AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS

isms forum spain

Guía para la gestión y notificación de brechas de seguridad

Con la colaboración de:

CCN Centro Criptológico Nacional

incibe_ INSTITUTO NACIONAL DE CIBERSEGURIDAD

Índice

1. Introducción

El tratamiento de datos personales con diversas finalidades y diferentes volúmenes de información y complejidad es una realidad dentro de la actividad cotidiana de las empresas.

La protección de las personas físicas en relación con el tratamiento de datos personales es un derecho fundamental, y en ese sentido la rápida evolución tecnológica y el nivel de globalización han planteado nuevos retos para la protección de datos personales.

El Reglamento General de Protección de Datos (RGPD) pretende establecer un marco más sólido y coherente para la protección de datos en la Unión Europea, siendo aplicable a partir del 25 de mayo de 2018. El RGPD señala que las medidas dirigidas a garantizar su cumplimiento deben tener en cuenta la naturaleza, el ámbito, el contexto y los fines del tratamiento así como el riesgo para los derechos y libertades de las personas.

El nuevo RGPD implica para los responsables el reto de adaptar de manera continua las condiciones de los tratamientos de datos personales que realizan. Esta adaptación es un reto, en especial para el tejido empresarial nacional principalmente compuesto de pymes y micropymes que se ven en la necesidad de llevar a cabo actividades como, por ejemplo, las relacionadas con el análisis de riesgos de los tratamientos que realizan.

Este esfuerzo de adaptación de los responsables y encargados de los tratamientos está, en definitiva, encaminado a favorecer el desarrollo de la economía digital y el fortalecimiento de los derechos y libertades de las personas, sin la confianza de los interesados, el desarrollo de la economía digital no será posible. En definitiva el RGPD se convierte en una herramienta para compatibilizar el desarrollo de la economía digital con garantías para los derechos y libertades de las personas y no debe ser considerado única y exclusivamente un nuevo modelo de cumplimiento. Con relación a la pro actividad para supervisar de forma constante los tratamientos de datos personales por parte de los encargados y los responsables de los tratamientos, el RGPD añade la notificación de las violaciones de seguridad

que puedan suponer un riesgo para los derechos y libertades de las personas físicas, a la autoridad de control competente, que en el caso de España se trata de la **Agencia Española de Protección de Datos** (AEPD). Aunque el vocablo "violaciones" es el utilizado en la traducción al castellano del RGPD el término que se utilizará en esta guía es el de "brechas de seguridad" por tratarse de un término que, desde el punto de vista semántico, señala con carácter general a los incidentes que pueden afectar o afectan a la seguridad de información y los datos personales.

Hasta la aplicación del RGPD, la obligación de notificar este tipo de brechas de seguridad a la AEPD se ceñía exclusivamente a operadores de servicios de comunicaciones electrónicas[1] y prestadores de servicios de confianza[2], sin embargo pasa a ser aplicable a cualquier responsable de un tratamiento de datos personales. Pero la obligación de notificar las brechas de seguridad es una parte de un todo que se integra dentro de lo que hasta ahora sería el registro y procedimientos de gestión de incidencias que a su vez forman parte de otra disciplina como es la gestión de la seguridad de la información.

Otros sujetos obligados a notificar incidentes de seguridad a los equipos de respuesta a incidentes de seguridad informática (CSIRT) designados son los operadores de servicios esenciales y proveedores de servicios digitales[3]. Además, los prestadores de servicios de la Sociedad de la Información[4] pueden notificar voluntariamente a equipos de respuesta a emergencias informáticas (CERT) competente, y en cualquier caso están obligados a prestar colaboración con éstos para la resolución de incidentes de ciberseguridad que tengan efectos significativos en la continuidad de los servicios que prestan.

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

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

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

[1] Artículos 41 y 44 de la **Ley 9/2014 General de Telecomunicaciones**

[2] Artículo 19.2 del **Reglamento 910/2014 del Parlamento Europeo y del Consejo**

[3] Artículos 14 y 16 de la **Directiva UE 2016/1148 NIS**

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

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

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

Con independencia del origen de la obligación legal, esta guía está orientada a proporcionar directrices generales en la gestión de brechas y, en especial, a aquellos casos en los que la brecha tenga o pueda tener incidencia en el ámbito del RGPD, es decir, en aquellos casos en los que la brecha de seguridad pueda afectar a los derechos y libertades de las personas. Por otra parte, hay que tener en cuenta que en el ámbito del RGPD la notificación podría no realizarse cuando sea improbable que la brecha de seguridad constituya un riesgo para los derechos y libertades de las personas físicas, mientras que, por ejemplo, en la LSSI hay que notificar todas con independencia de su gravedad.

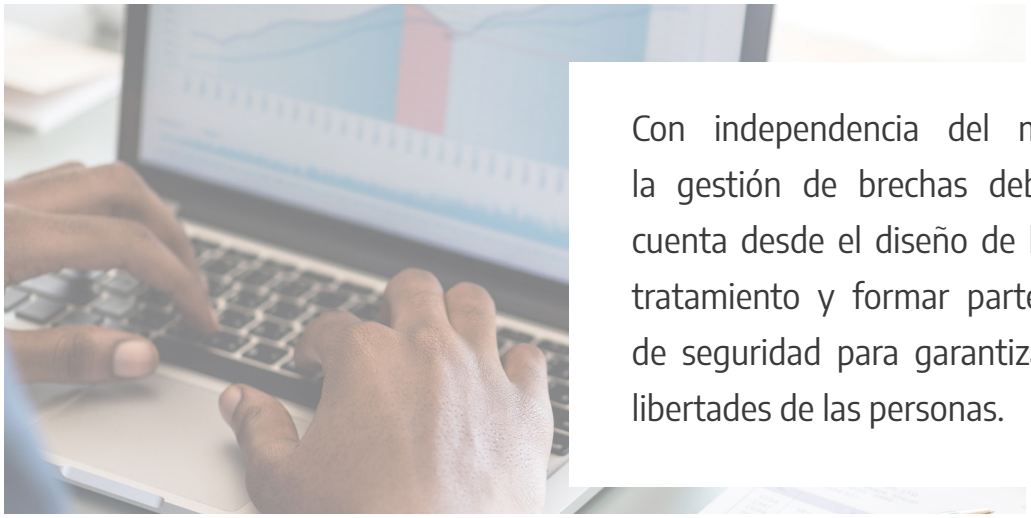
La gestión de brechas de seguridad no es una novedad para nuestros responsables, ya el Reglamento de Desarrollo de la LOPD (RDLOPD:RD 1720/2007) hacía referencia a la obligación de incluir en el documento de seguridad un procedimiento de notificación, gestión y respuesta ante las incidencias; procedimiento que además debería incluir el mantenimiento de un registro de incidencias. Esta obligación del RDLOPD dejará de ser preceptiva tras la plena aplicación del RGPD pero no por ello perderá su importancia y dejará de ser necesaria para garantizar la proactividad de los responsables en sus actividades de tratamiento.

Desde la AEPD se considera que el RDLOPD ha aportado cultura de gestión de brechas de seguridad entre nuestros responsables, cultura que en este momento sigue siendo aún más necesaria dada la evolución tecnológica en la que se ven envueltos los tratamientos de datos personales.

Por lo tanto, la gestión de brechas de seguridad no es una novedad y, además de la normativa de protección de datos, existen otras normas que recogen esta obligación. En el caso de las Administraciones públicas, el Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema

Nacional de Seguridad en el ámbito de la Administración Electrónica (ENS), en su capítulo VII (Art. 36) asigna el papel de coordinación en materia de respuesta a incidentes de seguridad al Centro Criptológico Nacional (CCN) con el objetivo de articular mecanismos de respuesta a los incidentes de seguridad mediante la estructura CCN- CERT (Centro Criptológico Nacional-Computer Emergency Reaction Team) obligando a la notificación de incidentes de seguridad a las Administraciones Públicas y en consecuencia, añadiendo la necesidad de gestionar las brechas de seguridad. Para facilitar esta labor el CCN dispone de la guía para la "Gestión y Notificación de Ciberincidentes" (CCN-STIC 817) que ha sido utilizada como referencia en la elaboración del presente documento y, además, proporciona de forma gratuita la herramienta LUCIA como canal para llevar a cabo las notificaciones de brechas de seguridad.

El ENS constituye una referencia para la selección de medidas de seguridad, de obligado cumplimiento en el caso de entidades del sector público y puede también resultar interesante para organizaciones privadas.



Con independencia del marco normativo, la gestión de brechas debe ser tenida en cuenta desde el diseño de las actividades de tratamiento y formar parte de las medidas de seguridad para garantizar los derechos y libertades de las personas.

En la práctica, el registro de incidencias sigue siendo una herramienta útil para los responsables y encargados de los tratamientos que en el RGPD se traduce en la obligación de documentar cualquier "violación" de seguridad de los datos personales y así lo pone de manifiesto el art. 35.5 del RGPD, por lo tanto la cultura del registro de incidencias y la gestión de brechas mantienen su valor en el nuevo contexto normativo.

Es evidente que cualquier organización que trate datos personales se encuentra expuesta a sufrir una brecha de seguridad que pueda o no repercutir en la privacidad de los interesados, de esta forma el proceso de la gestión de brechas se suma a los procesos de negocio ya existentes en una organización y

es una parte necesaria para mantener la normal actividad de cualquier entidad, proceso que al mismo tiempo se constituye en una de las medidas organizativas más importantes a la hora de salvaguardar la seguridad de los tratamiento y en consecuencia, los derechos y libertades de los interesados.

A diferencia de lo que suponía el Título VIII del RDLOPD en cuanto a la obligación de disponer de un registro de incidencias, en esta guía se dan pautas y recomendaciones dirigidas a la gestión de las brechas, se trata de una visión global relacionada con la forma de abordar una brecha de seguridad y de preparar a las entidades que tratan datos personales para enfrentarse a una situación crítica como puede ocurrir en ocasiones en que, además de daños para terceros, podría llegar a implicar riesgos directos para el propio negocio.

> La obligación de notificar las brechas de seguridad que afecten a los tratamientos de datos personales adquirirá un carácter universal, haciéndose extensible a todas aquellas entidades que lleven a cabo un tratamiento de datos de carácter personal en el ámbito de aplicación de dicha norma.

2. Objetivos de la guía

Desde la AEPD consideramos de interés general la colaboración con asociaciones y colectivos de expertos por este motivo, esta guía está promovida y coordinada por la AEPD e ISMS Fórum, con la participación de numerosos profesionales y expertos del sector, recogiendo la experiencia y conocimiento de empresas que tienen implantados procedimientos de gestión de incidentes de seguridad eficaces, por lo que se pretende que sea de utilidad para todos aquellos que quieran o necesiten familiarizarse con la temática relativa a la gestión y notificación de brechas de seguridad. Por otra parte, y como no podría ser de otra forma, tanto **INCIBE** como **CCN-CERT** también han participado en la elaboración final de esta guía aportando su experiencia y conocimiento en la gestión de brechas de ciberseguridad.

Esta guía va dirigida a responsables de tratamientos de datos personales de diversa índole que puedan estar afectados por brechas de seguridad de los datos, con el objetivo de facilitar la interpretación del RGPD en lo relativo a la obligación de notificar a la autoridad competente y, en su caso, a los afectados de modo que la notificación a la autoridad competente se haga por el canal adecuado, contenga información útil y precisa a efectos estadísticos y de seguimiento, y se adecúe a las nuevas exigencias del RGPD.

Se trata de una guía que pretende cubrir el amplio abanico del tejido empresarial español, pequeñas, medianas o empresas grandes de toda índole, empresas con grandes tratamientos de datos y empresas con tratamientos reducidos y que, del mismo modo, puede ser de ayuda a los responsables y encargados de tratamientos de las Administraciones Públicas involucrados en las tareas de gestión de las brechas de seguridad.

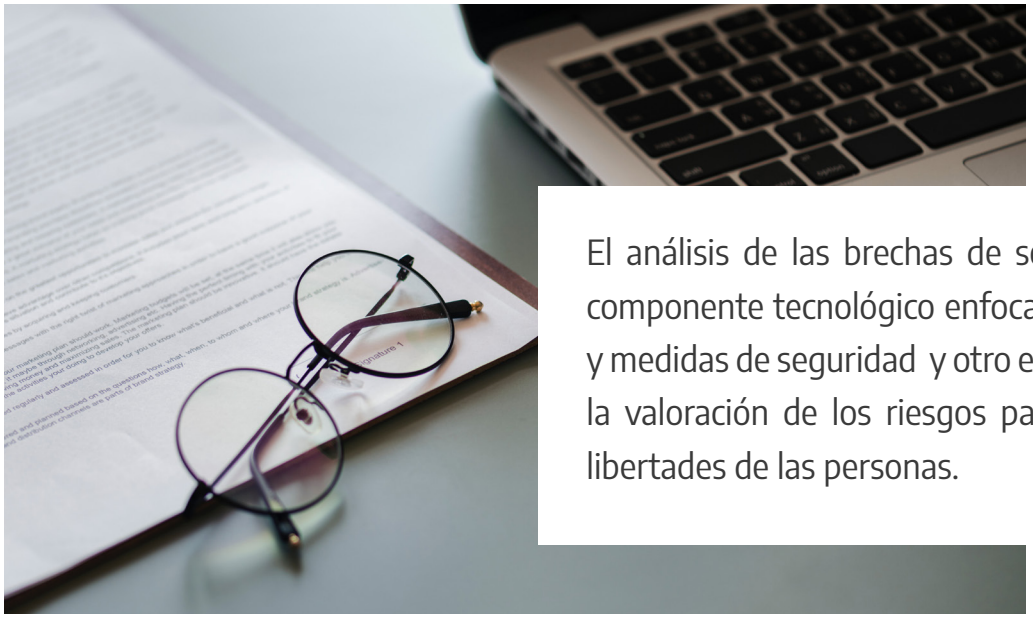
La difusión de la guía debe servir también para transmitir y divulgar a profesionales, interesados y el conjunto de la sociedad la importancia de la gestión, tratamiento y resolución de este tipo de incidentes, así como las medidas para su prevención, y no sólo su preceptiva notificación.

Pretende facilitar a los responsables y encargados de los tratamientos un plan de actuación para enfrentarse a las brechas en función de las fases habituales en las tareas implicadas para paliar o aminorar las consecuencias negativas, por ejemplo:

- Se ha realizado una clasificación de mecanismos de detección e identificación de las brechas
- Se establecen tipologías de brechas teniendo en cuenta su peligrosidad
- Se tiene en cuenta un plan de actuación con las figuras implicadas y los procesos que son necesarios tener en cuenta (análisis, clasificación, contención, respuesta, seguimientos, cierre,...)

- Se establecen prioridades para llevar a cabo la contención la solución y la custodia de evidencias
- Finamente la guía será de ayuda para llevar a cabo procesos de notificación en aquellos casos en que sean necesaria.

En definitiva esperamos que esta guía sea una ayuda para la **gestión integral** de las brechas de seguridad, elemento que debe entenderse como parte de su proactividad y no exclusivamente una forma de dar cumplimiento a la obligación de mantener un registro documental de las incidencias y las notificaciones.



El análisis de las brechas de seguridad tiene un componente tecnológico enfocado a los controles y medidas de seguridad y otro en que es necesario la valoración de los riesgos para los derechos y libertades de las personas.

Ambos aspectos implican la participación tanto de los responsables de seguridad (CISO) como de los delegados de protección de datos (DPD).

La gestión de la privacidad y de la seguridad son entidades distintas con objetivos comunes: salvaguardar los derechos y libertades de las personas y garantizar la seguridad de la información. Responsables de seguridad y delegados de protección de datos están obligados a trabajar juntos estableciendo vínculos colaborativos y ambos son clave cuando se trata de salvaguardar la seguridad de los tratamientos.

Pero la seguridad de los tratamientos no reside únicamente en estas dos figuras, la labor de concienciación y formación de todo el personal con acceso a los datos personales es también fundamental tanto para garantizar la seguridad de los tratamientos y en particular para la gestión de las brechas de seguridad. La implicación de todo el personal es, posiblemente, una de las cuestiones más

importantes cuando se habla de medidas organizativas para garantizar la seguridad (confidencialidad, integridad y disponibilidad) de los datos personales.

Una vez articulada la participación de todo el personal de una organización mediante medidas de formación, las posibilidades de éxito para proteger los datos personales serán mayores aunque esto nunca eliminará el riesgo de que se produzca una brecha de seguridad en términos absolutos.

Sin embargo no se debe caer en el error de que tanto los delegados de protección de datos como los responsables de seguridad son "responsables" de la licitud de los tratamientos de datos que intentan garantizar.

El responsable del tratamiento de datos personales es, en última instancia, quien decide acerca del tratamiento y quien asume la responsabilidad de los tratamientos de datos personales que se lleven a cabo en su organización. El delegado de protección de datos tiene el papel de supervisar la licitud de los tratamientos informando y asesorando al responsable; por su parte el responsable de seguridad es la persona encargada de supervisar los controles necesarios para proteger los datos y controlar su eficacia.

Pero la gestión de brechas de seguridad no se limita a la relación entre los responsables y la AEPD, cuando se habla de brechas de seguridad se hace referencia a una obligación que viene expresada por varios marcos normativos y sectoriales que en ocasiones implican distintas obligaciones de notificar y hacen necesaria la existencia de un mecanismo de ventanilla única que se constituya en un procedimiento que permita, al menos, la notificación inicial de forma única sin necesidad de llevar a cabo varias notificaciones en un momento que puede ser crítico para sus organizaciones. Gracias a la colaboración entre el CCN-CERT y la AEPD se va a disponer de un mecanismo centralizado de notificaciones sin descartar la vía de la notificación directa a la AEPD para aquellos responsables que así lo decidan. Con relación a las posibles sanciones que pudieran derivar de las mismas, decir que la notificación no implicará de forma directa la imposición de una sanción por parte de la AEPD, ésta sería el resultado de falta de diligencia de responsables y encargados cuando suponga la falta de medidas de

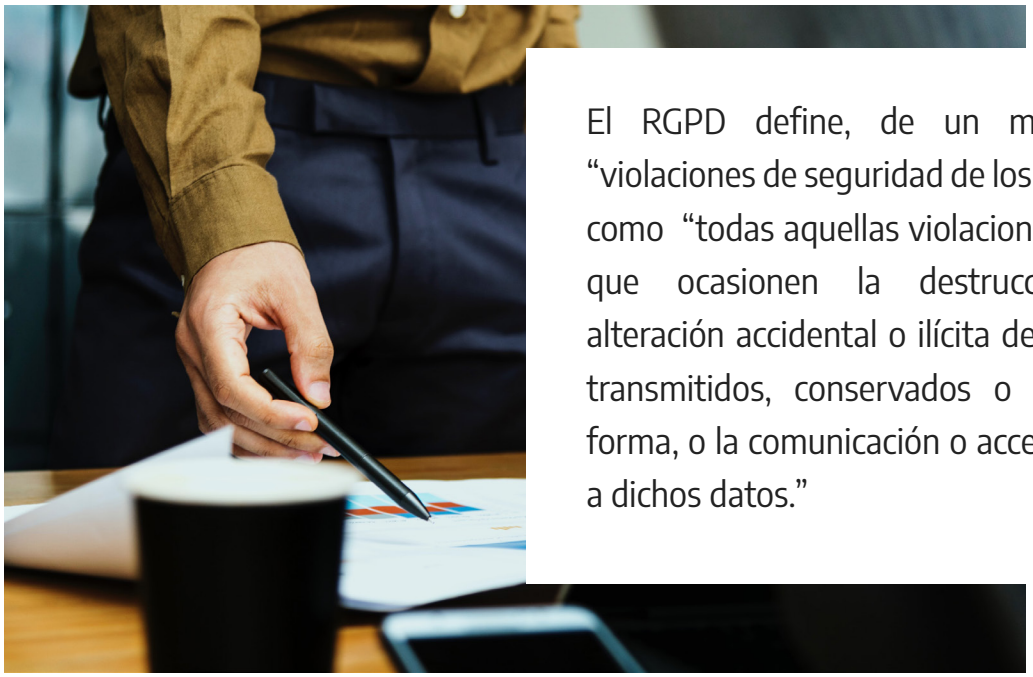
seguridad adecuadas de los tratamientos y se produzca un posible perjuicio para los derechos y deberes de los interesados. En este caso tendría sentido el inicio de un posible procedimiento sancionador.

Finalmente, la guía se estructura según la relación temporal entre los procesos más importantes de gestión de brechas de seguridad que se muestran en la siguiente figura, que coincide en gran medida con el Proceso de Gestión de Incidentes que muchas entidades utilizan habitualmente:

- Se presenta un primer apartado dedicado a la detección e identificación de brechas de seguridad. Este punto incluye detalles sobre cómo una organización debe estar preparada para detectar los incidentes de seguridad que puedan ocurrir, mediante mecanismos de detección apropiados. De entre todas las detecciones que se produzcan es necesario poder discernir cuales son realmente incidentes de seguridad y cuales no lo son, esto es identificar el incidente y realizar una clasificación preliminar del mismo. Para identificar incidentes de seguridad es de gran ayuda contar con un servicio de avisos o notificaciones como los que proporcionan INCIBE y CCN-CERT, también es de interés contar con la suscripción de servicios de avisos de los propios fabricantes de los productos de los que se disponga (bases de datos, productos web, etc.).
- Seguidamente se incluye un apartado dedicado al plan de actuación, en la que se presentan los aspectos básicos sobre cómo proceder ante un incidente que puede clasificarse como una brecha de seguridad.
- Este apartado contiene detalles sobre la realización de un proceso de análisis que permita obtener información para determinar con mayor precisión la clasificación del incidente.
- En los dos últimos apartados se profundiza en dos de los aspectos más importantes de la gestión de brechas de seguridad, se trata del proceso de respuesta y la notificación de la brecha a la autoridad de control competente.

3. ¿Qué se entiende por brecha de seguridad?

Hasta la publicación del RGPD se contaban con algunas definiciones generales sobre lo que podría considerarse una "brecha de seguridad". Así, el Esquema Nacional de Seguridad[5] (ENS) define un "incidente de seguridad" como aquel "suceso inesperado o no deseado con consecuencias en detrimento de la seguridad del sistema de información". En la misma línea, la Directiva NIS define "incidente" como "todo hecho que tenga efectos adversos reales en la seguridad de las redes y sistemas de información".



El RGPD define, de un modo amplio, las "violaciones de seguridad de los datos personales" como "todas aquellas violaciones de la seguridad que ocasionen la destrucción, pérdida o alteración accidental o ilícita de datos personales transmitidos, conservados o tratados de otra forma, o la comunicación o acceso no autorizados a dichos datos."

Debe quedar claro, tal como indica el Grupo de Trabajo del Artículo 29 (WP29), que la "violación" a la que se refiere el RGPD, aun siendo un tipo de incidente de seguridad, solo se aplica en la medida en que afecte a datos de carácter personal, y en consecuencia dicho incidente pueda comprometer al responsable del tratamiento en el cumplimiento de los principios del RPGD.

Por tanto, se debe tener en cuenta que, aunque todas las brechas de datos personales son incidentes de seguridad, no todos los incidentes de seguridad son necesariamente brechas de datos personales.

[5] Real Decreto 3/2010 por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica.

4. Nuevas obligaciones relativas a la gestión de brechas de seguridad

De acuerdo con el RGPD, tan pronto como el responsable del tratamiento tenga conocimiento de que se ha producido una brecha de la seguridad de los datos personales debe efectuar la correspondiente notificación a la autoridad de control competente, sin dilación y a más tardar en las 72 horas siguientes.

Cuando en el momento de la notificación no fuese posible cumplir con la obligación de facilitar toda la información exigida, que figura en el apartado sobre Notificación de esta guía, se facilitará de manera gradual, a la mayor brevedad y sin dilación.

La única excepción a esta obligación de notificación tendría lugar cuando, conforme al principio de responsabilidad proactiva, el responsable pueda demostrar que la brecha de la seguridad de los datos personales no entraña un riesgo para los derechos y las libertades de las personas físicas.

Por el contrario, cuando la brecha de seguridad entrañe un alto riesgo para los derechos y libertades de los titulares de los datos, además de la comunicación a la autoridad de control, el responsable del tratamiento deberá, adicionalmente, comunicar a los afectados la brecha de seguridad sin dilación indebida y con lenguaje claro y sencillo, de forma concisa y transparente, salvo en algunos supuestos, expuestos y determinados en esta Guía.

5. Marco normativo

Existen varios marcos normativos en los que se contempla la obligación de notificar brechas de seguridad con distintas motivaciones, al final del documento se incluye un anexo I donde se relacionan una serie de normas que contemplan la obligación de la gestión y notificación de brechas de seguridad en la fecha de publicación de esta guía.

Sin perjuicio de otras obligaciones que puedan afectar a los responsables, esta guía se refiere únicamente a aquellas brechas de seguridad que afecten a datos personales.

6. Gestión de brechas de seguridad: detección e indentificación y clasificación

El primer paso en la gestión de brechas de seguridad es ser conscientes de que en todas las organizaciones se tienen incidentes de seguridad y por tanto, se debe proceder a gestionar este tipo de incidentes en mayor o menor grado.

En la medida en que la organización esté **preparada** para **afrontar la gestión de un incidente** de seguridad permitirá a la organización responder de forma rápida, ordenada y eficaz al evento, minimizando las consecuencias del mismo sobre la propia organización y terceras partes implicadas. El nivel de respuesta a un incidente de seguridad dependerá del tamaño de la organización, del tipo de datos y la complejidad del tratamiento.

Para una buena gestión de brechas de seguridad, el responsable debe documentarlas debidamente según el artículo 33 del RGPD, a tal efecto, sigue siendo necesario disponer de un registro de incidencias como apuntaba el Título VIII del RD 1720/2007 en su Artículo 90[6].

Es recomendable, y en algunos casos obligatorio, que los responsables elaboren procedimientos, planes de actuación o los denominados "procedimientos de respuesta a incidentes". Estos procedimientos pueden ser muy sencillos en caso de pequeñas empresas con pequeños tratamientos de datos o más complejos en el caso de grandes empresas con tratamientos de mayor riesgo. En cualquier caso las **políticas de seguridad** de la información y protección de datos deben incluir una parte relativa a la gestión de brechas, con la consiguiente asignación de recursos humanos y medios materiales proporcionales a los tratamientos que se realizan. De igual modo, los encargados de tratamiento deben

[6] Aunque se cita el registro de incidencias, las medidas de seguridad a aplicar se determinarán en función de los riesgos identificados para cada tratamiento concreto.

establecer procedimientos similares para la gestión de los incidentes relacionados con las actividades de tratamiento que realicen por cuenta de un responsable, que permitan un tratamiento adecuado de los mismos y una comunicación apropiada con los responsables.

En definitiva, independientemente del tamaño y complejidad, las organizaciones, tanto si son responsables o encargados de tratamientos de datos personales, deben tener claramente establecido cómo van a proceder ante una brecha de seguridad, en algunos casos toda la gestión del incidente será interna y en muchos otros casos la gestión del incidente será realizada mayoritariamente de forma externa.

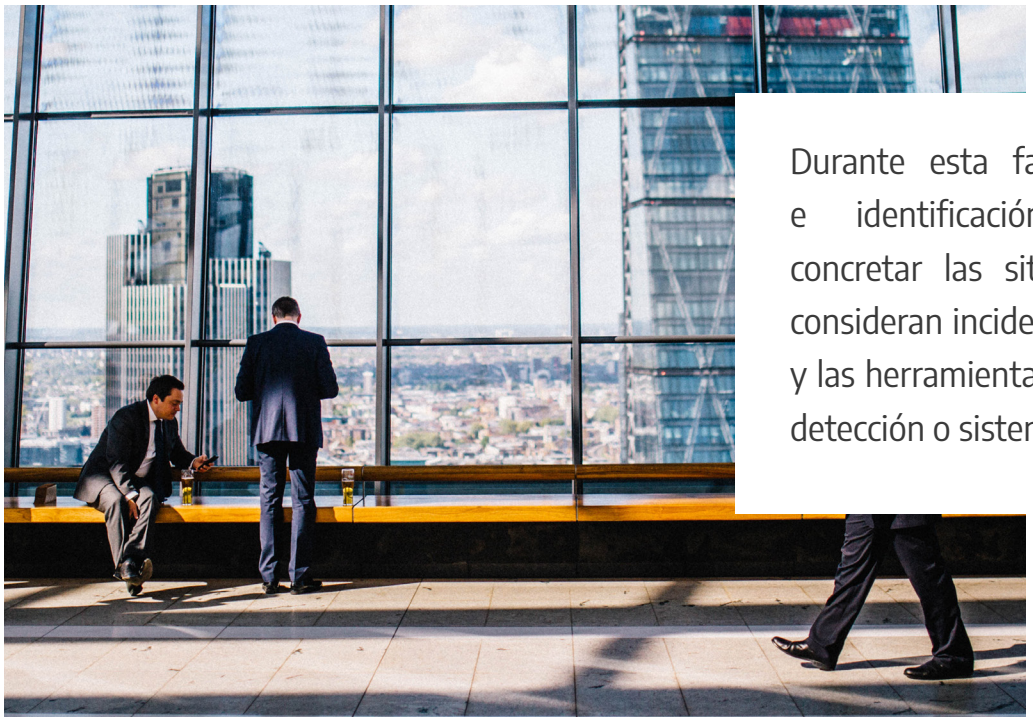
Dentro del procedimiento de gestión de incidentes anteriormente presentado, este apartado se centra en la Detección e Identificación, que se muestra destacado en color rojo en la siguiente figura:

Es necesario un proceso previo de Preparación en el que se decidirán las medidas técnicas y organizativas para poder afrontar un incidente. Esto incluye la identificación de los agentes implicados en la gestión de la brecha, el análisis de riesgos y/o evaluación de impacto en caso de que sean necesarias y la definición de los "planes de respuesta a incidentes" o "plan de contingencia".

El siguiente proceso consiste en detectar los incidentes de seguridad, sin el cual el resto de procesos no tendrían sentido. El citado proceso que debe funcionar de manera continua dentro de la operativa habitual de la organización en la que se establecen mecanismos de detección de eventos que permitan identificar un incidente de seguridad y su posterior clasificación como brecha de seguridad. Asímismo, también se realiza una clasificación preliminar del incidente, con el fin de tomar unas primeras acciones rápidas contra la amenaza. Una vez identificado el incidente de seguridad se activará el plan de actuación que incluirá una fase preliminar de análisis que permite conocer más detalles sobre el

incidente acontecido, además de una identificación y clasificación más precisa del mismo, un proceso de respuesta y otro de notificación en caso de que se confirme que el incidente de seguridad ha supuesto una brecha de seguridad.

6.1 Detección e identificación



Durante esta fase de detección e identificación se deberán concretar las situaciones que se consideran incidentes de seguridad y las herramientas, mecanismos de detección o sistemas de alerta.

Durante esta fase de detección e identificación se deberán concretar las situaciones que se consideran incidentes de seguridad y las herramientas, mecanismos de detección o sistemas de alerta con los que el responsable (bien por su cuenta, bien por cuenta de un encargado) va a contar para detectar un incidente, así como el análisis de la información que proporcionen dichas herramientas o sistemas de alerta. Estos mecanismos permitirán a la organización identificar una brecha de seguridad en caso de que se produzca.

El momento en que se detecta e identifica una brecha de seguridad es importante ya que el RGPD establece que el responsable del tratamiento debe notificar a la autoridad de control competente sin dilación indebida y, de ser posible, a más tardar 72 horas después de que haya tenido constancia de ella. En determinados casos se deberá notificar también a los afectados. Para más información al respecto consúltese el apartado de Notificación.

6.1.1 Formas de detección e identificación

La identificación de un incidente de seguridad puede producirse a través de fuentes internas a la organización o fuentes externas.

Fuentes internas

Se refiere los controles y mecanismos de seguridad dentro y alrededor de las instalaciones de la organización, así como los medios de acceso remoto a la información. Desde el punto de vista de la seguridad física, la detección se produciría ante el incumplimiento o vulneración de las medidas de seguridad adoptadas, como por ejemplo:

- Políticas específicas de mesas limpias, bloqueo de pantallas, accesos con usuario y contraseña, etc.
- Controles físicos como detección de intrusos, videovigilancia, control y registro de accesos a determinadas zonas, etc.
- Controles y procedimientos frente a daños ambientales o desastres naturales. En este sentido, cobra suma importancia la concienciación y formación de todo el personal de la organización para evitar situaciones de riesgo e incluso detectarlas y notificarlas.

En cuanto a los controles de ciberseguridad, atendiendo a las características particulares de la organización, se puede contar con medios manuales, como la notificación de problemas por parte del personal de la organización, y sistemas automatizados de detección de diferentes tipos, desde software antivirus hasta analizadores de logs.

Es preciso tener en cuenta que con frecuencia un incidente que tenga lugar en el ámbito de la seguridad física puede también tener repercusión en el contexto de la ciberseguridad y por lo tanto en los tratamientos de datos personales, de ahí la necesidad de mantener cierto grado de coordinación entre los responsables de la seguridad física y la ciberseguridad.

Sin ánimo de exhaustividad, se pueden considerar las siguientes fuentes de información:

- Notificaciones de usuarios: presencia de archivos con caracteres inusuales, recepción de correos electrónicos con archivos adjuntos sospechosos, comportamiento extraño de dispositivos, imposibilidad de acceder a ciertos servicios, extravío/robo de dispositivos de almacenamiento o equipos con información.
- Alertas generadas por software antivirus.
- Consumos excesivos y repentinos de memoria o disco en servidores y equipos.

- Anomalías de tráfico de red o picos de tráfico en horas inusuales.
- Alertas de sistemas de detección/prevención de intrusión (IDS/IPS).
- Alertas de sistemas de correlación de eventos.
- Análisis de registros de conexiones realizadas a través de proxys corporativos o conexiones bloqueadas en los cortafuegos.
- Análisis de registro de servidores y aplicaciones con intentos de acceso no autorizados.
- Análisis de registros en herramientas DLP (Data Loss Prevention).

También se debe considerar cualquier posible indicio de la ocurrencia de un incidente de seguridad en el futuro, como el análisis del resultado de un escáner de vulnerabilidades del sistema, el anuncio de un nuevo 'exploit' dirigido a atacar una vulnerabilidad que podría estar presente en el sistema o amenazas explícitas anunciando ataques a los sistemas de información de la organización[7] .

Fuentes externas

En muchas ocasiones es posible que la detección del incidente se produzca a través de la comunicación de un tercero (proveedores de servicios informáticos, proveedores de servicios de internet o fabricantes de soluciones de seguridad), por un cliente o por la comunicación o notificación que realicen a la empresa los distintos organismos públicos como el Instituto Nacional de Cyberseguridad (INCIBE), el Centro Criptológico Nacional (CCN), Fuerzas y Cuerpos de Seguridad del Estado, o incluso mediante información publicada en medios de comunicación.

Por ejemplo, una pequeña empresa que tiene subcontratados sus servicios informáticos y recibe una comunicación de incidente de parte de su consultoría informática o el caso de una gran empresa que recibe una comunicación directa por parte de un organismo público o cuando los responsables que tengan encargado el tratamiento de los datos a un tercero y reciben la comunicación de la brecha de seguridad por parte de éste.

6.1.2 Identificación y registro

El análisis de las fuentes de información antes mencionadas permitirá determinar si se está ante un incidente de seguridad o no, así como su naturaleza, clase, tipo, si dicho incidente ha afectado a datos de carácter personal y por tanto constituye una "brecha de los datos de carácter personal" descrita en el RGPD, y el nivel de riesgo al que se enfrenta la organización.

[7] Como apunta en la guía CCN-STIC-817

Una vez identificado el incidente es necesario contar con medios para documentar el seguimiento del mismo, quedando anotados todos los aspectos del incidente en un registro de incidencias.

Desde los síntomas y mecanismos de detección que permitieron identificarlo hasta las acciones y medidas de control adoptadas en cada una de las fases de gestión del incidente. En particular, la empresa deberá mantener como mínimo un registro documental de los incidentes de seguridad que hayan afectado a los datos de carácter personal[8], incluyendo el tipo de incidente, descripción del mismo, gravedad, estado y medidas adoptadas para su resolución. Por otra parte, una de las ventajas de disponer de este registro documental de incidencias es que, en ocasiones, incidentes de pequeña entidad pueden revelar la ocurrencia de un problema mayor previamente no identificado.

6.2 Clasificación

6.2.1 Clasificación de incidentes de seguridad

Los factores[9] que se pueden considerar a la hora de establecer criterios de clasificación son, entre otros:

- Tipo de amenaza: código dañino, intrusiones, fraude, etc. Se trata de una breve descripción del incidente en función de la información de la que se disponga.
- Contexto u origen de la amenaza: interna o externa.

[8] En virtud del artículo 33.5 de RGPD

[9] Párrafo 31 de la guía CCN-STIC-817

- Categoría de seguridad de los sistemas y datos afectados afectados.
- El perfil de los usuarios afectados.
- Número y tipología de los sistemas afectados.
- Impacto del incidente en la organización y en los derechos y libertades de los afectados.
- Requerimientos legales y regulatorios.
- Vector de ataque o método: ruta o medio por el que se ha materializado el incidente. El concepto de "vector de ataque" suele ser uno de los criterios más aceptados a nivel mundial y está directamente relacionado con la identificación del mismo.

A continuación se indican algunas tipologías de casos que pueden dar lugar a un incidente:

- **0-day (vulnerabilidad no conocida):** Vulnerabilidad que permite a un atacante el acceso a los datos en la medida en que es una vulnerabilidad desconocida. Esta vulnerabilidad estará disponible hasta que el fabricante o desarrollador la resuelva.
- **APT (ataque dirigido):** Se refiere a diferentes tipos de ataques dirigidos normalmente a recabar información fundamental que permita continuar con ataques más sofisticados. En esta categoría se encuadraría por ejemplo una campaña de envío de email con software malintencionado a empleados de una empresa hasta conseguir que alguno de ellos lo instale en su equipo y proporcione una puerta de entrada al sistema.
- **Denegación de servicio (DoS/DDoS):** Consiste en inundar de tráfico un sistema hasta que no sea capaz de dar servicio a los usuarios legítimos del mismo.
- **Acceso a cuentas privilegiadas:** El atacante consigue acceder al sistema mediante una cuenta de usuario con privilegios avanzados, lo que le confiere libertad de acciones. Previamente deberá haber conseguido el nombre de usuario y contraseña por algún otro método, por ejemplo un ataque dirigido.
- **Código malicioso:** piezas de software cuyo objetivo es infiltrase o dañar un ordenador, servidor u otro dispositivo de red con finalidades muy diversas. Una de las posibilidad para que el código dañino alcance a una organización es que un usuario lo instale de forma involuntaria.
- **Compromiso de la información:** Recoge todos los incidentes relacionados con el acceso y fuga, modificación o borrado de información no pública.
- **Robo y/o filtración de datos:** Se incluye en esta categoría la pérdida/robo de dispositivos de almacenamiento con información.
- **Desfiguración (Defacement):** Es un tipo de ataque dirigido que consiste en la modificación de la página web corporativa con la intención de colgar mensajes reivindicativos de algún tipo o cualquier

otra intención. La operativa normal de la web queda interrumpida, produciéndose además daños reputacionales.

- **Explotación de vulnerabilidades de aplicaciones:** Cuando un posible atacante logra explotar con éxito una vulnerabilidad existente en un sistema o producto consiguiendo comprometer una aplicación de la organización.
- **Ingeniería social:** Son técnicas basadas en el engaño, normalmente llevadas a cabo a través de las redes sociales, que se emplean para dirigir la conducta de una persona u obtener información sensible. Por ejemplo, el usuario es inducido a pulsar sobre un enlace haciéndole pensar que es lo correcto.

6.2.2 Tipo de brecha de seguridad

Una brecha de seguridad se puede clasificar en una o varias de las siguientes categorías:

- **Brecha de confidencialidad:** Tiene lugar cuando partes que no están autorizadas, o no tienen un propósito legítimo para acceder a la información, acceden a ella. La severidad de la pérdida de confidencialidad varía según el alcance de la divulgación, es decir, el número potencial y el tipo de partes que pueden haber accedido ilegalmente a la información.
- **Brecha de integridad:** se produce cuando se altera la información original y la sustitución de datos puede ser perjudicial para el individuo. La situación más grave ocurre cuando existen serias posibilidades de que los datos alterados se hayan utilizado de una manera que pueda dañar al individuo.
- **Brecha de disponibilidad:** su consecuencia es que no se puede acceder a los datos originales cuando es necesario. Puede ser temporal (los datos son recuperables pero tomará un periodo de tiempo y esto puede ser perjudicial para el individuo), o permanente (los datos no pueden recuperarse).

Valoración del alcance de la brecha de seguridad

La gestión de una brecha de seguridad requiere determinar la peligrosidad potencial del incidente y la estimación de la magnitud del impacto potencial en los individuos. Para esta evaluación se deberá recurrir al análisis de riesgos o evaluación de impacto realizado antes de la puesta en marcha de las actividades de tratamiento y a la clasificación previa del incidente.

6.2.3 Valoración del alcance de la brecha de seguridad

La peligrosidad dependerá de los siguientes factores:

- **La categoría o nivel de criticidad** respecto a la seguridad de los sistemas afectados. Siguiendo la clasificación genérica, podemos distinguir entre:
  - Crítico (afecta a datos valiosos, gran volumen y en poco tiempo)
  - Muy Alto (Cuando dispone de capacidad para afectar a información valiosa, en cantidad apreciable)
  - Alto (Cuando dispone de capacidad para afectar a información valiosa)
  - Medio (Cuando dispone de capacidad para afectar a un volumen apreciable de información)
  - Bajo (Escasa o nula capacidad para afectar a un volumen apreciable de información).

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

- **Datos legibles/ilegibles:** Datos protegidos mediante algún sistema de seudonimización (por ejemplo, cifrado o hash)
- **Volumen de datos personales:** expresados en cantidad (registros, ficheros, documentos) y/o en periodos de tiempo (una semana, un año, etc.)
- **Facilidad de identificación de individuos:** facilidad con la que se puede deducir la identidad de los individuos a partir de los datos involucrados en la brecha
- **Severidad de las consecuencias para los individuos:**
  - Baja: Las personas no se verán afectadas o pueden encontrar algunos inconvenientes que superarán sin ningún problema (tiempo de reingreso de información, molestias, irritaciones, etc.).
  - Media: Las personas pueden encontrar inconvenientes importantes, que podrán superar a pesar de algunas dificultades (costos adicionales, denegación de acceso a servicios comerciales, miedo, falta de comprensión, estrés, dolencias físicas menores, etc.).
  - Alta: Las personas pueden enfrentar consecuencias importantes, que deberían poder superar aunque con serias dificultades (malversación de fondos, listas negras de los bancos, daños a la propiedad, pérdida de empleo, citación judicial, empeoramiento de la salud, etc.).
  - Muy alta: Las personas pueden enfrentar consecuencias significativas, o incluso irreversibles, que

no pueden superar (exclusión o marginación social, dificultades financieras tales como deudas considerables o incapacidad para trabajar, dolencias psicológicas o físicas a largo plazo, muerte, etc.).

- **Características especiales de los individuos:** Si afectan a individuos con características especiales o con necesidades especiales.
- **Número de individuos afectados:** Dentro de una escala determinada, por ejemplo más de 100 individuos.
- **Características especiales del responsable del tratamiento (de la entidad en sí):** En base a la actividad de la entidad.
- **El perfil de los usuarios afectados**, su posición en la estructura organizativa de la entidad y, en su consecuencia, sus privilegios de acceso a información sensible o confidencial.
- **El número y tipología de los sistemas afectados.**
- **El impacto** que la brecha puede tener en la organización, desde los puntos de vista de la protección de la información, la prestación de los Servicios, la conformidad legal y/o la imagen pública. Va a estar relacionado con la categoría o criticidad de los servicios afectados y personas afectadas. En este aspecto diferenciamos entre los siguientes impactos:
  - Bajo (perjuicio limitado)
  - Medio (perjuicio grave)
  - Alto (perjuicio muy grave)
- **Los requerimientos legales y regulatorios:** Notificación de la brecha a la autoridad de control y cualquier otra obligación de notificación, comunicación a Fuerzas y Cuerpos de Seguridad del Estado en caso de delito.

7. Gestión de brechas de seguridad: Plan de actuación

Una vez detectado e identificado un incidente de seguridad es necesario entrar en una primera fase de análisis que permita recabar información y clasificar el incidente con mayor precisión. De la clasificación del incidente de seguridad dependerán las acciones a emprender durante los procesos de respuesta y notificación.

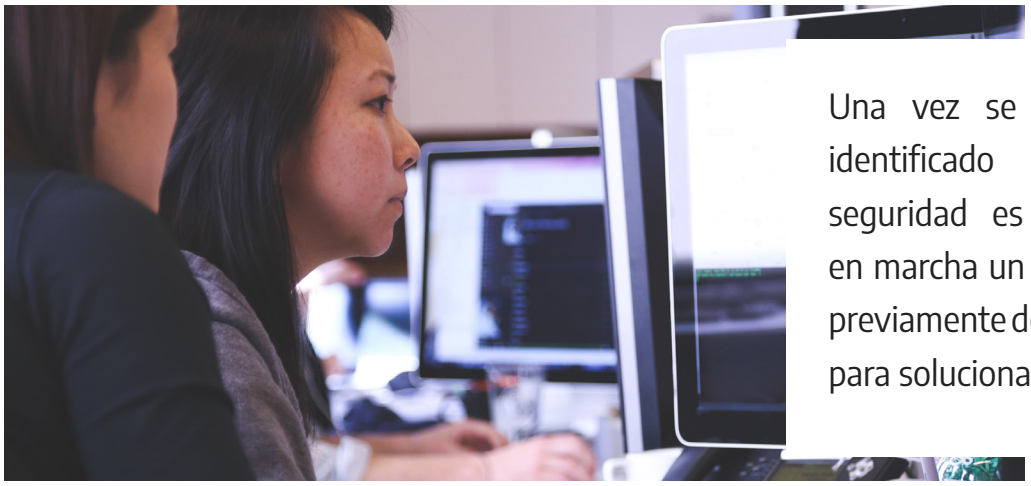
En caso de que el incidente de seguridad se acabe clasificando como una brecha de seguridad en la que se han comprometido datos personales se deberá iniciar también el proceso de notificación mediante el cual se notificará a la autoridad de control competente y se comunicará con los afectados cuando se cumplan las condiciones que exige el RGPD.

7.1 Figuras implicadas

Una vez que el incidente ha sido clasificado como una brecha de seguridad en la organización, y a efectos de una correcta y eficaz gestión de la misma, será necesaria la colaboración y actuación de las siguientes figuras:

- **Responsable del tratamiento:** le corresponde aplicar las medidas técnicas y organizativas apropiadas a fin de garantizar y poder demostrar que el tratamiento es conforme con el RGPD. Deberá notificar la brecha de seguridad a la autoridad de control competente, sin dilación indebida, y en su caso la comunicación con los afectados.

- **El responsable del tratamiento podrá contar con el asesoramiento de expertos en materia de seguridad** o los servicios informáticos propios o que pueda tener subcontratados. Así mismo podrá delegar la gestión de brechas de seguridad en servicios informáticos externos y/o los encargados del tratamiento. Encargado del tratamiento: notificará, sin dilación indebida, al responsable del tratamiento las brechas de seguridad de los datos personales de las que tenga conocimiento, con indicación de toda aquella información mínima y necesaria para su comunicación.
- **El responsable puede delegar en el encargado la gestión de las brechas de seguridad**, tanto en lo relativo a la respuesta como en lo relativo a la notificación, documentándose dicha delegación de funciones en el contexto de la relación contractual establecida. No obstante el responsable debe asegurarse de que se están tomando las acciones de respuesta, notificación y comunicación oportunas, dado que la delegación de funciones no implica la delegación de responsabilidad.
- **Delegado de Protección de Datos (DPD):** en los casos en los que se haya designado un Delegado de Protección de Datos (porque lo exija el RGPD o voluntariamente), éste ocupará un papel muy relevante liderando el plan de actuación en todos sus aspectos.
- **Autoridad de control competente:** se encargará de verificar que se cumple con el RGPD, y en este caso concreto en lo relativo a la gestión de la brecha de seguridad.



Una vez se ha detectado e identificado una brecha de seguridad es necesario poner en marcha un plan de actuación previamente definido y aprobado para solucionar el incidente.

Este plan comenzará con una primera fase de análisis en la que se termina de identificar y clasificar el problema, se pueden poner en marcha una serie de medidas tempranas de contención y se puede valorar una posible notificación temprana a la autoridad de control y/o los afectados. Posteriormente se podrá en marcha el proceso de respuesta y en caso de que sea necesario el proceso de notificación.

A continuación se introducen cada una de estas fases y en los siguientes apartados se presta más atención y se profundiza en los procesos de respuesta y notificación a la autoridad de control competente.

7.2 Análisis y Clasificación

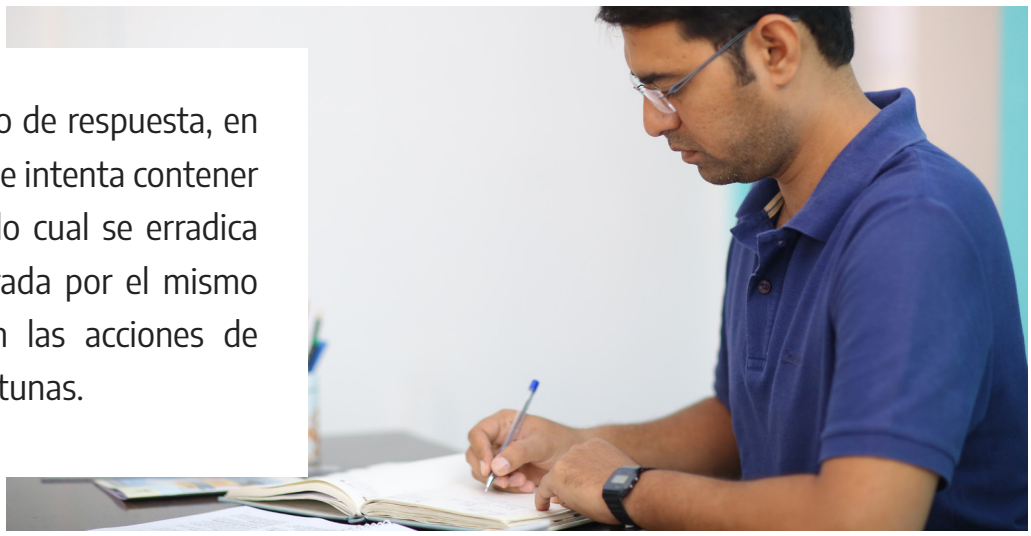
Dentro de esta fase, que incluye desde el momento en que se ha descubierto una brecha de seguridad deberían tenerse en cuenta los siguientes aspectos:

- **Recopilación y análisis de la información relativa a la brecha:** Los incidentes relacionados con la privacidad pueden tener múltiples orígenes. Como se indica en el apartado dedicado a detección e identificación, en ocasiones serán consecuencia de fallos de procesos que involucren el compromiso de información física confidencial, en estos casos las labores de investigación se basarán en contactar con usuarios finales involucrados, incluidos aquellos que hayan comunicado el incidente, así como proveedores si los hubiera. En otras múltiples ocasiones se tratará de incidentes tecnológicos que no solo pueden provenir de usuarios afectados, sino también de herramientas automatizadas de detección de intrusiones, antimalware o correladores de eventos. Todos ellos pueden ofrecer información de gran relevancia en las fases posteriores para lanzar acciones que puedan limitar los daños.
- **Clasificación de la brecha de seguridad:** Con toda la información aportada por los medios de detección y toda la información adicional recopilada es importante hacer una clasificación precisa del incidente de seguridad.
- Es especialmente **importante determinar si efectivamente se está ante una brecha de seguridad**, en cuyo caso es imprescindible evaluar el nivel de perjuicio que puede causar el incidente a los derechos y libertades de los afectados, determinando con el mayor grado de precisión posible el nivel de severidad de las consecuencias para los individuos. Es así mismo imprescindible determinar si se trata de una brecha de confidencialidad, integridad o disponibilidad, categoría y número de afectados, categoría y número de registros de datos, etc. Se han presentado más detalles sobre la clasificación de incidentes de seguridad en el apartado dedicado a clasificación de esta guía.
- **Investigación, comunicación y coordinación de los medios internos/externos implicados:** Es importante tener establecido de antemano cómo se va a tratar una incidencia de seguridad, quien se va a encargar de cada tarea y cómo se escalan a los equipos internos o externos adecuados. En ocasiones los medios para dar respuesta al incidente serán mayoritariamente externos (es el caso de pequeña y mediana empresa), pero en otros casos los medios serán en su mayoría internos. En cualquier caso la comunicación y coordinación entre equipos debe ser fluida y eficiente.
- **Puesta en marcha del plan de respuesta:** Especialmente de las primeras medidas de contención, tratando de limitar en lo posible los daños causados por el incidente. Por ejemplo, si un ordenador está infectado deberá ser desconectado de la red corporativa inmediatamente, o si una información ha sido difundida erróneamente a través de internet, deberá ser retirada. Estas medidas también proporcionan tiempo para poder desarrollar una solución adecuada sin el factor tiempo.
- **Puesta en marcha del proceso de notificación**, empezando por una valoración de notificación temprana a la autoridad de control competente, a afectados y en caso necesario a fuerzas de seguridad.

- **Estudio y activación de las posibles medidas a adoptar** para contener, mitigar o eliminar los daños que pudieran sufrir los afectados, esto es, un Plan de Contingencia elaborado previamente en la fase de preparación.

7.3 Proceso de respuesta

Durante el proceso de respuesta, en una primera fase se intenta contener el incidente, tras lo cual se erradica la situación generada por el mismo y se termina con las acciones de recuperación oportunas.



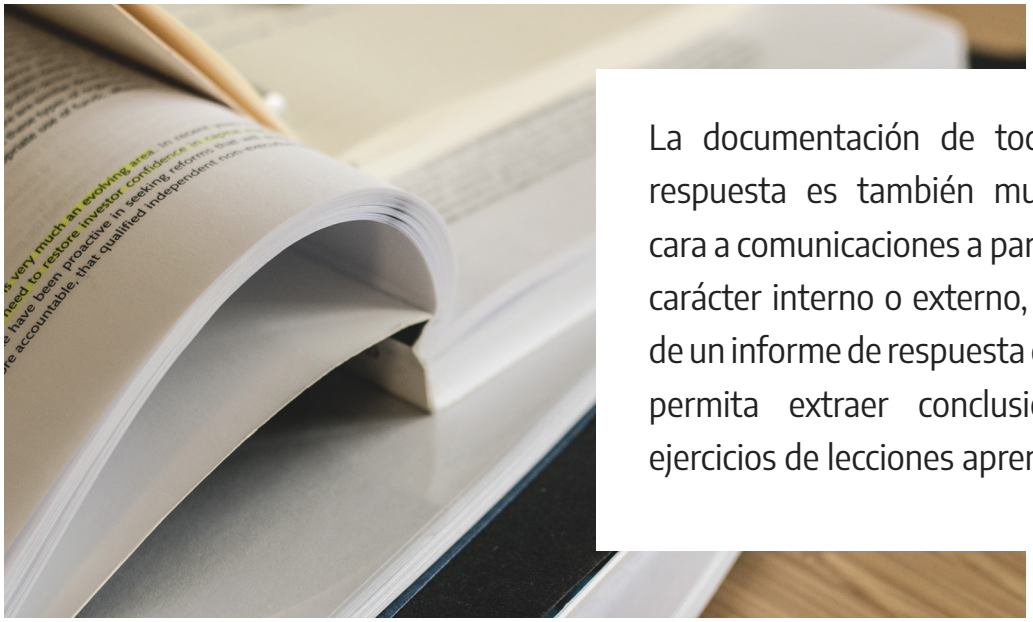
Estas fases no están perfectamente diferenciadas y es habitual que haya cierto solapamiento entre ellas.

Cuando se ha conseguido contener el incidente, la erradicación puede ser necesaria para solventar determinados efectos del incidente de seguridad, como por ejemplo, eliminar un malware o desactivar de cuentas de usuario vulneradas. También sirve para identificar y mitigar todas las vulnerabilidades que hubiesen sido explotadas.

Por último, la fase de recuperación tiene como objetivo el restablecimiento del servicio en su totalidad, confirmando su funcionamiento normal y evitando en la medida de lo posible que sucedan nuevos incidentes basados en la misma causa.

Esto puede implicar la adopción no solo de medidas activas, sino también implementando controles periódicos y eficaces que permitan el seguimiento pormenorizado de los procesos de mayor riesgo.

Durante todo el ciclo de vida de procedimiento de gestión de la brecha de seguridad, y en especial en el proceso de respuesta, debe tenerse en cuenta la recolección y custodia de evidencias que permitan disponer de información presentable ante terceros.



La documentación de todo el proceso de respuesta es también muy importante de cara a comunicaciones a partes interesadas de carácter interno o externo, y a la elaboración de un informe de respuesta que tras su análisis permita extraer conclusiones y elaborar ejercicios de lecciones aprendidas.

En el apartado dedicado al proceso de respuesta de esta guía se pueden consultar más detalles al respecto.

7.4 Proceso de notificación

Independientemente de las notificaciones internas que se deban producir y gestionar para gestionar un incidente de seguridad, el RGPD establece que en caso de brecha de la seguridad de los datos personales, el responsable del tratamiento la notificará a la autoridad de control competente sin dilación indebida y, de ser posible, a más tardar 72 horas después de que haya tenido constancia de ella, a menos que sea improbable que dicha brecha de la seguridad constituya un riesgo para los derechos y las libertades de las personas físicas.

El RGPD también establece los casos en los que una brecha de seguridad se debe comunicar al afectado, en concreto cuando sea probable que la brecha de la seguridad de los datos personales entrañe un alto riesgo para los derechos y libertades de las personas físicas.

Tanto la notificación a la autoridad de control competente como la comunicación al afectado son obligaciones del responsable del tratamiento, aunque puede delegar la ejecución de las mismas en otras figuras.

En el caso de grandes empresas con estructuras organizativas complejas, sería conveniente formalizar un **procedimiento de notificación**, en el que se establezca el proceso a seguir para comunicar las brechas de seguridad de los datos personales a las autoridades de control y, en casos graves, a los afectados. Dicho procedimiento podría incluir detalles sobre cómo deben escalarse las notificaciones internamente.

7.5 Seguimiento y cierre

El plan de actuación para la gestión de brechas de seguridad requiere de determinadas tareas de seguimiento y cierre. Entre dichas tareas cabe destacar las que se enumeran a continuación:

1. Valoración de contratación de un análisis forense digital experto.

En determinados casos está justificado que la investigación sea conducida por un experto forense que tendrá como misión fundamental el análisis de los hechos y la recopilación de evidencias precisas. Su intervención puede resultar de gran utilidad para evidenciar lo sucedido tanto en vía administrativa como en sede judicial.

2. Valoración de adopción de medidas procesales.

Se valorará la oportunidad de iniciar un procedimiento judicial, a los fines de imputación de hechos y de reparación de daño. Pero también deberán analizarse los riesgos y las consecuencias que se pudieran derivar de los mismos, teniendo en cuenta que, en ocasiones, el daño derivado del proceso judicial podría incrementar el perjuicio en lugar de reducirlo.
Una brecha de seguridad puede ocasionar daños materiales muy importantes, pero una mala gestión de los mismos, puede ocasionar consecuencias reputacionales todavía más dañinas. En este sentido, se debe tener en cuenta la repercusión que un incidente de seguridad puede tener en el ramo de la actividad empresarial, sobre clientes, proveedores, accionistas, empleados, y, en definitiva, sobre la sociedad en general debiendo preverse los efectos de la difusión de la brecha.

3. Realización de un informe final sobre la brecha de seguridad.

La gestión diligente del incidente exige una correcta organización de la documentación recopilada en relación al suceso. El responsable del tratamiento o en quien tenga delegadas dichas funciones, que podría ser el DPD, comprobará que las medidas correctoras adoptadas son adecuadas para la resolución de la brecha y para la minimización del riesgo en caso de que se produzca otra de similares

características, que ha concluido el proceso de comunicación a la Autoridad de Control y, en su caso, a los posibles afectados.
A fin de cerrar la brecha de seguridad se elaborará un Informe final sobre la trazabilidad del suceso y su análisis valorativo, en particular, en cuanto al impacto final.
Dicho Informe final recopilará toda la información y documentación relativa a la brecha de manera que se facilite el estudio y revisión por terceros, incluida la dirección de la empresa.
Los informes sobre las brechas y su impacto son una valiosa fuente de información con la que debe alimentarse el análisis y la gestión de riesgos. El uso de esta información servirá para prevenir la reiteración del impacto de una brecha.

4. Cierre de la brecha de seguridad

Una vez las acciones derivadas de los procesos del plan de actuación han concluido y se han alcanzado los objetivos, se procederá al cierre de la brecha de seguridad.

A modo de resumen, a lo largo de todo el ciclo de gestión de la brecha de seguridad quedarán cubiertos los siguientes aspectos:

- En primer lugar, deben hallarse identificados los responsables a quienes les corresponderá directamente reaccionar ante la brecha de seguridad que afectará al Responsable del tratamiento, a los Corresponsables del tratamiento y al Encargado del tratamiento, requiriéndose la debida coordinación previa entre ellos y el DPD (tanto del responsable como del encargado) y previsión de la comunicación a la Autoridad de Control.
- Desde una perspectiva temporal hay que tener en cuenta que, con anterioridad al surgimiento de una brecha de seguridad, se habrá de contar con un Análisis de Riesgos o Evaluación de Impacto[10] y la consecuente elaboración de un Plan de Contingencia acorde al riesgo que deberá incorporar, tanto medidas técnicas, como organizativas. Estas dos acciones estarán encuadradas en una fase de preparación previa.
- En el caso de que se produzca una brecha de seguridad será preciso efectuar una valoración del potencial daño a los datos de los afectados; el volumen de datos afectados y el nivel de datos personales afectados.
- Desde un punto de vista material debe distinguirse entre brecha de seguridad e incidente de seguridad. Incidente de seguridad es el término genérico y brecha de seguridad se refiere al incidente que afecta a datos personales.
- Una diferencia de tratamiento importante es que el incidente de seguridad que no suponga una brecha de seguridad no requiere comunicación a la autoridad de control mientras que éstas podrán, y deberán, bajo ciertas circunstancias, ser objeto de comunicación en el plazo de 72 horas a la autoridad de control bajo pena de sanción económica.

[10] En los casos exigidos por RGPD.

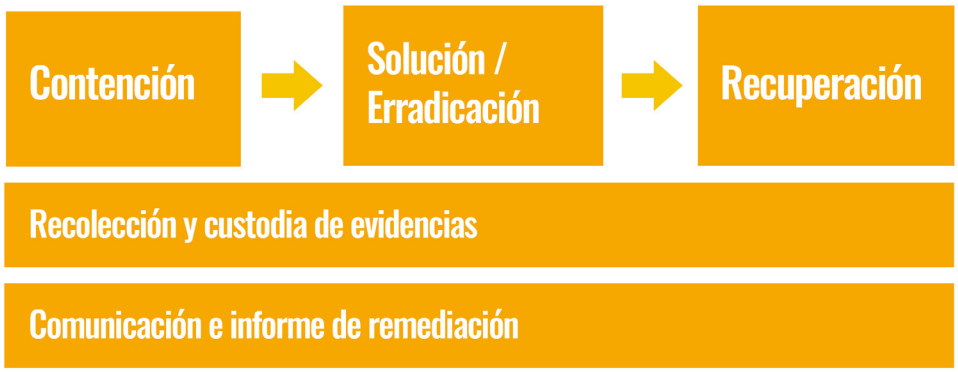
- Ante una brecha de seguridad se deberá proceder de inmediato a recopilar toda la información relevante, elaborar los análisis pertinentes y poner en marcha las medidas de mitigación adecuadas, así como valorar la posible comunicación a terceros, incluyendo en este grupo tanto a afectados como a las autoridades y agentes de la autoridad que deban conocer, investigar o juzgar lo acontecido.
- Se pondrá en marcha el protocolo de actuación previsto de conformidad con la clasificación de la brecha de seguridad detectada, que podrá ser: brecha de confidencialidad; de integridad o de disponibilidad.
- El propio protocolo de actuación estará sujeto a evaluación periódica a efectos de garantizar su eficacia frente a la concreta entidad de la brecha de seguridad producida e igualmente se ponderará el riesgo que suponga con la finalidad de establecer una graduación del mismo al objeto de ajustar la reacción oportuna.
- Asimismo, se recomienda efectuar una adecuada clasificación y tipología de afectados en atención a la diversa sensibilidad de los datos que se pueden ver afectados.
- Se recomienda especialmente que la investigación sea llevada a cabo por un experto en la materia que será quien pueda probar los hechos y asegurar la conservación de las evidencias.
- Ulteriormente se producirá un juicio de oportunidad sobre la incoación de acciones judiciales valorando las exigencias y presupuestos de cada orden jurisdiccional, así como la repercusión que generará.
- Por último, se recomienda concluir mediante un informe final que detalle la trazabilidad del suceso, vicisitudes, análisis valorativo y particularmente el impacto final.

8. Respuesta a brechas de seguridad

Aunque anteriormente se ha realizado un desarrollo continuo de todas las fases incluidas en el plan de actuación, en este apartado se va a realizar un desarrollo meticuloso de lo que implica el proceso de respuesta en el caso ya confirmado de brecha de seguridad con incidencia en los datos personales.

La gran mayoría de las acciones descritas en este apartado correrán a cargo de un equipo de respuesta a incidentes dentro del servicio de informática o del equipo de seguridad informática correspondiente, que podrá formar parte de la empresa o estar completamente externalizado.

Durante el proceso de respuesta, en una primera fase se intenta contener el incidente, tras lo cual se erradica la situación generada por el incidente y se termina con las acciones de recuperación oportunas. Estas fases no están perfectamente diferenciadas y es habitual que haya cierto solapamiento entre las mismas.



Fases de Respuesta de Incidentes

8.1 Contención del incidente

La contención del incidente proporciona tiempo para desarrollar una estrategia de respuesta a medida. Una parte esencial de la contención es la toma de decisiones rápidas como puede ser cerrar un sistema, aislarlo de la red, deshabilitar ciertas funciones, etc. Estas decisiones son más fáciles de tomar si existen estrategias predeterminadas que establezcan cómo se debe gestionar cada tipo de incidente.

Por ejemplo, en el equipo de un usuario de una pequeña empresa se detectan archivos con caracteres extraños y comportamientos anómalos del equipo, una primera medida de contención podría ser rápidamente desconectar el cable de red y/o desconectarlo de la red wifi. Si se han establecido los

procedimientos apropiados, esta medida la puede tomar el propio usuario de forma rápida antes incluso de confirmar si se trata de un incidente de seguridad.

Es una buena práctica que las empresas desarrollen políticas de actuación para la gestión de los incidentes en general y de los incidentes vinculados con datos personales en particular. La complejidad de estas políticas irá vinculada a las características, volumen y operaciones de tratamiento que se realicen sobre los datos y será conveniente llevar a cabo procesos de verificación que permitan validar el funcionamiento de las mismas.

Las medidas de contención podrán ser inmediatas o de aplicación progresiva en función del desarrollo de la resolución del incidente. Es conveniente determinar las medidas a implantar estableciendo un orden de prioridad, los responsables asignados, tiempos estimados y los efectos esperados.
Algunas medidas de contención serán sencillas y las podrá iniciar el usuario, sin embargo otras medidas son más complejas y deben estar en manos de personal especializado que se encargue de la seguridad informática de la empresa.

A continuación se enumeran someramente algunas de las medidas de contención que podrían ser de aplicación en función de cada caso:

- Si es posible, impedir el acceso al origen de la divulgación: dominios, puertos, servidores, la fuente o los destinatarios de la divulgación. Dependiendo del vector de ataque, impedir el acceso al origen: dominios, conexiones, equipos informáticos o conexiones remotas, puertos, parches, actualización del software de detección (antivirus, IDS, etc.) bloqueo de tráfico, deshabilitar dispositivos, servidores, etc.
- Suspender las credenciales lógicas y físicas con acceso a información privilegiada. Cambiar todas las contraseñas de usuarios privilegiados o hacer que los usuarios lo hagan de manera segura.
- Hacer una copia del sistema (clonado), hacer una copia bit a bit del disco duro que contiene el sistema, y luego analizar la copia utilizando herramientas forenses.
- Aislar el sistema utilizado para revelar los datos con el fin de realizar un análisis forense más tarde.
- Si los datos han sido enviados a servidores públicos, solicitar al propietario (o webmaster) que elimine los datos divulgados.
- Si no es posible eliminar los datos divulgados, proporcionar un análisis completo al departamento correspondiente (Legal, Compliance, RRHH, etc.) o a quien ejerza dichas funciones en la empresa.
- Vigilar la difusión de los documentos/datos filtrados en los diferentes sitios web y redes sociales (FB, Twitter, etc.) así como los comentarios y reacciones de los usuarios de Internet.

8.2 Solución / Erradicación

Tras la contención de un incidente, la erradicación puede ser necesaria para solventar determinados efectos del incidente de seguridad, como por ejemplo, eliminar un malware o desactivar de cuentas de usuario vulneradas.

También sirve para identificar y mitigar todas las vulnerabilidades que hubiesen sido explotadas.
Las tareas de erradicación deben contar con una descripción de alto nivel de las tareas, así como de la responsabilidad (equipo interno o externo e identificación del responsable de equipo) de cada una de ellas.

Algunos ejemplos de tareas de erradicación podrían ser las que se enumeran a continuación:

- Definir el proceso de desinfección, basado en firmas, herramientas, nuevas versiones/revisiones de software, etc. y probarlo. Asegurar que el proceso de desinfección funciona adecuadamente sin dañar servicios.
- Comprobar la integridad de todos los datos almacenados en el sistema, mediante un sistema de hashes por ejemplo, que permita garantizar que los ficheros no han sido modificados, especial atención debe ser tenida con relación a los ficheros ejecutables.
- Revisar la correcta planificación y actualización de los motores y firmas de antivirus.
- Análisis con antivirus de todo el sistema, los discos duros y la memoria.
- Restaurar conexiones y privilegios paulatinamente. Especial acceso restringido paulatino de máquinas remotas o no gestionadas.

Con objeto de planificar la respuesta al incidente deberá fijarse un plazo para la implementación de las tareas de erradicación.

En casos complejos que incluyan múltiples tareas y equipos de ejecución, deberá existir coordinación entre los distintos equipos.

Tras la aplicación de las medidas se debe verificar el correcto funcionamiento de éstas, confirmando su idoneidad para la erradicación del incidente. De ser así, se dará por terminada esta fase.

Se debe considerar también si las medidas aplicadas son de carácter temporal o si forman parte de una solución definitiva, y el sistema y/o la información afectada ha vuelto de nuevo de modo efectivo a su estado original.

Además debe asegurarse que la misma vulnerabilidad no podrá ser explotada en el futuro, o dicho en otros términos, se deberán de tomar medidas que eviten o eliminen la posibilidad de que un incidente vuelva a producirse. En este sentido será necesario alimentar el plan de riesgos de la entidad afectada revisando si el mapa de riesgos contemplaba la amenaza que ha dio lugar a la brecha de seguridad y, en caso afirmativo, reevaluar las medidas de salvaguarda asociadas a fin de garantizar su efectividad, para ello será necesario contar con la persona designada como responsable de riesgos de la entidad en caso que hubiera sido designada, pero antes será necesario realizar las medidas de recuperación que se describen a continuación.

8.3 Recuperación

Solucionada la brecha de seguridad y verificada la eficacia de las medidas adoptadas, se entra en la fase de recuperación, que tiene como objetivo el restablecimiento del servicio en su totalidad, confirmando su funcionamiento normal y evitando en la medida de lo posible que sucedan nuevos incidentes basados en la misma causa.

Esto puede implicar la adopción no solo de medidas activas, sino también implementando controles periódicos y eficaces que permitan el seguimiento pormenorizado de los procesos de mayor riesgo.

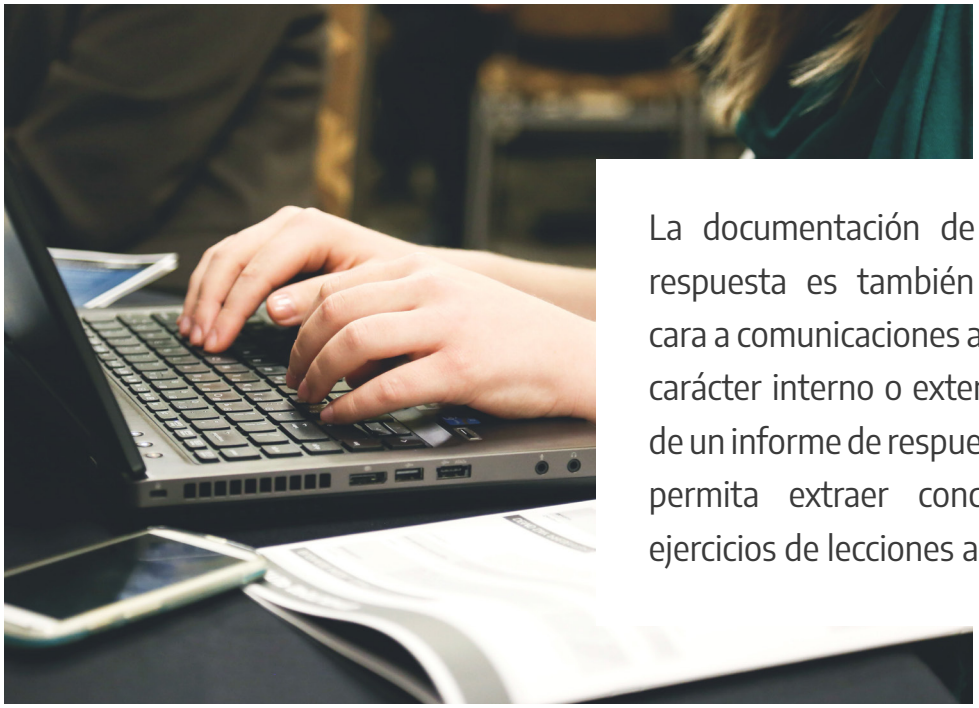
Identificación y análisis de soluciones (corto, medio, plazo): Se identificarán las distintas soluciones dirigidas a evitar nuevos incidentes de seguridad basados en la misma causa, así como a reducir el riesgo de los mismos. Debe hacerse contraste con las medidas adoptadas para solventar el incidente en cuestión y garantizar un análisis pormenorizado de soluciones.

Selección estrategia: Teniendo en cuenta el riesgo que quiera asumir la entidad así como la eficiencia y costes de las distintas opciones planteadas, se seleccionará la estrategia que deberá seguirse a futuro.

Implementación (suspensión medidas de contención excepcionales, implementación de medidas preventivas eviten incidente): Implementación de las medidas en base a la estrategia adoptada teniendo en cuenta tanto el proyecto de continuidad de negocio de la entidad como la criticidad y el propio riesgo intrínseco en los activos que hayan sido afectados por el incidente, sin olvidar los procesos afectados y los datos que se tratan en los mismos.

Verificación de recuperación e implementación de medidas: Se garantizará no solo el restablecimiento a la situación previa al incidente, sino que se revisará el análisis de riesgos y se recogerá la implementación en la entidad de controles adicionales y periódicos para evitar futuros incidentes similares.

8.4 Recolección y custodia de evidencias



La documentación de todo el proceso de respuesta es también muy importante de cara a comunicaciones a partes interesadas de carácter interno o externo, y a la elaboración de un informe de respuesta que tras su análisis permita extraer conclusiones y elaborar ejercicios de lecciones aprendidas.

En este proceso se van a tomar las acciones necesarias para contener y revertir el impacto que haya podido tener una brecha de seguridad. Estas acciones pueden incurrir en la modificación de evidencias, lo que puede imposibilitar el uso de la información registrada por los sistemas involucrados de cara a la presentación de esta información frente a terceros, y en especial su uso como prueba en procedimientos judiciales y administrativos.

Para tratar de garantizar que la información generada por los sistemas involucrados en una brecha de seguridad cumpla los objetivos de cumplimiento de la organización, de cara a que dichos registros puedan ser utilizados frente a terceros y/o en litigios, es necesario tener en consideración dos aspectos para cada brecha de seguridad.

- Por una parte definir la necesidad de uso de la información por parte de la organización en la propia fase de detección de la brecha de seguridad de cara a la recolección de evidencias.
- Por otra, establecer la cadena de custodia adecuada que satisfaga el uso de la información definido por la organización.

8.5 Comunicación/Informe de resolución (Interna/Externa)

En general, todo el proceso de respuesta al incidente debe quedar debidamente documentado, incluyendo las conclusiones de los técnicos y responsables del equipo para extraer lecciones aprendidas y ser incluidas en un informe de resolución.

Se recomienda disponer de la siguiente información para poder elaborar el citado informe:

- Descripción objetiva del incidente.
- Controles existentes en el momento del incidente.
- Enumeración de medidas efectivas de respuesta.
- Declaración de si a igual casuística el incidente se repetiría.
- Medidas de detección aplicadas para identificar nuevos casos.
- Registro de comunicaciones durante la respuesta.

Comunicación: dirección y partes interesadas.

La comunicación es fundamental durante todo el ciclo de vida del proceso de respuesta, y debe hacerse de una manera continua de modo que la dirección y responsables de seguridad tengan una visibilidad clara tanto del incidente como de las acciones tomadas para afrontarlo. Es especialmente importante cuando el incidente trasciende el perímetro de la organización y toma relevancia pública, ya que muy posiblemente los directivos serán preguntados por las acciones que se están llevando a cabo y posibles consecuencias.

Las tareas de comunicación no buscan la aprobación de la gerencia ni su toma de decisiones, simplemente se trata de un cuaderno de bitácora lo suficientemente actualizado para informar a la dirección y otras partes interesadas, de forma que también puedan cumplir con sus propias obligaciones.

Elaboración del informe de resolución.

Como se ha indicado anteriormente, la elaboración del informe de resolución tiene como objetivo servir de base para realizar ejercicios futuros de lecciones aprendidas. Con un carácter meramente interno, este informe debe facilitar a todos los equipos involucrados en la respuesta al incidente, el entendimiento sobre el porqué de las acciones tomadas así como las acciones marcadas para seguimiento en el corto, medio y largo plazo. También serán tenidos en cuenta los cambios necesarios que deberían ser incluidos en el análisis de riesgos de la organización.

En la medida de lo posible este informe debe incluir detalles técnicos sobre las diferentes acciones llevadas a cabo. Este informe se nutrirá en gran medida de la documentación elaborada durante el proceso de respuesta.

El informe de resolución se debe presentar en forma de línea temporal, de modo que facilite el seguimiento de las diferentes acciones, y debería incluir al menos información relativa a los siguientes apartados:

- Alcance e impacto del incidente.
- Controles preventivos existentes.
- Acciones de respuesta tomadas sobre las diferentes alternativas consideradas para la resolución de la brecha.
- Acciones tomadas para la prevención de futuras brechas.
- Impacto en la resolución del incidente de las acciones de respuesta tomadas.
- Acciones definidas para el seguimiento.

9. Notificación de brechas de seguridad

Aunque anteriormente se ha realizado un desarrollo continuo de todas las fases incluidas en el plan de actuación, en este apartado se realiza un desarrollo meticuloso de lo que implica el proceso de notificación de la brecha de seguridad en el caso ya confirmado de incidencia en los datos personales.

Según el artículo 33 del RGPD, en caso de brecha de la seguridad que afecte a los datos personales, el responsable del tratamiento la notificará a la autoridad de control competente sin dilación indebida y, de ser posible, a más tardar 72 horas después de que haya tenido constancia de ella, a menos que sea improbable que dicha brecha de la seguridad constituya un riesgo para los derechos y las libertades de las personas físicas.

Así mismo, el artículo 34 del RGPD establece que cuando sea probable que la brecha de seguridad de los datos personales entrañe un alto riesgo para los derechos y libertades de las personas físicas, el responsable del tratamiento la comunicará a los afectados sin dilación indebida.

Estas nuevas obligaciones para el responsable vienen a ampliar las previamente establecidas para operadores de servicios de comunicaciones electrónicas[11] y prestadores de servicios de confianza[12].

En el caso de grandes empresas, si previamente no estaba previsto dentro del proceso de gestión de incidentes, es conveniente formalizar un procedimiento de notificación, en el que se establezca el proceso a seguir para comunicar las brechas de seguridad de los datos personales a las autoridades de control y, en casos graves, a los afectados. Dicho procedimiento, que ha de ser conocido entre quienes deban utilizarlo y/o tener conocimiento del mismo, debe describir la manera en la que se comunica, e identificar al representante dentro de la organización que actuará como punto único a efectos de notificación ante la autoridad de control. Esta figura podrá ser el Delegado de Protección de Datos en el caso de que lo hubiera.

En caso de empresas pequeñas o con tratamientos sencillos, la persona encargada de la notificación podrá ser el propio responsable del tratamiento o a quien éste designe para ser el punto de contacto con la autoridad de control.

> La existencia de una política de notificaciones de brechas de seguridad se debe tener en cuenta con el fin de disponer de un criterio común a todos los tratamientos de datos personales que consten en el registro de actividades de tratamiento de una organización.

[11] Artículos 41 y 44 de la **Ley 9/2014 General de Telecomunicaciones**

[12] Artículo 19.2 del **Reglamento 910/2014 del Parlamento Europeo y del Consejo**

A modo orientativo se propone en el Anexo III de esta guía un posible modelo que puede ser utilizado como referencia en la toma de decisiones tanto para la notificación a la Autoridad de Control como a los propios interesados. En cada caso se debe de valorar los umbrales bajo los cuales el responsable procederá a la notificación.

9.1 Proceso de notificación a la autoridad de control

Como se ha comentado anteriormente, tan pronto como el responsable del tratamiento tenga conocimiento de que se ha producido una brecha de la seguridad de los datos personales debe, sin dilación y, a más tardar en las 72 horas siguientes a tener constancia, efectuar la correspondiente notificación a la Autoridad de Control. Se considera que se tiene constancia de una brecha de seguridad cuando hay una certeza de que se ha producido y se tiene conocimiento suficiente de su naturaleza y alcance.

El criterio a tener en cuenta para determinar si un incidente ha producido "una brecha de la seguridad de los datos personales" se recoge en el propio RGPD, e incluye "todas aquellas brechas de la seguridad que ocasionen la destrucción, pérdida o alteración accidental o ilícita de datos personales transmitidos, conservados o tratados de otra forma, o la comunicación o acceso no autorizados a dichos datos."

Esta comunicación se realizará con el modelo de comunicación descrito en el Anexo II, y deberá contener la siguiente información:

Datos identificativos y de contacto de:

- Entidad / Responsable del tratamiento
- Delegado de Protección de Datos (si está designado) o persona de contacto.
- Indicación de si se trata de una notificación completa o parcial. En caso de tratarse de una notificación parcial indicar si se trata de una primera notificación o una notificación complementaria.

Información sobre la brecha de seguridad de datos personales:

- Fecha y hora en la que se detecta.
- Fecha y hora en la que se produce el incidente y su duración.
- Circunstancias en que se haya producido la brecha de seguridad de datos personales (por ejemplo, pérdida, robo, copia, etc.)

- Naturaleza y contenido de los datos personales en cuestión.
- Resumen del incidente que ha causado la brecha de seguridad de datos personales (con indicación de la ubicación física y del soporte de almacenamiento).
- Posibles consecuencias y efectos negativos en los afectados.
- Medidas técnicas y organizativas que se hayan adoptado por parte del responsable del tratamiento según el apartado 33.2d) del RGPD.
- Categoría de los datos afectados y número de registros afectados.
- Categoría y número de individuos afectados.
- Posibles cuestiones de carácter transfronterizo, indicando la posible necesidad de notificar a otras autoridades de control.

Si en el momento de la notificación, no fuese posible facilitar toda la información, podrá facilitarse posteriormente, de manera gradual en distintas fases. La primera notificación se realizará en las primeras 72h, y al menos se realizará una comunicación final o de cierre cuando se disponga de toda la información relativa al incidente.

Cuando el responsable realice la primera notificación deberá informar si proporcionará más información a posteriori. También podrá aportar información adicional mediante comunicaciones intermedias a la autoridad de control bajo petición de esta, o cuando el responsable considere adecuado actualizar la situación de la misma.

Cuando la notificación inicial no sea posible en el plazo de 72 horas, la notificación deberá realizarse igualmente, y en ella deberán constar y justificarse los motivos de la dilación.
Las notificaciones deben ser sean claras, concisas y que incluyan la información necesaria para que puedan ser analizadas adecuadamente.

Es necesario que cualquier brecha de la seguridad de los datos personales, hechos relacionados, efectos y las medidas correctivas adoptadas así como la propia notificación, se registre y justifique documentalmente por el responsable, de modo que esta documentación permita a la autoridad de control verificar el cumplimiento de la obligación de notificación en todo su contenido.

9.2 Identificación de la autoridad de control

Cuando un incidente pueda afectar a los datos de personas en más de un Estado miembro, el responsable debe realizar una evaluación sobre cuál es la autoridad principal a la que deberá realizar la notificación y, en caso de duda, se debe como mínimo, notificar a la autoridad de control local donde la brecha ha tenido lugar. Actuará como autoridad de control principal, la del establecimiento principal o la del único establecimiento del responsable.

Los criterios para identificar el establecimiento principal son:

- Lugar donde tenga la sede principal el responsable.
- Lugar donde se toman las decisiones sobre fines y medios.

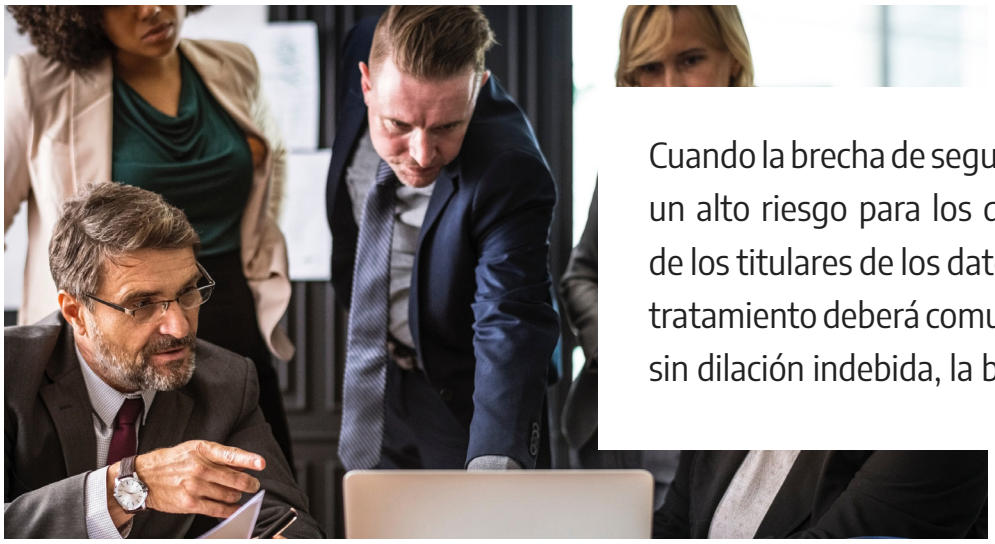
En el siguiente enlace publicado por el WP29, figura la información de contacto para cada autoridad de control: http://ec.europa.eu/newsroom/article29/news-overview.cfm

9.2.1 Canal de notificación a la AEPD

La notificación a la AEPD se realizará a través del formulario destinado a tal efecto publicado en la sede electrónica de la agencia, en https://sedeagpd.gob.es/sede-electronica-web/, cuyo modelo se incluye en el Anexo II.

A cada notificación se le asignará una referencia que el responsable deberá mantener e incluir en las sucesivas comunicaciones relacionadas si las hubiera, con el fin de proporcionar un seguimiento completo del incidente.

9.2.2 Proceso de comunicación al afectado



Cuando la brecha de seguridad pueda entrañar un alto riesgo para los derechos y libertades de los titulares de los datos, el responsable del tratamiento deberá comunicar a los afectados, sin dilación indebida, la brecha de seguridad.

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

- Cuáles son las obligaciones legales y contractuales.
- Riesgos que comporta la pérdida de los datos: daños físicos, daños reputacionales, etc.
- Existe un riesgo razonable de suplantación de identidad o fraude (en función del tipo de información que se ha visto afectada y teniendo en cuenta si la información estaba seudonimizada o cifrada).
- Hasta qué punto la persona afectada puede evitar o mitigar posibles daños posteriores.

Si después del análisis correspondiente es necesario realizar la notificación pero se prevé que la comunicación a los afectados puede comprometer el resultado de una investigación en curso, la comunicación podría posponerse siempre bajo la supervisión de la autoridad de control. La comunicación a los afectados se realizará a la mayor brevedad posible, en un lenguaje claro y sencillo y siempre en estrecha cooperación con la autoridad de control y las autoridades policiales, de acuerdo con sus orientaciones.

Esta comunicación, debería contener como mínimo:

- Datos de contacto del Delegado de Protección de Datos, o en su caso, del punto de contacto en el que pueda obtenerse más información.
- Descripción general del incidente y momento en que se ha producido.
- Las posibles consecuencias de la brecha de la seguridad de los datos personales.
- Descripción de los datos e información personal afectados.
- Resumen de las medidas implantadas hasta el momento para controlar los posibles daños.
- Otras informaciones útiles a los afectados para proteger sus datos o prevenir posibles daños.

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

La notificación indirecta, a través de avisos públicos en sitios web como blogs corporativos, o comunicados de prensa, se utilizará cuando para la notificación directa los costos sean excesivos o cuando no sea posible contactar con las personas afectadas (por ejemplo porque se desconocen, o los datos de contacto no están actualizados).

9.3 Excepciones a la notificación / comunicación

No será necesaria la notificación a la Autoridad de Control cuando el responsable pueda demostrar, de forma fehaciente, que la brecha de la seguridad de los datos personales no entraña un riesgo para los derechos y las libertades de las personas físicas.

Por ejemplo, si los datos ya se encontraban públicamente disponibles y su revelación no entraña ningún riesgo hacia el titular de los datos.

Asimismo no será necesaria la comunicación a los afectados cuando:

- El responsable ha tomado medidas técnicas y organizativas adecuadas, como que los datos no sean inteligibles para personas o máquinas no autorizadas con anterioridad a la brecha de seguridad de datos personales (mediante el uso de: cifrados de datos de última generación, minimización, disociación de datos, acceso a entornos de prueba sin datos reales, etc.).
- Por ejemplo, es probable que no sea necesaria la notificación si se pierde un dispositivo móvil y los datos personales que contiene están cifrados. Sin embargo, sí que es posible que se requiera de notificación si esta fuera la única copia de los datos personales, o por ejemplo, la clave de cifrado en posesión del responsable estuviera comprometida.
- El responsable ha tomado con posterioridad a la brecha de seguridad de datos personales las medidas de protección que mitiguen total o parcialmente el posible impacto para los afectados y garanticen que ya no hay posibilidad de que el alto riesgo se materialice. Por ejemplo, mediante la identificación y puesta en marcha inmediatamente de las medidas contra la persona que ha accedido a los datos personales antes de que pudieran hacer algo con ellos.
- Cuando la notificación a los afectados suponga un esfuerzo desproporcionado a nivel técnico y organizativo. Por ejemplo, cuando los detalles de contacto se hayan perdido como resultado de la brecha, o aquellos casos en los que se tenga que desarrollar un nuevo sistema o proceso para realizar la notificación, o se requiera la dedicación excesiva de

recursos internos para la identificación de los afectados. Ante esta situación, se realizará la notificación de manera pública a través de los canales establecidos por el responsable.

Si el responsable todavía no ha comunicado al afectado la brecha de la seguridad de los datos personales considerando el alto riesgo potencial, la autoridad de control podrá exigirle:

- que lo comunique,
- podrá decidir que se cumpla alguna de las condiciones mencionadas para que la comunicación a los afectados no sea obligada.

Anexo I. Marco Normativo

Europeo:

- REGLAMENTO (UE) 2016/679 DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos) - Artículos 33 y 34.
- Directiva (UE) 2016/1148 DEL PARLAMENTO EUROPEO Y DEL CONSEJO, de 6 de julio de 2016, relativa a las medidas destinadas a garantizar un elevado nivel común de seguridad de las redes y sistemas de información en la Unión (Directiva NIS) - Artículos 14, 16 y 20.
- REGLAMENTO (UE) n ° 910/2014 del Parlamento Europeo y del Consejo, de 23 de julio de 2014, relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior y por la que se deroga la Directiva 1999/93/CE (eIDAS) - Artículos 10, 17.6 y 19.3 y Considerandos 38 y 39.
- Directiva (UE) 2008/114 DEL CONSEJO, de 8 de diciembre, sobre la identificación y designación de Infraestructuras Críticas Europeas y la evaluación de la necesidad de mejorar su protección.

Nacional:

- Código de Protección de Datos Personales.
- Proyecto de Ley Orgánica de Protección de Datos - Disposición Adicional Decimosegunda.
- Real Decreto 704/2011, de 20 de mayo, por el que se aprueba el Reglamento de Protección de las Infraestructuras Críticas.
- Ley 8/2011, de 28 de abril, por la que se establecen medidas para la protección de las infraestructuras críticas.
- Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica - Artículos 24, 36 y Disposición Adicional cuarta.

Sectorial:

- Ley General 9/2014, de 9 de mayo, de Telecomunicaciones - Artículos 41 y 44
- REGLAMENTO (UE) 611/2013 de la Comisión, de 24 de junio de 2013, relativo a las medidas aplicables a la notificación de casos de brecha de datos personales en el marco de la Directiva 2002/58/CE del Parlamento Europeo y del Consejo sobre la privacidad y las comunicaciones electrónicas.

- **Ley 34/2002**, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico, que regula la Gestión de incidentes de ciberseguridad que afecten a la red de Internet. Disposición adicional novena.

Guías y Estándares:

- Directrices sobre notificación de brechas de la seguridad de los datos personales, adoptadas el 3 de octubre de 2017 por el Grupo de Trabajo del Artículo 29 (WP29).
- Directrices sobre notificación de incidentes graves de conformidad con la Directiva (EU) 2015/2366 (PSD2), adoptadas el 27 de julio de 2017 por la Autoridad Bancaria Europea.
- UNE-EN ISO/IEC 27001:2017. Tecnología de la información. Técnicas de seguridad. Sistemas de Gestión de la Seguridad de la Información. Requisitos.
- UNE-EN ISO/IEC 27002:2017. Tecnología de la Información. Técnicas de seguridad. Código de prácticas para los controles de seguridad de la información
- ISO/IEC 29100:2011 Information technologi – Security Techniques – Privacy framework

Anexo II. Formulario de NOTIFICACIÓN DE INCIDENTES DE SEGURIDAD DE DATOS PERSONALES de acuerdo al artículo 33 del RGPD

AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS

FORMULARIO NOTIFICACIÓN BRECHAS DE SEGURIDAD

1. Datos de la notificación

Tipo de notificación: ○ Inicial, ○ Adicional, ○ Completa
Referencia notificación inicial:_____ Fecha notificación inicial:_____

2. Identificación del Delegado de Protección de Datos o persona de contacto

NIF/NIE: _____ Nombre:_____
Apellidos:_____ Cargo:_____
Dirección:_____ C.P.:_____
Provincia:_____ Localidad:_____
Teléfono(s):_____/_____ e-mail:_____

3. Identificación del responsable del tratamiento

Nombre de la Organización: _____
Tipo de Organización: ○ Privada, ○ Pública
CIF:_____ Dirección distinta del DPD o persona de contacto: ☐
Dirección:_____ C.P.:_____
Provincia:_____ Localidad:_____
Teléfono(s):_____/_____ e-mail:_____

4. Identifiación del encargado del tratamiento

¿Hay otra organización implicada en la brecha de seguridad? ☐
Nombre de la Organización: _____
Tipo de Organización: ○ Privada, ○ Pública
CIF:_____
Dirección:_____ C.P.:_____
Provincia:_____ Localidad:_____
Teléfono(s):_____/_____ e-mail:_____

5. Información temporal de la brecha

Fecha detección de la brecha: _____ ○ Exacta, ○ Estimada.
Medios de detección de la brecha:

_____
_____
_____

Justificación de notificación tardía (notificación pasadas 72h desde la detección):

_____
_____
_____

Fecha inicio de la brecha: _____ ○ Exacta, ○ Estimada.
¿Está resuelta la brecha? ☐ Fecha de resolución: _____ ○ Exacta, ○ Estimada.

AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS

FORMULARIO NOTIFICACIÓN
BRECHAS DE SEGURIDAD

6. Sobre la brecha

Resumen del incidente:

Tipología:

- ☐ Brecha de confidencialidad (acceso no autorizado)
- ☐ Brecha de integridad (modificación no autorizada)
- ☐ Brecha de disponibilidad (desaparición o pérdida)

Medio por el que se ha materializado la brecha:

- ☐ Datos personales residuales en dispositivos obsoletos.
- ☐ Documentación perdida, robada o depositada en localización insegura.
- ☐ Eliminación incorrecta de datos personales en formato papel.
- ☐ Hacking.
- ☐ Malware (e.j. ransomware).
- ☐ Phishing.
- ☐ Correo perdido o abierto.
- ☐ Dispositivo perdido o robado.
- ☐ Publicación no intencionada.
- ☐ Datos personales mostrados al individuo incorrecto.
- ☐ Datos personales enviados por error.
- ☐ Revelación verbal no autorizada de datos personales.
- ☐ Otros:

Contexto:

- ○ Interna (acción no intencionada)
- ○ Externa(acción no intencionada)
- ○ Otros:
- ○ Interna (acción intencionada)
- ○ Externa (acción intencionada)

Medidas preventivas aplicadas antes de la brecha:

7. Sobre los datos afectados

Categoría de datos afectados:

- ☐ Datos básicos
- ☐ Credenciales de acceso o identificación
- ☐ Datos de contacto
- ☐ DNI, NIE y/o Pasaporte
- ☐ Datos económicos o financieros
- ☐ Datos de localización
- ☐ Sobre condenas e infracciones penales
- ☐ Otros:

AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS

FORMULARIO NOTIFICACIÓN BRECHAS DE SEGURIDAD

Categorías especiales de datos:

☐ Sobre el orígen racial ☐ Sobre la opinión política
☐ Sobre la religión o creencia ☐ Sobre la afiliación sindical ☐ Sobre la vida sexual
☐ De salud ☐ Genéticos ☐ Biométricos
☐ Desconocidos ☐ Otros: _____

Número aproximado de registros de datos personales afectados:

8. Sobre los sujetos afectados

Perfil de los sujetos afectados:

☐ Clientes ☐ Usuarios ☐ Empleados ☐ Suscriptores
☐ Estudiantes ☐ Pacientes ☐ Otros: _____

Número aproximado de personas afectadas:

9. Posibles consecuencias

Brecha de confidencialidad:

☐ Divulgación a terceros /difusión en internet ☐ Los datos pueden ser explotados con otros fines
☐ Enriquecimiento de otras bases de datos ☐ Otras: _____

Brecha de integridad:

☐ Datos han sido modificados aunque hayan quedado inservibles o irrecuperables ☐ Datos han sido modificados y utilizados para otros fines
☐ Otras: _____

Brecha de disponibilidad:

☐ Imposibilidad de la prestación de un servicio a los interesados ☐ Deterioro de las condiciones de prestación de un servicio a los interesados
☐ Otras: _____

Naturaleza del impacto potencial sobre los sujetos:

☐ Pérdida de control sobre sus datos personales ☐ Limitación de sus derechos ☐ Discriminación
☐ Usurpación de identidad ☐ Fraude ☐ Pérdidas financieras
☐ Reidentificación no autorizada ☐ Perdida de confidencialidad de datos afectados por secreto profesional
☐ Daños a la reputación ☐ Otras: _____

Severidad de las consecuencias para los individuos: ○ Baja ○ Media ○ Alta ○ Muy alta

Medidas tomadas para solucionar la brecha y minimizar el impacto sobre los afectados:

_____
_____
_____
_____
_____

AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS

FORMULARIO NOTIFICACIÓN BRECHAS DE SEGURIDAD

10. Comunicación a los interesados

¿Se ha comunicado la brecha a los interesados?

- ○ Si — Fecha en la que se informó: _____
  Número de sujetos informados: _____
  Medios o herramientas de comunicación: _____
- ○ No, pero serán informados — Fecha en la que se informará: _____
- ○ No serán informados — Justificación para no informar: _____
- ○ Pendiente de decidir

(Adjuntar contenido de la comunicación a los interesados)

11. Implicaciones trasfronterizas

¿Hay sujetos de otros Estados miembros de la UE afectados por la brecha? ☐

Marque los Estados que puedan estar afectados (A) y aquellos a los que haya notificado(N) la misma brecha de seguridad:

A	N		A	N		A	N	
☐	☐	Alemania	☐	☐	Austria	☐	☐	Bélgica
☐	☐	Bulgaria	☐	☐	Chipre	☐	☐	Croacia
☐	☐	Dinamarca	☐	☐	España	☐	☐	Eslovaquia
☐	☐	Eslovenia	☐	☐	Estonia	☐	☐	Finlandia
☐	☐	Gran Bretaña	☐	☐	Grecia	☐	☐	Hungría
☐	☐	Irlanda	☐	☐	Italia	☐	☐	Letonia
☐	☐	Lituania	☐	☐	Luxemburgo	☐	☐	Malta
☐	☐	Países Bajos	☐	☐	Polonia	☐	☐	Portugal
☐	☐	Rep. Checa	☐	☐	Rumania	☐	☐	Suecia

12. Documentos adjuntos

(Adjuntar documentos)

En_____,a____de_____20__

Anexo III. Ejemplos ilustrativos

A continuación se muestra un ejemplo orientativo para la toma de decisiones relacionada con la notificación de brechas de seguridad a la autoridad de control, el ejemplo parte de un modelo de tres parámetros: Volumen, tipología de datos e impacto.

Sobre la base de estos parámetros se establecen criterios y valores de la siguiente forma:

VOLUMEN (números de registros completos e identificativos)

- Menos de 100 registros (1)
- Más 1.000 (2)
- Entre 1.000 y 100.000 (3)
- Más de 100.000 (4)
- Más de 1.000.000 (5)

TIPOLOGÍA DE DATOS (Según GDPR y Sector)

- Datos no sensibles (x1)
- Datos sensibles (x2)

IMPACTO (EXPOSICIÓN)

- Nulo (2)
- Interno (dentro de la empresa - controlado) - (4)
- Externo (Perímetro proveedor, atacante) - (6)
- Pública (Accesible en Internet) - (8)
- Desconocido (10)

El cálculo del posible riesgo se podría obtener de la siguiente forma:

Riesgo = P x I
Riesgo = P (Volumen) x Impacto (Tipología x Impacto)
Ejemplo Fuga masiva pública: 5 x (2x10) = 100%

Una posible política de notificación de brechas sería la de notificar cualquier brecha que cumpla simultáneamente las siguientes circunstancias:

- Riesgo con valor cuantitativo en un umbral superior a 20 (más o menos).
- Ante la coincidencia de dos circunstancias cualitativas (Marcadas en albero).

Se podría recomendar comunicar a los interesados cualquier brecha que cumpla simultáneamente las siguientes circunstancias:

- Riesgo con valor cuantitativo superior a 40 (más o menos).
- Ante la coincidencia de dos circunstancias cualitativas (Marcadas en albero).

Ejemplo de incidente - CLASIFICACIÓN

Tipo de brecha	Confidencialidad
Taxonomía	Acceso a cuenta privilegiada Otorga acceso a información con datos sensibles
Origen de la amenaza	Externo
Gravedad	Alta
Volumen aproximado	Más de 200.000 registros

Ejemplo de incidente - ANÁLISIS

Volumen	Mas de 200.000 registros	4
Tipología de datos	Datos sensibles	2
Impacto	Alta	8
Riesgo	4 x (8x2)	64

Anexo IV. Referencias bibliográficas

Referencias bibliográficas:

- THE WORKING PARTY ON THE PROTECTION OF INDIVIDUALS WITH REGARD TO THE PROCESSING OF PERSONAL DATA (WP29) /Guidelines on Personal data breach notification under Regulation 2016/679/ Octubre 2017
- CENTRO CRIPTOLÓGICO NACIONAL/ Guía de Seguridad de las TIC CCN-STIC 817. Esquema Nacional de Seguridad. Gestión de ciberincidentes/ Julio 2016/
- CNPIC (Centro Nacional de Protección de Infraestructuras Críticas y Ciberseguridad)/ Identificación y reporte de incidentes de seguridad para operadores estratégicos. Guía básica de protección de Infraestructuras Críticas/ Diciembre 2013.
- CCN 403-gestion_de_incidentes_de_seguridad
- ISO 27035 Information security incident Management
- ISO 29151: 2017 Security techniques- codes of practice for personally identifiable information protection
- NIST Special Publication 800-61 rev2: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf
- UNE 71505: Sistema de Gestión de Evidencias Electrónicas.

Anexo V. Otros recursos

Vídeos:

- ¿Sabrías reaccionar a un incidente?
- Cómo prevenir la fuga de información
- ¿Cómo identificar una fuga de información? Monitoriza y analiza el tráfico
- ¿Sabes para qué sirve cada documento de tu plan de continuidad?
- Continuidad de negocio en circunstancias adversas
- Respuesta jurídica a ataques

Recursos formativos:

- https://www.incibe.es/protege-tu-empresa
- https://www.incibe.es/protege-tu-empresa/juego-rol-pyme-seguridad
- https://www.incibe.es/sites/default/files/contenidos/JuegoRol/juegorol_cuestionarioinicialrespuestaincidentes.pdf
- Guía de fuga de información
- Ciberseguridad en la identidad digital y la reputación online

AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS

isms forum spain

Con la colaboración de:

CCN Centro Criptológico Nacional

incibe_ INSTITUTO NACIONAL DE CIBERSEGURIDAD