientes, que representaban a miles de personas. Se disponía de copias de seguridad en formato electrónico. La mayoría de los datos se recuperaron, pero esta operación duró dos días laborables y dio lugar a retrasos importantes en el tratamiento de los pacientes a los que se canceló o aplazó su cirugía, y a una reducción del nivel de servicio debido a la falta de disponibilidad de los sistemas.

2.3.1 CASO N.º 3: medidas previas y evaluación del riesgo

36. El responsable del tratamiento debería haber adoptado las mismas medidas previas mencionadas en la parte 2.1 y en la sección 2.5. La principal diferencia con el caso anterior es la elevada gravedad de las consecuencias para una parte sustancial de los interesados[15].

[15] Para obtener orientación sobre las operaciones de tratamiento «que pueden entrañar un alto riesgo», véase la nota a pie de página 10.

37. La cantidad de datos vulnerados y el número de interesados afectados son elevados, ya que los hospitales suelen tratar grandes cantidades de datos. La indisponibilidad de los datos tiene un gran impacto en una parte sustancial de los interesados. Además, existe un riesgo residual de gran gravedad para la confidencialidad de los datos de los pacientes.

38. El tipo de violación, la naturaleza, la sensibilidad y el volumen de datos personales afectados por la violación son importantes. Aunque existía una copia de seguridad de los datos y pudieron recuperarse en unos días, sigue existiendo un alto riesgo debido a la gravedad de las consecuencias para los interesados derivadas de la falta de disponibilidad de los datos en el momento del ataque y los días siguientes.

2.3.2 CASO N.º 3: mitigación y obligaciones

39. Se considera necesaria una notificación a la AC, ya que se trata de categorías especiales de datos personales y la recuperación de los datos podría llevar mucho tiempo, lo que daría lugar a importantes retrasos en la atención al paciente. La información a los interesados sobre la violación es necesaria debido al impacto para los pacientes, incluso después de recuperar los datos cifrados. Aunque se han cifrado los datos relativos a todos los pacientes tratados en el hospital durante los últimos años, solo se vieron afectados los pacientes que tenían tratamiento programado en el hospital durante el período en que el sistema informático no estuvo disponible. El responsable del tratamiento debe comunicar la violación de la seguridad de los datos a dichos pacientes directamente. La comunicación directa a los demás pacientes, algunos de los cuales pueden no haber estado en el hospital desde hace más de veinte años, puede no ser necesaria debido a la excepción prevista en el artículo 34, apartado 3, letra c). En este caso, se optará en su lugar por una comunicación pública[16] o una medida semejante por la que se informe de manera igualmente efectiva a los interesados. En este caso, el hospital debe hacer público el ataque con programas de secuestro de archivos y sus efectos.

40. Este caso sirve de ejemplo para un ataque con programas de secuestro con riesgo para los derechos y libertades de los interesados. Deberá documentarse de conformidad con el artículo 33, apartado 5, notificarse a la AC de conformidad con el artículo 33, apartado 1, y comunicarse a los interesados de conformidad con el artículo 34, apartado 1. La organización también debe actualizar y corregir su gestión organizativa y técnica de la seguridad de los datos personales y sus medidas y procedimientos de reducción del riesgo.

Acciones necesarias en función de los riesgos detectados		
Documentación interna	Notificación a la AC	Comunicación a los interesados
✓	✓	✓

2.4 CASO N.º 4: secuestro sin copia de seguridad y con exfiltración

[16] El considerando 86 del RGPD explica que «[d]ichas 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».

El servidor de una empresa de transporte público fue objeto de un ataque con programas de secuestro y al atacante cifró sus datos. Según las conclusiones de la investigación interna, el violador no solo cifró los datos, sino que también los exfiltró. El tipo de datos vulnerados eran los datos personales de los clientes y empleados, y de los miles de personas que utilizaban los servicios de la empresa (por ejemplo, comprando billetes en línea). Además de los datos básicos de identidad, están implicados en la violación de la seguridad los números de los documentos de identidad y datos financieros como los datos de tarjetas de crédito. Existía una base de datos de respaldo, pero también fue cifrada por el atacante.

2.4.1 CASO N.º 4: medidas previas y evaluación del riesgo

41. El responsable del tratamiento debería haber adoptado las mismas medidas previas mencionadas en la parte 2.1 y en la sección 2.5. Aunque ya existía una copia de seguridad, también se vio afectada por el ataque. Este sistema por sí solo plantea dudas sobre la calidad de las medidas previas de seguridad informática del responsable del tratamiento y debe ser objeto de un examen más detenido durante la investigación, ya que, en un régimen de copias de seguridad bien diseñado, las múltiples copias de seguridad deben almacenarse de forma segura sin acceso desde el sistema principal, ya que, de lo contrario, podrían verse comprometidas en el mismo ataque. Además, los ataques con programas de secuestro pueden no ser descubiertos durante días cifrando lentamente datos raramente utilizados. Esto puede hacer inútiles múltiples copias de seguridad, por lo que se deben realizar copias de seguridad periódicamente y apartarlas. Esto aumentaría la probabilidad de recuperación, aunque con un aumento de la pérdida de datos.

42. Esta violación de la seguridad no solo afecta a la disponibilidad de los datos, sino también a la confidencialidad, ya que el atacante puede haber modificado o copiado datos del servidor. Por lo tanto, el tipo de violación de la seguridad entraña un alto riesgo[17].

43. La naturaleza, la sensibilidad y el volumen de los datos personales aumentan aún más los riesgos, ya que el número de personas afectadas es elevado, al igual que la cantidad global de datos personales afectados. Además de los datos básicos de identidad, en una violación de la seguridad están implicados documentos de identidad y datos financieros como los datos de tarjetas de crédito. Una violación de la seguridad de los datos en relación con estos tipos de datos entraña un alto riesgo en sí misma y, si se tratan conjuntamente, podrían utilizarse, entre otras cosas, para la usurpación de identidad o el fraude.

44. Debido a una lógica del servidor o a unos controles organizativos, los archivos de copia de seguridad se vieron afectados por el programa de secuestro, lo que impidió la recuperación de los datos y aumentó el riesgo.

45. Esta violación de la seguridad de los datos entraña un alto riesgo para los derechos y libertades de las personas, ya que probablemente podría dar lugar a daños materiales (por ejemplo, pérdidas financieras al verse afectados los datos de la tarjeta de crédito) y morales (por ejemplo, usurpación de identidad o fraude al verse afectados los datos del documento de identidad).

2.4.2 CASO N.º 4: mitigación y obligaciones

46. La comunicación a los interesados es esencial para que puedan tomar las medidas necesarias para evitar daños materiales (por ejemplo, bloquear sus tarjetas de crédito).

[17] Para obtener orientación sobre las operaciones de tratamiento «que pueden entrañar un alto riesgo», véase la nota a pie de página 10.

47. Además de documentar la violación de la seguridad de conformidad con el artículo 33, apartado 5, la notificación a la AC también es obligatoria en este caso (artículo 33, apartado 1) y el responsable del tratamiento también está obligado a comunicar la violación a los interesados (artículo 34, apartado 1). Esto último podría llevarse a cabo persona por persona, pero, en el caso de las personas para las que no se disponga de datos de contacto, el responsable del tratamiento debe hacerlo públicamente, siempre que dicha comunicación no sea susceptible de acarrear consecuencias negativas adicionales para los interesados, por ejemplo mediante una notificación en su sitio web. En este último caso, se requiere una comunicación precisa y clara, a simple vista en la página de inicio del responsable del tratamiento, con referencias exactas de las disposiciones pertinentes del RGPD. La organización quizá también deba actualizar y corregir su gestión organizativa y técnica de la seguridad de los datos personales y sus medidas y procedimientos de reducción del riesgo.

Acciones necesarias en función de los riesgos detectados		
Documentación interna	Notificación a la AC	Comunicación a los interesados
✓	✓	✓

2.5 Medidas organizativas y técnicas para prevenir o mitigar el impacto de los ataques con programas de secuestro de archivos

48. El hecho de que un ataque con programas de secuestro de archivos pueda haberse producido es normalmente signo de una o más vulnerabilidades en el sistema del responsable del tratamiento. Esto también se aplica a los casos de programas de secuestro en los que los datos personales se han cifrado, pero no se han exfiltrado. Independientemente del resultado y de las consecuencias del ataque, no puede subrayarse suficientemente la importancia de una evaluación global del sistema de seguridad de los datos, con especial hincapié en la seguridad informática. Las deficiencias detectadas y las brechas de seguridad deben documentarse y abordarse sin demora.

49. Medidas aconsejables:

(La lista de las siguientes medidas no es en modo alguno exclusiva ni exhaustiva. Más bien, el objetivo es proporcionar ideas de prevención y posibles soluciones. Cada actividad de tratamiento es diferente, por lo que el responsable del tratamiento debe tomar la decisión sobre qué medidas se ajustan más a la situación en cuestión.)

- Mantener actualizado el *firmware*, el sistema operativo y el *software* de aplicación en los servidores, máquinas clientes, componentes activos de red y cualquier otra máquina en la misma LAN (incluidos los dispositivos wifi). Garantizar que se aplican las medidas de seguridad informática adecuadas, asegurarse de que son eficaces y mantenerlas actualizadas periódicamente cuando el tratamiento o las circunstancias cambian o evolucionan. Esto incluye conservar registros detallados de qué parches se aplican en qué marca de tiempo.
- Diseñar y organizar los sistemas de tratamiento y las infraestructuras para segmentar o aislar sistemas y redes de datos a fin de evitar la propagación de programas maliciosos en la organización y a sistemas externos.
- La existencia de un procedimiento de copia de seguridad actualizado, seguro y probado. Los medios de copia de seguridad a medio y largo plazo deben mantenerse separados del almacenamiento de los datos operativos y fuera del alcance de terceros, incluso si se llevase a cabo un ataque con éxito (por ejemplo, copias de seguridad incrementales diarias y copias de seguridad completas semanales).
- Tener/obtener un *software* adecuado, actualizado, eficaz e integrado contra los programas maliciosos.

- Disponer de un sistema adecuado, actualizado, eficaz e integrado de detección y prevención de intrusiones y cortafuegos. Dirigir el tráfico de la red a través del cortafuegos/ detección contra intrusiones, incluso en el caso del trabajo desde casa o móvil (por ejemplo, utilizando conexiones VPN a mecanismos de seguridad de la organización al acceder a internet).
- Formar a los empleados sobre los métodos de reconocimiento y prevención de ataques informáticos. El responsable del tratamiento debe proporcionar medios para determinar si los correos electrónicos y los mensajes obtenidos por otros medios de comunicación son auténticos y fiables. Los empleados deben recibir formación para reconocer cuándo se ha producido un ataque de este tipo, cómo sacar el terminal de la red y su obligación de notificarlo inmediatamente al responsable de la seguridad.
- Hacer hincapié en la necesidad de identificar el tipo de código malicioso para comprobar las consecuencias del ataque y ser capaz de encontrar las medidas adecuadas para mitigar el riesgo. En caso de que un ataque con programas de secuestro haya tenido éxito y no se disponga de copias de seguridad, podrán aplicarse herramientas disponibles, como las del proyecto «No more ransom» (nomoreransom.org) para recuperar los datos. No obstante, en caso de que se disponga de una copia de seguridad segura, es aconsejable recuperar los datos a partir de ella.
- Enviar todos los registros a un servidor de registro central, o reproducirlos en él (posiblemente con inclusión de la firma o el sellado de tiempo criptográfico de las anotaciones de registro).
- Cifrado de alta seguridad y autenticación de múltiples factores, en particular para el acceso administrativo a los sistemas informáticos y gestión adecuada de claves y contraseñas.
- Pruebas de vulnerabilidad y penetración de forma periódica.
- Crear un equipo de respuesta a incidentes de seguridad informática (CSIRT) o un equipo de respuesta a emergencias informáticas (CERT) dentro de la organización, o adherirse a un CSIRT o CERT colectivo. Crear un plan de respuesta a incidentes, un plan de recuperación en caso de catástrofe y un plan de continuidad de las actividades, y asegurarse de que se someten a pruebas exhaustivas.
- Al evaluar las contramedidas, el análisis de riesgos debe revisarse, probarse y actualizarse.

3 ATAQUES CON EXFILTRACIÓN DE DATOS

50. Los ataques que aprovechan las vulnerabilidades de los servicios ofrecidos por el responsable del tratamiento a terceros a través de internet, por ejemplo, cometidos por ataques de inyección (por ejemplo, inyección SQL o rutas transversales), comprometiendo el sitio web y métodos similares, pueden parecerse a los ataques con programas de secuestro en el sentido de que el riesgo emana de la acción de un tercero no autorizado, pero estos ataques suelen tener como objetivo copiar, exfiltrar y usar indebidamente los datos personales con algún fin malicioso. Por lo tanto, son principalmente violaciones de la confidencialidad y, posiblemente, también de la integridad de los datos. Al mismo tiempo, si el responsable del tratamiento conoce las características de este tipo de violaciones de la seguridad, los responsables del tratamiento disponen de numerosas medidas que pueden reducir sustancialmente el riesgo de ejecución satisfactoria de un ataque.

3.1 CASO N.º 5: exfiltración de los datos de las solicitudes de empleo de un sitio web

Una agencia de empleo fue víctima de un ciberataque, que colocó un código malicioso en su sitio web. Este código malicioso hizo accesible a personas no autorizadas la información personal presentada a través de formularios de solicitud de empleo en línea y almacenada en el servidor web. 213 de estos formularios pueden estar afectados. Una vez analizados los datos afectados, se determinó que la violación de la seguridad no concernía a categorías especiales de datos. Las herramientas maliciosas instaladas tenían funcionalidades que permitían al atacante eliminar cualquier historial de exfiltración y también el seguimiento del tratamiento en el servidor y la captura de datos personales. El conjunto de herramientas solo se descubrió un mes después de su instalación.

3.1.1 CASO N.º 5: medidas previas y evaluación del riesgo

51. La seguridad del entorno del responsable del tratamiento de datos es sumamente importante, ya que la mayoría de estas violaciones pueden evitarse garantizando que todos los sistemas se actualizan constantemente, se codifican los datos sensibles y se desarrollan aplicaciones con arreglo a normas de seguridad estrictas, como la autenticación fuerte, medidas contra la fuerza bruta, ataques, «escape» o «saneamiento» de entradas de usuarios[18], etc. También son necesarias auditorías periódicas de seguridad informática, evaluaciones de vulnerabilidad y pruebas de penetración para detectar este tipo de vulnerabilidades de antemano y corregirlas. En este caso concreto, las herramientas de control de la integridad de los archivos en el entorno de producción podrían haber ayudado a detectar la inyección de código. (En la sección 3.7 se incluye una lista de medidas recomendables).

52. El responsable del tratamiento siempre debe empezar a investigar la violación de la seguridad identificando el tipo de ataque y sus métodos, con el fin de evaluar qué medidas deben adoptarse. Para hacerlo de forma rápida y eficaz, el responsable del tratamiento debe disponer de un plan de respuesta a incidentes que especifique las medidas rápidas y necesarias para controlar el incidente. En este caso concreto, el tipo de violación fue un factor de aumento del riesgo, ya que no solo se redujo la confidencialidad de los datos, sino que el infiltrado también tenía los medios para establecer cambios en el sistema, por lo que la integridad de los datos también era cuestionable.

53. La naturaleza, la sensibilidad y el volumen de los datos personales afectados por la violación deben evaluarse para determinar en qué medida la violación afectó a los interesados. Aunque no se vio afectada ninguna categoría especial de datos personales, los datos a los que se accedió contienen información considerable sobre las personas a través de los formularios en línea, y dichos datos podrían utilizarse indebidamente de diversas maneras (focalización con publicidad no solicitada, usurpación de identidad, etc.), por lo que la gravedad de las consecuencias debe aumentar el riesgo para los derechos y libertades de los interesados[19].

3.1.2 CASO N.º 5: mitigación y obligaciones

54. Si es posible, una vez resuelto el problema, la base de datos debe compararse con la almacenada en una copia de seguridad segura. Las experiencias extraídas de la violación de la seguridad deben utilizarse en la actualización de la infraestructura informática. El responsable del tratamiento debe devolver todos los sistemas informáticos afectados a un estado limpio conocido, remediar la vulnerabilidad y aplicar nuevas medidas de seguridad para evitar violaciones similares de la seguridad de los datos en el futuro, por ejemplo, controles de integridad de los expedientes y auditorías de seguridad. Si los datos personales no solo se exfiltraron, sino también se suprimieron, el responsable del tratamiento debe adoptar medidas sistemáticas para recuperar los datos personales en el estado en que se encontraban antes de la violación. Puede ser necesario aplicar copias de seguridad completas, cambios incrementales y luego posiblemente volver a ejecutar el tratamiento desde la última copia de seguridad incremental, lo que requiere que el responsable sea capaz de repetir los cambios realizados desde la última copia de seguridad. Esto podría exigir que el responsable del tratamiento disponga de un sistema diseñado para conservar los archivos diarios de entrada

[18] El escape o saneamiento de las entradas de usuarios es una forma de validación de las entradas que garantiza que solo se introduzcan en un sistema de información datos con un formato adecuado.

[19] Para obtener orientación sobre las operaciones de tratamiento «que pueden entrañar un alto riesgo», véase la nota a pie de página 10.

en caso de que deban tratarse de nuevo y requiere un método sólido de almacenamiento y una política de retención adecuada.

55. En vista de lo anterior, dado que es probable que la violación entrañe un alto riesgo para los derechos y libertades de las personas físicas, se debe informar a los interesados de ello (artículo 34, apartado 1), lo que significa, por supuesto, que la autoridad o autoridades de control pertinentes también deben participar en forma de notificación de violación la seguridad de los datos. Documentar la violación de la seguridad es obligatorio de conformidad con el artículo 33, apartado 5, del RGPD y facilita la evaluación de la situación.

Acciones necesarias en función de los riesgos detectados		
Documentación interna	Notificación a la AC	Comunicación a los interesados
✓	✓	✓

3.2 CASO N.º 6: exfiltración de la contraseña cifrada desde un sitio web

Se aprovechó una vulnerabilidad de inyección SQL para acceder a una base de datos del servidor de un sitio web de cocina. Los usuarios solo podían elegir seudónimos arbitrarios como nombres de usuario. Se recomendaba no usar direcciones de correo electrónico para este fin. Las contraseñas almacenadas en la base de datos se cifraban con un algoritmo fuerte y la sal no se vio comprometida. Datos afectados: contraseñas cifradas de 1 200 usuarios. En aras de la seguridad, el responsable del tratamiento informó a los interesados de la violación por correo electrónico y les pidió que cambiaran sus contraseñas, especialmente si se utilizaba la misma contraseña para otros servicios.

3.2.1 CASO N.º 6: medidas previas y evaluación del riesgo

56. En este caso concreto, la confidencialidad de los datos se ve comprometida, pero las contraseñas de la base de datos se cifraron con funciones *hash* con un método actualizado, lo que reduciría el riesgo respecto a la naturaleza, la sensibilidad y el volumen de los datos personales. Este caso no entraña riesgos para los derechos y libertades de los interesados.

57. Además, no se puso en peligro la información de contacto (por ejemplo, direcciones de correo electrónico o números de teléfono) de los interesados, lo que significa que no existe un riesgo significativo para los interesados de ser objeto de intentos de fraude [p. ej., recepción de correos electrónicos de suplantación de identidad (*phishing*) o mensajes de texto y llamadas telefónicas fraudulentos]. No se han visto implicadas categorías especiales de datos.

58. Algunos nombres de usuario podrían considerarse datos personales, pero el tema del sitio web no permite connotaciones negativas. Aunque hay que señalar que la evaluación del riesgo podría cambiar[20], si el tipo de sitio web y los datos a los que se accede pudieran revelar categorías especiales de datos personales (por ejemplo, el sitio web de un partido político o sindicato). El uso del cifrado más avanzado podría mitigar los efectos adversos de la violación. Garantizar que se permita un número limitado de intentos para iniciar sesión evitará el éxito de los ataques de conexión por fuerza bruta, reduciendo así en gran medida los riesgos que entrañan los atacantes que ya conocen los nombres de usuario.

[20] Para obtener orientación sobre las operaciones de tratamiento «que pueden entrañar un alto riesgo», véase la nota a pie de página 10.

3.2.2 CASO N.º 6: mitigación y obligaciones

59. En algunos casos, la comunicación a los interesados podría considerarse un atenuante, ya que los interesados también están en condiciones de tomar las medidas necesarias para evitar nuevos daños derivados de la violación, por ejemplo, cambiando su contraseña. En este caso, la notificación no era obligatoria, pero en muchos casos puede considerarse una buena práctica.

60. El responsable del tratamiento debe corregir la vulnerabilidad y aplicar nuevas medidas de seguridad para evitar violaciones de la seguridad de los datos similares en el futuro, como, por ejemplo, auditorías sistemáticas de seguridad del sitio web.

61. La violación debe documentarse de conformidad con el artículo 33, apartado 5, pero no es necesaria notificación o comunicación.

62. Asimismo, es muy aconsejable comunicar a los interesados una violación de la seguridad las contraseñas en cualquier caso, incluso cuando las contraseñas se almacenaron utilizando funciones *hash* con valores de sal con un algoritmo conforme a la técnica más avanzada. Es preferible utilizar métodos de autenticación que eviten la necesidad de procesar contraseñas en el lado del servidor. Debe darse a los interesados la posibilidad de tomar las medidas adecuadas en relación con sus propias contraseñas.

Acciones necesarias en función de los riesgos detectados		
Documentación interna	Notificación a la AC	Comunicación a los interesados
✓	X	X

3.3 CASO N.º 7: ataque de reutilización de credenciales en un sitio web bancario

Un banco sufrió un ciberataque contra uno de sus sitios web de banca en línea. El ataque tenía por objeto listar todos los identificadores de usuario posibles utilizando una contraseña trivial fija. Las contraseñas constan de ocho dígitos. Debido a una vulnerabilidad del sitio web, en algunos casos se filtró al atacante información relativa a los interesados (nombre, apellidos, sexo, fecha y lugar de nacimiento, código fiscal, códigos de identificación del usuario), incluso si la contraseña utilizada no era correcta o la cuenta bancaria ya no estaba activa. Esto afectó a unos 100 000 interesados. De ellos, el atacante se conectó con éxito a unas 2 000 cuentas que utilizaban la contraseña trivial que este había probado. Después de los hechos, el responsable del tratamiento pudo identificar todos los intentos ilegítimos de inicio de sesión. El responsable del tratamiento de datos pudo confirmar que, según los controles de lucha contra el fraude, estas cuentas no realizaron transacciones durante el ataque. El banco era consciente de la violación de los datos porque su centro de operaciones de seguridad detectó un elevado número de solicitudes de inicio de sesión dirigidas al sitio web. En respuesta, el responsable del tratamiento desactivó la posibilidad de iniciar sesión en el sitio web desactivándolo, y obligó a restablecer las contraseñas de las cuentas comprometidas. El responsable del tratamiento comunicó la violación únicamente a los usuarios con las cuentas comprometidas, es decir, a los usuarios cuyas contraseñas se vieron comprometidas o cuyos datos se habían comunicado.

3.3.1 CASO N.º 7: medidas previas y evaluación del riesgo

63. Es importante mencionar que los responsables del tratamiento que tratan datos de carácter muy personal[21] tienen una mayor responsabilidad a la hora de proporcionar una seguridad adecuada de los datos, por ejemplo, disponer de un centro de operaciones de seguridad y otras medidas de prevención, detección y respuesta de incidentes. El hecho de no cumplir estas normas estrictas dará lugar, sin duda, a medidas más serias durante la investigación de una AC.

64. La violación afecta a datos financieros que van más allá de la identidad y la identificación del usuario, lo que la hace especialmente grave. El número de personas afectadas es elevado.

65. El hecho de que una violación pueda producirse en un entorno tan sensible apunta a importantes brechas de seguridad de los datos en el sistema del responsable del tratamiento y puede ser un indicador de un momento en que la revisión y actualización de las medidas de que se trate son «necesarias» de conformidad con el artículo 24, apartado 1, artículo 25, apartado 1, y artículo 32, apartado 1, del RGPD. Los datos vulnerados permiten la identificación única de los interesados y contienen otra información sobre ellos (incluido el género, la fecha y el lugar de nacimiento) y, además, el atacante los puede utilizar para obtener las contraseñas de los clientes o para llevar a cabo una campaña de suplantación de identidad dirigida a los clientes del banco.

66. Por estas razones, se consideró que la violación de la seguridad de los datos entrañaba probablemente un alto riesgo para los derechos y libertades de todos los interesados afectados[22]. Por lo tanto, el hecho de que se produzcan daños materiales (por ejemplo, pérdidas financieras) y no materiales (por ejemplo, usurpación de identidad o fraude) es un resultado concebible.

3.3.2 CASO N.º 7: mitigación y obligaciones

67. Las medidas del responsable del tratamiento mencionadas en la descripción del caso son adecuadas. A raíz de la violación, también corrigió la vulnerabilidad del sitio web y adoptó otras medidas para evitar violaciones de la seguridad de los datos similares en el futuro, como añadir la autenticación de dos factores al sitio web en cuestión y pasar a una autenticación de clientes fuerte.

68. La documentación de la violación de la seguridad con arreglo al artículo 33, apartado 5, del RGPD, y la notificación a la autoridad de control de que se trate no son opcionales en este escenario. Además, el responsable del tratamiento debe notificar a los 100 000 interesados (incluidos aquellos cuyas cuentas no se hayan visto comprometidas) de conformidad con el artículo 34 del RGPD.

Acciones necesarias en función de los riesgos detectados		
Documentación interna	Notificación a la AC	Comunicación a los interesados
✓	✓	✓

[21] Como información de los interesados referida a métodos de pago tales como números de tarjeta, cuentas bancarias, pagos en línea, nóminas, extractos bancarios, estudios económicos o cualquier otra información que pueda revelar información económica relativa a los interesados.

[22] Para obtener orientación sobre las operaciones de tratamiento «que pueden entrañar un alto riesgo», véase la nota a pie de página 10.

3.4 Medidas organizativas y técnicas para prevenir o mitigar el impacto de los ataques informáticos

69. Al igual que en el caso de los ataques con programas de secuestro, independientemente del resultado y de las consecuencias del ataque, los responsables del tratamiento tienen la obligación de reevaluar la seguridad informática en casos similares.

70. Medidas aconsejables:[23]

(*La lista de las siguientes medidas no es en modo alguno exclusiva ni exhaustiva. Más bien, el objetivo es proporcionar ideas de prevención y posibles soluciones. Cada actividad de tratamiento es diferente, por lo que el responsable del tratamiento debe tomar la decisión sobre qué medidas se ajustan más a la situación en cuestión*.)

- Cifrado y gestión de claves de última generación, especialmente cuando se están tratando contraseñas, datos sensibles o financieros. Siempre se prefiere el método de dispersión y «salado» criptográficos de información secreta (contraseñas) frente al cifrado de contraseñas. Es preferible utilizar métodos de autenticación que eviten la necesidad de procesar contraseñas en el lado del servidor.
- Mantener actualizado el sistema (*software* y *firmware*). Garantizar que se aplican todas medidas de seguridad informática, asegurarse de que son eficaces y mantenerlas actualizadas periódicamente cuando el tratamiento o las circunstancias cambian o evolucionan. Para poder demostrar el cumplimiento del artículo 5, apartado 1, letra f), de conformidad con el artículo 5, apartado 2, del RGPD, el responsable del tratamiento debe mantener un registro de todas las actualizaciones realizadas, incluido también el momento en que se aplicaron.
- Usar métodos de autenticación fuerte, como autenticación de doble factor y servidores de autenticación, complementados por una política de contraseña actualizada.
- Las normas de desarrollo seguro incluyen el filtrado de la entrada del usuario (utilizando la lista blanca en la medida de lo posible), el escape de las entradas del usuario y las medidas de prevención de la fuerza bruta (como la limitación de la cantidad máxima de reintentos). Los «*firewalls* de aplicaciones web» pueden contribuir al uso eficaz de esta técnica.
- Establecido privilegios de usuario fuertes y una política de gestión del control de acceso.
- Utilizar un cortafuegos adecuado, actualizado, eficaz e integrado, detección de intrusiones y otros sistemas de defensa perimetral.
- Auditorías sistemáticas de seguridad informática y evaluaciones de vulnerabilidad (pruebas de penetración).
- Revisiones y pruebas periódicas para garantizar que puedan utilizarse copias de seguridad para recuperar los datos cuya integridad o disponibilidad se haya visto afectada.
- No hay identificador de sesión en URL en texto sin formato.

[23] Para el desarrollo seguro de aplicaciones web, véase también: https://www.owasp.org/index.php/Main_Page.

4 FUENTE INTERMA DE RIESGO HUMANO

71. Debe destacarse el papel del error humano en las violaciones de la seguridad de los datos personales, debido a su apariencia común. Dado que estos tipos de violaciones pueden ser tanto intencionadas como no intencionadas, es muy difícil para los responsables del tratamiento identificar las vulnerabilidades y adoptar medidas para evitarlas. La Conferencia Internacional de Autoridades de Protección de Datos y Protección de la Intimidad reconoció la importancia de abordar estos factores humanos y adoptó la resolución para abordar el papel de los errores humanos en las violaciones de la seguridad de los datos personales en octubre de 2019[24]. Esta Resolución hace hincapié en que deben adoptarse medidas de salvaguardia adecuadas para evitar los errores humanos y proporciona una lista no exhaustiva de tales salvaguardias y enfoques.

4.1 CASO N.º 8: exfiltración de datos comerciales por un empleado

Durante el período de preaviso, el empleado de una empresa copia los datos comerciales de la base de datos de la empresa. El empleado está autorizado a acceder a los datos únicamente para desempeñar sus funciones. Meses más tarde, después de dejar de trabajar, utiliza los datos así obtenidos (datos básicos de contacto) para alimentar un nuevo tratamiento de datos del que es responsable, con el fin de ponerse en contacto con los clientes de la empresa para atraerlos a su nueva actividad.

4.1.1 CASO N.º 8: medidas previas y evaluación del riesgo

72. En este caso concreto, no se adoptaron medidas previas para impedir que el empleado copiara la información de contacto de la clientela de la empresa, ya que necesitaba, y de hecho tenía, acceso legítimo a esta información para su trabajo. Dado que el desempeño de la mayor parte de los puestos de trabajo relacionados con los clientes requiere algún tipo de acceso de los empleados a datos personales, estas violaciones de la seguridad de los datos pueden ser las más difíciles de prevenir. Las limitaciones al alcance del acceso pueden limitar el trabajo que puede realizar el empleado en cuestión. Sin embargo, unas políticas de acceso bien pensadas y un control constante pueden ayudar a evitar estas infracciones.

73. Como es habitual, durante la evaluación del riesgo deben tenerse en cuenta el tipo de violación y la naturaleza, sensibilidad y volumen de los datos personales afectados. Estos tipos de violaciones suelen ser violaciones de la confidencialidad, ya que la base de datos suele dejarse intacta, y su contenido se copia «simplemente» para su uso posterior. La cantidad de datos afectados suele ser también baja o media. En este caso concreto, no se vieron afectadas categorías especiales de datos personales, ya que el empleado solo necesitaba la información de contacto de los clientes para poder ponerse en contacto con ellos después de abandonar la empresa. Por lo tanto, los datos en cuestión no son sensibles.

74. Aunque el único objetivo del antiguo empleado que copió los datos de forma maliciosa puede limitarse a obtener la información de contacto de la clientela de la empresa para sus propios fines comerciales, el responsable del tratamiento no está en condiciones de considerar que el riesgo para los interesados afectados sea bajo, ya que el responsable del tratamiento no tiene ningún tipo de garantía sobre las intenciones del empleado. Así pues, aunque las consecuencias de la violación de la seguridad podrían

[24] http://globalprivacyassembly.org/wp-content/uploads/2019/10/AOIC-Resolution-FINAL-ADOPTED.pdf.

limitarse a la exposición a la autocomercialización no solicitada del antiguo empleado, no se excluye un uso indebido adicional y más grave de los datos robados, en función de la finalidad del tratamiento establecido por el antiguo empleado[25].

4.1.2 CASO N.º 8: mitigación y obligaciones

75. La mitigación de los efectos adversos de la violación de la seguridad en el caso anterior es difícil. Podría ser necesario emprender acciones legales inmediatas para evitar que el antiguo empleado use indebidamente y divulgue los datos. Como siguiente paso, el objetivo debe ser evitar situaciones similares en el futuro. El responsable del tratamiento podría intentar ordenar al antiguo empleado que deje de utilizar los datos, pero el éxito de esta acción es dudoso en el mejor de los casos. Pueden ser útiles las medidas técnicas adecuadas, como la imposibilidad de copiar o descargar datos a dispositivos extraíbles.

76. No existe una solución única para estos tipos de casos, pero un enfoque sistemático puede ayudar a prevenirlos. Por ejemplo, la empresa puede considerar, cuando sea posible, retirar determinadas formas de acceso a los empleados que hayan manifestado su intención de abandonar o poner en marcha registros de acceso para poder registrar y marcar el acceso no deseado. El contrato firmado con los empleados debe incluir cláusulas que prohíban tales acciones.

77. En resumen, dado que la violación en cuestión no supondrá un riesgo elevado para los derechos y libertades de las personas físicas, bastará con una notificación a la AC. Sin embargo, la información a los interesados podría ser beneficiosa también para el responsable del tratamiento, ya que podría ser mejor que supieran por la empresa acerca de la fuga de datos en lugar de por el antiguo empleado que intenta ponerse en contacto con ellos. La documentación relativa a la violación de datos de conformidad con el artículo 33, apartado 5, es una obligación legal.

Acciones necesarias en función de los riesgos detectados		
Documentación interna	Notificación a la AC	Comunicación a los interesados
✓	✓	X

[25] Para obtener orientación sobre las operaciones de tratamiento «que pueden entrañar un alto riesgo», véase la nota a pie de página 10.

4.2 CASO N.º 9: transmisión accidental de datos a un tercero de confianza

Un agente de seguros observó que, gracias a la configuración defectuosa de un fichero Excel recibido por correo electrónico, podía acceder a información relativa a dos docenas de clientes que no pertenecían a su ámbito de aplicación. Está sujeto al secreto profesional y es el único destinatario del correo electrónico. El acuerdo entre el responsable del tratamiento de datos y el agente de seguros obliga al agente a señalar sin demora indebida una violación de datos personales al responsable del tratamiento. Por lo tanto, el agente señaló inmediatamente el error al responsable del tratamiento, que corrigió el archivo y lo envió de nuevo, pidiéndole que eliminara el mensaje anterior. De conformidad con el acuerdo mencionado, el agente debe confirmar la supresión en una declaración escrita, lo que hizo. La información obtenida no incluye categorías especiales de datos personales, sino solo datos de contacto y datos sobre el propio seguro (tipo de seguro, importe). Tras analizar los datos personales afectados por la violación, el responsable del tratamiento no identificó ninguna característica especial por parte de las personas o del responsable del tratamiento que pudiera afectar al nivel de impacto de la violación.

4.2.1 CASO N.º 9: medidas previas y evaluación del riesgo

78. En este caso, la violación no se deriva de una acción intencionada de un empleado, sino de un error humano involuntario causado por falta de atención. Estos tipos de violaciones pueden evitarse o reducirse en frecuencia mediante a) la aplicación de programas de formación, educación y sensibilización en los que los empleados conozcan mejor la importancia de la protección de los datos personales; b) la reducción del intercambio de ficheros por correo electrónico, utilizando en su lugar sistemas específicos para el tratamiento de datos de los clientes, por ejemplo; c) la doble comprobación de los archivos antes de enviarlos; d) la separación de la creación y el envío de archivos.

79. Esta violación de la seguridad de los datos solo afecta a la confidencialidad de los datos, y su integridad y accesibilidad se mantienen intactas. La violación de la seguridad de los datos solo afectó a dos docenas de clientes, por lo que la cantidad de datos afectados puede considerarse baja. Además, los datos personales afectados no contienen datos sensibles. El hecho de que el encargado del tratamiento se haya puesto inmediatamente en contacto con el responsable del tratamiento tras tener conocimiento de la violación de la seguridad de los datos puede considerarse un factor de reducción del riesgo. (También debe evaluarse la posibilidad de que los datos hayan sido enviados a otros agentes de seguros y, si se confirma, deben tomarse las medidas adecuadas). Debido a las medidas adecuadas adoptadas tras la violación de la seguridad de los datos, es probable que no tenga ninguna repercusión en los derechos y libertades de los interesados.

80. La combinación del bajo número de personas afectadas, la detección inmediata de la violación y las medidas adoptadas para reducir al mínimo sus efectos hacen que este caso concreto no entrañe ningún riesgo.

4.2.2 CASO N.º 9: mitigación y obligaciones

81. Por otra parte, también están en juego otras circunstancias atenuantes del riesgo: el agente está sujeto al secreto profesional; él mismo informó del problema al responsable del tratamiento; y suprimió el archivo a solicitud. La sensibilización y, posiblemente, la inclusión de medidas adicionales en la comprobación de documentos que impliquen datos personales probablemente ayudarán a evitar casos similares en el futuro.

82. Además de documentar la violación de la seguridad de conformidad con el artículo 33, apartado 5, no es necesario adoptar ninguna otra medida.

Acciones necesarias en función de los riesgos detectados		
Documentación interna	Notificación a la AC	Comunicación a los interesados
✓	X	X

4.3 Medidas organizativas y técnicas para prevenir o mitigar el impacto de las fuentes internas de riesgo humano

83. Una combinación de las medidas mencionadas a continuación —aplicadas en función de las características singulares del caso— debe ayudar a reducir las posibilidades de que se reproduzca una violación similar.

84. Medidas aconsejables:

(*La lista de las siguientes medidas no es en modo alguno exclusiva ni exhaustiva. Más bien, el objetivo es proporcionar ideas de prevención y posibles soluciones. Cada actividad de tratamiento es diferente, por lo que el responsable del tratamiento debe tomar la decisión sobre qué medidas se ajustan más a la situación en cuestión.*)

- Aplicación periódica de programas de formación, educación y sensibilización para los empleados sobre sus obligaciones en materia de privacidad y seguridad, y la detección y notificación de amenazas a la seguridad de los datos personales[26]. Desarrollar un programa de sensibilización para recordar a los empleados los errores más comunes que dan lugar a violaciones de datos personales y cómo evitarlas.
- Establecimiento de prácticas, procedimientos y sistemas sólidos y eficaces en materia de protección de datos y privacidad[27].
- Evaluación de las prácticas, procedimientos y sistemas de privacidad para garantizar la continuidad de la eficacia[28].
- Aplicar criterios adecuados de control de acceso y obligar a los usuarios a seguir las normas.
- Aplicar técnicas para forzar la autenticación de los usuarios al acceder a datos personales sensibles.
- Deshabilitar la cuenta del usuario relacionada con la empresa tan pronto como la persona abandone la empresa.
- Comprobar un flujo de datos inusual entre el servidor de archivos y los puestos de trabajo de los empleados.
- Establecer la seguridad de la interfaz de entrada/salida en el BIOS o mediante el uso de programas que controlen el uso de interfaces informáticas (bloqueo o desbloqueo, por ejemplo, USB/CD/DVD, etc.).
- Revisar la política de acceso de los empleados (por ejemplo, registrar el acceso a datos sensibles y exigir al usuario que introduzca una razón empresarial, de modo que esté disponible para las auditorías).
- Desactivar los servicios en la nube abierta.
- Prohibir e impedir el acceso a servicios de correo abierto conocidos.
- Desactivar de la función de pantalla de impresión en el sistema operativo.
- Aplicar una política de oficina limpia.
- Bloqueo automatizado de todos los ordenadores tras un determinado período de inactividad.
- Utilizar mecanismos [por ejemplo, testigo de autenticación (inalámbrico) para abrir/conectarse a cuentas bloqueadas] para los conmutadores de usuario rápidos en entornos compartidos.

---

[26] Sección 2), subsección i), de la Resolución para abordar el papel de los errores humanos en las violaciones de datos personales.

[27] Sección 2), subsección ii), de la Resolución para abordar el papel de los errores humanos en las violaciones de datos personales.

[28] Sección 2), subsección iii), de la Resolución para abordar el papel de los errores humanos en las violaciones de datos personales.

- Utilizar sistemas específicos para la gestión de datos personales que apliquen mecanismos adecuados de control de acceso y eviten errores humanos, como el envío de comunicaciones a un sujeto equivocado. El uso de hojas de cálculo y otros documentos de oficina no es un medio adecuado para gestionar los datos de los clientes.

5 DOCUMENTOS EN PAPEL Y DISPOSITIVOS EXTRAVIADOS O ROBADOS

85. Un tipo frecuente de caso es la pérdida o robo de dispositivos portátiles. En estos casos, el responsable del tratamiento debe tener en cuenta las circunstancias de la operación de tratamiento, como el tipo de datos almacenados en el dispositivo, así como los medios de apoyo y las medidas adoptadas antes de la violación para garantizar un nivel adecuado de seguridad. Todos estos elementos afectan a las posibles repercusiones de la violación de la seguridad de los datos. La evaluación del riesgo podría ser difícil, ya que el producto ya no está disponible.

86. Estos tipos de violaciones pueden clasificarse siempre como violaciones de la confidencialidad. Sin embargo, si no se dispone de copias de seguridad para la base de datos robada, el tipo de violación también puede constituir una violación de la disponibilidad y una violación de la integridad.

87. Los escenarios siguientes demuestran cómo influyen las circunstancias antes mencionadas en la probabilidad y gravedad de la violación de la seguridad de los datos.

5.1 CASO N.º 10: material robado que almacena datos personales cifrados

Durante una intrusión en una guardería infantil, se robaron dos tabletas. Las tabletas contenían una aplicación que contenía datos personales sobre los niños que asistían a la guardería. Nombre, fecha de nacimiento, datos personales sobre la educación de los niños. Tanto las tabletas cifradas que se desconectaron en el momento del robo como la aplicación estaban protegidas por una contraseña fuerte. Los datos de la copia de seguridad estaban a disposición del responsable del tratamiento de manera eficaz y fácil. Tras tener conocimiento del robo, la guardería emitió una orden a distancia para limpiar las tabletas poco después del descubrimiento del robo.

5.1.1 CASO N.º 10: medidas previas y evaluación del riesgo

88. En este caso concreto, el responsable del tratamiento de datos adoptó las medidas adecuadas para prevenir y mitigar los efectos de una posible violación de la seguridad de los datos mediante el cifrado de dispositivos, la introducción de una protección adecuada de las contraseñas y la protección de los datos almacenados en las tabletas. (En la sección 5.7 se incluye una lista de medidas recomendables).

89. Tras tener conocimiento de una violación de la seguridad de los datos, el responsable del tratamiento debe evaluar la fuente de riesgo, los sistemas que apoyan el tratamiento de datos, el tipo de datos personales implicados y las posibles repercusiones de la violación de datos en las personas afectadas. La violación de la seguridad de los datos descrita anteriormente habría afectado a la confidencialidad, la disponibilidad y la integridad de los datos en cuestión, sin embargo, debido a los procedimientos adecuados del responsable del tratamiento antes y después de la violación de la seguridad de los datos, ninguno de estos aspectos se vio afectado.

5.1.2 CASO N.º 10: mitigación y obligaciones

90. La confidencialidad de los datos personales de los dispositivos no se vio comprometida debido a la protección mediante contraseñas fuertes tanto en las tabletas como en las aplicaciones. Las tabletas estaban configuradas de tal manera que el establecimiento de una contraseña también significa que los datos en el

dispositivo están cifrados. Esto se vio reforzado por la acción del responsable del tratamiento de intentar borrar todo a distancia de los dispositivos robados.

91. Debido a las medidas adoptadas, la confidencialidad de los datos también se mantuvo intacta. Además, la copia de seguridad garantizaba la disponibilidad continua de los datos personales, por lo que no podría haberse producido ningún posible impacto negativo.

92. Debido a estos hechos, era poco probable que la violación de la seguridad de los datos descrita anteriormente entrañara un riesgo para los derechos y libertades de los interesados, por lo que no era necesaria ninguna notificación a la AC o a los interesados afectados. No obstante, esta violación de la seguridad de los datos también debe documentarse de conformidad con el artículo 33, apartado 5.

Acciones necesarias en función de los riesgos detectados		
Documentación interna	Notificación a la AC	Comunicación a los interesados
✓	X	X

5.2 CASO N.º 11: material robado que almacena datos personales no cifrados

El cuaderno electrónico de un empleado de una empresa proveedora de servicios fue robado. El cuaderno robado contenía nombres, apellidos, sexo, direcciones y fecha de nacimiento de más de 100 000 clientes. Debido a la indisponibilidad del dispositivo robado, no fue posible determinar si también se habían visto afectadas otras categorías de datos personales. El acceso al disco duro del cuaderno no estaba protegido por ninguna contraseña. Los datos personales pudieron recuperarse de las copias de seguridad disponibles diariamente.

5.2.1 CASO N.º 11: medidas previas y evaluación del riesgo

93. El responsable del tratamiento de los datos no adoptó ninguna medida de seguridad previa, por lo que el ladrón o cualquier otra persona que tuviera el dispositivo podía acceder fácilmente a los datos personales almacenados en el cuaderno robado.

94. Esta violación de la seguridad de los datos afecta a la confidencialidad de los datos almacenados en el dispositivo robado.

95. El cuaderno que contenía los datos personales era vulnerable en este caso porque carecía de protección mediante contraseña o cifrado. La falta de medidas de seguridad básicas aumenta el nivel de riesgo para los interesados afectados. Además, la identificación de los interesados afectados también es problemática, lo que también aumenta la gravedad de la violación de la seguridad. El considerable número de personas afectadas aumenta el riesgo, sin embargo, ninguna categoría especial de datos personales se vio afectada por la violación de la seguridad de los datos.

96. Durante la evaluación del riesgo[29], el responsable del tratamiento debe tener en cuenta las posibles consecuencias y efectos adversos de la violación de la confidencialidad. Como consecuencia de la violación de la seguridad, los interesados afectados pueden sufrir usurpación de identidad recurriéndose a los datos disponibles en el dispositivo robado, por lo que se considera que el riesgo es elevado.

[29] Para obtener orientación sobre las operaciones de tratamiento «que pueden entrañar un alto riesgo», véase la nota a pie de página 10.

5.2.2 CASO N.º 11: mitigación y obligaciones

97. Activar el cifrado del dispositivo y el uso de la protección mediante contraseña fuerte de la base de datos almacenada podría haber evitado que la violación de la seguridad de los datos entrañara un riesgo para los derechos y libertades de los interesados.

98. Debido a estas circunstancias, es necesaria la notificación de la AC, por lo que también es necesaria la notificación de los interesados afectados.

Acciones necesarias en función de los riesgos detectados		
Documentación interna	Notificación a la AC	Comunicación a los interesados
✓	✓	✓

5.3 CASO N.º 12: archivos en papel robados con datos sensibles

Se robó un cuaderno diario en papel de un centro de rehabilitación de drogodependientes. El diario contenía datos básicos de identidad y salud de los pacientes admitidos en el centro. Los datos solo se almacenaban en papel y los médicos que trataban a los pacientes no disponían de ninguna copia de seguridad. El diario no estaba guardado en un cajón o una sala cerrados, y el responsable del tratamiento no disponía de un régimen de control de acceso ni de ninguna otra medida de salvaguardia para la documentación en papel.

5.3.1 CASO N.º 12: medidas previas y evaluación del riesgo

99. El responsable del tratamiento no adoptó medidas de seguridad previas, por lo que la persona que encontró el diario podía acceder con facilidad a los datos personales almacenados en él. Además, la naturaleza de los datos personales almacenados en el diario hace que la falta de copia de seguridad de los datos sea un factor de riesgo muy grave.

100. Este caso sirve de ejemplo de violación de la seguridad de los datos de alto riesgo. Debido al incumplimiento de las precauciones de seguridad adecuadas, se perdieron datos sanitarios sensibles de conformidad con el artículo 9, apartado 1, del RGPD. Dado que en este caso se trataba de una categoría especial de datos personales, se incrementaron los riesgos potenciales para los interesados afectados, lo que también debe tener en cuenta el responsable del tratamiento que evalúa el riesgo[30].

101. Esta violación de la seguridad afecta a la confidencialidad, la disponibilidad y la integridad de los datos personales en cuestión. Como consecuencia de la violación, se rompe el secreto médico y terceros no autorizados pueden acceder a la información médica privada de los pacientes, lo que puede tener graves repercusiones en la vida personal del paciente. La violación de la disponibilidad también puede perturbar la continuidad del tratamiento de los pacientes. Dado que no puede excluirse la modificación o supresión de partes del contenido del diario, la integridad de los datos personales también se ve comprometida.

5.3.2 CASO N.º 12: mitigación y obligaciones

102. Durante la evaluación de las medidas de salvaguardia, también debe tenerse en cuenta el tipo de medio de apoyo. Dado que el diario de registro de pacientes era un documento físico, su salvaguardia debería haberse organizado de forma diferente a la de un dispositivo electrónico. La seudonimización de los nombres de los pacientes, la conservación del diario en un local protegido y en un cajón o sala cerrados, y un control de

[30] Para obtener orientación sobre las operaciones de tratamiento «que pueden entrañar un alto riesgo», véase la nota a pie de página 10.

acceso adecuado con autenticación al acceder al mismo podrían haber impedido la violación de la seguridad de los datos.

103. La violación descrita anteriormente puede afectar gravemente a los interesados afectados, por lo tanto, la notificación de la AC y la comunicación de la violación de la seguridad de los datos a los interesados afectados son obligatorias.

Acciones necesarias en función de los riesgos detectados		
Documentación interna	Notificación a la AC	Comunicación a los interesados
✓	✓	✓

5.4 Medidas organizativas y técnicas para prevenir o mitigar el impacto de la pérdida o robo de dispositivos

104. Una combinación de las medidas mencionadas a continuación —aplicadas en función de las características singulares del caso— debe ayudar a reducir las posibilidades de que se reproduzca una violación similar.

105. Medidas aconsejables:

(*La lista de las siguientes medidas no es en modo alguno exclusiva ni exhaustiva. Más bien, el objetivo es proporcionar ideas de prevención y posibles soluciones. Cada actividad de tratamiento es diferente, por lo que el responsable del tratamiento debe tomar la decisión sobre qué medidas se ajustan más a la situación en cuestión.*)

- Activar el cifrado del dispositivo (como BitLocker, Veracript o DM-Crypt).
- Utilizar un código de acceso o contraseña en todos los dispositivos. Cifrar todos los dispositivos electrónicos móviles de manera que requiera la introducción de una contraseña compleja para el descifrado.
- Usar autenticación de múltiples factores.
- Activar las funcionalidades de los dispositivos muy móviles que permiten localizarlos en caso de pérdida o extravío.
- Utilizar el *software*/la aplicación MDM (Gestión de dispositivos móviles) y la localización. Utilizar filtros antideslumbrantes. Cerrar cualquier dispositivo sin vigilancia.
- Si es posible y adecuado para el tratamiento de datos en cuestión, guardar los datos personales no en un dispositivo móvil, sino en un servidor final central.
- Si el puesto de trabajo está conectado a la LAN corporativa, hacer una copia de seguridad automática de las carpetas de trabajo siempre que sea inevitable que los datos personales se almacenen allí.
- Utilizar una VPN segura (por ejemplo, que requiera una clave de autenticación de segundo factor independiente para el establecimiento de una conexión segura) para conectar los dispositivos móviles a servidores *back-end*.
- Proporcionar cerraduras físicas a los empleados para que puedan proteger físicamente los dispositivos móviles que utilizan mientras estos permanecen sin vigilancia.
- Regulación adecuada del uso de los dispositivos fuera de la empresa.
- Regulación adecuada del uso de los dispositivos dentro de la empresa.
- Utilizar el *software*/la aplicación MDM (Gestión de dispositivos móviles) y activar la función de borrado remoto.
- Utilizar la gestión centralizada de dispositivos con derechos mínimos para que los usuarios finales instalen programas informáticos.
- Instalar controles de acceso físico.
- Evitar almacenar información sensible en dispositivos o discos duros móviles. Si es necesario acceder al sistema interno de la empresa, deben utilizarse canales seguros como se ha indicado anteriormente.

6 ERROR DE CORREO POSTAL

106. La fuente de riesgo es un error humano interno también en este caso, pero en este caso no hay ninguna acción malintencionada que haya dado lugar a la violación de la seguridad de los datos. Es el resultado de falta de atención. Poco puede hacer el responsable del tratamiento después de que se produzca, por lo que la prevención es aún más importante en estos casos que en otros tipos de violación de la seguridad.

6.1 CASO N.º 13: error de correo postal

Una empresa minorista embaló dos pedidos de calzado. Debido a error humano, se mezclaron dos albaranes, con el resultado de que tanto los productos como los albaranes correspondientes se enviaron a la persona equivocada. Esto significa que los dos clientes recibieron los pedidos del otro, incluidos los albaranes con los datos personales. Tras tener conocimiento de la violación de la seguridad de los datos, el responsable del tratamiento retiró los pedidos y los envió a los destinatarios adecuados.

6.1.1 CASO N.º 13: medidas previas y evaluación del riesgo

107. Las facturas contenían los datos personales necesarios para una entrega satisfactoria (nombre, dirección, más el artículo adquirido y su precio). Es importante determinar cómo podría haberse producido el error humano en primer lugar y si, en alguna manera, podría haberse evitado. En el caso concreto que se describe, el riesgo es bajo, ya que no estaban implicadas categorías especiales de datos personales u otros datos cuyo uso indebido pudiera tener efectos negativos sustanciales, la violación no es consecuencia de un error sistémico por parte del responsable del tratamiento y solo afecta a dos personas. No se pudo determinar identificar ningún efecto negativo para las personas.

6.1.2 CASO N.º 13: mitigación y obligaciones

108. El responsable del tratamiento debe prever la devolución gratuita de los artículos y los albaranes que los acompañan, y también debe pedir a los destinatarios equivocados que destruyan o supriman todas las copias de los albaranes que contengan los datos personales de la otra persona.

109. Incluso si la propia violación de la seguridad no supone un alto riesgo para los derechos y libertades de las personas afectadas y, por tanto, la comunicación a los interesados no está prevista por el artículo 34 del RGPD, no puede evitarse la comunicación de la violación a los interesados, ya que su cooperación es necesaria para mitigar el riesgo.

Acciones necesarias en función de los riesgos detectados		
Documentación interna	Notificación a la AC	Comunicación a los interesados
✓	X	X

6.2 CASO N.º 14: datos personales altamente confidenciales enviados por correo por error

El departamento de empleo de una administración pública envió un mensaje por correo electrónico sobre próximas formaciones a las personas registradas en su sistema como demandantes de empleo. Por error, se adjuntó a este correo electrónico un documento con todos los datos personales de estos demandantes de empleo (nombre, dirección de correo electrónico, dirección postal, número de seguridad social). El número de personas afectadas supera las 60 000. Posteriormente, la oficina se puso en contacto con todos los destinatarios y les pidió que eliminaran el mensaje anterior y no utilizaran la información contenida en el mismo.

6.2.1 CASO N.º 14: medidas previas y evaluación del riesgo

110. Deberían haberse aplicado normas más estrictas para el envío de dichos mensajes. Debe considerarse la introducción de mecanismos de control adicionales.

111. El número de personas afectadas es considerable, y la implicación de su número de seguridad social, junto con otros datos personales más básicos, aumenta aún más el riesgo, que puede considerarse elevado[31]. El responsable del tratamiento no puede contener la eventual distribución de los datos por parte de ninguno de los destinatarios.

6.2.2 CASO N.º 14: mitigación y obligaciones

112. Como se ha mencionado anteriormente, los medios para mitigar eficazmente los riesgos de una violación de la seguridad similar son limitados. Aunque el responsable del tratamiento solicitó la supresión del mensaje, no puede obligar a los destinatarios a hacerlo y, en consecuencia, tampoco puede tener la certeza de que cumplen la solicitud.

113. La ejecución de las tres acciones indicadas a continuación debe ser evidente en un caso como el presente.

Acciones necesarias en función de los riesgos detectados		
Documentación interna	Notificación a la AC	Comunicación a los interesados
✓	✓	✓

6.3 CASO N.º 15: datos personales enviados por correo por error

La lista de participantes en un curso de inglés jurídico que tiene lugar en un hotel durante cinco días se envía por error a quince antiguos participantes en el curso en lugar del hotel. La lista contiene nombres, direcciones de correo electrónico y preferencias alimentarias de los quince participantes. Solo dos participantes han cumplimentado sus preferencias alimentarias, declarando que son intolerantes a la lactosa. Ninguno de los participantes tiene una identidad protegida. El responsable del tratamiento descubre el error inmediatamente después de enviar la lista e informa a los destinatarios del error y les pide que supriman la lista.

6.3.1 CASO N.º 15: medidas previas y evaluación del riesgo

114. Deberían haberse aplicado normas estrictas para el envío de mensajes que contienen datos personales. Debe considerarse la introducción de mecanismos de control adicionales.

115. Los riesgos derivados de la naturaleza, la sensibilidad, el volumen y el contexto de los datos personales son bajos. Los datos personales incluyen datos sensibles sobre las preferencias alimentarias de dos de los participantes. Aunque la información de que alguien es intolerante a la lactosa constituye datos sanitarios, el riesgo de que estos datos se utilicen de forma perjudicial debe considerarse relativamente bajo. Si bien en el caso de los datos relativos a la salud se suele suponer que la violación puede entrañar un alto riesgo para el interesado[32], al mismo tiempo, en este caso concreto no se puede identificar ningún riesgo de que la violación provoque daños físicos, materiales o inmateriales al interesado debido a la divulgación no autorizada de información sobre la intolerancia a la lactosa. Contrariamente a otras preferencias

[31] Para obtener orientación sobre las operaciones de tratamiento «que pueden entrañar un alto riesgo», véase la nota a pie de página 10.

[32] Véanse las Directrices WP 250, p. 23.

alimentarias, la intolerancia a la lactosa no puede vincularse normalmente a ninguna creencia religiosa o filosófica. La cantidad de datos vulnerados y el número de interesados afectados también son muy bajos.

6.3.2 CASO N.º 15: mitigación y obligaciones

116. En resumen, puede afirmarse que la violación de la seguridad no tuvo ningún efecto significativo en los interesados. El hecho de que el responsable del tratamiento se pusiera inmediatamente en contacto con los destinatarios tras conocer el error puede considerarse un factor atenuante.

117. Si se envía un correo electrónico a un destinatario incorrecto o no autorizado, se recomienda que el responsable del tratamiento de datos envíe un correo electrónico de seguimiento con copia oculta a los destinatarios no intencionales pidiendo disculpas, indicando que se suprima el correo electrónico infractor y advirtiendo a los destinatarios de que no tienen derecho a seguir utilizando las direcciones de correo electrónico que se les han identificado.

118. Debido a estos hechos, era poco probable que esta violación de la seguridad de los datos entrañara un riesgo para los derechos y libertades de los interesados, por lo que no era necesaria ninguna notificación a la AC o a los interesados afectados. No obstante, esta violación de la seguridad de los datos también debe documentarse de conformidad con el artículo 33, apartado 5.

Acciones necesarias en función de los riesgos detectados		
Documentación interna	Notificación a la AC	Comunicación a los interesados
✓	X	X

6.4 CASO N.º 16: error de correo postal

Un grupo de seguros ofrece seguros de automóviles. Para ello, envía pólizas de contribución ajustadas periódicamente por correo postal. Además del nombre y la dirección del tomador del seguro, la carta contiene el número de matrícula del vehículo sin ocultar, las tasas de seguro del año en curso y del siguiente, el kilometraje anual aproximado y la fecha de nacimiento del tomador del seguro. No se incluyen los datos sanitarios de conformidad con el artículo 9 del RGPD, ni los datos de pago (datos bancarios) ni los datos económicos y financieros.

Las cartas se ensobran mediante ensobradoras automáticas. Debido a un error mecánico, se insertan dos cartas para distintos tomadores de seguro en un sobre y se envían a un tomador por correo postal. El tomador abre la carta en casa y examina su carta correctamente entregada, así como la carta de otro tomador entregado incorrectamente.

6.4.1 CASO N.º 16: medidas previas y evaluación del riesgo

119. La carta incorrectamente entregada contiene el nombre, la dirección, la fecha de nacimiento, el número de matrícula del vehículo sin ocultar y la clasificación de la tarifa de seguro del año en curso y del año siguiente. Los efectos sobre la persona afectada deben considerarse medios, ya que información no disponible públicamente, como la fecha de nacimiento o el número de matrícula del vehículos sin ocultar, y los detalles sobre el incremento de las tarifas de seguro se comunican al destinatario no autorizado. Se considera que la probabilidad de uso indebido de estos datos se sitúa entre baja y media. Sin embargo, si bien es probable que muchos destinatarios acaben tirando la carta recibida indebidamente a la basura, en casos concretos no puede excluirse por completo que la carta se publique en las redes sociales o que se contacte con el tomador del seguro.

6.4.2 CASO N.º 16: mitigación y obligaciones

120. El responsable del tratamiento debe conseguir la devolución del documento original a sus expensas. También se debe informar al destinatario equivocado de que no puede hacer un uso indebido de la información leída.

121. Probablemente nunca será posible evitar por completo un error de envío postal en un envío masivo que utilice máquinas totalmente automatizadas. Sin embargo, en caso de aumento de la frecuencia, es necesario comprobar si las máquinas ensobradoras están configuradas y se mantienen de forma correcta, o si algún otro problema sistémico da lugar a tal violación de la seguridad.

Acciones necesarias en función de los riesgos detectados		
Documentación interna	Notificación a la AC	Comunicación a los interesados
✓	✓	X

6.5 Medidas organizativas y técnicas para prevenir o mitigar el impacto de los errores en envíos postales

122. Una combinación de las medidas mencionadas a continuación, aplicadas en función de las características singulares del caso, debería ayudar a reducir las posibilidades de que se reproduzca una violación similar.

123. Medidas aconsejables:

(*La lista de las siguientes medidas no es en modo alguno exclusiva ni exhaustiva. Más bien, el objetivo es proporcionar ideas de prevención y posibles soluciones. Cada actividad de tratamiento es diferente, por lo que el responsable del tratamiento debe tomar la decisión sobre qué medidas se ajustan más a la situación en cuestión.*)

- Establecer normas exactas, sin margen de interpretación, para el envío de cartas o correos electrónicos.
- Formación adecuada para el personal sobre cómo enviar cartas o correos electrónicos.
- Cuando se envían correos electrónicos a varios destinatarios, se enumeran por defecto en el campo «cco».
- Se requiere confirmación adicional cuando se envían correos electrónicos a varios destinatarios, que no figuran en el campo «cco».
- Aplicación del principio de los cuatro ojos.
- Dirección automática en lugar de manual, con datos extraídos de una base de datos disponible y actualizada; el sistema de direccionamiento automático debe revisarse periódicamente para comprobar errores ocultos y configuraciones incorrectas.
- Aplicación del retraso del mensaje (por ejemplo, el mensaje puede suprimirse o modificarse en un plazo determinado tras hacer clic en el botón pulsar).
- Desactivar autocompletar al escribir en direcciones de correo electrónico.
- Sesiones de sensibilización sobre los errores más comunes que dan lugar a una violación de la seguridad de los datos personales.
- Sesiones de formación y manuales sobre cómo gestionar incidentes que den lugar a una violación de los datos personales y a quién informar (implicar al responsable de la protección de datos).

7 OTROS CASOS: INGENIERÍA SOCIAL

7.1 CASO N.º 17: usurpaciones de identidad

El centro de contacto de una empresa de telecomunicaciones recibe una llamada telefónica de alguien que se presenta como cliente. El supuesto cliente exige a la empresa que cambie la dirección de correo electrónico a la que deben enviarse los datos de facturación a partir de ese momento. El trabajador del centro de contacto valida la identidad del cliente pidiéndole determinados datos personales, según los procedimientos de la empresa. La persona que efectúa la llamada indica correctamente el número fiscal y la dirección postal del cliente requerido (porque tenía acceso a estos elementos). Tras la validación, el operador realiza el cambio solicitado y, a partir de ese momento, la información sobre facturación se envía a la nueva dirección de correo electrónico. El procedimiento no prevé ninguna notificación al anterior contacto por correo electrónico. Al mes siguiente, el cliente legítimo se pone en contacto con la empresa, preguntando por qué no recibe facturación a su dirección de correo electrónico, y niega cualquier llamada solicitando el cambio de contacto por correo electrónico. Posteriormente, la empresa se da cuenta de que la información se ha enviado a un usuario ilegítimo y revierte el cambio.

7.1.1 CASO N.º 17: evaluación del riesgo, mitigación y obligaciones

124. Este caso sirve de ejemplo sobre la importancia de las medidas previas. La violación de la seguridad de los datos, desde el punto de vista del riesgo33, presenta un alto nivel de riesgo, ya que los datos de facturación pueden proporcionar información sobre la vida privada del interesado (por ejemplo, hábitos o contactos) y causar daños materiales (por ejemplo, acecho o riesgo para la integridad física). Los datos personales obtenidos durante este ataque también pueden utilizarse para facilitar que se tome el control de las cuentas en esta organización o para aprovechar otras medidas de autenticación en otras organizaciones. Teniendo en cuenta estos riesgos, la medida de autenticación «adecuada» debe superar un nivel elevado, en función de qué datos personales puedan tratarse como resultado de la autenticación.

125. Como consecuencia de ello, tanto la notificación a la AC como la comunicación al interesado son necesarias por parte del responsable del tratamiento.

126. El proceso previo de validación del cliente debe perfeccionarse claramente a la luz de este caso. Los métodos utilizados para la autenticación no eran suficientes. La parte malintencionada pudo fingir ser el usuario previsto mediante el uso de información públicamente disponible y de información a la que tenía acceso de otro modo.

127. No se recomienda el uso de este tipo de autenticación estática basada en el conocimiento (en el que la respuesta no cambia y la información no es «secreta», como sería el caso con una contraseña).

128. En su lugar, la organización debe utilizar una forma de autenticación que dé lugar a un alto grado de confianza en que el usuario autenticado es la persona prevista, y no cualquier otra persona. La introducción de un método de autenticación de múltiples factores fuera de banda resolvería el problema, por ejemplo, para verificar la petición de cambio, enviando una solicitud de confirmación al contacto anterior; o añadir preguntas adicionales y exigir información solo visible en las facturas anteriores. Es responsabilidad del

[33] Para obtener orientación sobre las operaciones de tratamiento «que pueden entrañar un alto riesgo», véase la nota a pie de página 10.

responsable del tratamiento decidir qué medidas introducir, ya que conoce mejor los detalles y requisitos de su funcionamiento interno.

Acciones necesarias en función de los riesgos detectados		
Documentación interna	Notificación a la AC	Comunicación a los interesados
✓	✓	✓

7.2 CASO N.º 18: exfiltración de correos electrónicos

Una cadena de hipermercados detectó, tres meses después de su configuración, que algunas cuentas de correo electrónico se habían modificado y se habían creado normas para que cada correo electrónico que contuviera determinadas expresiones (por ejemplo, «factura», «pago», «transferencia bancaria», «autenticación de tarjetas de crédito», «datos de cuenta bancaria») se trasladara a una carpeta no utilizada y se enviara también a una dirección de correo electrónico externa. Además, en aquel momento ya se había producido un ataque de ingeniería social, es decir, el atacante, que se presentó como un proveedor, había cambiado los datos de la cuenta bancaria de dicho proveedor por los datos de la suya. Por último, en aquel momento se habían enviado varias facturas falsas que incluían los datos de la nueva cuenta bancaria. El sistema de seguimiento de la plataforma de correo electrónico terminó alertando sobre las carpetas. La empresa no pudo detectar cómo pudo el atacante acceder a las cuentas de correo electrónico para empezar, pero suponía que un correo electrónico infectado fue el responsable de dar acceso al grupo de usuarios a cargo de los pagos.

Debido a la transmisión de correos electrónicos basada en palabras clave, el atacante recibió información sobre 99 empleados: nombre y salario de un mes determinado en relación con 89 interesados; nombre, estado civil, número de hijos, salario, horas de trabajo e información restante sobre la percepción salarial de diez empleados cuyos contratos se habían extinguido. El responsable del tratamiento solo notificó a los diez empleados pertenecientes a este último grupo.

7.2.1 CASO N.º 18: evaluación del riesgo, mitigación y obligaciones

129. Aunque es probable que el atacante no tuviera por objeto recoger datos personales, ya que la violación podría dar lugar tanto a daños materiales (por ejemplo, pérdidas financieras) como inmateriales (por ejemplo, usurpación de identidad o fraude), o los datos podrían utilizarse para facilitar otros ataques (por ejemplo, suplantación de identidad), es probable que la violación de los datos personales entrañe un alto riesgo para los derechos y libertades de las personas físicas. Por lo tanto, la violación de la seguridad de los datos debe comunicarse a los noventa y nueve empleados y no solo a los diez empleados cuya información salarial se filtró.

130. Tras tener conocimiento de la violación de la seguridad, el responsable del tratamiento obligó a cambiar la contraseña de las cuentas afectadas, bloqueó el envío de correos electrónicos a la cuenta de correo electrónico del atacante, notificó al proveedor de servicios el correo electrónico utilizado por el atacante en relación con sus acciones, suprimió las normas establecidas por el atacante y perfeccionó las alertas del sistema de seguimiento para emitir una alerta tan pronto como se cree una norma automática. Alternativamente, el responsable del tratamiento podría suprimir el derecho de los usuarios a establecer normas de transmisión y solo sería necesario que el equipo del servicio informático lo hiciera únicamente previa solicitud, o podría introducir una política de que los usuarios deban comprobar e informar sobre las normas establecidas en sus cuentas una vez por semana o con mayor frecuencia, en ámbitos que manejen datos financieros.

131. El hecho de que una violación de la seguridad de los datos pueda producirse y no detectarse durante tanto tiempo y el hecho de que, en un plazo más largo, la ingeniería social podría haberse utilizado para modificar más datos, puso de manifiesto importantes problemas en el sistema de seguridad informática del responsable del tratamiento. Estos hechos deben abordarse sin demora, haciendo hincapié en las revisiones automatizadas y los controles de los cambio, la detección de incidentes y las medidas de respuesta. Los responsables del tratamiento de datos sensibles, información financiera, etc. tienen una mayor responsabilidad a la hora de garantizar una seguridad adecuada de los datos.

Acciones necesarias en función de los riesgos detectados		
Documentación interna	Notificación a la AC	Comunicación a los interesados
✓	✓	✓