www.ismsforum.es

II Guía [práctica] para la Gestión de Brechas de Datos Personales

febrero 2023

Una iniciativa de

isms forum

dpi DATA PRIVACY INSTITUTE

Febrero 2023

II Guía [práctica] para la Gestión de Brechas de Datos Personales

AUTORES

COORDINADORES	Javier Lomas Sampedro
	Susana Rey Baldomir
SUBCOORDINADORES	Elena Mora González
PARTICIPANTES	Gisela Reverter Dominguez
	Gustavo Lozano García
	Ignacio Puente Carrasco
	Jaime Requejo García-abril
	Josep Bardallo Gay
	Katsuko Saito Peña
	Marta Cañas Miralles
	Melania Haro Peredo
	Sonia Beulas Boix
	Tomás Sanz Morejón
	Victoria Wichmann
GESTIÓN DE PROYECTOS	Beatriz García González
DISEÑO/MAQUETACIÓN	Cynthia Rica Gómez

CONTENIDOS

CONTENIDOS

Introducción

Objetivo y alcance de la guía

En un mundo hiperconectado y cada vez más digital, los incidentes no pueden ser considerados algo privado que se pueda dejar en la esfera interna de quien los sufre, no hay islas de autogestión que no tengan influencia sobre los demás. La comunicación de los incidentes y la compartición de información entre todos los actores del ecosistema digital es una herramienta básica de defensa. Entre los profesionales de la ciberseguridad ya hace muchos años que se han venido produciendo iniciativas destinadas a establecer vías o espacios de compartición segura de esta información, no solo técnica sino también de gestión.

Con el desarrollo de la economía digital y su mayor peso económico y social, los diferentes legisladores han visto necesario incorporar estos procesos de conocimiento de los incidentes en las diferentes normativas que se han ido desarrollando, a través de las obligaciones de notificación de incidentes.

También el Reglamento General de Protección de Datos (RGPD) incluyó la doble obligación de, en determinadas circunstancias, notificar las brechas de datos personales a las autoridades de control y comunicarlas a las personas físicas.

En el caso concreto de las brechas de datos personales, la comunicación directa a las personas físicas afectadas las coloca en la posición en la que siempre deben estar, la salvaguarda de sus derechos y libertades, permitiéndoles de esa forma tomar las medidas que estén únicamente en su mano para minimizar el impacto de la brecha sobre las mismas. Además, la repercusión pública poco a poco va concienciando a la sociedad sobre los riesgos e importancia de una gestión adecuada de la seguridad en nuestra vida diaria.

Pero en muchos casos, desafortunadamente, solo el riesgo de sanción puede servir de incentivo para impulsar el cumplimiento en general del RGPD, en cuanto a la seguridad de los tratamientos, así como del deber de notificar y comunicar sobre estas brechas de datos y su gestión.

La norma está planteada para que los responsables tengamos que entender cada brecha, gestionarla adecuadamente, determinar si se debe de notificar a la autoridad de control y, en su caso, comunicar a los interesados; todo ello adoptando las medidas necesarias para contenerla cuanto antes, con el cuidado de ir acreditando una labor impecable durante la crisis, y todo ello en el plazo límite de 72 horas.

La presente ´Guía [práctica] para la gestión de brechas de datos personales´ (en adelante, la Guía), nació con la intención de complementar a la ´Guía para la notificación de brechas de datos personales´ de la Agencia, orientada a proporcionar directrices generales para la notificación y la comunicación a los interesados, precisando plazos y aspectos concretos del procedimiento y sobre el contenido de las notificaciones.

Retomando el espíritu de la primera Guía de notificación que ISMS publicó conjuntamente con la Agencia en el año 2018, nuestro objeto es servir de ayuda y orientación a los responsables y encargados de los tratamientos en todo lo que se debe hacer para poder gestionar y notificar adecuadamente. Con ese fin hemos tratado de incluir la experiencia adquirida por los Delegados de Protección de Datos (en adelante, DPD), que han venido aplicando los artículos 33 y 34 del RGPD durante estos años.

Las brechas ocurren, por mucho que invirtamos en ello, y tenemos que hacerlo, pero se sucederán, la seguridad cien por cien no existe, y habremos de convivir con ciertos niveles de riesgo siempre.

Pero como suele indicar la propia AEPD en sus resoluciones: "la identificación de una brecha de seguridad no implica la imposición de una sanción de forma directa por esta Agencia, ya que es necesario analizar la diligencia de responsables y encargados y las medidas de seguridad aplicadas."

La mejor manera de demostrar esta diligencia, nuestro obligado Accountability, es cumplir con el RGPD y poder demostrarlo. De esta manera, ya estaremos analizando los riesgos más importantes para los derechos y libertades de los interesados, estableciendo medidas para su reducción y de esta forma evitando, en la medida de lo posible, que se produzcan brechas o haciendo que, una vez producidas, su impacto sea menor en los interesados.

Si no se toman a tiempo las medidas adecuadas, las brechas de datos personales pueden entrañar daños y perjuicios para las personas físicas; responderemos no tanto por sufrirlas como por la gestión que hagamos de ellas, antes y después de que sucedan.

Es significativo que el Parlamento Europeo, en su Resolución de 10 de junio de 2021 sobre la ´Estrategia de Ciberseguridad de la UE para la Década Digital´, alerte sobre el aumento de los ciberataques y amenazas híbridas contra las infraestructuras europeas, y advierta acerca del bajo grado de preparación y de sensibilización de las empresas sobre este particular. En consecuencia, cree necesario fomentar que los productos conectados a Internet en la Unión sean seguros desde el diseño y armonizar las legislaciones nacionales en materia de ciberseguridad, en base a una aproximación al riesgo y a esquemas de certificación, recordando la importancia del factor humano en esta materia.

- Registro de Actividades de Tratamiento
- Análisis de Riesgos practicados
- Evaluaciones de Impacto
- Medidas de Seguridad y Mejora Continua
- Adopción de Políticas de Seguridad y Códigos de Conducta
- Realización Periódica de Auditorías, internas o externas
- Registros de Formación o Certificados
- Contratos de Encargo del Tratamiento
- Listado de Controles y Monitorización
- Plan de Comunicación y Formación

> La identificación de una brecha de seguridad no implica la imposición de una sanción de forma directa por esta Agencia, ya que es necesario analizar la diligencia de responsables y encargados y las medidas de seguridad aplicadas.

No es extraño, por tanto, que en la notificación, o tras esta, la autoridad de control nos requiera gran cantidad de información y documentación en un plazo de tiempo corto. Las organizaciones deberemos tener revisado y disponible en todo momento qué cumplimos y la documentación que lo acredite. Para en caso de brecha poder aportar aquella relativa al tratamiento o tratamientos implicados, las medidas implantadas para evitar lo que finalmente ha sucedido y todo lo que sirva para demostrar nuestra diligencia.

Esta Guía está hecha por y para los profesionales que tenemos que enfrentarnos a este tipo de amenazas, brechas de datos personales cada vez más frecuentes y graves, y ambiciona tan solo a resultar útil en esa labor, organizándola conforme a las fases del ciclo de vida de una brecha: antes, durante y después, es decir: planifica, gestiona, notifica y resuelve, para terminar con los análisis de los casos prácticos más característicos a los que nos podremos enfrentar.

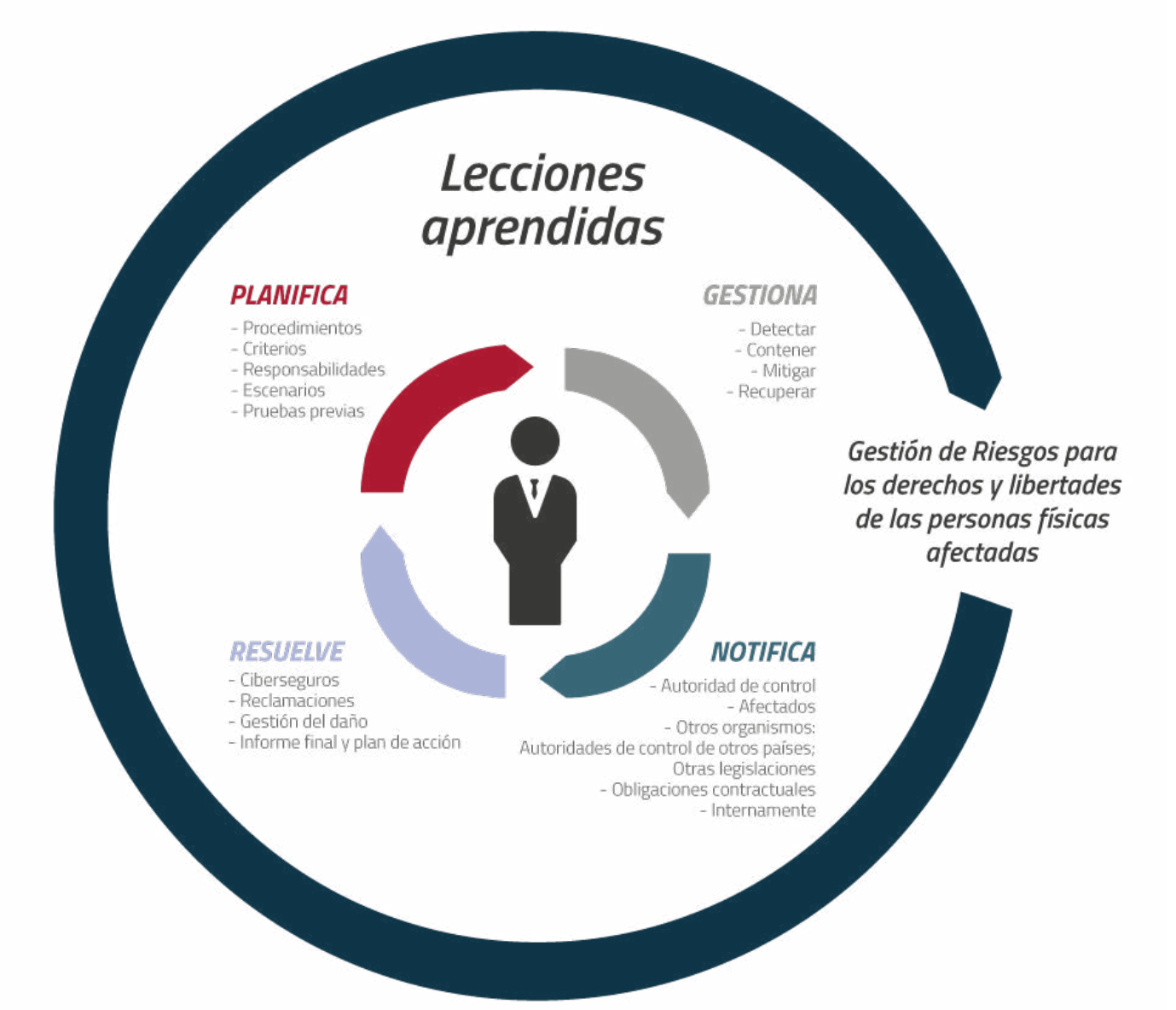
En esta segunda edición hemos tratado de hacerla aún más práctica, mediante un nuevo formato, que incluye además una propuesta de metodología de análisis de riesgos para los derechos y libertades para los interesados en caso de brecha de datos, y más casos prácticos adaptados a las nuevas herramientas de la AEPD.

Así mismo se añade un apartado de análisis de algunas Resoluciones de la AEPD, como una primera aproximación que nos pueda dar algunas pistas sobre buenas prácticas y también sobre errores en los procesos de gestión y notificación de brechas.

Esperamos que esta Guía nos ayude a conocer la posición y capacidad real que tienen cada una de nuestras organizaciones, públicas o privadas, ante estas inevitables y permanentes amenazas; revelando el bajo grado de preparación y de sensibilización para una gestión adecuada, nuestras fortalezas y debilidades que deberemos corregir en nuestras entidades, si queremos hacer de la gestión de las brechas de datos personales una herramienta útil de mejora.

1 CICLO DE VIDA DE LAS BRECHAS DE DATOS PERSONALES

Desde ese sentido práctico y diferenciador del que se ha querido dotar a esta Guía, con una clara orientación hacia la diligencia debida y el accountability, y tal y como se ha mencionado anteriormente, se la ha estructurado siguiendo las fases del ciclo de vida de las brechas: **antes, durante y después,** esto es, **planifica, gestiona, notifica y resuelve.**



Para el **antes**, tenemos la fase de **planifica**, desde la perspectiva de la anticipación diligente o previa preparación, para no tener que improvisar en caso de brecha.

En un segundo bloque, **durante** la brecha, estaremos en la fase de **gestiona**, donde la gestión rápida, ordenada y eficaz del incidente minimizará sus consecuencias sobre la propia organización y terceras partes implicadas, lo que sin duda será analizado con detenimiento por la AEPD. Si estamos preparados será más fácil mantener la calma durante la crisis.

Y, por supuesto, durante esa fase, las brechas de datos personales se **notifican** a la autoridad de control y, en su caso, se **comunican** a las personas físicas afectadas, en función del riesgo que supongan para los derechos y libertades de las personas físicas y para lo cual es fundamental realizar los análisis de riesgos pertinentes. Resultará determinante que, como organizaciones que hacemos tratamientos de datos personales, siempre tengamos en mente a las personas físicas y sus datos personales, cómo protegerlos y cómo se pudieran ver afectados en sus derechos y libertades fundamentales.

Además, habrá de tenerse en cuenta las posibles obligaciones de cada organización de notificación más allá de la AEPD: autoridades de control de otros países (ICO, CNIL, PUODO, etc.), otras legislaciones (LPIC, NIS, ENS, etc.), así como obligaciones contractuales e internamente a determinados órganos de control empresarial.

Después, completamos con **resuelve**, dando seguimiento a su evolución y evaluación por parte de la AEPD, lo que podría desembocar en la indeseada consecuencia de la apertura de un expediente sancionador.

Tampoco debemos olvidar la gestión ulterior a la comunicación a los afectados: aclaraciones, reclamaciones de daños a terceros, ciberseguros, etc. Todo ello culminando en la gestión del posible daño reputacional que también habrá que administrar y reparar.

No podemos olvidarnos de los análisis de **lecciones aprendidas** tras las brechas de datos personales experimentadas, que permitan realimentar el apartado de planifica con posibles mejoras; cómo gestionar y qué tener en cuenta en este punto, relacionándolo con el PDCA y el ciclo de mejora continua: sacar conclusiones, hacer seguimiento, corregir errores y elaborar un informe final, te ayudará a prevenir o paliar la próxima brecha.

2 PLANIFICA

La mejor planificación de una brecha de datos personales es evitar que se produzca, pero sabedores de que pueden hacerse realidad, es imprescindible prepararse para afrontarlas con la debida antelación. La planificación es por tanto una fase inicial clave en la que toda entidad, pública o privada, deberá estar preparada.

El enfoque actual de los procesos de gestión de brechas, como el que vamos a mantener en esta guía, mayoritariamente incluye una fase de ***planificación***, que se configura como un plan de contingencia definiendo diferentes escenarios en los que potencialmente podría ocurrir una brecha y estableciendo cuál sería el plan de respuesta. Tejer, para cada uno de esos escenarios claramente identificado, todo lo que se va a necesitar cuando se tenga que gestionar una brecha, que todo esté previamente ***preparado, documentado y probado***.

La capacidad de cada entidad para anticiparse a estos sucesos determinará el éxito o fracaso de las siguientes fases de ***gestión y notificación*** que se tendrán que afrontar en la resolución de cada brecha de datos personales.

Lo que no tengamos ya incorporado y rodado en nuestra organización, previo a sufrir la brecha, difícilmente podremos corregirlo en plena crisis, donde los tiempos se precipitan y las tensiones se incrementan exponencialmente a la falta de una adecuada planificación.

A fin de articular esta fase inicial de preparación, podemos considerar perfectamente aplicable lo que sostienen el CCN, INCIBE y CNPIC en su Guía Nacional de Notificación y Gestión de Ciberincidentes, que una buena anticipación y entrenamiento previo es clave para realizar una gestión eficaz de un incidente, en nuestro caso de una brecha de datos personales, para lo que hace falta tener en cuenta tres pilares fundamentales: las personas, los procedimientos y la tecnología.

2.1. Las Personas

—2.1.1. Formación y concienciación: Aprendiendo a identificar una brecha de datos personales y distinguirla de un incidente de seguridad

Sin ser conscientes de lo que es una brecha de datos personales difícilmente sabremos cómo gestionarla, ni cumplir con los artículos 33 y 34 del RGPD. Debemos por tanto aprender a identificarlas, ya que pudieran estar sucediendo sin que nos estemos enterando.

Si comparamos nuestro país frente a otros países de la Unión Europea, vemos que en España el indicador de brechas de datos personales notificadas es sensiblemente inferior al del resto de países.

Tan malo es sufrir muchas brechas de datos personales como declarar no haber sufrido ninguna, porque en el entorno digital actual significa que lo más probable es que no estemos detectando las brechas, lo que puede deberse a una inmadurez organizativa.

Para alcanzar el mínimo de nivel de madurez exigida a toda entidad, pública o privada, resulta fundamental la **comunicación y colaboración** entre todas las áreas de una organización y, en especial, la de **seguridad** y la de **protección de datos**. En cualquier otro caso, el procedimiento de gestión de incidentes de seguridad no será completo y suficiente si no tiene un apartado específico donde se aborden las brechas de datos personales y tipologías de incidentes que lo pueden ser.

En consecuencia, desde el área de protección de datos de cada entidad, ya tenga esta designado a un DPD o mediante cualquier otra fórmula adecuada a la norma, en función de ese rol expresamente encomendado en el RGPD, serán los ***únicos que están facultados*** para determinar si en un incidente de seguridad se han visto afectados datos personales y, en ese caso, tratarlo como brecha de datos personales.

Porque de eso se trata, de emplear a cada área la responsabilidad para lo que está preparada y mejor puede llevar a cabo, como es el caso del DPD, que por su formación y especialización sabe qué es un dato personal y que no.

Pero es que además podemos asegurar del DPD, dentro de su organización y cumpliendo con el trabajo que tiene encomendado, quizás sea el que mayor conocimiento tenga de cuáles son los datos personales tratados en la compañía, ya que trabaja con ellos todos los días, los ha registrado en su RAT y ha realizado los análisis de riesgos exigidos legalmente por cada tratamiento.

En consecuencia, si alguien debe ser llamado en el primer momento de ser detectado el incidente de seguridad, para que en muy poco tiempo evalúe si estamos ante un dato personal y lleve a cabo el preceptivo análisis de riesgos sobre los derechos y libertades de las personas físicas afectadas por dicho incidente, no es otro que el DPD.

Precisamente esa es la idea que tenía el legislador europeo, plasmada a lo largo de todo el RGPD, cuando pedía a la figura del DPD que tuviera ese conocimiento transversal de su organización y de sus procesos de negocio y, por tanto, de sus datos personales.

De esta forma evitaríamos situaciones en las que no se detecta una brecha de datos personales al inicio de la gestión de un incidente de seguridad porque a estas alturas todavía seguimos necesitando superar falsas creencias, como que las direcciones de correo electrónicos de empresa no son datos personales o que los datos públicos, los datos de localización de un teléfono móvil o la dirección de protocolo de internet (IP), tampoco lo son.

La protección de los datos personales que puedan verse impactados por un incidente de seguridad, o por su gestión, es demasiado importante como para dejarla en manos de una sola de las áreas implicadas, requieren del trabajo y coordinación de todas ellas.

Distinción de un incidente de seguridad

El Esquema Nacional de Seguridad (en adelante, 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 NIS2 define ´incidente´ como "todo hecho que comprometa la disponibilidad, autenticidad, integridad o confidencialidad de los datos almacenados, transmitidos o tratados, o los servicios ofrecidos por sistemas de redes y de información o accesibles a través de ellos"; y el propio RGPD define, de un modo amplio, las "brechas de datos personales" como "todas aquellas violaciones de la seguridad que ocasionen la destrucción, pérdida o alteración accidental o ilícita de datos personales transmitidos, conservados o tratados de otra forma, o la comunicación o acceso no autorizados a dichos datos".

Por tanto, no debemos confundir ***incidente de seguridad*** con ***brecha de datos***; toda brecha de datos personales supone una tipología de incidente de seguridad, sin embargo, al contrario, no sucede lo mismo.

En este sentido, podríamos definir ***evento o incidencia*** como cualquier desviación del funcionamiento normal de nuestra organización que podría afectar o no a su desarrollo normal. Mientras que ***incidente*** supondría la ya materialización del evento con una afectación negativa. Y ***brecha de datos personales*** sería aquel incidente en el que tenemos datos personales implicados.

Es decir, en la brecha de datos personales tenemos ya una materialización de un efecto negativo para el funcionamiento de los sistemas y/o procesos de la organización. Ya no hay riesgo de afectación, sino afectación real. Sin embargo, todavía queda un análisis de riesgos que hacer, y que consiste en ver cómo y en qué nivel puede afectar este suceso, ya no a nuestra organización, sino a las personas físicas cuyos datos se han visto impactados.

Que los sistemas de seguridad de la organización generen una alarma de tráfico de salida de nuestra organización hacia internet anómalo es un evento. Si detectamos que esa salida se está produciendo por una exfiltración de datos a causa de un ransomware, tenemos un incidente. Ya no hay "riesgo" de pérdida de confidencialidad de datos, sino que ésta se está produciendo realmente. Pero sólo si entre los datos exfiltrados hay datos de personas físicas, podremos decir que estamos ante una brecha de datos personales.

Buenas prácticas entre las áreas de protección de datos y seguridad de la información

A nivel operativo, para fomentar la colaboración entre las áreas de protección de datos y la de seguridad de la información, y hacer seguimiento de todos los sucesos relacionados con los incidentes de seguridad en las organizaciones, que por desconocimiento puedan llevar a obviar su naturaleza de brechas de datos personales, es recomendable incluir en los ***modelos de valoración de las incidencias***, dentro de los ***procesos de gestión de problemas*** (muy ligado a la filosofía ITIL: Information Technology Infrastructure Library) de las organizaciones, un ***análisis de riesgos*** sobre los derechos y libertades de las personas físicas que de forma probable puedan entrañar dichos incidentes de seguridad, dando cumplimiento al artículo 34 del RGPD, y al que por su importancia dedicaremos un especial desarrollo en el anexo III de esta Guía.

Precisamente para evitar que puedan pasar desapercibidas las brechas de datos personales, conviene revisar de forma regular, junto con los responsables de Tecnología de la Información, la tipología de apertura de ***tickets de servicio e incidencias*** por parte de los usuarios, de forma regular, para detectar si los conceptos de incidente de seguridad o brecha de datos son conocidos entre los empleados, e informan de ellos al área de protección de datos o, por el contrario, se están perdiendo por falta de concienciación y se vienen resolviendo por las áreas operativas (áreas de Negocio y TI) sin convocar ni dar cuenta, previamente o en el momento, al área de protección de datos.

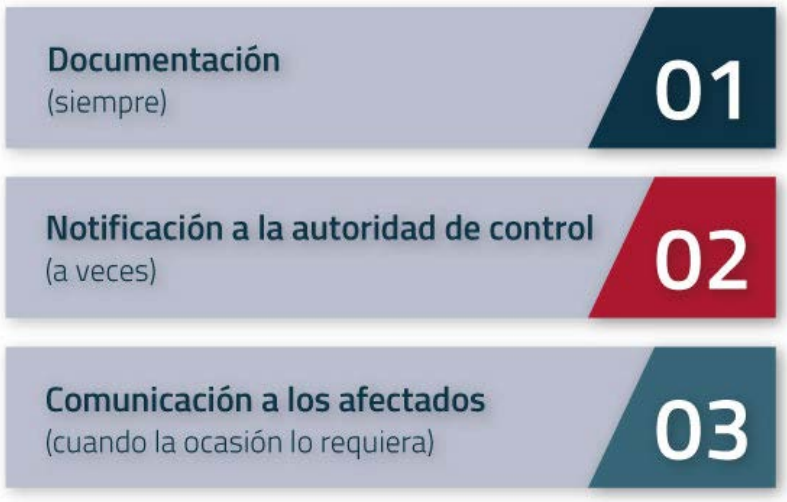
En este sentido, se puede venir observando cierta malinterpretación del artículo 34 del RGPD y los efectos que su no aplicación tienen en la documentación de los incidentes de seguridad y de las brechas de datos en las organizaciones. No podemos decir que algo se ha gestionado, si no se ha registrado en alguna parte y no hay evidencia de ello.

No debemos confundir nuestras obligaciones de notificación a la autoridad de control o de comunicación a los afectados, con nuestras obligaciones de documentación interna de cualquier incidente de seguridad. El análisis y valoración del riesgo para los afectados se debe realizar siempre valorando las medidas de seguridad que ya existían, las adoptadas, el número de afectados, pero sobre todo su severidad, esto es, el cómo puede afectar a los derechos y libertades de las personas físicas.

El hecho de que en algunos casos no tengamos la obligación de notificar a la AEPD o comunicar a los afectados, no avala que incumplamos nuestra obligación de documentar internamente cualquier incidente de seguridad o brecha de datos personales.

Una vez que ya tenemos claro el concepto y las obligaciones que conlleva, la organización debe tener su propia definición de gestión de incidentes y de gestión de brechas de datos personales, y aplicarla en el máximo caso de usos y escenarios sacados de su propia realidad o de sectores afines.

En los últimos años el EDPB , se ha pronunciado al respecto y estratifican claramente los incidentes de datos personales en tres fases muy diferenciadas:



2.1.2. Gobernanza y compromiso de la alta dirección

La Gobernanza en materia de brechas de datos personales es tanto o más importante aún que la Gestión de las brechas en sí; no podemos entender como diligencia ni responsabilidad proactiva en una organización que no se haya preocupado por los aspectos de Gobernanza.

Con Gobernanza nos referimos al contenido mínimo de las políticas y procedimientos de reporting que, dentro de las organizaciones, deben contribuir al mantenimiento de los sistemas de revisión y control que continuamente está monitorizando las actividades de tratamiento de datos personales y los requisitos exigidos por el RGPD y la LOPDGDD.

Con la Gobernanza también nos estamos refiriendo al sistema de control interno para supervisar el seguimiento del cumplimiento de las acciones de mejora que surten fruto de los ejercicios de puesta a prueba de los equipos de personas y procedimiento, así como de las experiencias vividas por cada organización en la resolución de sus incidentes de seguridad y brechas de datos personales.

La implicación de la Alta Dirección en esta materia, no solo se cumple con atender a la ***rendición de cuentas*** por parte del DPD, o el modelo adoptado para ese rol, en la planificación, gestión, notificación y resolución de brechas de datos personales, sino que comprende también su ***apoyo expreso*** en esta responsabilidad, dotándole de un presupuesto mínimo que permita al DPD cumplir con todas estas tareas, proporcionándole los medios técnicos y humanos necesarios para ello.

Será la Alta Dirección de cada organización la que debiera aprobar el Plan de Escenarios de Brechas de Datos Personales, de los que hablaremos más adelante, al igual que el resto de todas las Políticas y Procedimientos elaborados sobre esta materia.

Sin la implicación de la Alta Dirección, ninguna organización, pública o privada, podrá alcanzar el nivel de madurez suficiente para afrontar las brechas de datos personales como lo que son, riesgos corporativos importantes.

2.1.3. Asignación de roles y responsabilidades: áreas implicadas

Cualquier persona dentro de la organización con acceso directo o indirecto a los datos personales puede, de forma accidental o intencionada, provocar o detectar una brecha de datos personales. Por este motivo, es necesario anticiparse identificando las áreas potencialmente implicadas o conocedoras de un incidente de seguridad, asignando roles y responsabilidades para prevenirlos o, en caso de que sucedan, para gestionarlos de la manera más satisfactoria posible. Lo que servirá al doble fin de estar preparados en caso de que este suceda y para cumplir con el principio de responsabilidad proactiva del artículo 32 del RGPD.

La gestión de incidentes de seguridad no es solo responsabilidad de Tecnología, lo es de todas las áreas de actuación de las organizaciones.

Para clarificar esta tarea, el enfoque que recomendamos y que siguen muchas organizaciones es el que se conoce como modelo de las tres líneas de defensa, sin duda involucradas en la gestión anticipada de un incidente de seguridad, jugando un papel fundamental en la detección y prevención de los incidentes de seguridad:

Algunas de las acciones recomendadas en esta fase de planifica son:

- Realizar un inventario o registro de todas aquellas áreas o departamentos con acceso, directo o indirecto, a datos personales.
- Definir personas de contacto para cada una de aquellas áreas o departamentos.
- Realizar formaciones específicas y periódicas para estas personas de contacto con una doble finalidad:
  - Formarles en materias específicas sobre incidentes de seguridad; y
  - Que sean conocedores de que puedan tener eventualmente impacto o generar incidentes de seguridad.
- Incluir a estas áreas en los simulacros periódicos de incidentes de seguridad para detectar áreas de mejora que luego puedan ponerse en práctica.

Por tanto, es especialmente importante contar y coordinarse con las siguientes áreas:

01

Alta Dirección: es esencial involucrar e informar a los órganos de gobierno. Deben disponer de toda la información necesaria para poder tomar las decisiones pertinentes y conocer y anticiparse a las consecuencias y responsabilidades que pudieran derivarse.

02

Seguridad: este equipo debe dar soporte en todo momento al Delegado de Protección de Datos, comunicando cualquier cambio que pudiera modificar el análisis de riesgo inicial, y trabajando conjuntamente, tanto en esta fase como en la posteriores.

03

Departamento o roles con función de gestión de riesgos: el nuevo enfoque del RGPD implica que las medidas de seguridad deberán definirse en base a un análisis de riesgos previo, lo que hace conveniente contar con un mapa de riesgos que incluya la protección de datos personales. Mapa que incluirá la definición de los riesgos, los controles y planes de mitigación que resulten necesarios, y que deberá ser actualizado al menos anualmente. Este mapa nos servirá además a la hora de realizar Evaluaciones de Impacto en Protección de Datos. La función de riesgos (bien el departamento o bien las personas en quienes se haya delegado) es quien lleva ese control, pero no es el único. El DPD es quien debe preocuparse por el estado de dichos riesgos y todo ello bajo la batuta, en su caso, del departamento de riesgos.

04

Comunicación interna/externa y Marketing. Otra primera línea de defensa muy importante, pues están acostumbradas a comunicar a clientes internos y externos. Y en la fase previa a los incidentes nos pueden ayudar a sensibilizar y motivar a los empleados, e incluso a los clientes externos, a detectar incidentes en la organización o en sus proveedores. Asumen por tanto un rol preventivo, pero al mismo tiempo reactivo.

05

El papel de otros grupos de interés. En el concepto amplio de tratamiento de datos, que incluye la mera conservación del dato, hay otras partes interesadas que interactúan con nuestros procesos o tratan datos personales responsabilidad de nuestras organizaciones. Partes que tienen también responsabilidad en la gestión anticipada de un incidente de seguridad.

En ese grupo destacan los proveedores y, sobre todo, los que tengan el perfil de Encargados del Tratamiento, al gestionar datos personales por cuenta de la organización, como Responsable del Tratamiento. Los proveedores están obligados a avisar a las organizaciones si creen que alguna de sus órdenes incumple los principios del RGPD (y que por tanto pudiera desencadenar en una futura brecha de datos personales) así como de avisar a la mayor diligencia si detectan cualquier comportamiento anómalo en esta, en sus servidores, accesos remotos, correos electrónicos recibidos, etc; de ahí la importancia del contrato firmado entre ambas partes, cumpliendo con el art. 28 RGPD.

2.2. Los Procedimientos

–2.2.1. Protocolos internos

Otro elemento que ha de estar definido, documentado y preparado previamente es el de los protocolos relacionados con cuestiones y actuaciones que compondrán el procedimiento de gestión y notificación desde la perspectiva de la anticipación diligente antes del incidente:

- Estos protocolos deben plasmar las medidas preventivas incluyendo la implantación de una adecuada cultura ética y del riesgo.
- Igualmente, tiene gran trascendencia que la labor de concienciación y formación de todo el personal de la organización que en el ejercicio de sus funciones acceda a datos personales este protocolizada y exista un claro plan de formación incluido en los protocolos de Recursos Humanos.
- Deben estar adaptados a las características de cada organización.

No será suficiente que cada área disponga de su particular protocolo interno de actuación, la AEPD nos requerirá la presentación e implementación de protocolos unificados y acordados por todas las áreas implicadas de la organización, sobre todo de seguridad y protección de datos.

–2.2.2. Plan de Contingencia: escenarios posibles de brechas de datos personales

Este enfoque, similar al utilizado cuando se abordan los planes de continuidad de negocio, implica que definamos unos escenarios de "contingencia" que, a nuestros efectos, serían unos casos prácticos simulados, en los que se defina un escenario de brecha de datos concreta, diferenciando tipología del incidente en base a las variables de seguridad: confidencialidad, integridad, disponibilidad, e incluyendo también trazabilidad y no repudio.

Los escenarios deberán prever cómo se gestionará en ese caso concreto todo el ciclo de vida de la brecha, comenzando por detallar las medidas que se tomarán para contenerlo, erradicarlo o transferirlo lo antes posible, cómo se haría la comunicación a los afectados, si se generará un site nuevo, se utilizará su web corporativa o se comunicará por vía postal; a quién se convocaría en estos casos, estrategia a seguir ante casos de extorsión, etc. En cada escenario utilizaremos ejemplos de lecciones aprendidas o acciones que han implantado otras organizaciones similares. Y, como si de un escenario de contingencia realmente se tratase, se abordará a través de un Comité de Crisis.

Para definir cada uno de estos escenarios de contingencia o brecha en nuestra organización, debemos consultar las siguientes fuentes:

(i) A nivel interno, acceso a:

- Registro general de incidentes de seguridad del año anterior.
- Informe con todas las peticiones enviadas al área de Sistemas que hayan sido de prioridad alta o crítica o que puedan estar asociadas a categorías como incidencia, indisponibilidad, pérdidas o no visualización de información.
- Eventos de Seguridad física (informes de análisis de accesos a zonas críticas).
- Eventos de seguridad lógica, información que ha adquirido especial importancia con el incremento del teletrabajo (informes de accesos remotos a los sistemas de la organización).
- Sucesos importantes en otras organizaciones del propio grupo.

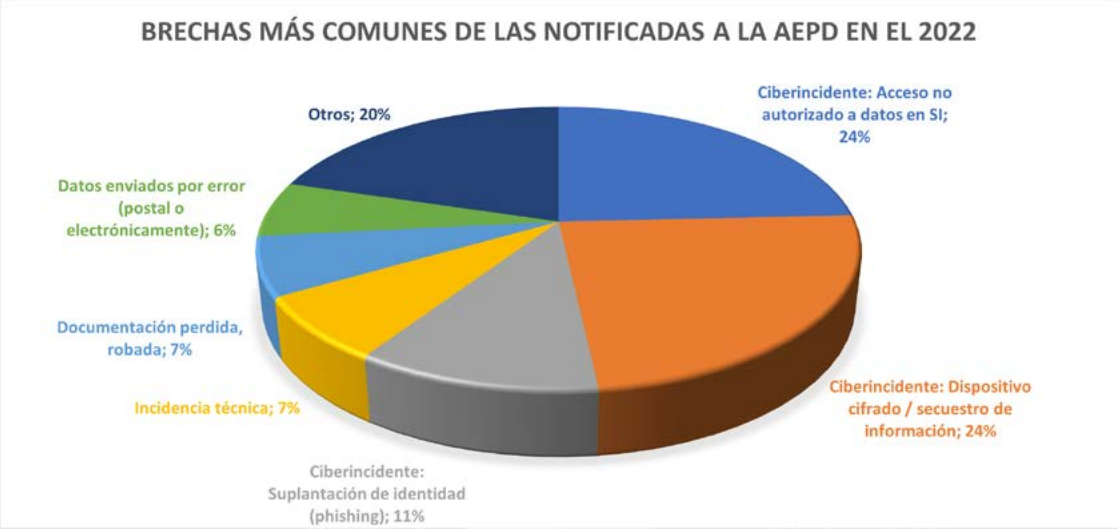
Es recomendable que el DPD se reúna con los principales propietarios de procesos de cada tratamiento que se contemplen en el Registro de Actividades de Tratamiento (en adelante, RAT) para acceder a toda esta información. En ese procedimiento se detallarán las responsabilidades de las partes, también su involucración, como alerta temprana ante detección de posibles incidentes en sus respectivas áreas de responsabilidad.

Además de con las áreas de Negocio, convendría aplicar este modelo de relación con las funciones de control como son seguridad, calidad, gestión de riesgos, compliance y auditoría interna. Con todas ellas, se compondrían los escenarios de brecha de datos personales más probables que finalmente serán considerados por cada organización.

(ii) A nivel externo, acceso a:

- Las publicaciones de brechas de seguridad comunicadas por otras organizaciones a nivel mundial.
- Consultas a publicaciones de INCIBE sobre incidentes.
- Contactos con homólogos de otras organizaciones del mismo sector o afines.
- Pertenencia a Asociaciones ligadas al ámbito de la privacidad.
- Consulta de procedimientos sancionadores en toda Europa[2], así como las publicaciones de procedimientos sancionadores de la propia AEPD.
- Los informes de brechas mensuales que publica la AEPD.

Revisa los informes de brechas periódicos publicados por la AEPD, te darán pistas para tus evaluaciones de riesgos y son "lo que está pasando ahora".



Una vez definido el Plan de Contingencia con los casos de uso de brechas de datos personales en la organización, que se revisarán anualmente, debemos detallar quién será el responsable de gestionarlo.

[2]Se puede obtener información en diversas webs como https://www.enforcementtracker.com/

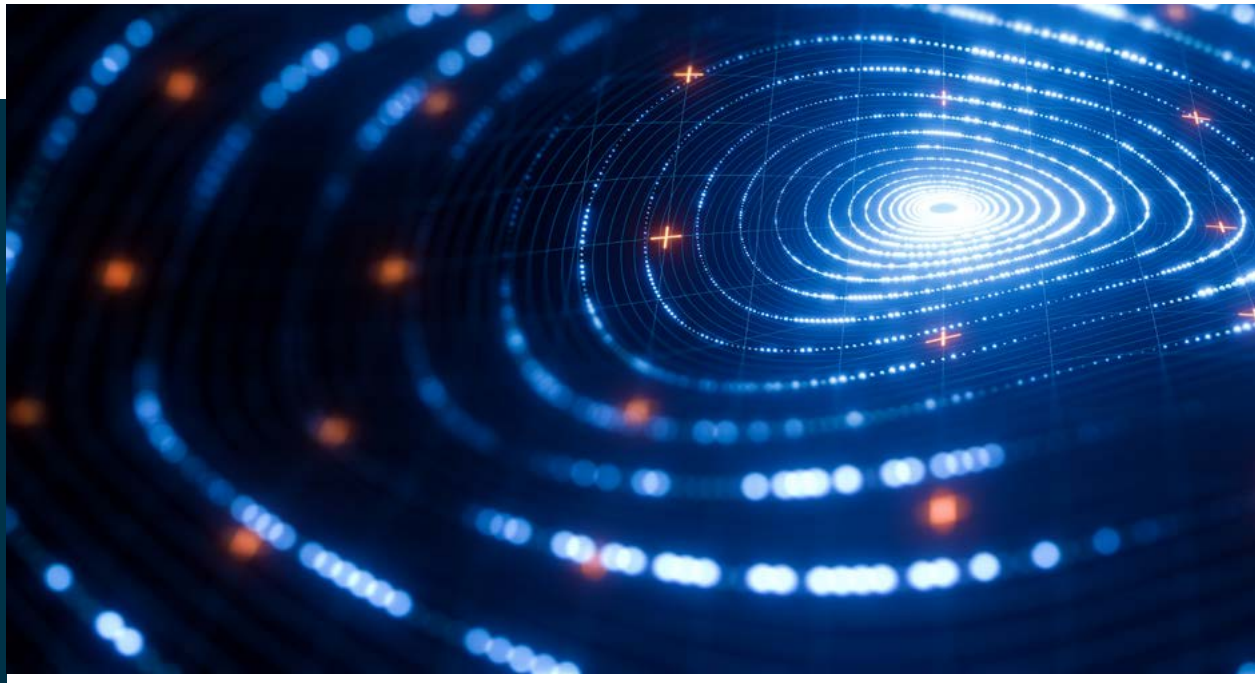
Descripción de los escenarios o casos de uso

Cada caso de uso se hará describiendo, si es requerida, las actuaciones siguientes:

- Documentación: qué documentar, dónde estará archivada, quien es el responsable.
- Registro de Actividades de Tratamiento: en concreto, descripción del proceso donde puede tener lugar esa brecha.
- Análisis de riesgos y Evaluación de Impacto: si procede, que por su especial importancia desarrollaremos en un anexo final de esta guía.
- Políticas y procedimientos e Instrucciones técnicas.
- Inventario de medidas de seguridad actuales.
- Activación o no de un comité de crisis o de contingencia y los actores implicados.
- Notificación a la AEPD: este punto lo desarrollamos en más detalle en el apartado de Notifica.
- Comunicación a los afectados: definir los procedimientos que se seguirán para decidir si una brecha ha de ser comunicada o no a los afectados.

En cada escenario es fundamental el rol del análisis de riesgos, si la situación se presenta, pues se contará con solo 72 horas desde que se ha determinado que el incidente de seguridad tiene carácter de brecha de datos personales, a la mayor diligencia debida, para notificar a la Autoridad de Control, exigencia que no siempre sucede en otros escenarios.

Ajusta tus medidas de seguridad en base a los riesgos y no al revés.



2.3. Probanza de Personas y Protocolos

Como ya comentamos al principio de este capítulo, hemos concebido la planificación de la gestión de brechas de datos personales como un área que bien merece ser incorporada como parte de los procesos habituales de Gestión de Contingencias Informáticas o de los Planes de Continuidad de Negocio de la organización.

La ISO22301, sobre continuidad de negocio, nos ahonda en la importancia de hacer un Plan de Pruebas de forma que al menos anualmente se compruebe si uno de esos escenarios es operativo y está bien diseñado. Por tanto, se viene exigiendo, por buenas prácticas de seguridad e incluso por ley en sectores más regulados e infraestructuras críticas, la prueba de los planes al menos una vez al año. También deberá probarse el Plan de Gestión de Brechas.

Es recomendable pues planificar un simulacro de brecha y documentar su realización, quién hace qué, medir los tiempos de respuesta de ese comité de crisis, aspectos de mejora en el desempeño de los roles dentro de dicho comité, etc. Documentación sistemática de los incidentes de seguridad.

Pero no solo debemos esperar a hacerlo anualmente, pues en caso de haber sufrido una brecha de datos personales real, es un buen momento para activar como una medida proactiva realizar este tipo de pruebas en la organización de forma más regular.

Una vez realizado el simulacro, se debe dejar bien documentado el alcance de la prueba, observaciones de lecciones aprendidas (qué fue bien, qué se puede mejorar…) e incorporar las mejoras a la actualización del documento Plan de Gestión de Brechas, que se actualizaría anualmente o siempre que haya un cambio imprevisto que lo determine (i.e. cambio de arquitectura de los sistemas, fusión/adquisición de organizaciones, cambios en el equipo del Comité de Crisis, etc.).

En esta fase, la concienciación al Comité Directivo es fundamental, se les involucrará en el diseño de las pruebas, estando al menos informados formalmente de su desarrollo y resultados. Para mayor eficacia, siempre que sea posible, recomendamos que las pruebas no se avisen salvo a la Alta Dirección, para revisar y analizar cómo reaccionan los responsables, propietarios de proceso y otras partes interesadas.

3 GESTIONA

Debemos aclarar que existe una gestión de la brecha ya desde el primer momento en que se intenta prevenir a través de todos los procesos ya indicados, desde la formación, documentación y organización y monitoreo hasta cuando se efectúan los análisis de riesgos sobre las consecuencias para los derechos y libertades de las personas que pudiera tener esa brecha.

En este sentido, se propone que la gestión de la brecha empiece en el momento en que se inicia un nuevo tratamiento de datos y se analizan los riesgos para los derechos y libertades de los interesados y, en su caso, se realiza una Evaluación de Impacto para la Protección de Datos. Eso es, en el momento en que se analiza la posibilidad de iniciar un nuevo tratamiento, la Entidad ya debería estudiar la posible afectación a los derechos y libertades de los interesados y detectar posibles brechas que se podrían llegar a producir en caso de que fallase alguna de las medidas de seguridad establecidas en el marco del tratamiento analizado.

En el Anexo 3 de la presente guía proponemos una posible metodología para incluir la Gestión de Brechas en los preceptivos análisis de riesgos para los derechos y libertades de los interesados, así como, si fuese necesario realizarlas, en las Evaluaciones de Impacto.

La gestión de una brecha empieza desde el minuto cero.

En este apartado nos fijaremos en las acciones que han de llevarse a cabo cuando ya se ha producido una brecha de datos personales que ha de ser gestionada adecuadamente, centrándonos en la gestión propiamente dicha del evento o incidente, así como su documentación.

Con todo lo aprendido y documentado en Planifica, y en el corto margen de tiempo de 72 horas naturales, debemos analizar si el evento que ya se ha producido es constitutivo de una brecha de datos, determinar si ha de ser notificada, y estar en condiciones de hacerlo siguiendo los procedimientos que la autoridad de control paute, analizar si se comunica o no a los afectados y organizar toda la documentación e indicadores que acompañará a esta notificación.

No debemos olvidar que tanto la identificación de un incidente de seguridad como brecha de datos como la obligación de su notificación debe basarse en al análisis de riesgos, no de que se produzca la brecha, que ya se ha materializado, sino de que se materialicen las posibles consecuencias para los derechos y libertades de los interesados que esta pueda tener. Análisis que partirá de los realizados en la fase de Planifica, para lo que proponemos seguir igualmente la metodología indicada en el Anexo 3.

3.1 Equipo de trabajo

El DPD o, donde no se haya nombrado, el equipo que ejerza la función de protección de datos en cada organización tendrá que asumir un rol de liderazgo, involucrando a todos aquellos departamentos que pueden ayudar a entender y determinar el alcance del incidente, así como a ponerle fin y mitigar las posibles consecuencias.

Pero la gestión de la brecha será un trabajo en equipo, y por lo tanto la asignación de roles y funciones cobra especial relevancia durante el incidente.

Responsable del negocio (de nuevo, la primera línea de defensa): Como regla general, para poder entender el alcance de un incidente es recomendable informar y coordinar una valoración inicial con el responsable del negocio. 01

Responsable de IT: Siempre que existan sistemas afectados o involucrados en un incidente de seguridad, es necesario comunicárselo al responsable de IT, quien deberá asumir la responsabilidad en el ámbito de las tecnologías de la información, analizando el incidente, su posible repercusión en los sistemas de la compañía, potenciales consecuencias y posibles soluciones. 02

Comunicación interna/externa: Dependiendo de la entidad del incidente será necesario involucrar al departamento de comunicación tanto interna como externa. Las comunicaciones tienen que estar coordinadas y encaminadas a que toda la organización actúe en el mismo sentido y al mismo tiempo para transmitir a los terceros (clientes, pacientes, proveedores, etc.) una información ordenada que les permita, en su caso, tomar consciencia de lo sucedido y mitigar potenciales perjuicios (i.e. modificar sus contraseñas, etc.). 03

Departamento o funciones de Riesgos: Es necesario mantenerlas informadas para que realice un seguimiento de lo sucedido y, en caso de ser necesario, para reevaluar el mapa de riesgos existente y, en su caso, fortalecer los controles definidos. 04

Asesores Externos: En algunas ocasiones será necesario reforzar la posición de la empresa contratando asesores externos a los que habrá que facilitar toda la información de una manera coordinada y ordenada facilitando su labor. 05

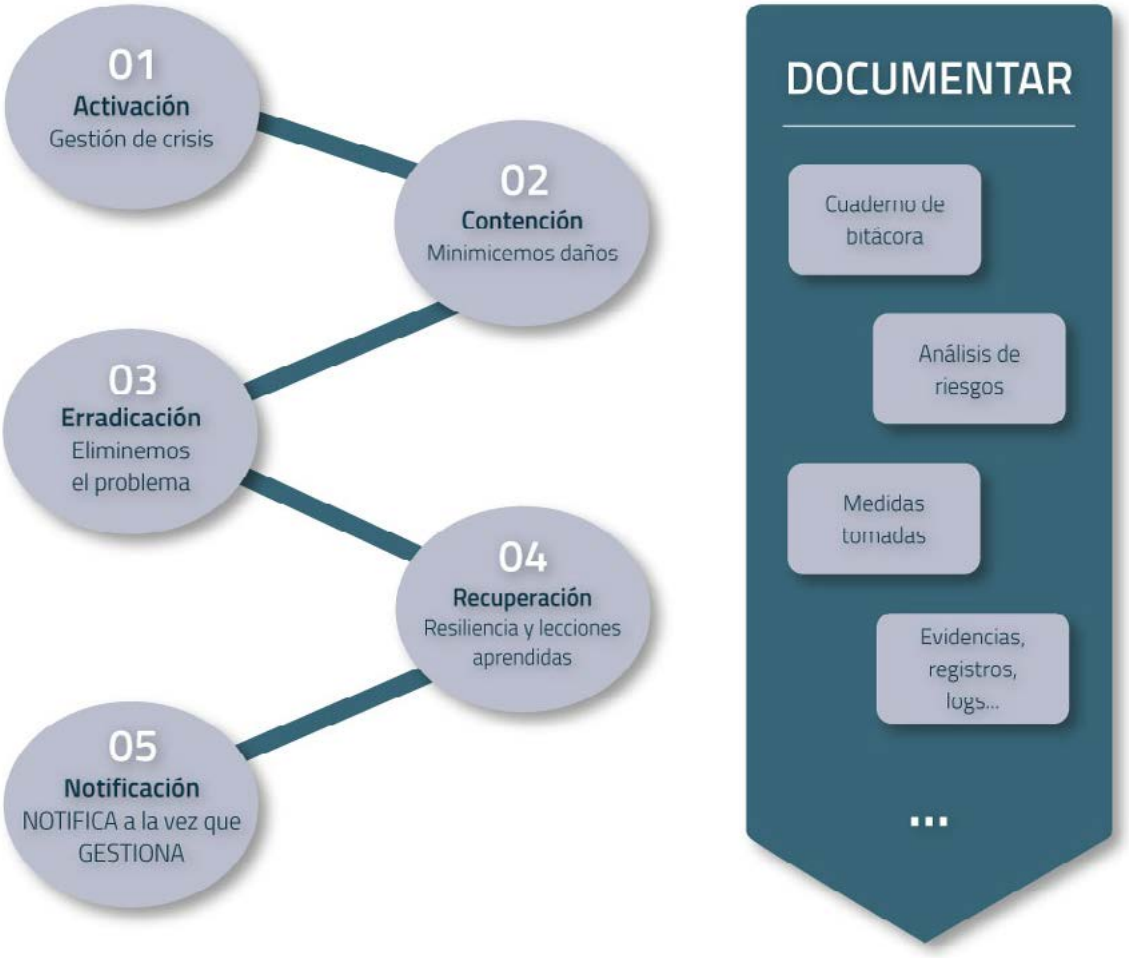
Proveedores y encargados del tratamiento, que puedan estar involucrados en el posible incidente, tanto por su detección temprana como porque el incidente se pudo generar por una vulnerabilidad o incidente en los procesos o instalaciones de dicho proveedor. 06

Durante la gestión del incidente, las organizaciones deberán valorar y, en su caso, acometer con la implicación de diferentes áreas, las siguientes acciones:

- Activación del comité de crisis.
- Activación del Plan de Continuidad de Negocio, cuando aplique.
- Creación de Grupo de Trabajo multidisciplinar con los responsables de procesos implicados (primera línea), así como con IT, privacidad y seguridad.
- Iniciación del trabajo de investigación del incidente.
- Plan de instrucciones para contener y evitar la propagación del ataque.
- Contacto con los equipos de seguridad de los principales responsables de negocio.
- Activación de reuniones permanentes con personal de las áreas de Seguridad, Privacidad y IT.
- Comunicado a responsables/encargados de tratamiento.
- Publicar comunicado oficial sobre el incidente en la página web corporativa.
- Contacto con el INCIBE y CCN-CERT
- En el caso de ser una entidad regulada: Contacto con el regulador (i.e. CNPIC).
- Activación del proceso de notificación de Brechas de datos personales.
- Notificación a la Agencia Española de Protección de Datos, en los casos que se requiera.
- Denuncia policial/judicial.

3.2 Fases de la gestión de la brecha de datos personales

En la gestión de las brechas de datos personales, desde el momento en que se ha concluido que el incidente es constitutivo de brecha, es determinante la premura de tiempos (recordemos las 72 horas naturales para notificar a la AEPD, así como todos los procesos de comunicación con afectados y grupos de interés, entre otros).



3.2.1 Activación del plan

Activa tu plan de gestión con premura, como si fuera una crisis interna.

En la gestión de las brechas de datos personales, desde el momento en que se ha concluido que el incidente es constitutivo de brecha, es determinante la premura de tiempos (recordemos las 72 horas naturales para notificar a la AEPD, así como todos los procesos de comunicación con afectados y grupos de interés, entre otros).

Activar el plan de gestión de brechas previsto debería incluir:

- Recopilación y análisis de la información relativa a la brecha: la mayoría de los incidentes relacionados con la protección de datos a día de hoy, tendrán un importante componente tecnológico, en los que la información de herramientas automáticas será básica para el análisis posterior del incidente. Pero en todos los incidentes existe un factor humano, que hará necesario contactar con todos los usuarios finales, los que detectaron la brecha también, los proveedores, los equipos de negocio y de sistemas, para recopilar toda la información posible.

- Clasificación del incidente: 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 la clasificación del incidente dependerán las acciones a emprender durante los procesos de gestiona y notifica.

- Es especialmente importante determinar si efectivamente se está ante una brecha de datos personales, en cuyo caso es imprescindible evaluar las consecuencias que puede causar el incidente a los derechos y libertades de los afectados, determinando con el mayor grado de precisión posible el nivel de perjuicio 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 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, quién 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 proceso de notificación, empezando por una valoración de notificación temprana a la autoridad de control competente y a los afectados y, en caso necesario, a fuerzas de seguridad.

- Y documentarlo todo, de forma que en cada fase tengamos acceso fácil a toda la información necesaria, que habremos recopilado y analizado. Siendo recomendable el formato de cuaderno de bitácora, que nos permitirá además el seguimiento de la evolución temporal de la brecha y de la relación entre este y las medidas tomadas en cada momento.

Mario Andretti: "Si sientes que todo está bajo control, es que no vas lo suficientemente rápido".

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

- Desconectar inmediatamente de la red corporativa todo ordenador que se sospeche que esté infectado con algún tipo de malware. Mantenerlo aislado con el fin de realizar un análisis forense más tarde.
- 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.

3.2.2 Contención del incidente

En la fase de contención se tratará de limitar en lo posible los daños causados por el incidente, poniendo en marcha el plan de respuesta, si lo tenemos preparado de Planifica, especialmente en cuanto en las primeras medidas de contención. Y complementándolas con aquellas que se puedan definir en cada momento. Estas medidas proporcionarán un margen de actuación para poder desarrollar una solución definitiva adecuada sin el factor tiempo.

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.

3.2.3 Erradicación

Contener un incidente significa que dejen de producirse sus efectos adversos, pero tras la contención, la erradicación puede ser necesaria para eliminar por completo su origen; como, por ejemplo, eliminar un malware o mitigar las vulnerabilidades identificadas la gestión del incidente. Estas fases no están perfectamente diferenciadas y es habitual que haya cierto solapamiento entre ellas.

Tan importante como contener es erradicar, y evitar que el incidente se propague o se repita.

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.

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

En la fase de erradicación 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 análisis de riesgos de la entidad afectada revisando si el mapa de riesgos contemplaba la amenaza que 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 si existe. Pero antes será necesario realizar las medidas de recuperación que se describen a continuación.

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.

3.2.4 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.

¿Has mirado si el mapa de riesgos contemplaba la amenaza que dio lugar a la brecha de seguridad? Si no, actualiza. Si no sabes de qué hablamos, realiza un análisis completo cuanto antes.

Esto puede implicar la adopción no solo de medidas activas, sino también la implementación de 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.

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.

3.2.5 Proceso de notificación

Aunque por su especial dimensión desarrollemos la notificación a la autoridad de control y la comunicación a los interesados en el siguiente apartado, para dotarlo de la relevancia que requiere, no debemos olvidar que se trata de una fase más de la gestión de los incidentes, que se debe englobar dentro de su ciclo de vida.

Nunca esperes a reportar una brecha a que se haya dado por solucionada. Será demasiado tarde.

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 datos personales a las autoridades de control y, en determinados casos, comunicación a los afectados. Dicho procedimiento podría incluir detalles sobre cómo deben escalarse las notificaciones internamente y quiénes son las personas encargadas de realizar cada una de las acciones dentro de la organización.

4 NOTIFICA

Un momento crucial en el ciclo de vida de una brecha de datos personales es la decisión de si es necesario notificar, o no, a la Autoridad de Control. Pero también deberemos acometer la comunicación a las personas físicas interesadas, cuando sus datos personales se hayan podido ver afectados y fuera probable que la brecha entrañe un alto riesgo para sus derechos y libertades. Por último, sopesaremos la comunicación a otras administraciones y organismos posiblemente involucrados en su gestión y/o resolución, así como a otras partes implicadas como accionistas, proveedores, socios de negocio, etc.

4.1 Notificación a la Autoridad de Control - AEPD

No toda brecha de datos personales se debe notificar a la Autoridad de Control, recordemos que en su propia Guía para la notificación de brechas de datos personales la AEPD recuerda que: "se notificará, cuando sea probable que la brecha constituya un riesgo para los derechos y libertades de las personas".

En el Anexo B de las directrices WP250[3]. se pueden encontrar algunos ejemplos sobre la valoración de la necesidad de notificar a la Autoridad de Control, y en las Directrices 01/2021 sobre ejemplos relativos a la notificación de brechas de datos personales se expone una colección muy completa de ejemplos.

[3]De dicha directriz queremos destacar esta reflexión, sobre los datos de estado de salud, pues hay una creencia generalizada de que en cuanto hay un dato de salud ya es una brecha notificable y creemos que esto no siempre es así.

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

Pero recientemente, en la Directriz 01/2021 precisamente indica algunos casos donde según el tipo de dato de salud afectado se puede considerar o no brecha notificable (ie no es lo mismo que sepan que tienes una alergia al gluten que el que padeces un cáncer o que estás en tratamiento psicológico). Debemos tener muy en cuenta el cómo puede llegar a afectar a la esfera personal, profesional o social de esa persona donde un dato relativo a psicología puede llevar a que esa persona no quiera salir de su domicilio, no encuentre trabajo fácilmente, deba cambiar su domicilio, etc...

Por tanto, si hay un riesgo improbable o limitado no es necesario notificar a la Autoridad de Control, pero en modo alguno podremos basarnos en una mera apreciación subjetiva, sino que deberá estar fundamentado en el análisis de riesgos y evaluación de Impacto que previamente tendríamos que haber realizado, como desarrollaremos en el anexo III de esta guía. Sin embargo, ante cualquier atisbo de duda sobre las conclusiones alcanzadas en los análisis de riesgos, nuestra recomendación será siempre notificar la brecha de datos personales, dada la especial relevancia de la transparencia cuando hablamos de riesgos para los derechos y libertades de los afectados, siempre prioritarios frente al riesgo a ser sancionado o riesgos reputacionales para nuestras organizaciones.

Ante la duda, preventivamente mejor notifica tu brecha de datos personales.

Como hemos venido destacando hasta ahora en la Guía, para evaluar el impacto o riesgo sobre dichos derechos y libertades de las personas físicas afectadas, también será fundamental la revisión de la actuación de las organizaciones responsables de los tratamientos, tanto antes como después de producida la brecha, y en concreto:

- Si el responsable ha tomado previamente medidas técnicas y organizativas adecuadas que eviten los riesgos anteriores, minimicen los daños a los derechos y libertades y/o los hagan reversibles; y
- Si el responsable ha tomado con posterioridad a la brecha de datos personales las medidas de protección que mitiguen total o parcialmente el posible impacto para los afectados y garanticen que ya no hay posibilidad de que el alto riesgo para sus derechos y libertades se materialice. Por ejemplo, mediante la identificación y puesta en marcha inmediatamente de medidas como la revocación, cancelación o bloqueo de credenciales de acceso o certificados digitales comprometidos, o mediante el restablecimiento de los servicios y copias de seguridad de los datos de forma que no puedan comprometerse otros datos personales.

Una vez determinada la necesidad de notificar a la Autoridad de Control, lo que hay que identificar es la Autoridad de Control a la que realizar dicha comunicación.

Criterios de especial incidencia para determinar el riesgo de posible afección a los derechos y libertades de las personas:

-Tipo de brecha de datos personales.

-Naturaleza, carácter sensible y el volumen de datos personales.

-Facilidad de identificación de las personas.

- Gravedad de las consecuencias para los derechos y libertades de las personas.
- Probabilidad de que se materialicen las consecuencias para los derechos y libertades de las personas afectadas.
- Características particulares del responsable de tratamiento.
- Número de personas afectadas.
- Impacto: Nulo, interno/controlado, externo (entorno proveedor), público (internet) o desconocido.
- Consideraciones generales.

Esto es especialmente relevante cuando un incidente pueda afectar a los datos de personas en más de un Estado miembro. En estos casos, 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 notificar, como mínimo, 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.

El Comité Europeo de Protección de Datos, EDPB por sus siglas en inglés, ha publicado las Directrices 9/2022[4] sobre la notificación de brechas de datos personales con sujeción al RGPD. El EDPB muestra también una lista de ejemplos no exhaustivos que ayudarán a los responsables del tratamiento a determinar si deben notificar en diferentes escenarios de brecha de datos personales, y les ayudarán también a distinguir entre riesgo y alto riesgo para los derechos y libertades de las personas.

La Guía para la notificación de brechas de datos personales publicada por la AEPD amplía y detalla los plazos y aspectos concretos sobre el procedimiento para notificar y el contenido de las notificaciones, por lo que recomendamos su estudio y seguimiento en cuanto a las directrices ahí fijadas.

Utiliza la guía de la AEPD para saber cómo notificar, sigue los pasos.

[4] https://edpb.europa.eu/our-work-tools/documents/public-consultations/2022/guidelines-92022-personal-data-breach_en

4.2 Comunicación a los interesados

En cambio, contrastando con el espacio y concreción que la citada Guía de la AEPD dedica a la notificación a la autoridad de control, es mucho menor el que reserva para la comunicación a las personas físicas afectadas.

Por eso, más allá de lo dispuesto en el artículo 34 del RGPD, las organizaciones deberán definir los procedimientos que se seguirán para decidir si una brecha ha de ser comunicada o no a las personas físicas afectadas.

Conforme al referido artículo 34 del RGPD, para evaluar la comunicación debemos tener en cuenta, **tanto el alto riesgo para los derechos y libertades de los afectados como una combinación de la probabilidad de que sucedan hechos que supongan efectos negativos para estos y el impacto o severidad que tendría de ser así.** No hay que olvidar que en este punto el incidente ya ha sucedido, pero es posible que todavía no haya tenido impacto en los afectados.

La severidad se materializa en **riesgos de exclusión, marginación social, dificultades financieras tales como deudas importantes, imposibilidad de trabajar o encontrar trabajo o pérdida de empleo, dolencias físicas o psicológicas a largo plazo, empeoramiento de la salud, muerte, estrés, miedo, acceso a servicios comerciales,** que pueda experimentar como consecuencia de la brecha. Podemos partir de la nueva guía de la AEPD, de junio de 2021, para la ***"Gestión del riesgo y evaluación de impacto en tratamientos de datos personales"***, para definir los riesgos a tener en cuenta en cada caso.

Sin perder este foco, necesitaremos tener en cuenta diversas variables principales en la evaluación, que hemos tomado de la experiencia de las brechas de datos personales que hemos ido evaluando en nuestras organizaciones así como de la base teórica que nos aportan el Informe de ENISA "***Recommendations for a methodology of the assessment of severity of personal data breaches***", de Diciembre 2013, y el artículo 3.2 del Reglamento 611/2013 que provee guías en la notificación para el sector de servicios de comunicación electrónica.

Con todo esto, hemos formulado en el Anexo III de la Guía, al que nos remitimos, la propuesta de una posible metodología para incluir la Gestión de Brechas en los preceptivos análisis de riesgos para los derechos y libertades de los interesados, así como, si fuese necesario realizarlas, en las Evaluaciones de Impacto. Metodología que también nos servirá para realizar el análisis de riesgos para los derechos y libertades de los interesados una vez materializada la brecha concreta.

En esta línea y siguiendo también con lo destacado en el capítulo anterior de Planifica, de la importancia de aprender a identificar una brecha de datos personales, para poder hacer una correcta valoración y análisis de riesgos sobre los derechos y libertades de las personas físicas, estas son las variables que siempre debemos tener en cuenta:

Tipología de brecha

Confidencialidad, integridad, disponibilidad, no repudio y mixta.

Lo habitual hasta ahora es que las brechas estén relacionadas con la confidencialidad, a continuación, la disponibilidad y por último la integridad. Pero hay que tener en cuenta las circunstancias de cada caso (p. ej. si se pierde un resultado médico o se borrad un historial clínico es mucho más severo para el riesgo físico y vital de esa persona que el que dicho dato médico cayese en manos de un tercero por error).

El no repudio o la auditabilidad es otra dimensión nueva que emerge a raíz del deber de diligencia donde la carga de la prueba ahora está en las compañías.

Tipo de datos y su combinación

A veces una combinación de datos básicos y de contacto puede ser mucho más delicada que los datos de carácter especialmente protegido, lo que ha de tenerse también en cuenta en el análisis del riesgo para los interesados.

El robo de datos de contacto puede allanar el camino para que se contacte con el interesado y se realicen fraudes, conocer la dirección física puede conllevar riesgos de robo, agresiones, etc. y además es más complicado de contener que si el robo es de una dirección de mail, ya que no cambiamos tan fácilmente de domicilio. Hemos podido ver que, en ocasiones, el robo de dichos datos básicos y de contacto pueden ser más peligrosos para los derechos y libertades de los afectados que si se tiene acceso a datos del estado de salud, sin otro contexto mayor. Lo importante es lo que revelan sobre la identidad de esa persona, no el tipo de dato en sí.

Tipo de colectivos

Si entre los datos hay información de clientes que pueden ser menores de edad, o pertenecen a colectivos más desfavorecidos o en riesgo de exclusión, tercera y cuarta edad, víctimas de violencia de género, etc. en estos casos toda la muestra de datos se considerará como más sensible y más severa que si solo hay datos de otros tipos de clientes. Los empleados nos merecen una especial sensibilidad y, por tanto, a estos efectos, y sobre todo si hubiera datos de sus familiares, los consideramos como un colectivo de riesgo más vulnerable.

Volumen de registros

Obviamente el volumen de registros "con datos personales" afectados, que no el número de afectados/personas, ya que aquí lo que nos prima es evaluar el alto riesgo que puede conllevar en una sola persona natural o física. Que eso afecte a 100, o 10.000 afectados más, a título individual no lo vemos relevante para esta evaluación. Sí lo es el número de registros sobre esa persona.

Riesgo de identificación electrónica

Como dice el RGPD, dato personal es también aquel que te hace fácilmente identificable. Por tanto, debemos evaluar si públicamente es fácil obtener más información sobre ese conjunto de datos que lo haga identificable. Incluso el tipo de apellidos comprometidos es muy importante aquí (no es igual comprometer el apellido Pérez o López que un apellido que apenas tenga coincidentes).

Aquí también es importante la aplicación o no de técnicas de pseudonimización como es el uso de algoritmos de hash robustos (MD5 o SHA1 ya no lo son) y sobre todo que las llaves de cifrado o descifrado no hubieran resultado comprometidas.

Riesgo de identificación física

De cara a la esfera de afección a las relaciones sociales, muy importante a la hora de evaluar el alto riesgo de afección a los derechos y libertades del individuo, debemos tener en cuenta aspectos como el grado de notoriedad pública de esas personas, pero no solo esto, sino también criterios demográficos como si la persona que ha recibido la información erróneamente vive en el mismo código postal que el afectado, el tamaño de dicha localidad en sí.

Intencionalidad

La intencionalidad de la persona que ha cometido un error o no y la intencionalidad de quien ha recibido una información personal es decisiva para determinar el alto riesgo a los afectados. Si la persona, y más si es un empleado interno o un exempleado, creemos que ha cometido la brecha intencionadamente puede suponer un alto riesgo.

En cuanto al receptor de los datos, si simplemente nos avisa del error y procede a eliminarla sin más, es muy distinto a si el receptor empieza a solicitar una indemnización a cambio de no publicar ese dato, si lo ha cifrado y pide un rescate por ello, o si dice que ya lo ha difundido.

Tipo de receptor y sujeción previa a confidencialidad

Imaginemos que la brecha de confidencialidad se produce porque se envía unos datos incorrectos a quien no se debe. Si eso datos llegan a otro departamento o, empleado o a un proveedor con el que tengo un contrato firmado, que incluye cláusulas de confidencialidad, y por tanto hay una relación contractual podré solicitarle que por favor lo elimine. Si ese dato llega a un cliente distinto, empieza a ser más delicado, y si llega a un extraño o a un lead/referencia con la que no tengo nada firmado, el riesgo es mayor.

Tratamiento de datos afectado con relación al tipo de Responsable

Si el tratamiento afectado se considera un tratamiento a gran escala por parte del responsable o encargado o una actividad principal y nuclear del mismo, el riesgo es mucho mayor porque el caso que hayamos detectado puede ser solo la punta del iceberg, aflorando una situación mucho más delicada y estructural en la compañía. Además, denotará que la compañía no ha sido diligente anticipando los riesgos como se debería. Esta variable no determina si una situación es o no brecha, solo indicamos que ayuda en la ponderación del riesgo de materializarse y en su contención.

Si es un proceso residual se podrán tomar medidas de contención más ágiles para controlar la posible brecha.

Medios de materialización de la brecha

El contexto en que ocurre o vector de ataque hace variar el riesgo. No es lo mismo que un dato se revele en un entorno de fase de pruebas de desarrollo informático a un programador externo que no debería haber datos de clientes en entorno de pruebas o preproductivo que el origen de la brecha sea por un ciberincidente del tipo phishing, virus, hacking, malware, APT, etc.

Duración

Si durante el análisis se determina que la duración del incidente es de apenas horas o días, es mucho menor el riesgo que si el incidente data de meses o años atrás o incluso si somos incapaces de determinar este hecho.

Estado de control sobre la información

Si hay pérdida de control sobre la información (internet profundo, redes sociales, prensa digital, etc.) el riesgo para los afectados es mucho mayor que si la información está controlada.

Desde luego, si sabemos a quién llegó la información podemos controlar mucho mejor qué puede llegar a hacer con ella y por lo tanto el riesgo siempre será menor.

Desde luego, si la información está cifrada o codificada de algún modo que haga muy complejo su descifrado es determinante para valorar si se trata de una brecha notificable o solo un incidente de seguridad.

Calidad y perfilado de las bases de datos

No es lo mismo que se obtenga una base de datos sin cualificar, que pueda contener datos inexactos o incompletos o no actualizados que otra que haya sido actualizada recientemente.

Del mismo modo, el perfilado es muy importante para determinar colectivos concretos, que pueden venderse más fácilmente en el Internet profundo, a la competencia, etc. Si la base de datos está sin segmentar que la pérdida o el robo vaya dirigido a una base de datos perfilada y que pudiera tener un alto valor o simplemente un alto riesgo para los afectados (ej.: una base de datos con todos los vacunados en una CCAA no es lo mismo que robar los datos de los clientes que han contratado el último mes una póliza de seguro o comprado un servicio cualquiera).

Auditabilidad, trazabilidad de logs y no repudio

A la hora de evaluar la severidad y de catalogar el incidente en muchas de las anteriores variables, es fundamental que las organizaciones tomen las medidas de seguridad acordes al riesgo de ese tratamiento y en concreto, es muy importante que las organizaciones cuenten con los logs suficientes, entendibles y no manipulables como para reproducir lo sucedido y poder guardar evidencias que corroboren los hechos, y tomar medidas acordes. Si una compañía no cuenta con ese log, no es capaz de reproducir lo sucedido, y determinar la identidad, fecha y hora del suceso, el riesgo para el afectado puede ser mucho mayor, ya que es más complicado hacer reversibles los efectos y tomar medidas eficaces.

Reversibilidad de los efectos

De cara a la esfera de afección a las relaciones sociales, muy importante a la hora de evaluar el alto riesgo de afección a los derechos y libertades del individuo, debemos tener en cuenta aspectos como el grado de notoriedad pública de esas personas, pero no solo esto, sino también criterios demográficos como si la persona que ha recibido la información erróneamente vive en el mismo código postal que el afectado, el tamaño de dicha localidad en sí.

4.2.1 Formas y plazos para comunicar

Cuando la brecha de datos personales 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 la brecha de seguridad, sin dilación indebida.

Monitoriza bien el proceso de comunicación.

Para ayudar a la toma de decisión sobre la comunicación o no a los afectados, se puede hacer uso de la herramienta Comunica-brecha de la Agencia Española de Protección de Datos[6].

Como se ha comentado anteriormente, la herramienta es una ayuda a la toma de decisión, pero la misma debe ser tomada por el responsable del tratamiento de los datos que han sufrido la brecha, tal y como se detalla en el artículo 34 del RGPD.

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

En las antes referidas Directrices 9/2022, sobre la notificación de brechas de datos personales con sujeción al RGPD, establece el EDPB que dicha comunicación debe realizarse de manera aislada, por separado de otro tipo de comunicaciones, usando los máximos medios posibles incluyendo la mensajería directa (correo electrónico o SMS), y realizarla en el lenguaje del Estado en el que reside el interesado.

En todo caso esta debe realizarse en un lenguaje claro y sencillo, usando los datos que consten en los sistemas del Responsable debidamente facilitados por el afectado, mediante medios seguros y siempre en estrecha cooperación con la autoridad de control y las autoridades policiales, de acuerdo con sus orientaciones.

Preferentemente, la comunicación 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. El canal por el que se haga podrá variar según el volumen de afectados.

[6] https://www.aepd.es/en/guides-and-tools/tools/comunica-brecha-rgpd

Si comunicas a los afectados, usa medios fehacientes (graba las llamadas, envía correos electrónicos con acuse de lectura, envía correo postal certificado) deja evidencia del qué, del cómo y a quién has comunicado.

En el caso de una sola persona o muy pocas, llamar por teléfono es lo más recomendable, si bien siempre se debe enviar la explicación por escrito y a ser posible con acuse de entrega y lectura. Habrá pues que estar atentos a devoluciones de mensajes por fallos de entrega, direcciones de correo incorrectas y sobre esos casos, pensar otras alternativas.

4.2.2 Notificaciones indirectas

Una de las últimas vías que contemplamos es la de la notificación indirecta. Hay diversas formas y esto siempre será debido a que se desconocen los datos de contacto o se tiene seguridad de que los datos de contacto no están actualizados.

Evita, salvo que no veas otra solución, la notificación indirecta (hacerlo público), parece la vía más rápida pero no siempre es la más certera.

Si esto es así, y decidimos hacerlo público, podemos o bien usar canales telemáticos como nuestra web o webblog o incluso redes sociales en los perfiles o bien podemos utilizar el canal más tradicional del envío postal o el comunicado de prensa/aparición en prensa o radio.

- Medios Telemáticos: Para ello preferiblemente es aconsejable un video o mensaje de no más de dos minutos del máximo representante de la compañía y que ocupará un lugar destacado en la página web o blog, de forma que en ningún caso pueda pasar desapercibidos, no puede estar ni a un solo nivel de profundidad en la navegación.

  La compañía además debe monitorizar las visualizaciones de ese video, su apertura completa o parcial, si es compatible e interoperable con todos los navegadores principales.

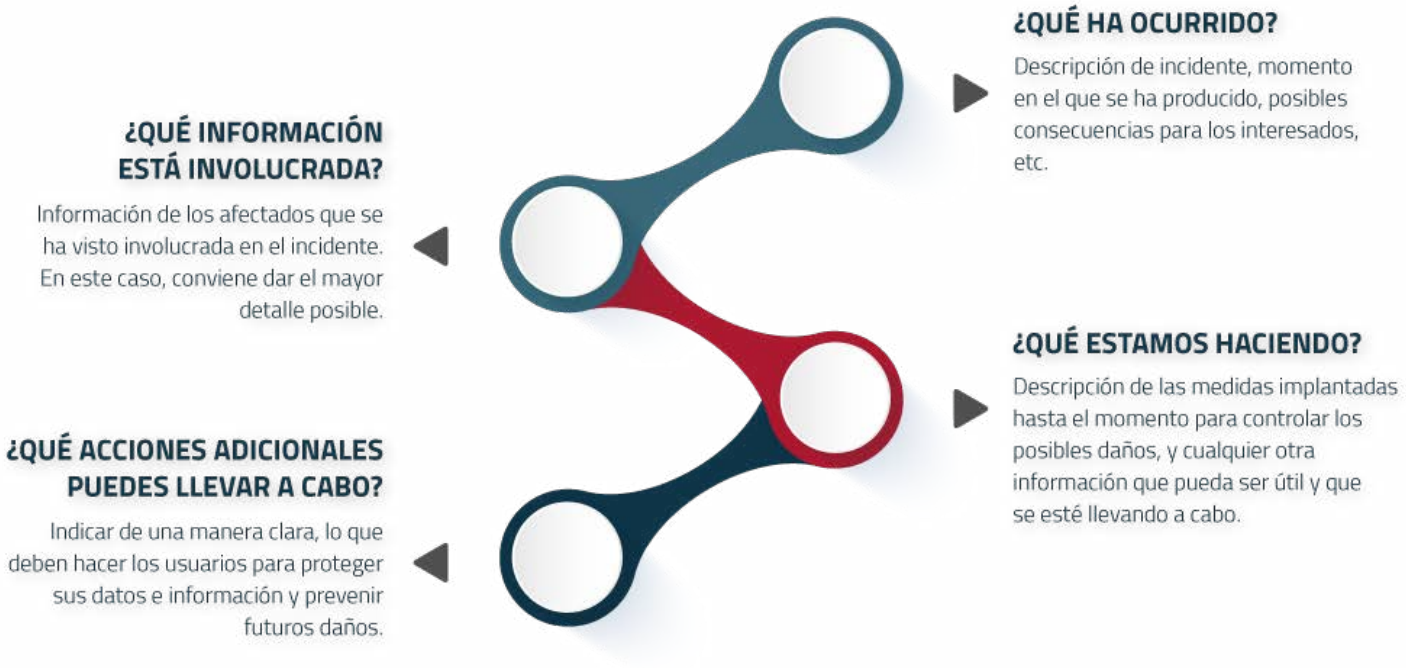
- Según el perfil de los afectados, la compañía no debe descartar los comunicados de prensa o radio (i.e., si tenemos un colectivo de personas muy mayores afectadas y sin acceso a internet probablemente) o a la dirección postal, con notificación de entrega certificada. Estos medios son más costosos, pero volvemos a la idoneidad de contar con una póliza ciberriesgo ya que este tipo de costes son cubiertos por las aseguradoras.

4.2.3 Contenido de la comunicación a los afectados

Toda comunicación a los afectados debe tener un contenido mínimo en el que se detalle lo acontecido.

Utiliza un lenguaje claro acorde al público al que se dirige.

Como ejemplo, una comunicación a los afectados puede estar dividida en 4 partes:



Además, es necesario informar los datos de contacto del DPD, o en su caso, del punto de contacto en el que pueda obtenerse más información.

4.2.4 Supuestos de no comunicación a afectados

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.

Asimismo, no será necesaria la comunicación a los afectados cuando:

- El responsable ha tomado con anterioridad a la brecha medidas técnicas y organizativas adecuadas, como, por ejemplo, que la información esté seudonimizada.
- El responsable ha tomado con posterioridad a la brecha de datos personales las medidas de protección que mitiguen total o parcialmente el posible impacto para los afectados y garanticen que ya no hay posibilidad de que el alto riesgo 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. 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 datos personales considerando el alto riesgo potencial, la Autoridad de Control podrá exigirle: (i) que lo comunique; o (ii) podrá decidir que se cumpla alguna de las condiciones mencionadas para que la comunicación a los afectados no sea obligada.

Si no es necesario realizar la comunicación, se debe dejar por escrito, haciendo un informe en el que se detalle el porqué de la no notificación a los afectados, de cara a disponer de evidencias claras sobre la decisión.

4.3 Otros reguladores

Además de la notificación a las diferentes Autoridades de Control en materia de protección de datos que pudiese ser necesario realizar, es posible que para determinados sectores de actividad (operadores de servicios de comunicaciones electrónicas, prestadores de servicios de confianza, operadores de servicios esenciales, proveedores de servicios digitales, operadores de telecomunicaciones, prestadores de servicios de la sociedad de la información, compañías aseguradoras, servicios financieros, etc.), existan también obligaciones de comunicación y/o notificación ante determinados incidentes de seguridad (haya o no afectación de datos personales) a otras autoridades o reguladores con competencias en la materia, como podría ser el caso de las CSIRT, INCIBE-CERT, CCN- CERT, etc.

Además, en el ámbito del sector público el organismo que tiene asignado el papel de coordinador en materia de respuesta a incidentes de seguridad es el CCN y CCN-CERT.

A lo que hay que añadir la Oficina de Coordinación de Ciberseguridad: empresas prestadoras de servicios y que deben cumplir con la Directiva NIS (Real Decreto 43/2021, de 26 de enero, por el que se desarrolla el Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información).

Es importante tener en cuenta las sinergias entre todas las obligaciones de notificación y realizar estas de manera coordinada, coherente y sin que supongan, en la medida de lo posible, duplicidades en cuanto a la carga de trabajo para los equipos.

4.4 Terceros: encargados, ciberseguros

En cuanto a otras organizaciones terceras a las que pueda ser necesario notificar una brecha de datos, uno de los casos más importantes son aquellos clientes para los que nuestra compañía ejerza de **Encargado del Tratamiento**. En estos casos las obligaciones de comunicación y plazos vendrán regulados en la relación contractual. La transparencia y la información facilitada a nuestros clientes en tiempo y forma podrá ser definitoria para la evolución futura de la relación cliente-proveedor, desde una mejora de imagen por la adecuada gestión de la brecha hasta que se pueda considerar un incumplimiento contractual penalizable por su parte.

Es importante tener escrita la metodología de comunicación con estos clientes, y un plan de comunicación periódico que muestre en todo momento la situación de sus datos. Además, la información debe cubrir los mismos parámetros que la notificación a la AEPD, puesto que es probable que este cliente, como Responsable de Tratamiento, precise de nuestra información para a su vez cumplir con sus obligaciones de notificación de forma adecuada.

En cuanto a **nuestros proveedores** también es importante, sobre todo si están participando en alguna parte del proceso afectado, informarles de la misma. Si por algún motivo tus equipos informáticos estuvieran infectados y el proveedor remotamente se conectase a los mismos, puede verse afectado por riesgos como suplantación de identidad en las comunicaciones o escalada de privilegios en paralelo.

Avisa a tus proveedores para que estén al corriente de los hechos y te ayuden a contener la brecha o a definir su alcance.

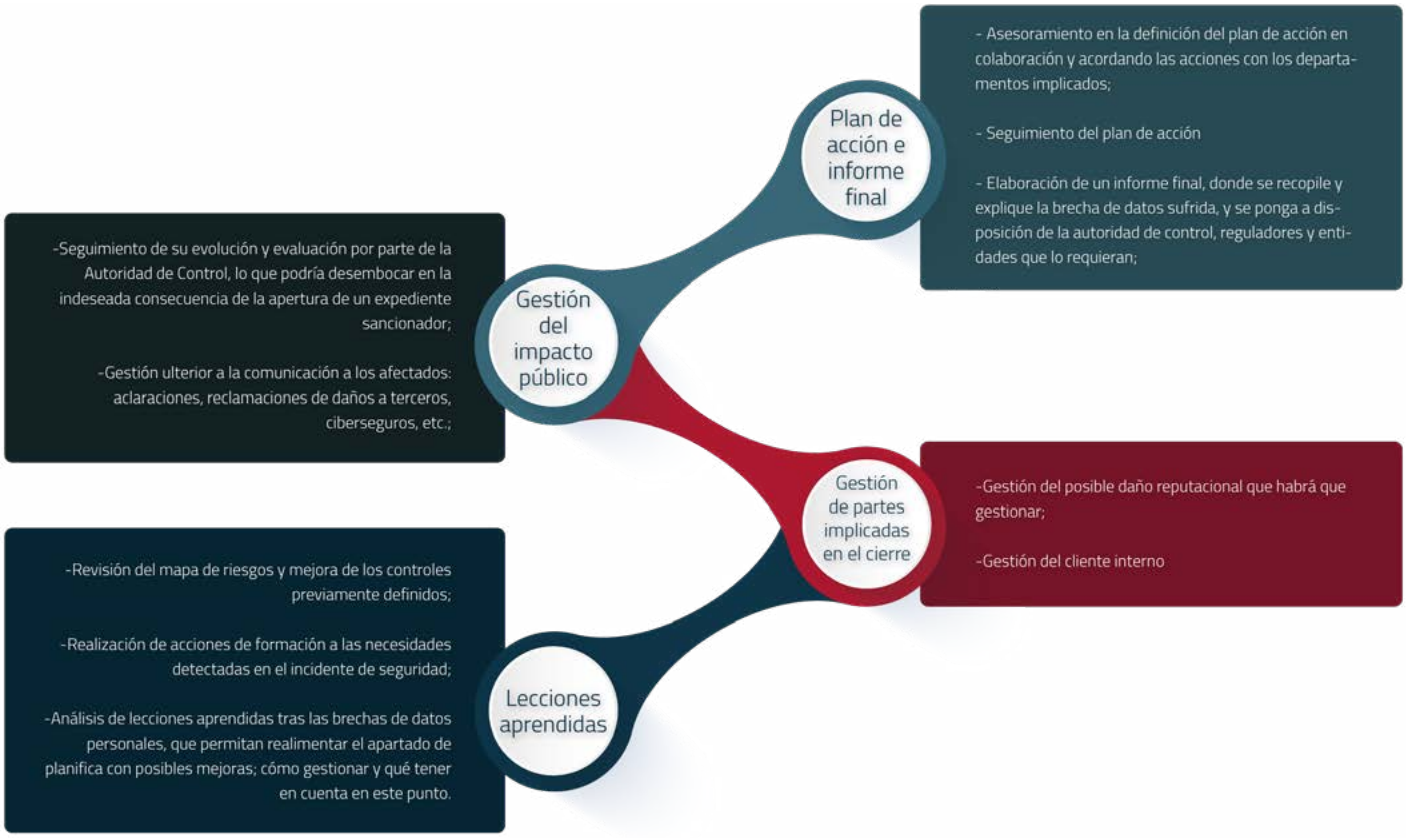
Los **ciberseguros** siguen creciendo exponencialmente y no debemos olvidar que es posible que sean otros terceros con los que probablemente debamos mantener una comunicación fluida durante la brecha sobre todo si tenemos incluidos servicios de soporte en caso de incidentes. Es imprescindible informar cuanto antes para que se analice si el seguro cubre los efectos de la brecha y alcance, para que abran expediente sobre el tipo de brecha sufrida. Y en todo momento habrá que informar de la evolución de la brecha y de los requerimientos de información que plantee la AEPD tras la comunicación y las respuestas dadas a los mismos.

La no comunicación en plazo y forma puede considerarse un incumplimiento de las condiciones de contratación del seguro y que se pierda la cobertura del mismo.

Otros terceros a los que hay que comunicar son las **empresas matrices**, sobre todo en las empresas multinacionales, puesto que es probable que haya que comunicar la resolución al DPD Global, siguiendo los procedimientos y políticas internas de cada empresa.

5 RESUELVE

El ciclo de vida de una brecha de datos personales no concluye con la notificación a la Autoridad de Control y la comunicación a los afectados, exigidas por el RGPD, sino que se extiende y complementa mediante una serie de acciones.



Una vez concluida la brecha de datos personales: saca conclusiones, haz seguimiento, corrige errores y elabora un informe final. Esto te ayudará a prevenir o paliar la próxima brecha.

5.1. Plan de acción e Informe final

Una vez gestionado el incidente de seguridad es recomendable definir un plan de acción dónde se definan una serie de acciones encaminadas a evitar que se repita el mismo incidente de seguridad y corregir posibles errores detectados. El DPD o la función de protección de datos tiene un rol fundamental a la hora de dar seguimiento a ese plan de acción y verificar que es adecuado y que se cumple en tiempo y forma. Si se requiere presupuesto para la remediación, la Dirección deberá dotarlo o asumir el riesgo de esa repetición, en función del nivel de apetito al riesgo de cada organización.

Además del Plan de acción, habrá que evaluar si se toman ciertas medidas extra, como, por ejemplo:

- Valoración de contratación de un análisis forense experto, ya que en determinados casos está justificado que la investigación sea conducida por un tercero 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.

- En muchas ocasiones las brechas son motivadas por actos delictivos que estamos obligados a denunciar o poner en conocimiento de la policía.

- Valoración de adopción de medidas procesales, 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, debiendo preverse los efectos de la difusión de la brecha.

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.

Resulta esencial que el responsable del tratamiento documente todas las actuaciones realizadas en relación con el incidente y/o brecha de seguridad, no solamente porque así lo indique el art. 33.5 RGPD sino sobre todo porque es la forma en que el responsable podrá demostrar y acreditar su diligencia y cumplimiento, ex. Art. 5.2. RGPD, en la propia gestión de la brecha. Además, dicha documentación permitirá a las Autoridades de Control verificar la actuación llevada a cabo por el propio responsable y a este el confeccionar y/o emitir un informe final de todo lo ocurrido.

En cuanto al **Informe final**, la propia Agencia Española de Protección de Datos viene recomendando su elaboración incluyendo la trazabilidad del suceso y su análisis valorativo, en particular, en cuanto al impacto final. Este informe final servirá de valiosa fuente de información de cara a alimentar el análisis y la gestión de riesgos para prevenir la reiteración de una brecha.

Una brecha similar será una reiteración que probablemente suponga una falta de diligencia sino podemos justificarla adecuadamente.

La Autoridad de Control podrá exigir que se aporte un Informe final como consecuencia de una siguiente notificación de brecha de datos personales, para contrastar por su parte que se han aprendido las lecciones necesarias, se han emprendido las correcciones y mejoras oportunas para prevenirlas y se han llevado a cabo las medidas comprometidas con dicha Autoridad de Control al tiempo de sufrirse la brecha original.

Además, el informe final servirá para recopilar toda la información y documentación relativa a la brecha de forma que se facilite su estudio y revisión por la dirección de la empresa y otras terceras partes implicadas. Para ello deberá incluir descripción, trazabilidad y análisis valorativo de todo lo acontecido en las diferentes fases de gestión de la brecha; así como de las diferentes medidas adoptadas antes, durante (o consecuencia directa del propio incidente y/o brecha) y después de la brecha.

Por lo que se recomienda disponer de la siguiente documentación:

- 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.

En este sentido, y a título de ejemplo, se aporta como Anexo II un modelo de informe final de cierre de la brecha.

5.2. Gestión de partes implicadas

–5.2.1. AEPD

Es fundamental realizar un seguimiento al menos quincenal de las brechas notificadas e informar a la AEPD ante cualquier requerimiento de información por su parte, o, de manera proactiva, siempre que consideremos que alguna novedad o nueva información pueda ser de interés para el proceso en curso. No debemos esperar a que nos pregunten por el estado de la brecha, debemos anticiparnos.

Para ello, podrá utilizarse el modelo de informe final del Anexo II u otro modelo estándar para el *reporting* y seguimiento de las acciones previstas por la organización y que previamente se han comunicado a la AEPD, así como de evolución de la brecha. Toda nueva información que a lo largo de la fase final de la brecha pueda suponer un cambio en el análisis de riesgos, debe documentarse y lanzar el proceso de modificación de nuestro plan de acción inicial.

Es importante que todas las áreas implicadas en la Gestión de la brecha reporten al DPD la información para tener un informe unificado y coherente de seguimiento, que permita conocer realmente tanto a la compañía como a la autoridad de control la situación real de la misma y su afectación o no a los derechos y libertades de los interesados. Es básica esta comunicación directa con las áreas de IT, de ciberseguridad, pera también de Negocio, Riesgos, Comunicación, Atención al cliente, etc. Entre la información a tener muy en cuenta está el número de afectados, los tipos de datos, si se ha verificado o no su exfiltración, la afección a las operaciones de la compañía, quejas o reclamaciones de los afectados recibidas o información de la compañía publicada en la Darkweb, entre otros.

–5.2.2. Personas físicas afectadas

No solo ha de informarse a los afectados durante la fase de notificación, si así resulta exigible o también si la compañía ha valorado que se debe informar aun no siendo necesario. También ha de tenerse en cuenta cuestiones sobre las personas interesadas en el cierre de la brecha.

Por una parte, será necesario analizar la respuesta de los interesados una vez han sido comunicados, y si se han presentado reclamaciones, individuales o conjuntas, que deberán gestionarse más allá del cierre de la propia brecha, como reclamaciones de daños o por incumplimientos contractuales.

Pero también realizar un seguimiento y apoyo a estos en cuanto a las medidas de reparación del daño sufrido, que como acción proactiva puede servir tanto de cara a reducir el impacto en la imagen de la empresa como adelantarse a requerimientos de cualquier organismo administrativo de control.

Una vez finalizada la gestión de la brecha, estas posibles acciones deberán ser gestionadas por otras áreas de la empresa como atención al cliente o legal, siguiendo el procedimiento estándar, pero con acceso a la documentación necesaria sobre la brecha y su gestión.

Y, obviamente, en las situaciones en las que se considere pertinente, habrá que tener en cuenta la pertinencia de una comunicación final a los afectados para informar del cierre de la brecha y de próximos pasos que se darán.

–5.2.3. Terceros: encargados, ciberseguros

Las necesarias notificaciones de información a terceros, como sucede con la AEPD y otros reguladores, no finalizan con la notificación inicial, sino que durante la gestión y cierre de la brecha, habrá que tener en cuenta la información que a cada uno de estos interesados deberemos facilitar.

Entre estos terceros será importante comunicar el cierre de la brecha a aquellos clientes de los que seamos encargados, ya que esta información la necesitarán ellos a su vez dentro de su proceso de Resuelve interno.

E igualmente los ciberseguros han de recibir pertinente información desde los primeros momentos de acontecer la brecha, pero sobre todo en el cierre podrá requerírsenos más documentación o algún tipo específico de información que debemos estar preparados para aportar.

En caso de ser necesario realizar esta comunicación a otras partes, se preparará una comunicación detallada y dirigida específicamente a cada una de ellas, evitando realizar una comunicación general a todas, porque probablemente cada una tenga sus requerimientos.

5.3. Gestión del impacto público

Sin duda, el posible daño reputacional causado sobre la organización como consecuencia de la notificación de una brecha, es uno de los riesgos que este tipo de incidentes genera para la propia compañía, y que también habrá que administrar y reparar, tomando medidas de reducción o mitigación desde las áreas más dedicadas a la comunicación, imagen de marca e inclusive negocio.

Sabes que si hay una sanción tras la brecha se hará pública en el portal de la AEPD, anticipa que respuesta se debe dar alineada con la Dirección.

En función de cómo resuelva la AEPD la notificación de la brecha y de si la brecha se ha comunicado o no a los interesados, las acciones a llevar a cabo podrían ser distintas. Y probablemente se extiendan temporalmente bastante allá del cierre de la gestión de la brecha como tal.

–5.3.1. Comunicación interna: dirección, empleados, accionistas y socios

La comunicación a la dirección es fundamental durante todo el ciclo de vida del proceso de respuesta, y debe hacerse de 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 posiblemente los directivos serán preguntados por las acciones que se están llevando a cabo y posibles consecuencias.

También es recomendable ser transparentes con nuestros empleados publicando una nota informativa en la intranet corporativa o por correo electrónico informando de lo sucedido. Nuestro plan de formación y concienciación de privacidad debe contar con un apartado de lecciones aprendidas y cómo informar sobre estos incidentes.

Seamos transparentes con nuestros empleados, informémosles de las brechas internas y sobre todo comuniquémosle si sus datos están afectados. ¡Es cliente interno! La seguridad y la privacidad es responsabilidad de todos

La comunicación interna es muy importante porque va a demostrar la gobernanza de la privacidad en la compañía. Hemos hablado mucho de gestión y la palabra gobernanza o buen gobierno, que no se recoge ni en el RGPD, ni en nuestra Ley Orgánica 03/2018 de Protección de Datos, es clave con el principio de Responsabilidad proactiva.

En ocasiones, compartir esta información dentro de un mismo grupo empresarial establecido en distintos países y con distintas tecnologías, operativas, ayuda a detectar nuevos riesgos operativos, o simplemente ideas de mejora que ni siquiera habían advertido.

Debemos por tanto moderar el mensaje, en términos de generalizarlo, omitir datos personales identificativos para que pueda ser escalable en la misma compañía e idealmente incluso en la industria o sectores afines.

Especial cuidado con la circulación de la información de una brecha dentro de las organizaciones, o el detalle que se haga de ella, podría suponer o resultar a su vez en otra brecha de datos, de muy difícil justificación y podría suponer apertura de expediente sancionador.

5.4. Lecciones aprendidas

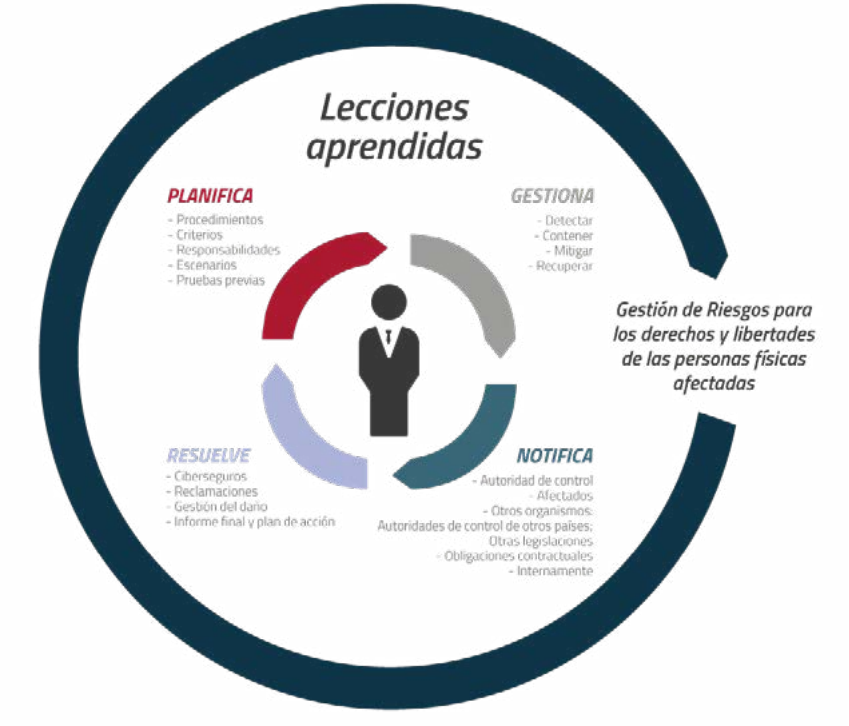
Partiendo del informe final de la brecha, y dentro de la diligencia debida, debería hacerse un ejercicio final de lecciones aprendidas, que permita conocer sobre todo lo que fue mal en la gestión de la brecha concreta o qué elementos son susceptibles de mejora. Y con esta información, siguiendo la filosofía del ciclo PDCA (Plan, Do, Check, Act) de mejora continua, se alimenta la fase de PLANIFICA con mejoras en procesos y procedimientos, planes de formación, nuevos casos de uso, etc.

Este ejercicio es recomendable hacerlo dentro de una reunión de cierre con todas las áreas implicadas, en la que además de los elementos subjetivos de evaluación, podrán estudiarse indicadores clave.

Pero, sobre todo, es imprescindible utilizar toda la información recopilada durante la Gestión de la brecha, para realimentar la fase de PLANIFICA en su apartado de análisis de riesgos, reevaluando riesgos conocidos, introduciendo otros nuevos, añadiendo o modificando controles.

Así mismo, e independientemente de lo que se haga para cada brecha concreta, una revisión anual con el Comité Directivo de todas las brechas de protección de datos o de los principales incidentes de seguridad, junto con el DPD y el CISO, para revisar los riesgos manifestados, cómo se han mitigado y los que quedan pendientes de abordar, nos dará la necesaria visión de conjunto para priorizar las tareas en base a los riesgos y prioridades de la compañía.

Toda la información recopilada durante la Gestión, Notificación y Resolución de una brecha de datos nos será de gran utilidad para para comenzar de nuevo a PLANIFICAR como nos enfrentaremos a la siguiente brecha.



ANEXO I

CUMPLIMIENTO NORMATIVO Y PROTOCOLOS INTERNOS DE ACTUACIÓN

Protocolos relacionados con cuestiones y actuaciones que compondrán el procedimiento de gestión y notificación desde la perspectiva de la anticipación diligente antes del incidente:

Cumplimiento normativo de protección de datos:

- **Reglamento (UE) 2016/679** del Parlamento Europeo y del Consejo, de 26 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 - **RGPD**.
- **Ley Orgánica 3/2018**, de 5 de diciembre, de Protección de Datos Personales y garantías de los Derechos Digitales - **LOPDGDD**.
- **Ley 34/2002**, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico - **LSSI.**
- **Ley 9/2014**, de 9 de mayo, General de Telecomunicaciones - **LGT**.
- **Ley 40/2015**, de 1 de octubre, de Régimen Jurídico del Sector Público y Real Decreto 203/2021, de 30 de marzo, por el que se aprueba el Reglamento de actuación y funcionamiento del sector público por medios electrónicos - Esquema Nacional de Seguridad - **ENS**.
- **Directiva NIS2 (UE) 2022/2555 del Parlamento Europeo y del Consejo de 14 de diciembre de 2022** relativa a las medidas destinadas a garantizar un elevado nivel común de ciberseguridad en toda la Unión, por la que se modifican el Reglamento (UE) nº 910/2014 y la Directiva (UE) 2018/1972 y por la que se deroga la Directiva (UE) 2016/1148 (Directiva SRI 2).

- ***Guías y herramientas de las Agencias Europeas de Protección de Datos***, en especial:

  o La Guía para la Gestión y notificación de brechas de seguridad publicada por la Agencia Española de Protección de Datos - AEPD.

  o Guía para la notificación de brechas de datos personales, de junio de 2021, de la Agencia Española de Protección de Datos - AEPD.

  o Gestión del riesgo y evaluación de impacto en tratamientos de datos personales, de junio de 2021, de la Agencia Española de Protección de Datos – AEPD.

  o Directrices 1/2021 sobre ejemplos de notificación de violaciones de la seguridad de los datos personales Adoptadas el 14 de diciembre de 2021, del Comité Europeo de Protección de Datos – EDPB.

  o Directrices 2/2022, de 14 de marzo de 2022, sobre la aplicación del artículo 60 del RGPD, del Comité Europeo de Protección de Datos - EDPB por sus siglas en inglés).

  o Directrices 9/2022, sobre la notificación de violaciones de datos personales con sujeción al RGPD, del Comité Europeo de Protección de Datos - EDPB.

  https://edpb.europa.eu/our-work-tools/documents/public-consultations/2022/guidelines-92022-personal-data-breach_en

  o Evalúa-Riesgo RGPD v2, ayuda para realizar los análisis de riesgos para los derechos y libertades de los interesados, de la Agencia Española de Protección de Datos - AEPD.

  o Comunica-Brecha RGPD, ayuda a valorar la obligación de informar a las personas físicas afectadas por una brecha de datos personales, de la Agencia Española de Protección de Datos - AEPD.

  o Asesora Brecha RGPD, ayuda a valorar la obligación de notificación, de la Agencia Española de Protección de Datos – AEPD.

Cumplimiento normativo de protección de datos:

El principio de accountability, u obligación de documentar cualquier violación de seguridad de los datos personales, según indican los artículos 33 y 35.5 del RGPD, quedara reflejada en los siguientes documentos internos:

- Registro de eventos.
- Informe de seguimiento (cuaderno de bitácora).
- Informe de resolución del incidente.
- Informe de la incidencia al DPO.
- Comunicación a la AEPD.
- Comunicación a los interesados.

Medidas procedimentales y jurídicas internas

- Política Global de Privacidad.
- Política de gestión de riesgos sobre Protección de datos.
- Procedimiento de actualización del Registro de Actividades de Tratamiento.
- Procedimiento de gestión Privacy by Design and by Default.
- Medidas de seguridad preventivas, organizativas y técnicas.
- Plan de Acción RGPD.
- Procedimiento de Notificación a la Autoridad de Control.
- Procedimiento comunicación a afectados.
- Sistema de Gestión de Seguridad de la Información (SGSI).

Deberes con responsables y encargados de tratamiento en relación

- Registro de tratamiento de datos.
- Registro de incidencias.
- Análisis de Riesgo y PIAS.
- Políticas organizativas de seguridad y códigos de conducta.
- Auditorias periódicas de seguridad.
- Auditorías de Protección de datos.
- Procedimientos y protocolos internos recomendables y con proveedores/ clientes.
- Análisis Gap respecto a lo estipulado en los contratos y acuerdos de encargo, así como tras las acciones de monitorización y control.
- Desarrollo de Plan de Acción, de respuesta y gestión de incidentes.
- Revisión de los modelos existentes.

Estos protocolos, además de tener que estar adaptados a las características de cada organización, deben plasmar las medidas preventivas incluyendo la implantación de una adecuada cultura ética y de riesgo.

Igualmente, tiene gran trascendencia la labor de concienciación y formación de todo el personal de la empresa que en el ejercicio de sus funciones acceda a datos personales.

ANEXO II

MODELO DE INFORME FINAL

Área/Departamento:

Delegado de Protección de Datos:

Fecha:

1. ANTECEDENTES

1.1. Breve resumen sobre el tratamiento o tratamientos impactados y sobre el proceso afectado por la brecha, que sirva para entender el posible impacto en los interesados.

2. IDENTIFICACIÓN DE IMPLICADOS

2.1. Responsable del Tratamiento

2.2. Encargado del Tratamiento o Encargados

2.3. DPD o persona de contacto

2.4. Persona que detecta el incidente de seguridad y área

3. SOBRE EL INCIDENTE

3.1 Descripción

3.1. Causa/as del Incidente y/o Brecha

3.2. Tipo de Brecha. Clasificación del Incidente

3.3. Tipo de brecha (C, I, D), taxonomía, origen amenaza, gravedad, volumen

3.4. Datos Afectados: tipología, volumen e impacto

4. ACCIONES Y/O MEDIDAS ANTERIORES AL INCIDENTE

4.1. Registro de Actividades de Tratamiento

4.2. Análisis de Riesgos o Evaluaciones de Impacto en Privacidad y/o Seguridad

4.3. Medidas de Seguridad Existentes (organizativas y/o técnicas)

4.4. Protocolos internos, PCN, etc.

4.5. Auditorías realizadas en materia privacidad y/o seguridad

4.6. Auditorías a encargados del tratamiento implicados

5. ACCIONES Y/O MEDIDAS TRAS DETECTAR EL INCIDENTE

5.1. Principales medidas técnicas de respuesta. Detección, Contención, Mitigación, Recuperación

5.2. Comunicaciones a Autoridades (en caso afirmativo, indicar cuáles). Incibe, CCN-Cert, AEPD, Denuncias FF.CC., Acciones judiciales, etc. [Justificar porqué se ha realizado o por qué no la notificación legal o tardía, especialmente]

5.3. Comunicaciones a interesados. Justificar porqué se ha realizado o por qué no

5.4. Otras Comunicaciones. Proveedores, empleados, Responsables del tratamiento si aplica, etc.

6. CRONOLOGÍA DE LA BRECHA

6.1. Resumen Cronológico (resumen de la bitácora de la brecha)

7. CIERRE O RESOLUCIÓN DE LA BRECHA

7.1. Plan de Acción. Medidas adoptadas como consecuencia del incidente y que permanecerán en el tiempo. Valoración de la implantación de dichas medidas de cara al cierre definitivo de la brecha

7.2. Lecciones aprendidas. Acciones adoptadas para explicar lo sucedido: reunión explicativa comité crisis, dirección, de seguridad, etc.

7.3. Resumen Valoración final. Nota valorativa sobre impacto, las acciones implementadas, resolución de la brecha, lecciones, etc.

7.4. Comunicación final Autoridades y/o Reguladores. Justificar porqué se ha realizado o porqué no.

ANEXO III

RELACIÓN DEL PROCESO DE GESTIÓN DE RIESGOS Y EVALUACIÓN DE IMPACTO DE LOS TRATAMIENTOS DE DATOS PERSONALES CON LA GESTIÓN Y ANÁLISIS DE LAS BRECHAS DE DATOS PERSONALES

Este apartado de la Guía busca ampliar la fase inicial de planificación de las organizaciones incorporando el análisis de las posibles brechas de datos personales al proceso de gestión de riesgos y/o evaluación de impacto de los nuevos tratamientos de datos.

Conviene recordar que la obligación que establece el art. 33 del RGPD para el responsable del tratamiento es de notificar a la autoridad de control una brecha de datos personales en los casos en los que sea probable que la misma constituya un riesgo para los derechos y libertades de las personas físicas afectadas. Adicionalmente, en el supuesto en el que se concluya que el riesgo es alto, también se deberá comunicar a los interesados.

Lo anterior implica que, una vez identificada la brecha de datos personales, el responsable del tratamiento tiene la obligación de estudiar el impacto que puede llegar a tener la misma en los derechos y libertades de las personas afectadas y, en caso de concluir que existe riesgo de afectación a los mismos, notificar la brecha a la autoridad competente.

Por otro lado, la Guía publicada por la AEPD relativa a la "Gestión del riesgo y evaluación de impacto de los tratamientos de datos personales" (LINK) recoge la necesidad de que la gestión del riesgo esté integrada con el resto de los procesos de la entidad y que no se realice de una forma aislada. En este sentido, incorpora como caso particular de gestión integral las obligaciones del responsable del tratamiento respecto de la notificación a la Autoridad de Control de las brechas de datos personales, así como la comunicación de estas a los interesados. Concretamente, se hace hincapié en que "gestión del riesgo y gestión de brechas son dos tareas que deben ser gestionadas de manera conjunta con el fin de evitar incongruencias que pudieran repercutir negativamente en el proceso de gestión de un tratamiento de datos personales o en los propios encargados".

Teniendo en cuenta todo lo anterior, este apartado busca proponer a los responsables del tratamiento un método que permita integrar el proceso de gestión de riesgos de los tratamientos con el procedimiento de gestión de brechas.

Proponemos incorporar un análisis del potencial impacto de una brecha previo al momento de detección de la misma, en el marco del proceso de gestión de riesgos y evaluación de impacto de los tratamientos de datos personales.

Los principales aspectos que se deberían analizar serían los siguientes:

- En primer lugar, estudiar qué factores de riesgo, inherentes al tratamiento, pueden suponer la materialización de una brecha de datos personales.
- Por otro lado, determinar qué consecuencias o daños y perjuicios se pueden derivar del tratamiento de datos teniendo en cuenta los factores de riesgo identificados.
- Por último, identificar qué derechos y libertades de los interesados pueden verse afectados por los daños que se pueden producir en el caso en el que tenga lugar una brecha.

1. Identificación de los factores de riesgo inherentes al tratamiento

El primer aspecto que se debe incorporar al análisis es determinar las posibles causas que podrían llegar a suponer la materialización de una brecha. Para ello, el responsable deberá identificar los factores de riesgo inherentes al propio tratamiento, entendidos como las fuentes que pueden propiciar la materialización de una brecha de datos personales que afecte en los derechos y libertades de los interesados.

Siguiendo lo dispuesto por la AEPD en la Guía previamente referenciada, una forma de determinar los factores de riesgo inherentes a un tratamiento de datos personales es adoptar como referencia la normativa y otras guías vigentes. En este sentido, el RGPD y sus normas de desarrollo, las directrices del CEPD y la propia AEPD han identificado un listado de posibles factores de riesgo que pueden ser inherentes a diferentes tratamientos de datos.

En el marco del proceso de gestión de brechas en el que se encuadra esta Guía, el enfoque del responsable debe ser el de determinar qué factores de riesgo pueden potencialmente implicar la materialización de una brecha. Sin embargo, conviene puntualizar que este análisis no exime al responsable de la necesidad de realizar un análisis de los factores de riesgo que puedan tener afectación sobre otro ámbito en el marco del proceso de gestión de riesgos y/o evaluaciones de impacto de los tratamientos de datos.

A continuación, se identifican los factores de riesgo especificados en las normas y guías anteriormente referenciados:

Factores de riesgo relacionados con la finalidad o propósito del tratamiento de datos
Perfilado
Evaluación de sujetos
Predicción
Control del empleado
Control del acceso a internet
Observación
Monitorización
Supervisión
Rastreo de contactos
Control físico de acceso
Localización
Identificación unívoca
Decisiones automatizadas sin intervención humana
Tratamiento automatizado para soporte a la toma de decisiones
Decidir sobre o impedir el ejercicio de derechos fundamentales
Decidir sobre el control del interesado de sus datos personales
Decidir sobre el acceso a un servicio
Decidir sobre la realización o ejecución de un contrato
Decidir sobre el acceso a servicios financieros
Efectos jurídicos sobre las personas
Evaluación y/o predicción de posibilidad de enfermedad/salud genéticamente
Conservación con fines de archivo

Factores de riesgo relacionados con las tipologías de datos utilizadas
Documentos personales
Información de aplicaciones de registro de actividades vitales
Aspectos personales
Preferencias de consumo, hábitos, gustos, necesidades
Rendimiento laboral
Situación económica
Estado financiero
Datos de medios de pago
Datos de comportamento
Datos de localización
Datos muy personales no recogidos en clasificaciones anteriores
Datos sanitarios
Datos biométricos
Datos genéticos
Categorías especiales de datos o que permitan inferirlos
Categorías especiales de datos seudonimizados
Datos personales relativos a condenas e infracciones penales
Metadatos
Identificadores únicos
Datos y metadatos de las comunicaciones electrónicas y datos inferidos de las comunicaciones electrónicas
Datos de navegación web

Factores de resigo relacionados con la extensión y alcance del tratamiento
Sistemático
Exhaustivo sobre las personas
Involucra a gran número de sujetos
La duración del tratamiento es elevada
La actividad de tratamiento tiene un gran alcance geográfico
Tratamiento a gran escala
Recopilación excesiva de datos con relación al fin del tratamiento

Factores de riesgo relacionados con la categoría de interesados
Menores de 14 años
Víctimas de violencia de género
Menores dependientes de sujetos vulnerables
Personas bajo guardia y custodia de víctimas de violencia de género
Mayores con algún grado de discapacidad
Personas mayores
Personas con enfermedades mentales
Discapacitados
Personas que acceden a servicios sociales
Sujetos en riesgo de exclusión social
Empleados
Solicitantes de asilo
Pacientes
Sujetos vulnerables

Factores de riesgo derivados de las condiciones técnicas del tratamiento
Sistema de información hospitalaria
TV interactiva
Servicios Web
Aplicaciones móviles
Sistemas de registro de localización
Reconocimiento facial
Huella dactilar
Internet de las cosas
Uso innovador o nuevas soluciones organizativas
Uso innovador de tecnologías consolidadas
Tecnologías combinadas con otras
Nuevas tecnologías
Alto grado de fragmentación de los actores que intervienen en el desarrollo e implementación de los productos/servicios que implementan el tratamiento
Tratamientos automatizados
Sistema inteligente
Videovigilancia

Factores de riesgo derivados de la recogida y generación de datos
Acceso a base de datos de referencia de crédito
Acceso a base de datos sobre fraudes
Acceso a base de datos sobre blanqueo de capitales o financiación del terrorismo
Datos personales obtenidos en zonas de acceso público
Recogida de datos de los medios sociales públicos
Recogida de datos de redes de comunicaciones
Recogida de datos de aplicaciones
Datos procedentes de dos o más tratamientos con finalidades diferentes
Datos procedentes de dos o más responsables distintos
Asociación de conjuntos de datos
Combinación de conjuntos de datos
Enlace de registros de bases de datos de dos o más tratamientos con finalidades o responsables diferentes
Recogida de datos por un responsable distinto al que trata y aplica excepción de información
Falta de transparencia del momento preciso de la recogida de datos
Nuevas formas de recogida de datos con riesgos para los derechos y libertades

Factores de riesgo derivados del contexto del tratamiento
Excede las expectativas del interesado
Posible reversión no autorizada de la seudonimización
Posible pérdida de control por el responsable de los datos procesados por el encargado del tratamiento
Podría determinar la situación financiera
Podría determinar la solvencia patrimonial
Podría deducir información relacionada con categorías especiales de datos
Pudiera privar a los afectados de sus derechos y libertades
Pudiera impedir el control sobre sus datos personales
Puede provocar exclusión
Puede provocar discriminación
Posible usurpación de identidad
Posible fraude
Posible daño reputacional
Posible perjuicio económico significativo
Posible perjuicio moral significativo
Posible perjuicio social significativo
Posible pérdida de confidencialidad de datos sujetos al secreto profesional
Podría impedir el ejercicio de un derecho
Podría impedir el acceso a un servicio
Podría impedir el acceso a un contrato
Podría recoger datos personales distintos de los usuarios de servicio
Posible manipulación de las personas
Posibilidad de autocensura
Posibilidad de provocar un cambio cultural para claudicar derechos y libertades
Usos imprevistos o no deseados que pudieran afectar a derechos fundamentales

Factores de riesgo relacionados con el contexto del responsable del tratamiento de datos
Sociedad de la Información
Empresa de biotecnología
Empresa de mercadotecnia
Hospitales
Investigadores privados
Entidad de evaluación de información crediticia
Entidad de evaluación de fraude
Entidad financiera
Empleador
Proyectos de investigación
Ensayos clínicos

Factores de riesgo relacionados con las comunicaciones de datos realizadas en el marco del tratamiento
Transferencia habitual a estados u organizaciones en otros países sin un adecuado nivel de protección
Falta de trasparencia de los actores involucrados en el tratamiento
Difusión libre de identificadores únicos

2. Análisis de las posibles consecuencias o los daños y perjuicios que podrían ocasionarse con motivo de una brecha en el marco del tratamiento

En segundo lugar, con el objetivo de estimar qué impacto podría tener una brecha de datos personales sobre los derechos de los interesados, es necesario identificar los posibles escenarios en los que se puede materializar una brecha y determinar sus consecuencias teniendo en cuenta los factores de riesgo previamente identificados.

Para ello, el responsable debería analizar las posibles consecuencias o los daños y perjuicios que se podrían ocasionar con motivo de una brecha de datos personales sobre los interesados en el caso en el que se materialice una brecha de datos personales. A continuación, se acompaña un listado orientativo de los potenciales daños y perjuicios para los derechos de los interesados o de las posibles consecuencias que podrían darse. Es relevante recordar que, en esta fase del análisis, el objetivo es determinar las consecuencias derivadas del hecho de que se materialice una brecha de datos personales.

Ha de tenerse especialmente en cuenta que esta evaluación debe realizarse en sentido amplio, teniendo en consideración también las posibles consecuencias que estén fuera del alcance del tratamiento analizado y del que la organización es responsable.

Por ejemplo, en el marco del estudio de una brecha de datos de confidencialidad que afecte al DNI, se podría incorporar la usurpación de identidad de las personas afectadas como posible consecuencia. Para valorar el alcance, no solo hemos de pensar en si con esos datos es posible que usurpen la identidad del afectado ante nosotros, sino también en si los datos afectados pueden ser utilizados en otros entornos o ante otros responsables con el mismo fin. Según los criterios que la AEPD está aplicando en sus procedimientos desde hace años, debemos evaluar si los datos exfiltrados sumados a otros más o menos públicos que pueden obtenerse, por ejemplo, en Internet, podrían servir para esa usurpación.

Consecuencias o daños y perjuicios	
Usurpación de identidad	Entendida como la acción apropiarse una persona de la identidad de otra, haciéndose pasar por ella para acceder a recursos y beneficios, actuando en el tráfico jurídico simulando ser la persona suplantada.
Fraude	Engaño económico con la intención de conseguir un beneficio, y con el cual alguien queda perjudicado.
Pérdida financiera	Pérdida económica o monetaria experimentada por el interesado.
Impedir acceder a un servicio o contrato	Situación en la cual la decisión resultante del tratamiento desemboca en una prohibición o limitación a la contratación u obtención de un servicio del responsable o de otra organización.
Otros daños y perjuicios materiales	Cualesquiera otros daños y perjuicios materiales que el tratamiento pueda causar en las personas.
Discriminación	Acción en la cual se trata de forma distinta a quien se encuentra en la misma situación que otro sujeto.
Exclusión o marginación social	Una afectación a la confidencialidad de los datos personales, o un mal uso de los mismos, que podría tener como consecuencia que la persona sufra algún tipo de exclusión o marginación social, incluyendo el entorno laboral.
Romper el secreto profesional	Situación en la cual un profesional cuya ley deontológica le obliga a guardar secreto por su actividad profesional, puede infringir dicha obligación y revelar la información confidencial que le ha trasladado una persona.
Impedir ejercer control sobre sus datos personales	Situación en la cual se limita o prohíbe a un interesado hacer uso de aquellos derechos y obligaciones que la normativa de protección de datos les otorga (derechos ARCO, a no ser objeto de decisiones automatizadas, a ser informado del tratamiento, etc.).
Impacto negativo en su reputación	Situación en la cual una persona ve menoscabado su prestigio, notoriedad o buen nombre a raíz del tratamiento.
Impedir ejercer sus DDFF	Situación en la cual el tratamiento limita o restringe el ejercicio de los derechos fundamentales atribuidos al interesado.
Revelar o inferir más información del interesado que la necesaria para el tratamiento	Situación en la cual el tratamiento o el resultado de las operaciones de tratamiento del mismo permitirían al responsable o a un tercero inferir más información del interesado y usar la misma para otros fines.
Revelar categorías especiales de datos	Situación en la cual el tratamiento o el resultado de las operaciones de tratamiento del mismo permitirían al responsable o a un tercero inferir información relacionada con categorías especiales de datos.
Revelar condenas penales / administrativas	Situación en la cual el tratamiento o el resultado de las operaciones de tratamiento de este permitirían al responsable o a un tercero inferir información relacionada con condenas o sanciones penales o administrativas.
Revelar su rendimiento en el trabajo	Situación en la cual el tratamiento permite conocer el rendimiento de una persona en su trabajo y, con ello, afectar a su reputación profesional.
Revelar su situación económica	Situación en la cual el tratamiento permite conocer aspectos relativos a la situación económica de una persona y, con ello, afectar a su reputación personal.
Revelar sus intereses personales	Situación en la cual el tratamiento permite conocer aspectos personales de una persona relacionados con sus gustos o aficiones y, con ello, afectar a su reputación personal.
El tratamiento pueda derivar en una influencia o manipulación del interesado en su toma de decisiones	Situación en la cual el tratamiento afecta a la capacidad de toma de decisiones profesionales, económicas o de consumo de un interesado de forma desleal y sin ponerlo en conocimiento del afectado.
El tratamiento puede exceder las expectativas del interesado	Situación en la cual el tratamiento de datos supera lo que se estima necesario para el cumplimiento de la finalidad del tratamiento.
Otros daños y perjuicios inmateriales	Cualesquiera otros daños y perjuicios inmateriales que el tratamiento pueda causar en las personas.

A partir de la identificación de las posibles consecuencias que pudiera tener una brecha de datos personales sobre los derechos de los interesados, el responsable del tratamiento podrá determinar de forma concreta y específica, en el marco del tratamiento de datos analizado, qué medidas de seguridad debe adoptar para disminuir la probabilidad de que suceda la brecha (medidas preventivas), así como para minimizar o limitar el impacto de sus consecuencias (medidas correctivas), en caso de que ocurra.

3. Análisis de los derechos y libertades de los interesados potencialmente afectados por una brecha

Finalmente, se debe incorporar al análisis un estudio de qué derechos y libertades de los interesados podrían verse afectados en el caso en el que tenga lugar una brecha en el marco del tratamiento de datos concreto. Este estudio debería, como mínimo, analizar la posible afectación o interferencia en los derechos fundamentales.

Se acompaña a continuación un listado de los derechos fundamentales que se deben analizar, en cualquier caso. Adicionalmente, el responsable deberá valorar la posibilidad de añadir otros derechos que pudieren verse afectados, teniendo en cuenta el contexto del tratamiento y del su sector de actividad.

Derecho a la igualdad (art. 14 CE)
Derecho a la no discriminación (art. 14 CE)
Derecho a la vida (art. 15 CE)
Derecho a la integridad física y moral (art. 15 CE)
Derecho a la libertad ideológica (art. 16 CE)
Derecho a la libertad religiosa (art. 16 CE)
Derecho al honor (art. 18 CE)
Derecho a la intimidad personal y familiar (art. 18 CE)
Derecho a la propia imagen (Art. 18 CE)
Derecho al secreto de las comunicaciones (Art. 18.3 CE)
Derecho a la libertad de expresión (Art. 20 CE)
Derecho a la libertad de información (Art. 20 CE)
Derecho de reunión (Art. 21 CE)
Derecho de asociación (Art. 22 CE)
Derecho de acceso a la función pública (Art. 23.2 CE)
Derecho a la tutela judicial efectiva (Art. 24 CE)
Derecho de petición (Art. 29 CE)
Derecho a la libertad profesional y derecho a trabajar (Art. 15 Carta UE DDFF)
Derecho a la propiedad (Art. 17 Carta UE DDFF)
Derecho a la diversidad lingüística (Art. 22 Carta UE DDFF)
Derechos de las personas mayores (Art. 25 Carta UE DDFF)
Derecho a la integración de las personas discapacitadas (Art. 26 Carta UE DDFF)
Derechos de los trabajadores (Art. 28 CE / Art. 27 / Art. 28 / Art. 30 / Art. 31 / Art. 33 Carta UE DDFF)
Derecho a la seguridad social y ayuda social (Art. 34 Carta UE DDFF)
Protección de consumidores (Art. 38 Carta UE DDFF)

4. Beneficios de la realización de un análisis preliminar de riesgos enfocado a la posibilidad de materialización de una brecha

A modo de conclusión, el objetivo de este apartado es proponer un método para que el responsable pueda llevar a cabo un estudio del tratamiento de datos que incorpore, desde un momento inicial, el análisis enfocado a la eventual materialización de una brecha.

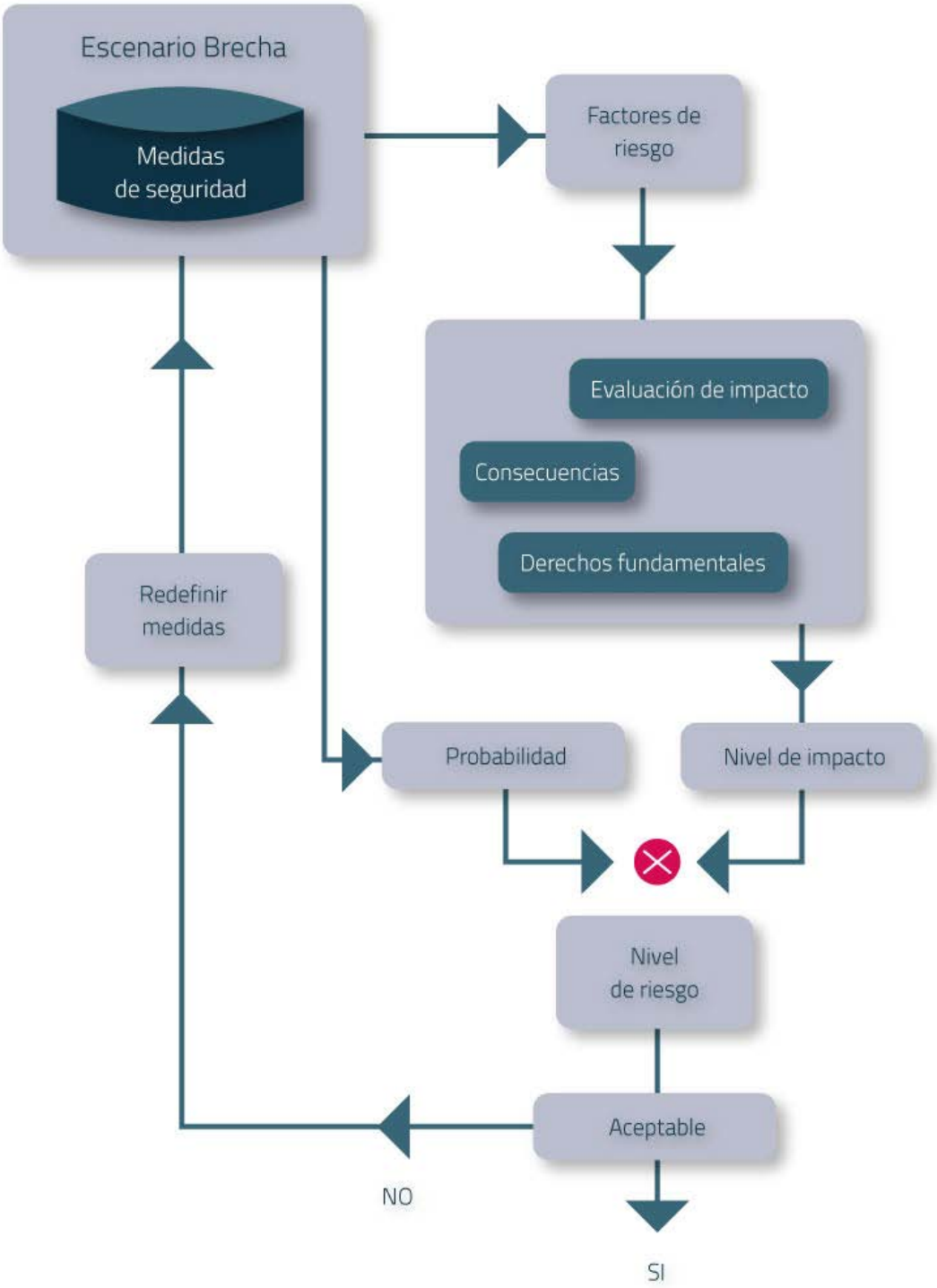
> El análisis del tratamiento de datos personales enfocado en brechas debe incorporar una valoración de los factores de riesgo inherentes al tratamiento de datos, las consecuencias o daños y perjuicios que podrían ocasionarse si se llegase a materializar una brecha y de qué derechos y libertades de los interesados podrían llegar a verse afectados.

Partiendo de este análisis, el responsable del tratamiento tendrá la capacidad de identificar, de forma específica y para el tratamiento de datos concreto, aquellas medidas de seguridad que le permitirán prevenir la materialización de brechas o, en caso de que lleguen a ocurrir, minimizar su impacto en los derechos de los afectados.

Adicionalmente, el hecho de disponer de un análisis exhaustivo enfocado a posibles brechas desde un primer momento también permite al responsable, en el caso en el que llegue a materializarse, poder dar una respuesta rápida y estudiar el impacto que puede tener sobre las personas afectadas de una forma más eficiente y contextualizada.

De este modo, se consigue reforzar la respuesta del responsable ante la brecha y garantizar un adecuado cumplimiento de las obligaciones de notificación tanto a la AEPD como a los interesados, si procede.

Por último, una vez gestionadas las posibles brechas que tengan lugar, el responsable debería llevar a cabo una revisión del análisis realizado previamente para verificar si es necesario ampliar o modificar


Escenario Brecha
Medidas de seguridad
Factores de riesgo
Evaluación de impacto
Consecuencias
Derechos fundamentales
Redefinir medidas
Probabilidad
Nivel de impacto
Nivel de riesgo
Aceptable
NO
SI

Ejemplo basado en el tratamiento de datos realizado por dos responsables a través de una aplicación móvil

Con el siguiente caso queremos ejemplificar el proceso que se podría seguir para incorporar al análisis de riesgos y/o evaluación de impacto en la privacidad de un tratamiento de datos, el potencial riesgo para los derechos y libertades de los interesados derivado de una brecha de datos personales. En este ejemplo compararemos, de un modo muy simplificado, dos escenarios que a priori podrían parecer semejantes pero que en sus resultados no lo son en absoluto.

Una empresa de desarrollo de software está desarrollando dos Apps móviles para dos clientes diferentes utilizando los mismos procesos de desarrollo de software. Como Encargado del Tratamiento diligente y en colaboración con cada uno de los Responsables del Tratamiento, realiza un análisis de riesgos de los tratamientos de datos que llevará a cabo cada uno de sus clientes a través de la APP.

Estos clientes son:

1) Una plataforma de pagos online que utilizará la App para permitir que sus clientes puedan realizar de forma rápida y sencilla transferencias bancarias. Cada usuario de la App de pagos online tendrá asignada una cuenta bancaria sobre la que podrá operar libremente desde la APP.

2) Una plataforma de streaming de vídeo que ofertará la App para los hijos de sus clientes, de forma que esta les permita ver en sus móviles cierta parte de los contenidos de la plataforma. Esta App no les permitirá ni acceder ni modificar los datos personales relativos a los titulares del servicio. Cada credencial de acceso a la App permitirá la visualización de vídeos desde un único dispositivo.

En ambos casos, la Política de Privacidad y Seguridad desde el diseño seguida por el Encargado del Tratamiento implica que el acceso a la App se realice mediante un **usuario y contraseña**, con el establecimiento de las medidas de seguridad estándar en la industria para este tipo de aplicaciones móviles:

(i) contraseña de complejidad mínima determinada;

(ii) bloqueo ante un número determinado de intentos fallidos de autenticación;

(iii) las contraseñas se almacenan hasheadas; y

(iv) la comunicación entre la App y el back-end se realiza de forma cifrada.

En este análisis simplificado, el DPO del Encargado analiza las posibles consecuencias derivadas del escenario de brecha o caso de uso "Robo de credenciales". Este escenario se incorpora al análisis de los tratamientos de datos derivados de todos sus proyectos estándar de desarrollo de App móviles al haber determinado previamente que la probabilidad de que se materialice este escenario de brecha es Alta ya que todos los años se producen este tipo de vulneración de credenciales.

En el análisis realizado para el tratamiento de datos por la App de pago online, se debería tener en cuenta, como mínimo, los siguientes factores de riesgo inherentes al tratamiento:

Finalidad o propósito del tratamiento de datos	Decidir sobre el acceso a un servicio Decidir sobre la realización o ejecución de un contrato Decidir sobre el acceso a servicios financieros Efectos jurídicos sobre las personas
Tipologías de datos	Documentos personales Datos de medios de pago
Extensión y alcance del tratamiento	Involucra un gran número de sujetos
Categoría de interesados	N/A
Condiciones técnicas	Aplicaciones móviles
Recogida y generación de datos	Recogida de datos de aplicaciones
Contexto del tratamiento	Podría determinar la situación financiera Posible usurpación de la identidad Posible fraude Posible perjuicio económico significativo Posible pérdida de confidencialidad de datos sujetos al secreto profesional Podría impedir el acceso a un servicio Podría impedir el acceso a un contrato
Contexto del responsable	Entidad financiera
Comunicaciones de datos	N/A

Partiendo de la base de los factores de riesgo inherentes al tratamiento identificados, las posibles consecuencias para los derechos y libertades de los afectados por el escenario de brecha de datos personales relativo al robo de credenciales serían:

(i) Usurpación de la identidad

(ii) Fraude

(iii) Perdida financiera

(iv) Impedir acceder a un servicio o contrato.

El impacto de las consecuencias indicadas está catalogado como Significativo, llegando a afectar al derecho fundamental de Derecho a la propiedad (Art. 17 Carta UE DDFF). Con una probabilidad Alta de partida, el nivel de riesgo es Muy Alto.

Por otro lado, el análisis de riesgo inicial realizado para el tratamiento de datos derivado de la App-Acceso-Streaming-Vídeo deberá incorporar, como mínimo, los siguientes factores de riesgo:

Finalidad o propósito del tratamiento de datos	Decidir sobre el acceso a un servicio Decidir sobre la realización o ejecución de un contrato
Tipologías de datos	Documentos personales
Extensión y alcance del tratamiento	Involucra un gran número de sujetos
Categoría de interesados	Menores de 14 años
Condiciones técnicas	Aplicaciones móviles
Recogida y generación de datos	Recogida de datos de aplicaciones
Contexto del tratamiento	Posible usurpación de la identidad Podría impedir el acceso a un servicio Podría impedir el acceso a un contrato
Contexto del responsable	N/A
Comunicaciones de datos	N/A

Con base en los factores de riesgo inherentes al tratamiento de datos realizado en la App de Video Streaming, las potenciales consecuencias identificadas serían :

(i) Usurpación de la identidad

(ii) Fraude

(iii) Impedir acceder a un servicio o contrato.

En este caso, sin embargo, tenemos que todas las consecuencias son reversibles simplemente devolviendo al usuario legítimo el control de la cuenta, lo que supone un impacto Muy limitado, y no hay afección a ningún derecho fundamental. Con la misma probabilidad Alta que en el caso anterior, ahora tenemos un riesgo residual Bajo.

Por lo tanto, partiendo del análisis de riesgos inicial podemos ver como las consecuencias de que se materialice la misma brecha, concretamente el robo de credenciales, son diferentes en función del tratamiento de datos específico y, por lo tanto, las medidas de seguridad que se deberían incorporar en cada caso deben ser también distintas.

En este sentido, se confirma que las medidas estándar no resultan suficientes para una App de pago online, ya que el nivel de riesgo residual sigue siendo Muy Alto y será necesario aplicar más medidas, hasta que el riesgo residual se reduzca a niveles aceptables; mientras que para una App-Acceso-Streaming-Vídeo sí.

Los documentos resultantes del análisis de riesgos realizado en la fase de Planifica de las brechas, serán un listado de medidas de seguridad, complementado por el análisis de riesgo para los derechos y libertades de los interesados que, partiendo de esta metodología, justifica que son suficientes para mitigar los riesgos detectados. Estos documentos se podrán aportar en caso de que sea necesario notificar una brecha acaecida sobre el tratamiento analizado.

Este mismo proceso de análisis deberá seguirse para todos los posibles escenarios de brechas que pudieran tener lugar en el marco de un tratamiento de datos.

Ahora supongamos que el Responsable del Tratamiento de cada App sufriese, una vez implantada la App, una brecha del escenario analizado: robo de credenciales. Durante la gestión de la brecha, a la hora de realizar el preceptivo análisis del riesgo para los derechos y libertades de los interesados, deberán adoptar como referencia el análisis previo realizado en el marco del proceso de gestión del riesgo y/o evaluación de impacto del tratamiento de datos que recogerá las medidas preventivas adoptadas por la organización.

Adicionalmente, para calcular cual es el riesgo real de la brecha para los derechos y libertades de los interesados, deberá incorporar al análisis la referencia a las medidas paliativas adoptadas con posterioridad a la brecha y valorar el impacto que tendrá la misma sobre los interesados, así como la probabilidad de que se materialicen las consecuencias identificadas.

Por ejemplo, supongamos que la medida paliativa adoptada en ambos casos es la misma; resetear las contraseñas conculcadas y facilitar al cliente legítimo las nuevas credenciales.

- Para el caso de la App-Streaming infantil el cliente recuperará el acceso al servicio de la App, sin que se produzca ninguna consecuencia más para él, por lo que el riesgo para sus derechos y libertades ha devenido nulo.
- Para el caso de la App-de pagos online, el tercero malicioso perderá el acceso a la App pero habrá tenido oportunidad de acceder a datos personales de los afectados y, por lo tanto, podrá utilizarlos para usurpar su identidad en futuras ocasiones. Asimismo, habrá podido realizar transferencias dinerarias con origen la cuenta del cliente legítimo, que recuperará el acceso a la App pero tendrá dificultades para recuperar el dinero transferido. Con lo que el riesgo para sus derechos y libertades será Muy Alto, requiriendo notificación a la Agencia y comunicación a los interesados.

Este escenario de brecha también sirve para visibilizar que, si en el caso de la App-de pagos online se hubiesen adoptado medidas de seguridad preventivas adicionales, como incorporar factores de autenticación reforzada de conocimiento (algo que sepa el interesado, como una contraseña), posesión (algo que tenga el interesado, como un teléfono móvil o una tarjeta) e inherencia (algo que sea el interesado, como la verificación a través de la huella dactilar), se hubiese podido reducir la probabilidad de materialización de la brecha. En este caso a pesar de que se hubieran visto comprometidas las contraseñas, no se hubieran materializado la Usurpación de identidad y las consecuencias no se podrían llegar a materializar. Por lo tanto, el riesgo no sería Muy alto sino Bajo y no sería necesario notificar a la Agencia.

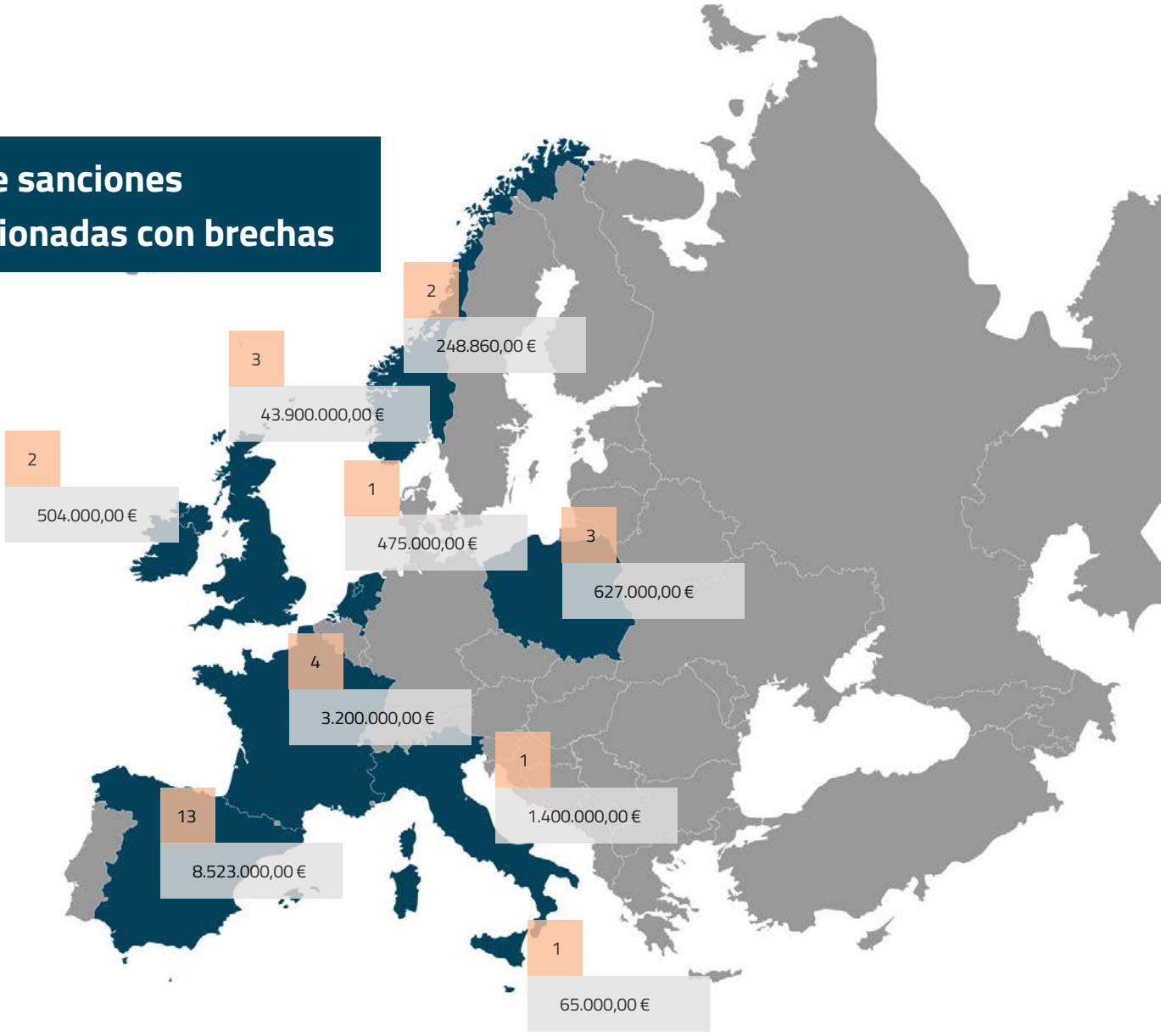
Del análisis de los casos anteriores podemos extraer la relevancia de analizar los riesgos del tratamiento de datos y, en su caso, llevar a cabo una evaluación del impacto en la privacidad por parte del Responsable del Tratamiento que incorpore las posibles consecuencias que podría tener para los derechos y libertades de los interesados el hecho de que se materialice una brecha de datos personales. Este análisis permitirá a las organizaciones concretar el detalle de las medidas de seguridad que se deben adoptar en cada tratamiento para evitar o, en su caso, mitigar las consecuencias de una brecha de datos personales, siendo dichas medidas diferentes en función del contexto del responsable y del tratamiento de datos concreto.

ANEXO IV

CONCLUSIONES AL ANÁLISIS DE ALGUNAS RESOLUCIONES SOBRE BRECHAS DE DATOS PERSONALES ADOPTADAS POR LA AEPD

¿EN QUÉ MOMENTO PASAMOS DE SER VÍCTIMAS A SER SANCIONADOS?

N° de sanciones relacionadas con brechas



Fuente https://www.enforcementtracker.com/		
Periodo: diciembre -2020 noviembre 2022		
Criterio: Que se refieran a alguno de estos artículos		
	Artículo 5.1.f RGPD:	Principio del tratamiento: seguridad adecuada
	Artículo 32 RGPD:	Medidas de seguridad
	Artículo 33 RGPD:	Notificación de brechas
	Artículo 34 RGPD:	Comunicación de brechas

En este apartado de la guía hemos tratado de hacer un análisis, si bien no pormenorizado, por la complejidad y dedicación que pueda demandar, si una primera aproximación en cuanto a la supervisión que las diferentes autoridades de control europeas realizan de las brechas de datos personales de las que tienen noticia, ya sea a través de las notificaciones realizadas por responsables y encargados de los tratamientos o de oficio.

Aunque siempre ha de tenerse en cuenta que no toda brecha de datos va a suponer la apertura de requerimiento informativo y todavía en menos de ellas la incoación de un expediente sancionador, el análisis estadístico de sanciones entre los diferentes países de Europa, ya nos sirve para comprobar la gran disparidad de criterios que existe entre ellos. Disparidad que se refleja tanto en los artículos por los que son sancionados los responsables en caso de brechas, como por el número y el montante de las sanciones. Parece ser que está todavía pendiente de establecer mecanismos que permitan la unificación de criterios a lo largo de toda la Unión, tan necesaria para establecer un mercado interior realmente único.

Por otra parte, hemos querido analizar algunos de los expedientes tramitados por la AEPD en los últimos años, sobre brechas de datos sufridas por entidades públicas y privadas, a fin de promover el acercamiento de los profesionales de protección de datos y de ciberseguridad a la toma de decisiones de nuestra autoridad de control a través de sus resoluciones.

Aunque hayan transcurrido casi cinco años desde que se empezó a exigir el cumplimiento del RGPD, es todavía muy poco tiempo para asentar conclusiones definitivas, pero sí es momento para empezar a definirlas. Y a ello ha contribuido sin duda la Sentencia1 del Tribunal Supremo de 15 de febrero de 2022, para la formación de la jurisprudencia, en la que establece que "la obligación de adoptar las medidas necesarias para garantizar la seguridad de los datos personales no puede considerarse una obligación de resultado, que implique que producida una filtración de datos personales a un tercero exista responsabilidad con independencia de las medidas adoptadas y de la actividad desplegada por el responsable del fichero o del tratamiento".

Análisis de Riesgos previo a la brecha – Imprescindible:

La única forma de demostrar que las medidas de seguridad establecidas antes de la brecha eran adecuadas y necesarias es presentar un análisis de riesgos previo, del que emanen estas medidas, con una metodología que permita entender el proceso completo de análisis, así como las acciones previas y posteriores que deriven de él.

Análisis de Riesgos para los interesados vs. la empresa:

En la comunicación y el análisis de brecha, se debe poder diferenciar entre los riesgos que aplican a la empresa y al interesado, siendo el último el principal foco del DPO. Se debe entender la importancia de la afectación de categorías especiales de datos personales, como son los datos de salud, que deberían gozar de especial protección y consideración

Decisiones sobre notificación y/o comunicación de brechas - Análisis de Riesgos:

La única justificación válida para la no notificación, notificación tardía, o no comunicación de una brecha a los interesados, es la presentación de un Análisis de Riesgos para los derechos y libertades de los interesados de la propia brecha. Siendo en caso de no hacerse así, muy elevado el riesgo de sanción por incumplimiento de los artículos 33 y 34 del RGPD.

Documentar y documentar:

Los retrasos en la notificación y/o comunicación de una brecha pueden justificarse siempre y cuando se cuente con documentación que demuestre que los análisis de riesgos no mostraban riesgos para los interesados que hiciesen necesario su notificación, con el conocimiento que en cada momento del ciclo de vida de la brecha se contaba.

Disponibilidad:

No solo son objeto del artículo 32 y 34 brechas relacionadas con la integridad y/o la confidencialidad de los datos. Las brechas de disponibilidad también han de ser evaluadas, gestionadas y, en función de los riesgos para los interesados que supongan, notificadas; son las grandes olvidadas porque es mucho más común que sean recuperables y que no siempre supongan riesgos para los interesados.

Lecciones aprendidas sobre brechas en otros incumplimientos:

Es importante destacar que los responsables no solo deben tomar medidas de seguridad a base de un análisis interno, sino que a medida que va madurando los procedimientos y la inteligencia de los ataques es importante revisar el contexto mundial y en especial del mismo sector. La comunicación e investigación sobre los análisis de riesgos, posibles controles y en especial nuevos tipos de ataques pueden ayudar a estar mejor preparados. Por cada brecha, debe existir una lección aprendida que debe poder traducirse en acciones.

Calidad en la gestión de la brecha:

Se entiende que, si bien existen medidas técnicas y organizativas que los responsables y encargados de los tratamientos deben cumplir, en algunas ocasiones, las sanciones impuestas por la agencia de control se ven agravadas por la falta de contestación adecuada ante los requerimientos y denuncias. Además, las medidas deben ser consecuencia de un previo análisis de riesgo el cual tenga en mente el impacto al interesado.

Finalmente, la conclusión más importante a considerar, tal y como hemos venido sosteniendo a lo largo de toda la guía, es que, si bien la seguridad cien por cien no existe, sin que sea exigible por tanto la infalibilidad de las medidas adoptadas por los responsables y encargados de los tratamientos, sí resulta en cambio exigible cumplir y poder demostrar nuestra diligencia debida, nuestro obligado "Accountability". Y si, además, podemos objetivar la demostración de esa diligencia debida a través de los análisis de riesgos para los derechos y libertades de las personas físicas objeto de los tratamientos de datos personales, podremos presentar una defensa clara ante cualquier actuación de revisión por parte de la autoridad de control.

RESOLUCIÓN - aepd		
Título Resolución:	**Archivo de Actuaciones**	
Organización - Pública / Privada - Sector:	**Organización Pública - Ministerio de Trabajo y Economía Social (MITES)**	
	DESCRIPCIÓN BRECHA	
Descripción Brecha Breve cronología	9 junio 2021: el MITES informa en twitter que ha sufrido un ciberataque. Conforme la Resolución: "*La brecha de seguridad, categorizada como de disponibilidad, se produce como consecuencia de ataque ransomware que han comprometido las credenciales de acceso a los servicio* s". Diversos medios de información se hacen eco de la noticia y la amplian indicando que es un ataque similar al sufrido por el SEPES meses antes, debido al ransomware RyuK. Como medida de contención, se apaga todo el parque informático del MITES, se desconecta de internet y de la Red SARA. Lo que provoca una brecha de disponibilidad de servicios. Posteriormente se fueron restaurando los sistemas en base a las copias de seguridad de determinadas aplicaciones, recuperando paulatinamente todos los servicios. La AEPD inicia de oficio actuaciones previas de investigación.	
	COMUNICACIONES EFECTUADAS - reclamado	
	SI/NO	Justificación Principal
Notificado a la aepd	**NO**	No figuran en el expediente las alegaciones del MITES al respecto, pero sí las conclusiones de la AEPD: "*inicialmente, no se pudo determinar hasta qué punto existía un riesgo para los derechos y libertades de los afectados, por lo que sabiendo que, si es improbable dicho impacto, no hay que notificarla a la autoridad de control* ."
Comunicado a los afectados	**NO**	No figura justificación alguna en el expediente, pero se puede entender que si se considera que no era necesario notificar la brecha, tampoco comunicarlo a los interesados.
	PARAMETROS EVALUADOS	**VALOR**
Sobre la brecha	**Cómo ha sido el incidente**	Intencionado
	Origen del incidente	Externo
	Consec. Del ciberinciden.	Si
Sobre las consecuencias	**Consec. Del incidente**	Pérdida de disponibilidad de los sistemas del Responsable
Sobre las consecuencias	**Se ha recuperado los datos personales**	Se revertió el efecto después mediante la recuperación paulatina de sistemas y datos desde copias de respaldo.
	Grado en el que podría afectar	Pérdida de disponibilidad de los tratamientos
	Se ha materializado alguno de los daños	Sí
	Probabilidad de que el daño anterior se materialice	Materializado
Categoría de datos	**Tipos de datos afectados en personas físicas**	No hay información en el Expediente
Personas afectadas	**Hay menores o vulnerables**	No hay información en el Expediente
	Volumen de personas afectadas por la brecha	No hay información en el Expediente
Inform. Temporal	**Momento en el que se conoció**	Inmediata por los efectos que tuvo
Inform. Temporal	**Actuación ante la brecha**	Temprana y diligente
	FUNDAMENTOS DE DERECHO - RESOLUCIÓN - aepd	
Artículos Infracción:	**Artículo 32:** AEPD concluye: *'en el momento de producirse la brecha de seguridad,* ***no consta que el MITES no dispusiese de medidas de seguridad razonables*** *en función de los posibles riesgos estimados'* y *'* ***no existen evidencias de no que se ha actuado de forma diligente*** *una vez conocida la brecha de seguridad y que las medidas adoptadas con posterioridad al incidente aquí analizado no fueron adecuadas'* . **Artículo 33:** AEPD concluye que no hubo vulneración de este artículo ya que "***inicialmente, no se pudo determinar hasta qué punto existía un riesgo para los derechos y libertades de los afectados*** *, por lo que sabiendo que, si es improbable dicho impacto, no hay que notificarla a la autoridad de control'.*	
Artículos Agravantes y Atenuantes:	No aplica	
Resolución	Se decide el archivo de actuaciones en base a que ***"no se han encontrado evidencias que acrediten la existencia de infracción en el ámbito competencial de la Agencia Española de Protección de Datos"*** .	

CONCLUSIONES - guía
1) Los incidentes que afecten a la disponibilidad de los datos también son brechas de datos, que han de cumplir con los artículos 32, 33 y 34 RGPD, "*puesto que los datos personales no pueden ser tratados de forma legítima porque se han destruido, perdido o cifrado* ". 2) Puede causar cierta extrañeza la conclusión de la AEPD de la no existencia de vulneración del artículo 32 sobre la base de que *'no consta que el MITES no dispusiese de medidas de seguridad razonables',* ya que si nos ceñimos al art. 32 RGPD, es obligación del Responsable o el Engarcado aplicar las "*medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo* " y *'será responsable del cumplimiento de lo dispuesto en el apartado 1 y capaz de demostrarlo («responsabilidad proactiva»)',* principio de Accountability del art. 5.2 RGPD. 3) En cuanto a la posibilidad de vulneración del art. 33 RGPD, vuelve la AEPD a desconcertarnos cuando lo descarta sobre la base de que *'inicialmente, no se pudo determinar hasta qué punto existía un riesgo para los derechos y libertades de los afectados, por lo que sabiendo que, si es improbable dicho impacto, no hay que notificarla a la autoridad de control'.* Conclusión que pudiera contradecir el tenor del mencionado art. 33, en la que toda brecha ha de comunicarse "a *menos que sea improbable que dicha violación de la seguridad constituya un riesgo* ", ya que si no se puede determinar el nivel de riesgo, no se podrá determinar que sea improbable. De seguir con el criterio de la AEPD expresado en esta resolución, la obligación de notificación solo se daría cuando se hubiera podido determinar la existencia de un riesgo concreto para los interesados, no siendo necesario notificar situaciones en las que no sea posible establecer si existe o no ese riesgo. Lo que se enfrenta a criterios de otras autoridades de control europeas, en las que en caso de que no se pueda determinar que no hay riesgos, existe el deber de notificación.

RESOLUCIÓN - aepd		
Título Resolución:	Resolución procedimiento sancionador - Sanción	
Organización - Pública / Privada - Sector:	Organización Privada - Telecomunicaciones	
	DESCRIPCIÓN BRECHA	
Descripción Brecha Breve cronología	La AEPD recibe 9 reclamaciones de interesados a los que se les había realizado uno o más duplicados de su tarjeta SIM, resultando de ello varios fraudes bancarios tales como transferencias no autorizadas, solicitud de préstamos o pagos no autorizados por el interesado. Mediante la obtención por parte de los delincuentes del control sobre las líneas telefónicas de los afectados, estos podían obtener el segundo factor de autorización necesario para realizar las operaciones bancarias descritas. La realización de los duplicados de tarjeta SIM se llevó a cabo por medios presenciales y telefónicos, proporcionando los delincuentes, aparentemente, copias del DNI de los interesados en los establecimientos comerciales de la responsable, o superando, en caso de solicitud no presencial, las políticas de seguridad establecidas por la responsable del tratamiento, dado que en todos los casos, los ciberdelincuentes contaban con información previa de los intersados.	
	COMUNICACIONES EFECTUADAS - reclamado	
	SI/NO	Justificación Principal
Notificado a la aepd	**NO**	No se trata como una brecha de seguridad, sino como una falta de responsabilidad proactiva por no ser capaces de acreditar la efectividad de las medidas de seguridad.
Comunicado a los afectados	**NO**	Emana de la no existencia de brecha a entender de la Agencia.
PARAMETROS EVALUADOS		**VALOR**
Sobre la brecha	**Cómo ha sido el incidente**	Intencionado
	Origen del incidente	Externo
	Consec. Del ciberinciden.	Si
Sobre las consecuencias	**Consec. Del incidente**	Pérdida de disponibilidad de las líneas telefónicas de los interesados
Sobre las consecuencias	**Se han recuperado los datos personales**	Se revertió el efecto mediante la realización de un duplicado de SIM a los interesados originales
	Grado en el que podría afectar	Pérdida de disponibilidad de las líneas telefónicas de los interesados
	Se ha materializado alguno de los daños	Sí
	Probabilidad de que el daño anterior se materialice	Materializado
Categoría de datos	**Tipos de datos afectados en personas físicas**	Número de teléfono
Personas afectadas	**Hay menores o vulnerables**	No hay información en el Expediente
	Volumen de personas afectadas por la brecha	9
Inform. Temporal	**Momento en el que se conoció**	Casi inmediata por los efectos que tuvo
Inform. Temporal	**Actuación ante la brecha**	Reacción temporal tardía y falta de diligencia
	FUNDAMENTOS DE DERECHO - RESOLUCIÓN - aepd	
Infracción	**Arts. 5.1.f) y 5.2 RGPD:** La Agencia determina que "*no se impone la sanción por aquellos casos en los que se han presentado reclamaciones, sino porque estos casos ponen de relieve el incumplimiento de las garantías en materia de seguridad (artículo 5.1.f) RGPD) y de responsabilidad proactiva (artículo 5.2 del RGPD) que se pone de manifiesto la deficiencia de las medidas de seguridad adoptadas'*	
Agravantes y Atenuantes:	**Agravantes:** (i) Naturaleza, gravedad y duración; (ii) Número de interesados afectados; (iii) Nivel de los daños y perjuicios sufridos: se considera como alto con motivo de que el control de la línea da acceso a la realización de operaciones bancarias; (iv) Intencionalidad o negligencia en la infracción. Se considera negligente; (v) Grado de responsabilidad del responsable: Se considera que las medidas técnicas y organizativas implementadas son insuficientes; (vi) Toda infracción anterior cometida por el responsable; (vii) Categorías de datos personales afectados: consideran que "El dato personal afectado por el tratamiento tiene una naturaleza especialmente sensible porque facilita la suplantación de identidad";(viii) Vinculación de la actividad del infractor con la realización de tratamientos de datos de carácter personal **Atenuantes:** (i) Medidas tomadas por el responsable para paliar los daños y perjuicios sufridos por los interesados; (ii) Grado de cooperación con la autoridad de control; (iii) Los beneficios obtenidos como consecuencia de la comisión de la infracción; se descartan; (iv) El sometimiento por parte del responsable o encargado, con carácter voluntario, a mecanismos de resolución alternativa de conflictos, en aquellos supuestos en los que existan controversias entre aquellos y cualquier interesado	
Resolución	AEPD les sanciona por una infracción del artículo 5.1.f) y 5.2 del RGPD, tipificada en el artículo 83.5.a) del RGPD, con una multa de **3.940.000 euros (tres millones novecientos cuarenta mil euros).**	
	CONCLUSIONES - guía	
1.- La AEPD no la considera una brecha de datos, sino como una ***falta de responsabilidad proactiva y aplicación de medidas de seguridad insuficientes*** . En concreto se constata "la falta de un modelo eficaz de evitación del riesgo de suplantación de identidad, la ausencia de medidas de seguridad adecuadas y tendentes a asegurar el procedimiento de identificación y entrega de la tarjeta SIM, la materialización de los riesgos, la reacción temporal tardía frente a los hechos descritos, amén de la insuficiencia de las medidas adoptadas (pues ha reaccionado al recibir los requerimiento de la AEPD y no ha evitado la repetición posterior como muestran las tres reclamaciones posteriores presentadas ante la AEPD). 2.- La AEPD ha tenido en cuenta que la adopción de medidas de seguridad por la entidad sancionada se ha producido, no tras el análisis de los riesgos que implica el tratamiento de los datos, sino cuando se han puesto en conocimiento del responsable los hechos con el traslado de las reclamaciones presentadas ante la AEPD. 3.- La adopción de medidas de seguridad no es una obligación absoluta y, por tanto, no exige una obligación de resultado. El modelo flexible al riesgo impuesto por el RGPD -partiendo de la doble configuración de la seguridad como un principio relativo al tratamiento y una obligación para el responsable o el encargado del tratamiento- no impone en ningún caso la infalibilidad de las medidas, sino su adecuación constante a un riesgo, que, como en el supuesto examinado la AEPD lo ha considerado cierto, probable y no desdeñable, alto y con un impacto muy significativo en los derechos y libertades de los ciudadanos. En este caso, la AEPD pone de relieve la insuficiencia de esas medidas de seguridad adoptadas, entendiéndolo como un hecho objetivo, y la necesidad de que se adopten medidas adecuadas para reducir significativamente los casos de duplicados fraudulentos de tarjetas SIM 4.- En lo que respecta al **error humano**, la AEPD considera que una vez, dos veces, pudiera tratarse como un error humano que sobrepase las medidas de seguridad. Continuos errores humanos lo que exteriorizan es un problema más profundo en la organización, una falta de visión de los riegos, de análisis y de planificación (privacidad desde el diseño), una ausencia de dimensionamiento de las medidas de seguridad, una omisión en la implantación de las adecuadas o de revisión de las inadecuadas y la inexistencia de demostración del cumplimiento.		

RESOLUCIÓN - aepd		
Título Resolución:	Archivo de Procedimiento sancionador	
Organización - Pública / Privada - Sector:	Organización Privada - Banca	
	DESCRIPCIÓN BRECHA	
Descripción Brecha Breve cronología	Septiembre 2019: Los sistemas internos de control de la organización detectan comportamientos anómalos en el acceso a datos personales. Octubre 2019: Una investigación interna concluye que dos exempleados, antes de causar baja en el banco en julio, se habían apoderado y habían divulgado a terceros ajenos a la entidad información personal. Para ello habrían usado sus privilegios como empleados para acceder a fichas de clientes, extraer información, y posteriormente enviarla vía correo electrónico fuera de la organización. En paralelo con la investigación interna, el Responsable había enviado burofaxes a ambos exempleados requiriendo que se abstuviesen de utilizar los datos extraídos ilícitamente. También se advierte a la nueva entidad para la que trabajaban, para que tome medidas preventivas para evitar el uso de citados datos. Enero 2020: se notifica la brecha de datos personales a la Agencia. Febrero 2020: se llega a un acuerdo de confidencialidad y no concurrencia con los empleados, que además presentan certificado de destrucción de todas la información exfiltrada.	
	SI/NO	Justificación Principal
Notificado a la aepd	**SI**	
Comunicado a los afectados	**NO**	La Entidad justifica que no procedía la comunicación a los afectados sobre la base de haber adoptado las medidas apropiadas para evitar que la violación de seguridad tuviera implicación en los derechos y libertades de los clientes afectados.
	PARAMETROS EVALUADOS	**VALOR**
Sobre la brecha	**Cómo ha sido el incidente**	Intencionado
	Origen del incidente	Interno
	Consec. Del ciberinciden.	No
Sobre las consecuencias	**Consec. Del incidente**	Exfiltración de datos de clientes del Responsable
Sobre las consecuencias	**Se ha recuperado los datos personales**	Sí. El responsable llegó a un acuerdo con los terceros que habían exfiltrado los datos para su destrucción y no utilización de los mismos.
	Grado en el que podría afectar	Divulgación a terceros de su información personal
	Se ha materializado alguno de los daños	Se concluye que los datos personales divulgados no hayan sido utilizados por terceros
	Probabilidad de que el daño anterior se materialice	Baja una vez tomadas las medidas anteriores
Categoría de datos	**Tipos de datos afectados en personas físicas**	Datos identificativos y económico-financieros
Personas afectadas	**Hay menores o vulnerables**	NO
	Volumen de personas afectadas por la brecha	219
Inform. Temporal	**Momento en el que se conoció**	Temprana y vía control interno
Inform. Temporal	**Actuación ante la brecha**	Temprana y diligente
	FUNDAMENTOS DE DERECHO - RESOLUCIÓN - aepd	
Infracción:	**Artículo 33:** la AEPD inicia procedimiento sancionador por una presunta infracción de este artículo, al haber transcurrido varios meses desde que se detecta la actividad sospechosa y se produce la comunicación de la brecha. Tras las alegaciones del Responsable al inicio del procedimiento, este es archivado porque se acepta que la notificación de la brecha se realizó en el momento en el que se advirtió que era probable que la misma constituyera un riesgo para los derechos y las libertades de las personas, toda vez que el análisis de la entidad para la toma de decisión relacionada con la notificación de brechas de seguridad a la autoridad de control, se efectúa conforme a los parámetros de la Guía para la gestión y notificación de brechas de seguridad. Además, la AEPD señala que la entidad investigada tenía implementadas medidas de seguridad que, en principio, eran las adecuadas y que al detectar el ataque, se adoptaron de manera inmediata una serie de medidas de seguridad adicionales con el fin de minimizar los riesgos y extremando las dificultades para el acceso y extracción de la información.	
Agravantes y Atenuantes:	No aplica	
Resolución	Se archiva el procedimiento sancionador	
	CONCLUSIONES - guía	

1.- La actuación de la entidad, notificando la brecha y facilitando información y documentación sobre la existencia de medidas de seguridad adecuadas al nivel de riesgo, aunque sin un análisis de riesgos como tal por tratarse de tratamientos iniciados con anterioridad a mayo de 2018, hace considerar a la AEPD que no ha habido infracción al art. 32 por parte de la entidad, a pesar de materializarse la brecha.
La Agencia utiliza el criterio del Tribunal Supremo en su Sentencia 188/2022, de 15 febrero 2022, de que la obligación de medidas de seguridad recogida en el artículo 32 del RGPD es de medios y no de resultado; pero para su aplicación resulta imprescindible que el Responsable aporte las medidas de seguridad implantadas, pruebas de su existencia y funcionamiento, así como su carácter pertinente, adecuado y suficiente en función del nivel de riesgo al que esté sometido un tratamiento.
2.- El archivo del procedimiento sancionador no se basa únicamente en la alegación del Responsable de que hasta Enero no hubo constancia de que la brecha suponía un riesgo para los interesados, sino que la entidad ha podido aportar un análisis para la toma de la decisión de no notificar en fechas previas, basado en las recomendaciones de la AEPD en su guía para la gestión y notificación de brechas de esas fechas.
No solo es necesario poder justificar que no se notifica la brecha sobre la base de un criterio adecuado, también es requisito demostrar que se realizó un análisis en cada momento del ciclo de vida de la gestión de la brecha y que las decisiones se tomaron en base a estos análisis.
3.- Es imprescindible contar con un procedimiento de gestión de brechas, seguirlo y documentar cada fase del mismo con las conclusiones y decisiones tomadas, de lo contrario, corremos el riesgo de que se llegue a sancionar el incumplimiento del plazo de 72 horas, cuando realmente haya motivos fundados para no hacerlo.
4.- Podría en consecuencia resultar conveniente que la entidad incluya en la primera notificación de una brecha la justificación de por qué se notifica en ese momento y no en otro anterior. Es probable pensar que de haberse seguido en el caso estudiado, pudiera ser que ni siquiera se hubiera iniciado el expediente sancionador.

RESOLUCIÓN - aepd		
Título Resolución:	Resolución Procedimiento Sancionador - Terminación por Apercibimiento	
Organización - Pública / Privada - Sector:	Organización Privada - Servicios	
	DESCRIPCIÓN BRECHA	
Descripción Brecha Breve cronología	Una vulnerabilidad conocida sobre un sistema de información técnicamente obsoleto propicia la posible exfiltración de información personal de un elevado número de clientes, información no especialmente protegida ni especialmente sensible. 9 julio 2019: Incibe comunica al Encargado del Tratamiento una posible intrusión en sus sistemas 10 julio 2019: el Encargado comunica al Responsable una posible intrusión y este comprueba que efectivamente ha existido 12 julio 2019: se toman medidas de contención de la brecha por parte del Responsable 28 agosto 2019: el Responsable del tratamiento notifica la brecha a la AEPD.	
	COMUNICACIONES EFECTUADAS - reclamado	
	SI/NO	Justificación Principal
Notificado a la aepd	**SI**	
Comunicado a los afectados	**NO**	La entidad investigada manifiesta que han considerado que no era necesaria la comunicación a los posibles afectados después de valorar los parámetros de volumen (entre 1.000 y 100.000), la tipología de los datos (datos no sensibles) e impacto (externo) considerando un riesgo (nivel 18) que indica que no es necesario el envío de comunicación a los clientes afectados
	PARAMETROS EVALUADOS	**VALOR**
Sobre la brecha	**Cómo ha sido el incidente**	Intencionado
	Origen del incidente	Externo
	Consec. Del ciberinciden.	Si
Sobre las consecuencias	**Consec. Del incidente**	Exfiltración de datos de clientes del Responsable
Sobre las consecuencias	**Se ha recuperado los datos personales**	No se ha podido revertir el efecto de la brecha, puesto que los datos una vez exfiltrados han pasado a estar fuera el alcance del Responsable
	Grado en el que podría afectar	Ni el Responsable ni la Agencia hacen un análisis sobre las posibles consencuencias de la brecha, o al menos esto no se plasma en la Resolución.
	Se ha materializado alguno de los daños	
	Probabilidad de que el daño anterior se materialice	
Categoría de datos	**Tipos de datos afectados en personas físicas**	Datos identificativos, de contacto y demográficos
Personas afectadas	**Hay menores o vulnerables**	NO
	Volumen de personas afectadas por la brecha	75.000
Inform. Temporal	**Momento en el que se conoció**	Tardía. Fue necesario recuperar el estado de los sistemas usando copias de respaldo de entre 3-4 meses anteriores a la fecha de notificación de Incibe.
Inform. Temporal	**Actuación ante la brecha**	Temprana y diligente
	FUNDAMENTOS DE DERECHO - RESOLUCIÓN - aepd	
Infracción:	**Artículo 32:** La AEPD fundamenta su infracción en que la "*entidad investigada no ha aportado el análisis de riesgos de los tratamientos de los que es responsable, lo que impide evaluar las medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo, careciendo de la capacidad de garantizar la confidencialidad, integridad, disponibilidad y resiliencia permanentes de los sistemas y servicios de tratamiento, lo que ha provocado el acceso por tercero no autorizado a los datos alojados en su sistema de información*". **Artículo 33:** La AEPD fundamental su infraccion en el retraso de casi dos meses desde que el Responsable tuvo conocimiento de la brecha, por haberselo comunicado su Encargado del Tratamiento, hasta que lo notificó a la Agencia; sin que el Responsable hubiese aportado argumento alguno para explicar el retraso. **Artículo 34:** A pesar de la justificación aportada por el Responsable para no haber comunicado a los afectados y que finalmente la AEPD no ha considerado la infracción de este artículo, su resolución indica que *'no obstante, la entidad investigada deberá responsabilizarse de la ausencia de tal comunicación y, en su caso, de la preceptiva evaluación de impacto según señala el art 35 del RGPD, tras la nueva evaluación del riesgo requerida en la parte resolutiva de esta Resolución'*. **Artículo 28:** Aunque no es un artículo objeto del expediente, se analiza la actuación del Encargado del Tratamiento y se concluye que este informó en tiempo y forma a la entidad responsable .	
Agravantes y Atenuantes:	**Art. 76.3 LOPDGDD**: En atención a la complejidad de los sistemas de información afectados, así como las acciones tomadas tendentes a minimizar las consecuencias negativas de la citada brecha de seguridad de los datos personales de sus clientes, se considera conforme a derecho no imponer sanción consistente en multa administrativa y sustituirla por la sanción de apercibimiento.	
Resolución	Se procede a sancionar al Responsable por infracción de los artículos 32 y 33. Además requiere al Responsable a apotar en el plazo de 3 meses el procedimiento de actuación y notificación ante la AEPD de incidentes de seguridad, así como una auditoría de seguridad que certifique que los sistemas afectados ya no son susceptibles.	
	CONCLUSIONES - guía	

1.- Las medidas de seguridad deben estar justificadas en un análisis de riesgos previo a la brecha, única forma de justificar que las medidas eran pertinentes, adecuadas y suficientes a tenor de los riesgos. Este análisis debe facilitarse siempre en la notificación de la brecha.
2.- La AEPD introduce una consideración muy interesante sobre qué riesgos han de ser tenidos en cuenta a la hora de definir las medidas, haciendo referencia a que habrá que tener encuenta no solo los datos directamente afectados, sino la posiblidad de que búsquedas en internet sobre estos datos exfiltrados *'puede ofrecer resultados que combinándolos con los ahora accedidos por terceros ajenos, nos permitan el acceso a otras aplicaciones de los afectados o la creación de perfiles de personalidad, que no tienen por qué haber sido consentida por su titular'*. Añadiendo que *'esta posibilidad supone un riesgo añadido que se ha de valorar y que aumenta la exigencia del grado de protección en relación con la seguridad'*.
En consecuencia, los riesgos a ser evaluados no deberán tener en cuenta únicamente riesgos directamente de las aplicaciones o tratamientos realizados por el Responsable afectado, sino que tendrán que incluir otros riesgos como el acceso a otros servicios, aplicaciones o tratamientos fuera del Responsable original. Por ejemplo, en el caso de datos que no sean suficientes para producir una suplantación de identidad ante el Responsable afectado por la brecha, habrá de evaluarse igualmente si estos solos o conjuntamente con otros datos públicos, sí pueden ser suficientes para que el interesado sufra una suplantación de identidad en otros proveedores de servicios, a la hora de considerar si el riesgo para el interesado de Suplantación de Identidad existe o no en el caso evaluado.
3.- La comunicación o no a los interesados ha de basarse en un análisis de riesgos para sus derechos y libertades.
4.- No se justifica el retraso en la notificación a la Agencia de la brecha, lo que de por sí es un infracción que se sanciona.
5.- Con la Resolución no termina la gestión de la brecha, porque la Agencia requiere no solo que el Responsable solvente los incumplimientos detectados sino que debe aportar, en un plazo de 3 meses, las pruebas de que lo ha hecho.
6.- No obstante, a la hora de imponer algún tipo de sanción, la Agencia sí tiene en cuenta tanto la complejidad técnica de la brecha como todas las actuaciones que el Responsable realizó y justificó posteriormente haber realizado, para minimizar sus consecuencias.

RESOLUCIÓN - aepd		
Título Resolución:	Resolución Procedimiento Sancionador - Terminación por Pago Voluntario	
Organización - Pública / Privada - Sector:	Organización Privada - Seguros	
	DESCRIPCIÓN BRECHA	
Descripción Brecha Breve cronología	El 4-02-2021 un particular interpone una reclamación ante la AEPD, en la que manifiesta que ha recibido en su dirección de correo electrónico, en numerosas ocasiones, autorizaciones de pruebas médicas de terceros que no conoce. En algunos casos se incluye el tipo de prueba diagnóstica. Cada vez que recibía uno de estos correos el reclamante lo fue poniendo en conocimiento de la entidad (atención al cliente), de manera reiterada, reenviando la totalidad de los 51 correos electrónicos recibidos de 32 afectados distintos, sin que la reclamada actuara de ninguna forma hasta recibir traslado de la reclamación por la AEPD. La entidad mantuvo su error desde el 16-04-2020 al 9-03-2021. Aunque la entidad ha sufrido una brecha de seguridad de datos personales que se ha prolongado durante casi un año y de la que ha tenido constancia desde el principio, no lo ha notificado a la AEPD.	
	COMUNICACIONES EFECTUADAS - reclamado	
	SI/NO	Justificación Principal
Notificado a la aepd	**NO**	No se ha realizado ninguna justificación, lo que agrava la sanción ya que no se ha podido justificar la no notificación.
Comunicado a los afectados	**NO**	Emana de la falta de notificación previa ante la AEPD.
	PARAMETROS EVALUADOS	**VALOR**
Sobre la brecha	**Cómo ha sido el incidente**	Accidental
	Origen del incidente	Interno
	Consec. Del ciberinciden.	SI
Sobre las consecuencias	**Consec. Del incidente**	Datos personales de salud de otros clientes expuestos a tercera persona ajena.
Sobre las consecuencias	**Se ha recuperado los datos personales**	No se ha podido revertir el efecto de la brecha, puesto que los datos una vez exfiltrados han pasado a estar fuera el alcance del Responsable
	Grado en el que podría afectar	Ni el Responsable ni la Agencia hacen un análisis sobre las posibles consencuencias de la brecha, o al menos esto no se plasma en la Resolución.
	Se ha materializado alguno de los daños	
	Probabilidad de que el daño anterior se materialice	
Categoría de datos	**Tipos de datos afectados en personas físicas**	Datos de Salud
Personas afectadas	**Hay menores o vulnerables**	-
	Volumen de personas afectadas por la brecha	32
Inform. Temporal	**Momento en el que se conoció**	Desde el inicio, cuando se lo comunicó el reclamante, el 13-10-2020
Inform. Temporal	**Actuación ante la brecha**	Tardía, solo cuando la AEPD le trasladó la reclamación realizada por el particular.
	FUNDAMENTOS DE DERECHO - RESOLUCIÓN - aepd	
Infracción	**Art. 5.1.f) RGPD** (infracción tipificada Art. 83.5): la AEPD considera que la entidad no ha garantizado una seguridad adecuada de los datos personales, vulnerando en este caso su confidencialidad. **Art. 32 RGPD** (infracción tipificada Art. 83.4.a): la AEPD considera que como consecuencia de la implantación de medidas deficientes de seguridad se han visto expuestos a tercera persona ajena los datos personales de salud de otros clientes, que se han visto desprovistos del control sobre ellos. **Art. 33 RGPD** (infracción tipificada Art. 83.4.a): la AEPD considera que la entidad ha vulnerado la obligación de notificar ante la misma la brecha de datos personales sufrida, a pesar de las reiteradas advertencias del reclamante durante un año.	
Agravantes y Atenuantes	Art. 83.2.a RGPD: el error se mantuvo durante un año con advertencias reiteradas sin que actuara de ninguna forma. Art. 83.2.g RGPD: afectadas categorías especiales de datos personales, como son los datos de salud, que deberían gozar de especial protección y consideración. Art. 76.2.a LOPDGDD: carácter continuado de la infracción. Art. 76.2.b LOPDGDD: vinculación de la actividad del infractor con la realización de un volumen elevado de tratamientos de datos personales continuos.	
Resolución	Propuesta de sanción : (i) 100.000 € - por infracción del Art. 5.1.f) RGPD; (ii) 60.000 € - por infracción del Art. 32 RGPD; y (iii) 60.000 € - por infracción del Art. 33 RGPD. Finalmente la entidad sancionada reconoció su responsabilidad y pagó voluntariamente el importe total de 132.000 €	
	CONCLUSIONES - guía	
1.- La falta de diligencia por parte de la entidad ante la comunicación reiterada de los envíos de datos personales indebidos por parte del cliente que los recibía, manteniendo el error durante un año. 2.- La importancia de la afectación de categorías especiales de datos personales, como son los datos de salud, que deberían gozar de especial protección y consideración. 3.- La consideración por la Agencia de que no se trata de un fallo humano concreto, sino de una defectuosa configuración del CRM, lo que pone manifiesto que dichos errores son tan sólo la muestra de la falta de medidas de seguridad adoptadas por el responsable. 4.- La consideración de la infractora como una entidad especializada con la realización de un volumen elevado de tratamientos de datos personales continuos. 5.- La injustificada falta de notificación a la Agencia de la brecha.		

RESOLUCIÓN - aepd		
Título Resolución:	Resolución de terminación del procedimiento de pago voluntario	
Organización - Pública / Privada - Sector:	Organización Privada - Banca	
	DESCRIPCIÓN BRECHA	
Descripción Brecha Breve cronología	25 marzo 2020: un interesado denuncia que la entidad reclamad facilita el detalle de los últimos movimientos de su tarjeta en la entidad mediante un sistema de atención telefónica automatizado en el que únicamente se pide como dato identificativo el DNI del cliente. 25 septiembre 2020: tras darle traslado de la reclamación, la entidad manifiesta que no se indicó el plazo de respuesta, lo que supone un error en la tramitación y solicita la parálisis del procedimiento de acuerdo al artículo 76.2 de la ley 39/2015 hasta que el error sea subsanado y se le solicite de nuevo la información. 4 diciembre 2020: se admite la reclamación presentada por el interesado y se lleva a trámite. 10 diciembre 2020: se envía el requerimiento al reclamado.	
	COMUNICACIONES EFECTUADAS - reclamado	
	SI/NO	Justificación Principal
Notificado a la aepd	NO	No aplica
Comunicado a los afectados	NO	No aplica
	PARAMETROS EVALUADOS	**VALOR**
Sobre la brecha	**Cómo ha sido el incidente**	No aplica
	Origen del incidente	No aplica
	Consecuencias Del ciberincidente	No aplica
Sobre las consecuencias	**Consec. Del incidente**	No se han materializado
Sobre las consecuencias	**Se ha recuperado los datos personales**	No aplica
	Grado en el que podría afectar	Acceso a los datos
	Se ha materializado alguno de los daños	No hay información en el Expediente
	Probabilidad de que el daño anterior se materialice	No hay información en el Expediente
Categoría de datos	**Tipos de datos afectados en personas físicas**	Datos bancarios
Personas afectadas	**Hay menores o vulnerables**	No
	Volumen de personas afectadas por la brecha	Gran volumen de afectados
Inform. Temporal	**Momento en el que se conoció**	Tras la primera comunicación de la AEPD.
Inform. Temporal	**Actuación ante la brecha**	Deficiente
	FUNDAMENTOS DE DERECHO - RESOLUCIÓN - aepd	
Infracción:	**Art. 32 RGPD**: se requiere que el reclamado adopte medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado utilizando mecanismos que permitan: (i) la seudonimización y el cifrado de datos personales; (ii) la capacidad de garantizar la confidencialidad, integridad, disponibilidad y resiliencia permanentes de los sistemas y servicios de tratamiento; (iii) la capacidad de restaurar la disponibilidad y el acceso a los datos personales de forma rápida en caso de incidente físico o técnico; (iv) un proceso de verificación, evaluación y valoración regulares de la eficacia de las medidas técnicas y organizativas para garantizar la seguridad del tratamiento.	
Agravantes y Atenuantes:	Art.83.2.a): el número de clientes de la entidad es elevado al igual que el número de afectados. Art 83.2.b): negligencia por la ausencia de las medidas de seguridad adecuadas, siendo la entidad solvente. Art. 83.2.d): se agrava debido a la plena consciencia de las medidas de seguridad necesaria para el tratamiento de datos personales debido al constante trato de estos datos por la actividad que realiza el reclamado. Art 83.2.f): por la falta de colaboración con la Agencia.	
Resolución	De conformidad con lo previsto en el artículo 58.2.b) del RGPD, por la presunta infracción del artículo 32 del RGPD, tipificada en el artículo 83.4.a) del RGPD. La reducción por el pago voluntario de la sanción es acumulable a la que corresponde aplicar por el reconocimiento de la responsabilidad, el importe de la sanción quedaría establecido en 120.000€ (ciento veinte mil euros).	
CONCLUSIONES - guía		
1.- Aunque aún no se haya materializado una brecha de datos, las deficiencias en materia de medidas de seguridad que se tengan en el diseño de los sistemas de tratamiento automatizado ya suponen una responsabilidad y una infracción, según constata la AEPD. Para el uso de buenas prácticas, se recomienda la protección de estos datos desde el diseño, siguiendo así el Reglamento General de Protección de Datos. 2.- También ha de darse prioridad a este tipo de brechas y enfocar los esfuerzos desde el primer momento de su conocimiento en vez de intentar posponer los posibles daños recibidos. 3.- No hay peor brecha que la que no se gestiona		

RESOLUCIÓN - aepd		
Título Resolución:	RESOLUCIÓN DE TERMINACIÓN DEL PROCEDIMIENTO POR PAGO VOLUNTARIO	
Organización - Pública / Privada - Sector:	Organización Privada	
	DESCRIPCIÓN BRECHA	
Descripción Brecha Breve cronología	La parte reclamante pone de manifiesto a la Agencia que ha recibido un email por parte del responsable del portal web de la organización informando que un tercero no autorizado había logrado acceder a la base de datos en la que se encontraban datos de localización y contacto de las personas que habían facilitado esta información en el portal web a través de un formulario. El Responsable aseguró haber corregido todas las vulnerabilidades que hacían posible el acceso, implantado protocolos de incidentes de seguridad y adoptado una serie de medidas, como el cifrado de la información almacenada.	
	COMUNICACIONES EFECTUADAS - reclamado	
	SI/NO	Justificación Principal
Notificado a la aepd	Sí	
Comunicado a los afectados	Sí	
	PARAMETROS EVALUADOS	**VALOR**
Sobre la brecha	**Cómo ha sido el incidente**	No malicioso
	Origen del incidente	Externo
	Consec. Del ciberinciden.	Sí
Sobre las consecuencias	**Consec. Del incidente**	No se han materializado
Sobre las consecuencias	**Se ha recuperado los datos personales**	No aplica
	Grado en el que podría afectar	Acceso ilícito a los datos
	Se ha materializado alguno de los daños	No
	Probabilidad de que el daño anterior se materialice	Baja tras medidas técnicas aplicadas
Categoría de datos	**Tipos de datos afectados en personas físicas**	Datos identificativos, de contacto, datos de localización aproximada y en algunos casos datos identificativos de hijos menores de edad.
Personas afectadas	**Hay menores o vulnerables**	Sí
	Volumen de personas afectadas por la brecha	47.000 afectados
Inform. Temporal	**Momento en el que se conoció**	22 de octubre 2021
Inform. Temporal	**Actuación ante la brecha**	22 de octubre 2021
	FUNDAMENTOS DE DERECHO - RESOLUCIÓN - aepd	
Infracción:	Artículo 5.1.f: en el presente caso, consta que los datos personales de los afectados, obrantes en la base de datos de la organización, fueron indebidamente expuestos a un tercero. Artículo 32: si bien el análisis de riesgos que aportan es el reporte de salida generado por la herramienta GESTIONA EIDP de esta Agencia, el mismo carece de la identificación de factores que hagan referencia a posibles amenazas de ataques web relacionadas con la pérdida de confidencialidad, disponibilidad o integridad de los datos personales tratados a través del propio portal. Artículo 33: existe dilación temporal en relación con la notificación de la brecha a esta Agencia y a los afectados.	
Agravantes y Atenuantes:	Art 83.2 RGPD: g) la categoría sensible de los datos de carácter pesonal afectados por la infracción Art76.2 LOPDGDD: b)La vinculación entre la actividad del reclamado y la realización del tratamiento de datos f)Afectación a datos de menores de edad.	
Resolución	Debido al artículo 64.2.b) de la ley 39/2025 las sanciones serán de: 30.000 euros (treinta mil euros) por la infracción del artículo 5.1.f) del RGPD, 20.000 euros (veinte mil euros) por la infracción del artículo 32 del RGPD, tipificada en el artículo 83.5 del RGPD 2.000 euros (dos mil euros) por la infracción del artículo 33 del RGPD, tipificada en el artículo 83.4 del RGPD Se resuelve una sanción total de 50.000 euros (cincuenta mil euros) quedando en 31.200 euros debido a las reducciones por alegación de responsabilidad consideradas en el artículo 85 de la LPACAP.	
CONCLUSIONES - guía		
1.- Tras la resolución se puede observar la necesidad de subsanar ciertos requerimientos por parte del reclamado. 2.- La identificación y gestión del riesgo requiere un proceso mucho mas exahustivo que el simple uso de una herramienta, aunque esta sea la de la propia Agencia. 3.- La Agencia basa su sanción que la necesidad de establecer un mayor criterio de seguridad y sobre todo de análisis de riesgo ya que se evidencia `l*a falta del mismo derivando en brechas de seguridad y privación de derechos y libertades de los interesados* ".		

RESOLUCIÓN - aepd		
Título Resolución:	RESOLUCIÓN DE TERMINACIÓN DEL PROCEDIMIENTO POR PAGO VOLUNTARIO	
Organización - Pública / Privada - Sector:	Organización Privada - Telecomunicaciones	
	DESCRIPCIÓN BRECHA	
Descripción Brecha Breve cronología	Tras ejercer su derecho a oposición y supresión, el afectado aporta captura de 26 SMS entre el 22 de septiembre y el 15 de octubre de 2020. Ese mismo mes el afectado accede a su área personal en la entidad reclamada y accede a datos de terceros, incluyendo datos identificativos, de contacto y bancarios con la posibilidad de realizar trámites. El afectado amplía la denuncia por la utilización de datos de manera fraudulenta y reiterada tras recibir SMS informando al usuario de la existencia de problemas técnicos para la gestión de sus solicitudes y la posterior subsanación de los mismos. 19 julio 2020: el interesado reclama ante la Agencia por no haber visto atendido su derecho de oposición tras recibir múltiples SMS publicitarios de la reclamada. La reclamación no se admite por considerarse que el Responsable ha gestionado el derecho de oposición. 16 octubre 2020: el interesado vuelve a reclamar porque sigue recibiendo SMS comerciales de la reclamada 31 octubre 2020: amplia reclamación porque ha recibido SMS con clave de acceso a un espacio privado de cliente de la Reclamada que le ha permitido acceder a la información personal y confidencial de un tercero. La entidad reclamada contesta en varias ocasiones que ha procedido a eliminar el número de teléfono móvil del reclamante de las bases de datos que gestiona, pero los envíos de SMS siguen produciéndose.	
	COMUNICACIONES EFECTUADAS - reclamado	
	SI/NO	Justificación Principal
Notificado a la aepd	NO	No aplica
Comunicado a los afectados	NO	No aplica
	PARAMETROS EVALUADOS	**VALOR**
Sobre la brecha	**Cómo ha sido el incidente**	No malicioso
	Origen del incidente	Interno
	Consec. Del ciberinciden.	No
Sobre las consecuencias	**Consec. Del incidente**	Vulneración de derechos y pérdida de confidencialidad de datos
Sobre las consecuencias	**Se ha recuperado los datos personales**	No aplica
	Grado en el que podría afectar	Acceso ilícito a los datos y vulneración de derechos
	Se ha materializado alguno de los daños	Sí
	Probabilidad de que el daño anterior se materialice	Materializado
Categoría de datos	**Tipos de datos afectados en personas físicas**	Datos identificativos, de contacto y bancarios.
Personas afectadas	**Hay menores o vulnerables**	No
	Volumen de personas afectadas por la brecha	1
Inform. Temporal	**Momento en el que se conoció**	19 de julio de 2020
Inform. Temporal	**Actuación ante la brecha**	Insuficiente por reiteración de la misma
	FUNDAMENTOS DE DERECHO - RESOLUCIÓN - aepd	
Infracción	Artículo 5 y 32 RGPD: el hecho de que la entidad reclamada posibilitara la visualización de datos personales de una tercera persona ajena al reclamante, permiten constatar que el reclamado no ha podido garantizar la seguridad en el tratamiento de los datos personales de sus clientes, mostrando con ello una grave falta de diligencia, por vulneración de los principios de integridad y confidencialidad de los datos personales, así como la responsabilidad proactiva del responsable del tratamiento de demostrar su cumplimiento. Artículo 17 RGPD: incumplimiento del derecho de supresión de los datos personales del interesado, cuando éste había ejercido el derecho de oposición ante la entidad y está había incluso confirmado que había gestionado correctamente dicho derecho. Artículo 21 de la LSSI: por el envío de una gran cantidad de SMS publicitarios o comerciales, sin la autorización del interesado y después de que la entidad reclamada afirmara que habían atendido la solicitud de del interesado de no volverle a enviar SMS.	
Agravantes y Atenuantes:	Art.83.2: se agrava la situación debido a la duración de la infracción por más de un año; la negligencia en la infracción tras el incumplimiento de las obligaciones en la gestión de datos personales; la forma en que llegó la información a la autoridad de control con denuncias y inadmisión de la denuncia previa por parte del reclamante debido a que el reclamado aseguró haber tomado las medidas necesarias al respecto no siendo cierto. Art. 83.2.k): se agrava la situación debido a la continuación de la infracción con el envío de SMS al reclamante, pese a que el reclamado asegurara su borrado de datos en la base de datos. Art.40 de la LSSI: existencia de intencionalidad por la falta de un sistema de obtención de consentimiento informado adecuado; plazo de tiempo elevado en el que se comete la infracción sin ser solventada.	
Resolución	50.000 euros (cincuenta mil euros) por la infracción del artículo 17 del RGPD. 30.000 euros (treinta mil euros) por la infracción del artículo 32 del RGPD. 50.000 euros (cincuenta mil euros) por la infracción del artículo 5.1.f) del RGPD. 20.000 euros (veinte mil euros) por la infracción del artículo 21 de la LSSI. Total de 150.000 euros (ciento cincuenta mil euros) reducida a 90.000 euros (noventa mil euros) si el pago se realizase previo a la resolución.	
	CONCLUSIONES - guía	
1.- Se concluye que por parte del reclamado son necesarias una serie de medidas urgentes para subsanar lo aquí dispuesto. Es grave la dejadez demostrada en la verificación de las denuncias previas ya existentes, teniendo como medida de contención la comunicación con el cliente en vez de la solventación directa del problema. 2.- No debe existir jamás una falta de seguimiento de estos asuntos y menos cuando se ha notificado y comunicado al interesado que se iba a solventar, demostrando luego que no se ha realizado. Agrava más aún la situación ver que no solo no existe la solventación del problema si no que el reclamante descubre nuevas infracciones. 3.- Es necesaria, por tanto, un ejercicio de verificación del plan de acción a llevar ante estas situaciones para que no se puedan ver tan perjudicados los clientes del servicio del reclamado.		

II Guía [práctica] para la Gestión de Brechas de Datos Personales

www.ismsforum.es
info@ismsforum.es
(+34) 915 63 50 62

@ISMSForum
ISMS Forum

Una iniciativa de

isms forum
dpi DATA PRIVACY INSTITUTE