

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



Un documento de

isms
FORUM

INTERNATIONAL
INFORMATION
SECURITY
COMMUNITY

dpi
DATA PRIVACY INSTITUTE

JUNIO 2022

COORDINADORES:

Susana Rey Baldomir
Javier Lomas Sampedro

SUBCOORDINADORES

Elena Mora González
Oscar López Benito

PARTICIPANTES

Carmen Tejeira
Patricia Muleiro
Gustavo Lozano
María José Carmona
Marta Concepción Cañas
Gisela Reverter
Oscar Antonio Sánchez
Sonia Beulas
Rosa Corredera
Maria Soledad Capozzi
Francisco Lázaro
Ignacio Puente

REVISORES

Esmeralda Saracíbar
Carmen López

DISEÑO Y MAQUETACIÓN

Cynthia Rica Gómez

ÍNDICE DE CONTENIDOS

1	INTRODUCCIÓN: OBJETIVO Y ALCANCE DE LA GUÍA	6
2	EL ACCOUNTABILITY COMO MEJOR ESTRATEGIA ANTE LAS BRECHAS	8
3	CICLO DE VIDA DE LAS BRECHAS DE DATOS PERSONALES	9
4	PLANIFICA	10
4.1	.APRENDIENDO A IDENTIFICAR UNA BRECHA DE DATOS PERSONALES	10
4.2	.DEFINICIÓN DE INCIDENTE DE SEGURIDAD	11
4.3	. DOCUMENTACIÓN SISTEMÁTICA DE LOS PROBLEMAS E INCIDENTES	12
4.4	.DEFINAMOS ESCENARIOS	12
4.5	. DESCRIPCIÓN DE LOS ESCENARIOS/CASOS DE USO	14
4.6	GOBERNANZA Y COMPROMISO DE LA ALTA DIRECCIÓN	15
4.7	PROTOCOLOS INTERNOS	15
4.8	ASIGNACIÓN DE ROLES Y RESPONSABILIDADES. ÁREAS IMPLICADAS	15
4.9	PUESTA A PRUEBA DE LOS PROTOCOLOS	18
5	GESTIONA	20
5.1	EQUIPO DE TRABAJO	20
5.2	FASES DE LA GESTIÓN DE LA BRECHA DE DATOS PERSONALES	22
5.2.1	ACTIVACIÓN DEL PLAN	22
5.2.2	CONTENCIÓN DEL INCIDENTE	24
5.2.3	ERRADICACIÓN	25
5.2.4	RECUPERACIÓN	26
5.2.5	PROCESO DE NOTIFICACIÓN	27
6	NOTIFICA	28
6.1	NOTIFICA A LA AEPD	28
6.2	COMUNICA A LAS PERSONAS FÍSICAS AFECTADAS	30
6.2.1	FORMAS Y PLAZOS PARA COMUNICAR	34
6.2.2	NOTIFICACIONES INDIRECTAS	35
6.2.3	CONTENIDO DE LA COMUNICACIÓN A LOS AFECTADOS	36
6.2.4	SUPUESTOS DE NO COMUNICACIÓN A AFECTADOS	36
7	RESUELVE	38
7.1	AEPD	39
7.2	OTROS REGULADORES	39
7.3	PERSONAS FÍSICAS AFECTADAS	40
7.4	IMPACTO PÚBLICO	40

7.5 TERCEROS: ENCARGADOS, CIBERSEGUROS	41
7.6 COMUNICACIÓN INTERNA: DIRECCIÓN, EMPLEADOS, ACCIONISTAS Y SOCIOS	42
7.7 SEGUIMIENTO Y CIERRE	43
7.8 INFORME FINAL.	44
ANEXO I - PROTOCOLOS INTERNOS	46
ANEXO II - MODELO DE INFORME FINAL	48
ANEXO III - CASOS PRÁCTICOS	50
• RANSOMWARE	51
• EMPLEADO QUE SE LLEVA LA BASE DE DATOS DE CLIENTES A LA COMPETENCIA	56
• ERROR EN PASE A PRODUCCIÓN DE UNA WEB DE VENTA ONLINE CON AFECTACIÓN INTERNACIONAL	60
• SUPLANTACIÓN DE IDENTIDAD EN OPERADORA DE TELECOMUNICACIONES	68
• DESTRUCCIÓN SOPORTES DE INFORMACIÓN	71
• BRECHA DE SEGURIDAD EN TU PROVEEDOR EN LA NUBE	77
• BRECHA RELACIONADA CON EL PAPEL	85
• BRECHA DE SEGURIDAD OCASIONADA POR UN ERROR HUMANO EN EL SISTEMA DE ENVÍO DE COMUNICACIONES A CLIENTES.	89
• ROBO DE CUENTAS CORREO, REGISTROS WEB, ETC	92

1

INTRODUCCIÓN: OBJETIVO Y ALCANCE DE LA GUÍA



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.

Cuando en mayo de 2018 se hizo exigible el Reglamento General de Protección de Datos (en adelante, RGPD), una de las principales novedades a las que nos tuvimos que enfrentar como responsables y encargados de los tratamientos de datos personales en nuestras organizaciones, fue la doble obligación de, en determinadas circunstancias, notificar las brechas de datos personales a las autoridades de control y comunicarlas a las personas físicas afectadas.

Desde hace muchos años se han venido produciendo iniciativas destinadas a establecer vías o espacios donde compartir información, no solo técnica sino también de gestión, entre los profesionales de la ciberseguridad. En un mundo hiperconectado, los incidentes no son 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.

Aunque la obligación de notificar las brechas de seguridad a las diferentes autoridades de control naciese como un instrumento de ayuda y apoyo a las empresas y organizaciones que las estuviesen sufriendo y de prevención para el resto, no debemos olvidar que 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 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.

Cuando la Agencia Española de Protección de Datos (en adelante, AEPD) publicó en 2018, en colaboración con el ISMSForum, la **‘Guía para la gestión y notificación de brechas de seguridad’**, ya se buscaba “facilitar la interpretación del RGPD en lo relativo a la obligación de notificar (...) de modo que la notificación a la autoridad competente se haga por el canal adecuado, contenga información útil y precisa”.

Tras apenas tres años desde la publicación de aquella primera guía, la AEPD acaba de publicar en mayo de este 2021, la **‘Guía para la notificación de brechas de datos personales’**, orientada a proporcionar directrices generales en la notificación de brechas de datos personales y en la comunicación a los interesados, precisando plazos y aspectos concretos sobre el procedimiento para notificar y sobre el contenido de las notificaciones. Recomendamos a nuestros lectores que tengan por referencia la guía de la AEPD sobre todo para entender cómo y cuándo se debe tanto notificar a la AEPD como comunicar a los afectados por una brecha.

La presente **‘Guía [práctica] para la gestión de brechas de datos personales’** (en adelante, la Guía), nace con la intención de complementar a la de la Agencia, retoma el espíritu de la primera en su objetivo de 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 tenido que aplicar los artículos 33 y 34 del RGPD durante estos tres primeros años.



Uno de los más importantes mensajes de la primera guía de 2018 es que la mera notificación de una brecha de seguridad no supone la imposición de una sanción por parte de la AEPD, lo que sí resultaría de la falta de diligencia. Debemos cuidar y anticiparnos al máximo para evitar, además, el impacto reputacional de trascender que la brecha sufrida se debió en parte a nuestra acción u omisión.

Para ello, hemos organizado la presente Guía 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.

Esperamos que esta Guía nos ayude a conocer la posición y capacidad real que tienen cada una de nuestras organizaciones ante estas inevitables y permanentes amenazas; revelando lo preparados que realmente estamos para una gestión adecuada, nuestras fortalezas y las debilidades que deberemos corregir en nuestras organizaciones, si queremos hacer de la gestión de las brechas de datos personales una herramienta útil de mejora.



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.

2

EL ACCOUNTABILITY COMO MEJOR ESTRATEGIA ANTE LAS BRECHAS

Las brechas ocurren, por mucho que invirtamos en ello, y tenemos que hacerlo, pero se sucederán, no hay riesgo cero. Por ello, la mejor planificación y gestión que podamos hacer de las brechas de datos personales en nuestras organizaciones se hará cumpliendo y demostrando que cumplimos el RGPD, nuestro obligado accountability.

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.

Además, cabe la posibilidad de que, tras la notificación a la autoridad de control de una brecha de datos personales, nos requiera ampliar la información sobre ese incidente, lo que tendrá que cumplirse en un plazo de tiempo corto. Las organizaciones deberemos tenerlo ya previsto, tener revisado en todo momento qué cumplimos y cómo acreditarlo, prueba de nuestra diligencia debida y accountability, con la disponibilidad de la documentación que lo acredite:

- Registro de Actividades de tratamiento – RAT: relativo al tratamiento donde ocurrió la brecha;
- Análisis de riesgos practicados;
- Evaluaciones de Impacto del Tratamiento (relativo a dónde ocurrió la brecha);
- 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 diplomas de superación (si tras la brecha hubo personas internas o externas involucradas);
- Contratos y anexos relativos a los encargados o responsables que hubieran participado de esa brecha;
- Listado de controles y monitorización puestos en práctica para evitar que sucediera lo que haya pasado;
- Plan de Comunicación; mensajes del DPD convocando al comité de crisis, informando a la Alta Dirección sobre el incidente, comunicación interna del incidente a interesados.



La seguridad 100% no existe, ser diligente no va de cero riesgos, va de balancearlos; marca tu nivel de tolerancia al riesgo y que lo apruebe la Alta Dirección.

CICLO DE VIDA DE LAS BRECHAS DE DATOS PERSONALES

3

Desde ese sentido práctico y diferenciador del que se ha querido dotar a esta Guía, con una clara orientación hacia la diligencia debida y 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; procedimientos, criterios, asignación de responsabilidades, pruebas previas conformarán la preparación previa para no tener que improvisar en caso de brecha.

En un segundo bloque, durante la brecha, estaremos en la fase de **gestiona**, donde revisaremos la importancia para la organización de estar preparada para afrontar el incidente de seguridad de forma rápida, ordenada y eficaz, minimizando sus consecuencias sobre la propia organización y terceras partes implicadas, lo que sin duda será analizado con detenimiento por la AEPD. Si estamos preparados para: detectar-analizar-contener-mitigar-recuperar una brecha, 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.

Por último, pero no menos importante, 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.

4

PLANIFICA

La mejor planificación de una brecha es evitar que se produzca, pero como sabemos que se van a producir, lo mejor es prepararse para esas situaciones previamente. Planificación es por tanto una fase clave donde cada organización debe tener claramente identificado todo lo que va a necesitar en la fase de gestión para que esté previamente preparado, documentado y probado.



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

4.1. Aprendiendo a identificar una brecha de datos personales

Empecemos por el principio, el concepto inicial. Debemos ser muy conscientes de lo que es una brecha de datos personales para saber cómo gestionarla y cumplir con el artículo 33 y 34 del RGPD. Debemos aprender a identificarlo en nuestras organizaciones. Pueden estar sucediendo ya brechas que pasen desapercibidas para el DPD.

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.

Es fundamental la **comunicación** entre la función de gestión de seguridad y la de protección de datos y 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 ser¹.

¹En la 1ª Encuesta sobre Brechas de Seguridad del ISMS Forum más del 30% de los encuestados en empresas que operan en el mercado español únicamente dicen no haber sufrido brechas en los dos últimos años, frente al 20% de empresas que operan en mercados internacionales.

¹En esta misma encuesta se observa que mientras que el porcentaje de empresas sin brechas en dos años en el caso de que el encuestado tenga funciones de privacidad en la compañía está en el entorno del 25%, para el caso de CISOs en exclusiva, este valor sube al 45%

4.2. Definición de 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 NIS define 'incidente' como "todo hecho que tenga efectos adversos reales en la seguridad de las redes y sistemas de información" y el propio RGPD define, de un modo amplio, las "violaciones de seguridad de los datos personales" como "todas aquellas violaciones de la seguridad que ocasionen la destrucción, pérdida o alteración accidental o ilícita de datos personales transmitidos, conservados o tratados de otra forma, o la comunicación o acceso no autorizados a dichos datos".

En el proceso de Gestión de Problemas del marco de ITIL/ISO20000 se distingue entre incidente e incidencia, siendo esto segundo una serie de eventos que denotan que existe un problema y que, si no se afronta, puede terminar en incidente de seguridad.

Además, no hay que 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.

A nivel operativo, es recomendable incluir en los modelos de valoración de las incidencias, dentro del proceso de gestión de problemas (muy ligado a la filosofía ITIL) de la organización un primer análisis de riesgos en protección básico. Así como revisar, 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 el concepto de brecha está bien interiorizado entre los empleados o se está perdiendo por una falta de concienciación y se viene resolviendo por las áreas operativas (áreas de Negocio y TI) sin ser informado previamente.

Por ejemplo, que los sistemas de seguridad de la compañía 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 esta se está produciendo realmente. Pero sólo si entre los datos exfiltrados hay datos de nuestros clientes, por ejemplo, tenemos una brecha de datos personales.

Siguiendo con este ejemplo, tenemos una brecha materializada claramente. Pero aún nos queda evaluar según la tipología de datos si realmente hay riesgo o no para los interesados cuyos datos se están exfiltrando. No sería lo mismo en este sentido que se traten de datos públicos, por ejemplo, que no tendrían impacto negativo en los interesados, o que sean datos financieros detallados que pueden provocar pérdidas dinerarias importantes en los mismos.



4.3. Documentación sistemática de los problemas e incidentes

Venimos 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 privacidad 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 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.

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 operativizarla al máximo con casos de uso y escenarios sacados de su propia realidad o de sectores afines.

Para ello creemos que puede ser de utilidad remitirles tanto a la Opinión 03/2014 que en su momento emitiese el WP art 29 (actual EDPB) o al WP 250 de dicho EDPB, así como a la más reciente Guía 01/2021 de Casos Prácticos de Notificación de Brechas de datos (EDPB) donde se estratifican claramente los incidentes de datos personales en tres fases muy diferenciadas:

- Documentación (siempre).
- Notificación a la autoridad de control (a veces).
- Comunicación a los afectados (cuando la ocasión lo requiera).

4.4. Definamos escenarios

La AEPD aclara que, si bien no hay un margen temporal establecido para concluir los análisis de riesgos, los mismos deben realizarse con la máxima celeridad y diligencia aplicando un enfoque de “contingencia” y por tanto no vale que retrasemos la notificación de una posible brecha porque tenemos un análisis de riesgo que se dilata y dilata a la espera de evidencias y respuestas de terceros.

En este sentido, nuestra recomendación es que reproduzcamos la típica filosofía con que se abordan los planes de continuidad de negocio y planes de contingencias en las organizaciones. Reproducir esta filosofía 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 seguridad concreta, diferenciando tipología del incidente en base a las tres variables de seguridad: confidencialidad, integridad y disponibilidad.

No queremos decir con esto que una compañía deba tener un Plan de Continuidad de Negocio, aunque recordemos que la disponibilidad y resiliencia son ahora requisitos exigidos por el RGPD, es probable que algunas no lo tengan; lo que recomendamos es reproducir su filosofía. Aunque en el caso de que sí exista el Plan de Continuidad de Negocio, se recomienda que incluya, bien de forma transversal en todos los escenarios o con escenarios específicos, la forma de actuar en función del tipo de brecha de datos personales.

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 empresas similares. Y, como si de un escenario de contingencia realmente se tratase, se abordará a través de un Comité de Crisis.

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

A nivel interno:

- Acceso al 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 compañía).
- Sucesos importantes en otras compañías del propio grupo empresarial.

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, a través de un modelo de interfaz de funciones, conseguir toda esta información. En ese procedimiento se detallará 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, es interesante este modelo de interfaz o 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 la organización.

Esta información interna se completaría con otra obtenida de fuentes externas, como sería a través de la consulta y análisis de:

- Los informes de brechas mensuales que publica la AEPD.
- Las publicaciones de brechas de seguridad comunicadas por otras compañías a nivel mundial.
- Consultas a publicaciones de INCIBE sobre incidentes.
- Contactos con homólogos de otras empresas del mismo sector o afines.
- Pertenencia a Asociaciones ligadas al ámbito de la privacidad.
- Consulta de procedimientos sancionadores en toda Europa², así como las publicaciones de procedimientos sancionadores de la propia 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 Casos de Uso de Brechas de Datos Personales en la organización, debemos detallar quién será el responsable de gestionarlo. Estos casos de uso se deben ir revisando con carácter anual e incorporando otros nuevos, con base en la revisión de todos los anteriores orígenes de datos.

4.5. Descripción de los escenarios/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.
- 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

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

4.6. Gobernanza y compromiso de la alta dirección

Una vez definido el Plan de Escenarios de Brechas de Datos Personales, debiera ser presentado y aprobado por la alta dirección de la organización, al igual que el resto de políticas y procedimientos elaborados sobre esta materia.

La Gobernanza (otra palabra que no aparece en el RGPD) en materia de brechas de datos personales es tanto o más importante aún que la Gestión de las brechas en sí. No entendemos diligencia ni accountability en una compañía que no se ha preocupado por los aspectos de Gobernanza.

Con Gobernanza nos referimos al contenido mínimo de las políticas y procedimientos de *reporting* tanto de este tipo de pruebas como en general del sistema de revisión y control que continuamente está monitorizando las actividades de tratamiento y los requisitos exigidos por el RGPD y la LOPDGDD. No solo al *reporting*, también al sistema de control interno para supervisar el seguimiento del cumplimiento de las acciones de mejora que surten fruto de esas pruebas de contingencia y cómo la alta dirección se encarga de cuestionar la rendición por parte del DPD, de dotar de un presupuesto mínimo que le permita gestionarlas y proporcionarles esos medios técnicos y humanos necesarios para ello.

4.7. 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 la labor de concienciación y formación de todo el personal de la empresa que en el ejercicio de sus funciones acceda a datos personales.
- Deben estar adaptados a las características de cada organización.

4.8. 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. Así mismo, a lo largo de las fases de gestión de un incidente existirán muchas áreas implicadas.



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 – artículo 32 del RGPD.

Algunas de las acciones recomendadas en esta fase serían:

- 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 como puede ser en el campo de 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 en los que detectar áreas de mejora que luego puedan ponerse en práctica.

Es especialmente importante contar y coordinarse con las siguientes áreas:

- **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.
- **Seguridad.** Este equipo debe dar soporte en todo momento al DPD, comunicando cualquier cambio que pudiera modificar el análisis de riesgo inicial, y trabajando conjuntamente, tanto en esta fase como en la posteriores.
- **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.

- **Otras primeras líneas de Defensa:** sin duda todas las líneas de defensa están involucradas en la gestión anticipada de un incidente de seguridad.

La primera línea juega el papel fundamental de la detección y de la prevención de que suceda el incidente de seguridad. Son quienes están en primera línea de los procesos y los datos, tratándolos y por tanto su alerta temprana y su capacidad para reconocerlos es básica.

La segunda línea tiene un enfoque más preventivo y Auditoría más detectivo, pero también son claves.

Para anticipar los incidentes de seguridad es clave la gestión de los riesgos desde el inicio. Para ello el enfoque que recomendamos y que siguen muchas organizaciones es el que se conoce como modelo de las tres líneas de defensa.

EL MODELO DE LAS TRES LINEAS DE DEFENSA



Adaptado de la Guía emitida por ECIIA/FERMA sobre la 8va Directiva de Derecho de Sociedades de la Unión Europea, artículo 41

Como resumen básico, la primera línea son todas las áreas operativas y de gestión (i.e. legal, financiero, logística, contratación, prestaciones, atención al cliente, RRHH, etc.) que son las que realizan los procesos y siguen los procedimientos establecidos.

La segunda línea es la que define los controles y aplica medidas sobre cómo deben ser los procedimientos para que no se materialicen esos riesgos (DPD, Compliance, Gestión de Riesgos e incluso Calidad o Seguridad en algunas organizaciones son segunda línea).

La tercera línea de defensa es Auditoría, quien hace un aseguramiento independiente de que la primera línea de defensa actúa conforme a lo que le ha dicho su segunda línea, la de riesgos.

- **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 empresa o en sus proveedores. Asumen por lo tanto un rol preventivo, pero al mismo tiempo reactivo.
- **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 de partes interesadas queremos destacar la importancia de los proveedores y, sobre todo, de los que tengan el perfil de Encargados del Tratamiento, y que por tanto están gestionando datos de carácter personal, aunque haya sido la compañía, como Responsable del Tratamiento, quien haya definido la finalidad o el medio de cómo hacerlo.

Los proveedores están obligados ahora a avisar a las compañías si creen que alguna de sus órdenes incumple los principios del RGPD (y que por tanto pudiera detonar 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.



La gestión de incidentes de seguridad no es solo un tema de Tecnología, lo es de todas las áreas de actuación de las organizaciones, identificadas como líneas de defensa.

4.9. Puesta a prueba de los protocolos

Como ya comentamos al principio de esta sección, 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 compañía.

La filosofía que indica 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 Brechas³.

³Una de las conclusiones extraídas de la 1ª Encuesta sobre Brecha de Datos Personales de ISMSForum es que tras haber sufrido una brecha las empresas se sienten menos preparadas para acometer la siguiente. Es decir, se detectan puntos de mejora, sobre todo en cuanto al conocimiento sobre la Gestión de Brechas dentro de las organizaciones.

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, etc⁴.

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 compañías, cambios en el equipo del Comité de Crisis, etc.).

La concienciación al Comité Directivo es fundamental, se les involucrará en el diseño de las pruebas o al menos se les informará formalmente del desarrollo de estas pruebas y resultados. Para mayor eficacia, 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.

⁴Tener en cuenta en el diseño de esos escenarios, en caso de que se utilicen sets de datos, que se haya anonimizado o desvirtuado la información de forma tal que no pueda acabarse notificando un correo electrónico a un cliente de la compañía por un error en dichas pruebas.

5

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 efectúan los análisis de riesgos para determinar si hubo tal brecha o no.



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. Este apartado se centra en la gestión propiamente dicha del evento o incidente, su documentación, notificación a la entidad de control y comunicación a los interesados. Con toda la documentación del Planifica, y en el corto margen de tiempo de 72 horas naturales, desde que nuestro análisis de riesgo nos concluye que ha tenido lugar una brecha, deberemos tomar la decisión de notificar la brecha, y estar en condiciones de hacerlo siguiendo los procedimientos que esta pautas, si se comunica o no a los afectados y organizar toda la documentación e indicadores que acompañará a ese reporte.

5.1. 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 de seguridad, 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.

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.
- Comunicado a los empleados.
- Comunicado a los proveedores.
- Comunicado a otros grupos de interés (accionistas, sindicatos, comunidad local, entidades financieras, aseguradoras).

En la fase de gestión de la brecha será muy importante tener en cuenta a los siguientes grupos y áreas de trabajo de la compañía y su función en esta fase de la brecha.

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

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.

Comunicación interna/externa: Dependiendo de la entidad del incidente de Seguridad 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.).

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.

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.

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.

5.2. Fases de la gestión de la brecha de datos personales

En gestión de las brechas de datos personales, desde el momento en que se ha concluido que el incidente de seguridad 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).

La fase de Gestión propiamente dicha de la brecha, consta a su vez de seis sub-fases: (i) activación del plan; (ii) contención; (iii) erradicación; (iv) recuperación; (v) documentación y comunicación; y (vi) seguimiento y cierre.

5.2.1. Activación del plan



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

Como dijimos en el Planifica, lo primero de todo es ser rápidos en esta fase, tratar el incidente como una gestión de crisis en la organización (en el momento en que se concluye que se trata de una brecha, todas las partes interesadas deben ser sensibles a esta premura).

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 de la brecha de seguridad: con toda la información aportada por los medios de detección y toda la información adicional recopilada es importante hacer una clasificación precisa del incidente de seguridad. De la clasificación del incidente de seguridad dependerán las acciones a emprender durante los procesos de gestión y notificación.

- Es especialmente importante determinar si efectivamente se está ante una brecha de datos personales, en cuyo caso es imprescindible evaluar el nivel de perjuicio que puede causar el incidente a los derechos y libertades de los afectados, determinando con el mayor grado de precisión posible el nivel de severidad de las consecuencias para los individuos. Es así mismo imprescindible determinar si se trata de una brecha de confidencialidad, integridad o disponibilidad, categoría y número de afectados, categoría y número de registros de datos, etc. Se han presentado más detalles sobre la clasificación de incidentes de seguridad en el apartado dedicado a clasificación de esta Guía.
- Investigación, comunicación y coordinación de los medios internos/externos implicados: es importante tener establecido de antemano cómo se va a tratar una incidencia de seguridad, 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 plan de respuesta: especialmente de las primeras medidas de contención, tratando de limitar en lo posible los daños causados por el incidente. Por ejemplo, si un ordenador está infectado deberá ser desconectado de la red corporativa inmediatamente, o si una información ha sido difundida erróneamente a través de internet, deberá ser retirada. Estas medidas proporcionan un margen de actuación para poder desarrollar una solución adecuada sin el factor tiempo.
- Puesta en marcha del proceso de notificación, empezando por una valoración de notificación temprana a la autoridad de control competente 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”.

5.2.2. Contención del incidente

Las medidas de contención podrán ser inmediatas o de aplicación progresiva en función del desarrollo de la resolución del incidente. Es conveniente determinar las medidas a implantar estableciendo un orden de prioridad, los responsables asignados, tiempos estimados y los efectos esperados.

Algunas medidas de contención serán sencillas y las podrá iniciar el usuario, sin embargo, otras medidas son más complejas y deben estar en manos de personal especializado que se encargue de la seguridad informática de la empresa.

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

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

5.2.3. 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.

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

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

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

En 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 plan 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.

5.2.4. 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.

5.2.5. 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.

6

NOTIFICA

Un momento crucial en el ciclo de vida de un incidente de seguridad es la decisión de si es necesario notificar o no, ya como brecha de datos personales, a la Autoridad de Control. Pero también debemos acometer la comunicación a los interesados, si hubiese un alto riesgo para sus derechos y libertades, así como a otras administraciones y grupos de interés.

6.1. Notifica a la 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 WP250⁵, 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.

Serán de especial incidencia algunos de los criterios ya referidos en la fase de planifica, que usaremos 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.
- Características particulares del responsable de tratamiento.
- Número de personas afectadas.
- Consideraciones generales.

⁵De 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, 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 organizaciones⁶.



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

Como hemos venido destacando en toda esta 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 evitan los riesgos anteriores, minimizan los daños a los derechos y libertades y/o los hacen 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 comunicar a la Autoridad de Control, lo que hay que identificar es la Autoridad de Control a la que realizar dicha comunicación.

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.



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

⁶Las estadísticas muestran que el porcentaje de brechas de datos personales notificadas a la AEPD que han supuesto apertura de expediente sancionador es realmente bajo. Así mismo, una de las conclusiones de la 1ª Encuesta sobre Brecha de Seguridad de ISMS Forum es que aquellas empresas que han tenido al experiencia de una brecha real, no han observado en prácticamente caso alguno, impacto negativo ni sobre su imagen de marca ni sobre su negocio.

Dado la reciente publicación por parte de la AEPD de su Guía para la notificación de brechas de datos personales, estimamos que no es necesario extendernos más sobre este tema, ya que esta 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.

6.2. Comunica a las personas físicas afectadas

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 los afectados.

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 a dicho artículo 34 del RGPD, para evaluar la comunicación debemos tener en cuenta 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 caso⁷.

Sin perder este foco, tendremos 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.

En línea con estos informes, las variables a ser tenidas 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 borra 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.

⁷ <https://www.aepd.es/es/documento/gestion-riesgo-y-evaluacion-impacto-en-tratamientos-datos-personales.pdf>

- **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**

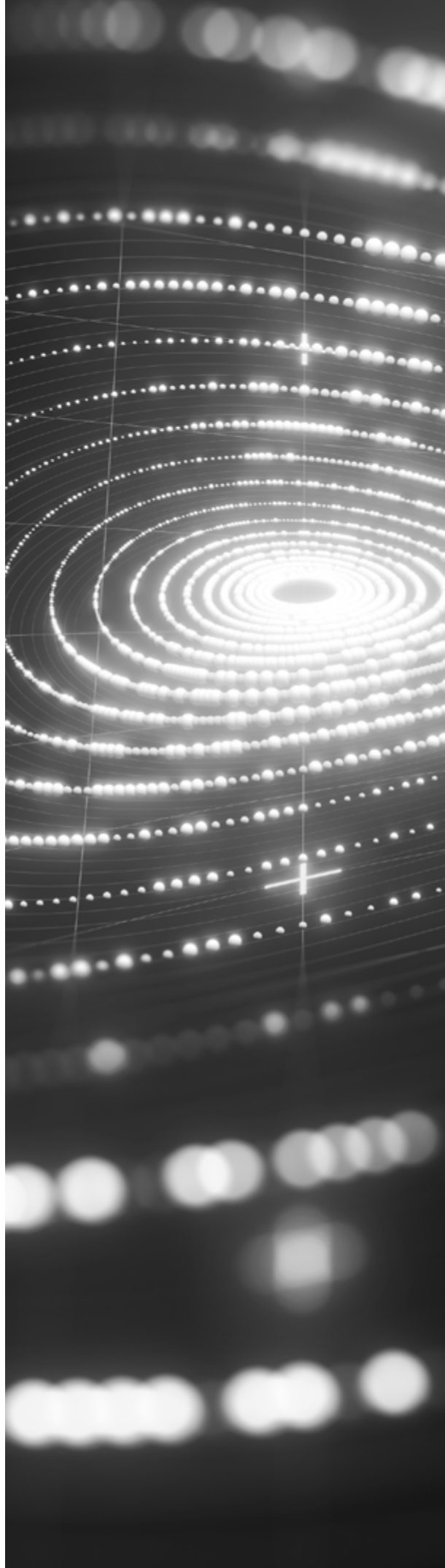
Si entre los datos hay información de clientes que pueden ser menores de edad, o pertenecen a colectivos más desfavorecidos o en riesgo de exclusión, tercera y cuarta edad, víctimas de violencia de género, etc. en estos casos toda la muestra de datos se considerará como más sensible y más severa que 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**

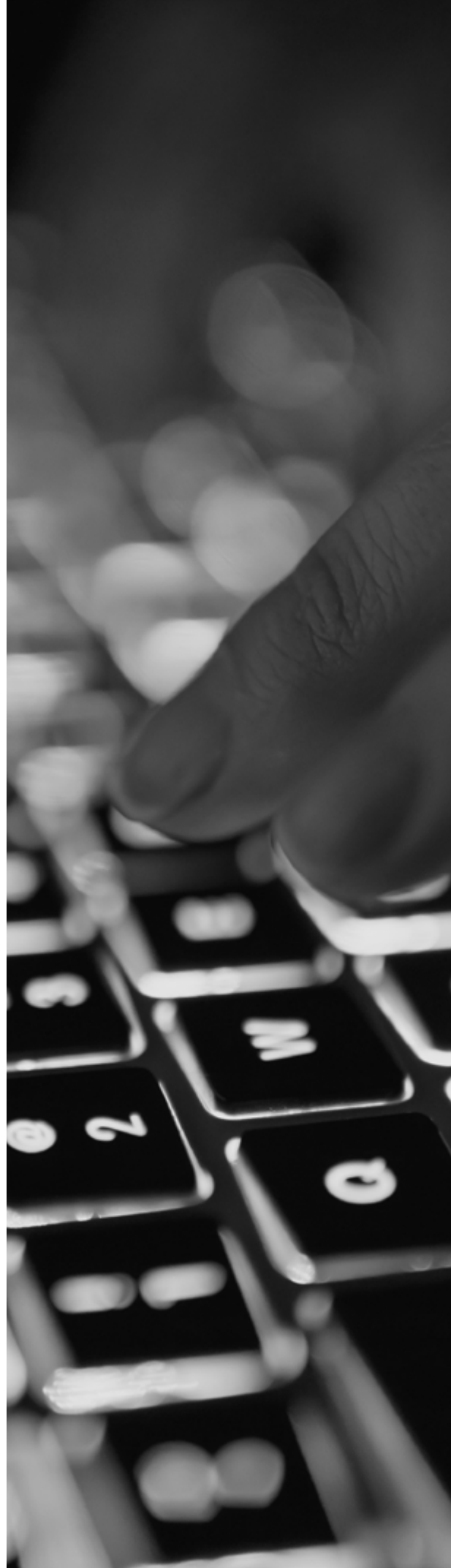
La intencionalidad de la persona que ha cometido un error o no y la intencionalidad de quien ha recibido una información personal es decisiva para determinar el alto riesgo a los afectados. Si la persona, y más si es un empleado interno o un ex empleado, creemos que ha cometido la brecha intencionadamente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

- **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.

- **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.

- **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).

- **Reversibilidad de los efectos**

En la evaluación de los efectos para los derechos y libertades del afectado, es muy importante si el daño es reversible o no y cómo puede afectar a esa persona. Por ejemplo, imaginemos que se revelan datos de un donante vivo o de la identidad de los padres de un niño adoptado y que se revelan a este o la publicación de imágenes en redes sociales de un empleado que resulta despedido. En esos casos, una vez revelado, ya es imposible volver atrás y olvidar lo conocido o el despedido puede judicialmente ser reinsertado en la plantilla, pero todos los empleados ya conocen una información sobre el mismo que no deberían, y eso puede condicionar su relación con este, afectarle psico-emocionalmente, sus posibilidades de promoción internas, etc.

- **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.

En cada caso de uso se debe abordar también si hay encargados del tratamiento implicados, no podemos desarrollar este plan dejando al margen esta importante figura, por lo que revisaremos los contratos firmados para comprobar su adecuación al artículo 28 del RGPD.

6.2.1. Formas y plazos para comunicar

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



Monitoriza bien el proceso de comunicación.

La comunicación a los afectados se realizará a la mayor brevedad posible, en un lenguaje claro y sencillo y siempre en estrecha cooperación con la autoridad de control y las autoridades policiales, de acuerdo con sus orientaciones.

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.

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.

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.



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.

6.2.2. 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 weblog 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.

6.2.3 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:

- ¿Qué ha ocurrido? Descripción de incidente, momento en el que se ha producido, posibles consecuencias para los interesados, etc.
- ¿Qué información está involucrada? Información de los afectados que se ha visto involucrada en el incidente. En este caso, conviene dar el mayor detalle posible.
- ¿Qué estamos haciendo? Descripción de las medidas implantadas hasta el momento para controlar los posibles daños, y cualquier otra información que pueda ser útil y que se esté llevando a cabo.
- ¿Qué acciones adicionales puedes llevar a cabo? Indicar de una manera clara, lo que deben hacer los usuarios para proteger sus datos e información y prevenir futuros daños.

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.

6.2.4. 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 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.



7

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 las acciones siguientes:

- Elaboración de un informe final, donde se recopile y explique la brecha de datos sufrida, y se ponga a disposición de la autoridad de control;
- Asesoramiento en la definición del plan de acción en colaboración y acordando las acciones con los departamentos implicados;
- Seguimiento periódico del plan de acción definido, señalando hitos y responsables;
- Revisión del mapa de riesgos y mejora de los controles previamente definidos;
- Adaptación y realización de acciones de formación a las necesidades detectadas en el incidente de seguridad;
- Seguimiento de su evolución y evaluación por parte de la Autoridad de Control, lo que podría desembocar en la indeseada consecuencia de la apertura de un expediente sancionador;
- Gestión ulterior a la comunicación a los afectados: aclaraciones, reclamaciones de daños a terceros, ciberseguros, etc.;
- Gestión del posible daño reputacional que también habrá que administrar y reparar;
- Análisis de lecciones aprendidas tras las brechas de datos personales experimentadas, que permitan realimentar el apartado de planificación con posibles mejoras; cómo gestionar y qué tener en cuenta en este punto.



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.

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.

7.1. AEPD

Como dato significativo, más de un tercio de las brechas que se notificaron estos últimos tres años en materia de RGPD se notifican en estado pendientes de resolver, por lo que es fundamental un seguimiento al menos quincenal de las mismas e ir informando a la AEPD. No debemos esperar a que nos pregunten por su estado, 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, para 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 en la Darkweb, entre otros.

7.2. Otros reguladores

Por otra parte, además de la notificación a la AEPD en el caso de que se hayan visto afectados datos personales (Brecha); es posible que determinadas empresas, dependiendo del sector de actividad en el que se encuentren (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, bancos, etc.), tengan también que comunicar y/o notificar 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.

Ya en la guía anterior del ISMS se indicaba: *“Por lo tanto, la gestión de brechas de seguridad no es una novedad y, además de la normativa de protección de datos, existen otras normas que recogen esta obligación. En el caso de las Administraciones públicas, el Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica (ENS), en su capítulo VII (Art. 36) asigna el papel de coordinación en materia de respuesta a incidentes de seguridad al Centro Criptológico Nacional (CCN) con el objetivo de articular mecanismos de respuesta a los incidentes de seguridad mediante la estructura CCN- CERT (Centro Criptológico Nacional-Computer Emergency Reaction Team) obligando a la notificación de incidentes de seguridad a las Administraciones Públicas y en consecuencia, añadiendo la necesidad de gestionar las brechas de seguridad.*

Para facilitar esta labor el CCN dispone de la guía para la “Gestión y Notificación de Ciberincidentes” (CCN-STIC 817) que ha sido utilizada como referencia en la elaboración del presente documento y, además, proporciona de forma gratuita la herramienta LUCIA como canal para llevar a cabo las notificaciones de brechas de seguridad.

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

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).

7.3. 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. Una vez finalizada la gestión de la brecha propiamente dicha, estas posibles acciones deberán ser gestionadas por otras áreas de la empresa como atención al cliente o legal, siguiendo procedimientos estándar, pero con acceso a toda 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 comunicación final a estos para informar del cierre de la brecha y de próximos pasos que se darán.

7.4. Impacto público

Sin duda, el miedo al 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.



Sabes que si hay una sanción tras la brecha se hará pública en el portal de la AEPD, anticipa respuestas alineadas por la Alta 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.

En todo caso, es necesario que al cierre de la brecha se estudie el posible impacto público y se tomen medidas de reducción o mitigación desde las áreas más dedicadas a la comunicación, imagen de marca e inclusive negocio, como puede ser la comunicación a través de oficinas de prensa y medios de comunicación.

Aunque no hay que olvidar que una mala gestión previa de la brecha hará más difícil estas gestiones, o inclusive imposible, y que una buena gestión del impacto público comienza ya en la fase de planificación.

7.5. Terceros: encargados, ciberseguros

En el cierre de las brechas hay una serie de terceros con los que la empresa puede tener diferentes relacionados a los que es importante comunicar la evolución y cierre de la brecha de datos personales. Siendo necesario conocer el tipo de relación con estos terceros, qué información se les deberá facilitar y cuál no dentro de los informes internos.

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 fijada la metodología de comunicación con estos clientes, escrita preferentemente, y un plan de comunicación periódico y frecuente, que muestre en todo momento la situación de sus datos. Además, obviamente, 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.

De cara a ciertos proveedores también es importante, sobre todo si los mismos participaron o están participando en alguna parte del proceso afectado, el lugar donde ocurriese la brecha. 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 nos ayuden a contener la brecha o 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. Es imprescindible haber informado cuanto antes para que analicen si el seguro cubre los efectos de la brecha y con qué alcance, que abran expediente sobre el tipo de brecha sufrida. Y en todo momento habrá que mantenerlos debidamente informados 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 más que probable que haya que comunicar la resolución al DPD Global, siguiendo los procedimientos y políticas de protección globales (ver “Planifica”).

En caso de ser necesario realizar esta comunicación a otras partes, es necesario preparar una comunicación detallada y dirigida específicamente a cada una de las partes, no conviene realizar una comunicación general a todas, porque probablemente cada una tenga sus dudas.

7.6. 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 una manera continua de modo que la dirección y responsables de seguridad tengan una visibilidad clara tanto del incidente como de las acciones tomadas para afrontarlo. Es especialmente importante cuando el incidente trasciende el perímetro de la organización y toma relevancia pública, ya que muy posiblemente los directivos serán preguntados por las acciones que se están llevando a cabo y posibles consecuencias.

También es recomendable que seamos transparentes con nuestros empleados, en este sentido es una buena práctica publicar una pequeña nota en la intranet corporativa o por correo electrónico a los empleados informando de lo sucedido. En cierto modo nuestro plan de formación y concienciación de privacidad debiera contar con un apartado de lecciones aprendidas y boletines 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 comunicación interna es muy importante porque va a demostrar la gobernanza de la privacidad en esa compañía. Hemos hablado mucho de gestión y la palabra gobernanza o buen gobierno, como ya hemos mencionado, no se recoge ni en el RGPD, ni en nuestra Ley Orgánica 03/2018 de Protección de Datos, pero es una palabra alineada con el principio de Accountability.

En este sentido, la organización debe informar no solo a sus clientes o partes cuyos datos se vieron afectados. Debe informar también al máximo órgano de gobierno, el Consejo de Administración, sus accionistas y compañías matrices (en el caso de multinacionales) sobre el hecho ocurrido y sus posibles consecuencias, no solo referentes a una posible sanción, sino también en términos de daño reputacional, ética y negocio responsable, así como sobre las medidas tomadas y el estado de la situación.

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 otra brecha de datos, de muy difícil justificación y podría suponer apertura de expediente sancionador.

7.7. Seguimiento y cierre

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

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

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

III.- 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.

7.8. Informe final.

A fin de cerrar la brecha de seguridad se elaborará un Informe final sobre la trazabilidad del suceso y su análisis valorativo, en particular, en cuanto al impacto final. Dicho Informe final recopilará toda la información y documentación relativa a la brecha de manera que se facilite el estudio y revisión por terceros, incluida la dirección de la empresa.

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

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

Los informes sobre las brechas y su impacto son una valiosa fuente de información con la que debe alimentarse el análisis y la gestión de riesgos. El uso de esta información servirá para prevenir la reiteración del impacto de una brecha.

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.

Por lo tanto, como parte final del proceso de documentación y gestión de la propia brecha, es más que recomendable el emitir un informe final que comprenda una descripción, trazabilidad y análisis final 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.

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

Con este informe final, 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 de mejora continua, se alimenta la fase de Planifica con mejoras en procesos y procedimientos, planes de formación, nuevos o mejorados 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.

Finalmente, debería generarse algún tipo de medidas y plan de seguimiento, a implantar tras el incidente, que se seguirán ya dentro de los procesos o foros generales de la empresa.

Así mismo, e independientemente de lo que se haga para cada brecha concreta, una versión 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.

Podría resultar recomendable que se aporte o, mejor, se mantenga a disposición de la Autoridad de Control dicho Informe final que, en cualquier caso, sí podrá ser exigido por la misma como consecuencia de una siguiente notificación de brecha de datos personales, para contrastar por parte de dicha autoridad que se han aprendido las lecciones necesarias y 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.

ANEXO I

PROTOCOLOS INTERNOS

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).
- Guías de las Agencias Europeas de Protección de Datos, en especial, la Guía para la Gestión y notificación de brechas de seguridad publicada por la Agencia Española de Protección de Datos.
- 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 (UE) 2016/1148 del Parlamento Europeo y del Consejo de 6 de julio de 2016 relativa a las medidas destinadas a garantizar un elevado nivel común de seguridad de las redes y sistemas de información en la Unión (Directiva NIS).

Accountability

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.
- Auditorías 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 porqué no la notificación legal o tardía, especialmente]
- 5.3. Comunicaciones a interesados. Justificar porqué se ha realizado o porqué 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.

CASOS PRÁCTICOS

Como se ha comentado a lo largo de la Guía, una de las actividades que es necesario llevar a cabo, cuando sucede una brecha de datos personales, es la evaluación del riesgo. Esto es importante ya que en función de dicho análisis puede ser necesario realizar la notificación de la brecha a la Autoridad de Control o incluso a los afectados. De hecho, no hay que perder de vista que tal y como establece el RGPD en su artículo 33, “el responsable del tratamiento la notificará a la autoridad de control competente de conformidad con el artículo 55 sin dilación indebida y, de ser posible, a más tardar 72 horas después de que haya tenido constancia de ella, a menos que sea improbable que dicha violación de la seguridad constituya un riesgo para los derechos y las libertades de las personas físicas” y en el artículo 34 se establece que “cuando sea probable que la violación de la seguridad de los datos personales entrañe un alto riesgo para los derechos y libertades de las personas físicas, el responsable del tratamiento la comunicará al interesado sin dilación indebida”.

Por este motivo y con el objetivo de ejemplificar cómo podría llevarse a cabo este análisis de riesgos, se muestran a continuación una serie de casos prácticos, seleccionados por un grupo de trabajo tanto de DPD's como de CISO's que, bien por su frecuencia o por sus características, fueran los más relevantes de cara a este estudio.

Antes de comenzar con los distintos casos prácticos es necesario mencionar que estos casos son completamente ficticios y que se han seleccionado aquellos parámetros asociados a la brecha que se describe que pudieran ser relevantes. En este sentido, la existencia de estos casos prácticos no exime al responsable del tratamiento de hacer su propio análisis de riesgos ya que la realidad puede variar significativamente en unas situaciones u otras y por lo tanto condicionar completamente el resultado de la valoración de riesgo realizada. Además, el responsable es quien mejor conoce los detalles del tratamiento de datos personales que realiza, las características de los sujetos de datos, las circunstancias de la brecha de seguridad y el resto de los factores que permiten obtener una valoración del riesgo acertada.

En particular, como se verá más adelante, ante un mismo suceso el impacto a la privacidad de las personas puede ser muy diferente y, por lo tanto, las conclusiones sobre la necesidad o no de notificar variar significativamente. A fin de mostrar esta realidad, en los casos prácticos en ocasiones se incluyen determinadas casuísticas o situaciones que condicionan de algún modo el resultado del análisis de riesgo.

En todos los casos prácticos se seguirá un mismo esquema: se comenzará con una descripción del caso para continuar con la identificación de los aspectos relevantes en la valoración de la brecha y finalizar con el resultado del análisis asociado a la necesidad o no de notificar a la Autoridad de Control y, en su caso, a los afectados.

El ransomware es un tipo de malware, o software malicioso, que secuestra archivos y, en ocasiones, equipos o dispositivos móviles enteros impidiendo el acceso a la información, generalmente cifrándola. Su nombre proviene del inglés “ransom” que significa secuestro, ya que este tipo de malware, en ocasiones, se utiliza para pedir un rescate a cambio de descifrar los archivos y devolver el acceso a los datos al propietario. Además, en los últimos tiempos ha evolucionado integrando la exfiltración de datos, de forma que la extorsión se refiere tanto al secuestro de los datos como a la amenaza de hacerlos públicos.

Es una de las amenazas más concurrente y dañina que ha sufrido una gran evolución en los últimos años. Produciéndose un incremento en determinados meses del año 2020 de más de un 100% en comparación con el mismo mes del año anterior⁸.

Uno de los motivos por los que se ha producido este crecimiento exponencial de estos ataques es, tal y como indica el INCIBE⁹, la rentabilidad que tiene para los delincuentes:

- cada vez hay más dispositivos «secuestrables»,
- es más fácil «secuestrar» la información debido a los avances de la criptografía,
- los ciberdelincuentes pueden ocultar su actividad para lanzar ataques masivos,
- al utilizar sistemas de pago anónimo internacionales es más difícil el seguimiento del delito.

Todo esto hace que las compañías cada vez estén más expuestas a este tipo de amenazas, pero el impacto que puede tener para las mismas puede ser muy diferente. Es más, desde el punto de vista de brecha de datos personales hay que tener en cuenta que no todo incidente de seguridad o ciberincidente tiene por qué ser brecha de datos personales. Para que sea considerado como tal es necesario que afecte a datos personales.

Descripción del caso práctico

El Hospital X es un centro de referencia a nivel nacional por los importantes procesos de Digitalización que ha llevado a cabo y que le permite gestionar de forma mucho más eficiente y eficaz la atención hospitalaria y, sobre todo, la gestión de los quirófanos. Incrementado su capacidad operatoria, reduciendo problemas y errores médicos en los mismos. Para ello cuenta con software de Gestión integral del Hospital, con acceso para el personal sanitario y también con un equipo de TI reforzado.

En el Hospital X se detecta un ataque de ransomware que ha originado el cifrado de determinados equipos y cuya cronología de lo ocurrido sería la siguiente:

- 01 de diciembre: uno de los médicos del hospital recibe un correo electrónico que, aunque parece inocuo, al ejecutarlo produce la descarga en el equipo de un malware que será el utilizado posteriormente para efectuar el cifrado de los equipos.
- Del 01 de diciembre al 24 de diciembre: el atacante procede a intentar desplegar el malware en distintos equipos y servidores.

⁸<https://www.ccn-cert.cni.es/informes/informes-ccn-cert-publicos.html> informe CCN-CERT BP/04 Ransomware de mayo de 2021

⁹<https://www.incibe.es/protege-tu-empresa/herramientas/servicio-antiransomware>

- 24 de diciembre a las 21 horas¹⁰: el equipo de TI del Hospital X comienza a recibir alertas de mal funcionamiento de múltiples de sus equipos y servidores. Inmediatamente se comienzan a analizar las alertas junto con el equipo de seguridad. Se detectan archivos cifrados en varios equipos, por lo que se concluye que se está sufriendo un ataque de ransomware.
- 24 de diciembre a las 24 horas: se toma la decisión de proceder a desconectar el equipo identificado de la red, así como el resto de equipos no considerados imprescindibles y a aislar determinados segmentos de la red de comunicaciones con el objetivo de¹¹:
 - Evitar que la acción de cifrado alcance al contenido alojado en las unidades de red accesibles desde el equipo infectado.
 - Eludir que el código dañino pueda contactar con su servidor de mando y control.
- 25 de diciembre a las 10 horas: tras la contención inicial del incidente, y una vez que se observa que no se están produciendo nuevas alertas en los equipos no identificados como infectados, se comienza el proceso de recuperación y restauración de los sistemas afectados, así como el análisis forense completo de lo sucedido.
- 27 de diciembre a las 10 horas: se presenta el análisis forense inicial a la dirección del Hospital X. Tras el estudio realizado se ha concluido que el vector de entrada ha sido un correo electrónico enviado a uno de los médicos del hospital, que al ser abierto el 01 de diciembre descargó el malware que fue utilizado por los ciberdelincuentes. También se ha observado como entre el día 1 y el día 24 del mismo mes, el atacante fue intentando desplegar el malware en distintos servidores y equipos, no consiguiéndolo en todos los casos.

Solo con la información anterior no se puede saber la gravedad de la situación ni el impacto que ha podido tener el incidente en la privacidad de las personas, ni en el riesgo para sus derechos y libertades. Es necesario seguir analizando lo ocurrido, para lo que los logs o información de registro juegan un papel básico en el análisis forense, que deberá ser lo más detallado posible. Es importante identificar el origen del ataque, las actividades realizadas por el atacante entre la fecha de infección y la de detección, los sistemas y archivos realmente afectados, de si se contaba con copias de respaldo de los mismos que garanticen su

¹⁰Momento de comienzo de gestión del incidente

¹¹<https://www.ccn-cert.cni.es/informes/informes-ccn-cert-publicos.html>
informe CCN-CERT BP/04 Ransomware de mayo de 2021





disponibilidad, etc. Y con estos datos, junto con el impacto que haya producido el incidente, se podrá inferir si se ha tratado de una brecha de datos personales y si ha afectado a su disponibilidad, integridad o también a su confidencialidad. A continuación, se muestran distintas situaciones que pueden darse asociado a un ataque de ransomware con el objetivo de mostrar las grandes diferencias entre unas situaciones u otras. La casuística puede ser infinita, pero se seleccionan estas que, de algún u otro modo, pueden haberse producido en alguna entidad:

Situación 1: el cifrado que se produjo fue de un número reducido de equipos, pero justamente eran unos equipos que tenían información relevante del hospital de las que se realizaban copias periódicas. Entre dicha información no había datos personales. Fue necesaria la restauración de las copias de respaldo y se produjo un impacto operativo en el hospital al no ser posible acceder a dicha información, pero no hubo ningún impacto en la privacidad de las personas y el hecho no supuso ningún riesgo para los derechos y libertades de las personas.

Situación 2: el cifrado fue de un número reducido de equipos, pero justamente uno de ellos estaba asociado a una de las máquinas utilizadas en el quirófano y en el mismo se encontraba información de salud de las operaciones que se encontraban previstas. Dicho equipo tuvo que ser sustituido y, por las características técnicas que debía tener, dicha sustitución llevó más tiempo del inicialmente previsto. Además, no se pudo recuperar la información y todo esto hizo que hubiera que cancelar determinadas operaciones que se encontraban planificadas.

Situación 3: el cifrado fue de un volumen de equipos significativo que hizo necesaria la activación del plan de continuidad de negocio, pero el cifrado no afectó ni al correo electrónico ni a los sistemas y bases de datos del hospital. Además, tras las tareas de análisis forense se pudo identificar exactamente cómo se había producido el ataque y se confirmó que no se había producido ninguna exfiltración de datos.

Situación 4: el cifrado fue de un volumen de equipos significativo que hizo necesaria la activación del plan de continuidad de negocio, pero a la hora de realizar la restauración de la información se detecta que había información que no había sido posible recuperar. Además, el plan de continuidad de negocio no se encontraba actualizado y esto hizo que los tiempos de respuesta fueran mayores a lo establecido suponiendo un impacto significativo en las personas, ya que no podían acceder a sus historias clínicas, y hubo que cancelar distintas citas e incluso operaciones.

Situación 5: el cifrado fue de un número reducido de equipos, pero antes del cifrado los hackers accedieron a la base de datos de pacientes y realizaron una exfiltración de más de 100.000 datos personales.

Aspectos relevantes en la valoración de la brecha

A la hora de valorar este tipo de brechas, el primer aspecto a tener en consideración es el origen del incidente y, en este caso, se trata de un incidente externo, intencionado y que está asociado a un ciberincidente.

Además, suele estar asociado a pérdidas de disponibilidad de la información o incluso pérdida de la confidencialidad en aquellos casos en los que se pueda llegar a producir un acceso no autorizado a los datos o incluso una fuga de información.

Adicionalmente, hay otra serie de aspectos que serán los más relevantes a la hora de valorar este tipo de brechas:

- **Volumen de afectados:** entendiendo afectados como personas que han podido verse impactadas por la pérdida de disponibilidad de su información, porque no hayan podido acceder a los tratamientos que tenían previstos o, en el caso de que haya habido un acceso a los datos, el volumen de datos accedidos.
- **Tipología de datos:** no es lo mismo que los datos afectados no incluyan datos personales a que sí que lo contemplen o que incluso los datos sean sensibles. Además, también habrá que identificar si se trata de datos de personas especialmente vulnerables.
- **Consecuencias de la brecha:** hay que tener en consideración si la brecha no supone más que pequeñas molestias a las personas o si, por el contrario, realmente afecta a sus derechos o prestación de determinados servicios o se produce una pérdida de confidencialidad de la información.
- **Duración:** es necesario determinar la duración del incidente y cómo afecta a la continuidad del negocio.

Resumen de la valoración

A partir de la información anterior se realiza la valoración de la brecha a fin de confirmar la situación:

PARÁMETROS EVALUADOS		SITUACIÓN 1	SITUACIÓN 2	SITUACIÓN 3	SITUACIÓN 4	SITUACIÓN 5
Sobre la brecha	Como ha sido el incidente	Intencionado	Intencionado	Intencionado	Intencionado	Intencionado
	Origen del incidente	Externo	Externo	Externo	Externo	Externo
	Consec. de ciberinciden.	Si	Si	Si	Si	Si
Sobre las consecuencias	Consec. del incidente	Cifrado un nº reducido de equipos pero relevantes para negocio	Cifrado un nº reducido de equipos - uno relevante	Cifrado un nº significativo de equipos	Cifrado un nº significativo de equipos	Cifrado nº reducido de equipos y acceso no autorizado a datos y fuga de información
Sobre las consecuencias	Se ha recuperado la disponibilidad de datos personales	N/A - No ha afectado a datos personales	No ha sido posible recuperar los datos	Si	De algunos no	Si
	Grado en el que podría afectar	N/A	Pueden encontrar inconvenientes importantes (al no poderse recuperar los datos y haberse tenido que cancelar determinadas operaciones)	No se verán afectadas o levemente	Pueden encontrar inconvenientes importantes	Pueden encontrar inconvenientes importantes
	Se ha materializado alguno de los daños	N/A	Si	No	No	Si
	Probabilidad de que el daño anterior se materialice	N/A	alta	baja	alta	
Categoría de datos	Tipos de datos afectados en personas físicas	N/A	Datos de salud	Datos básicos	Datos de salud	Datos de salud
Personas afectadas	Hay menores o vulnerables	N/A	No	No	No	No
	Volumen de personas afectadas por la brecha	0	menos 100 (hubo que cancelar 12 operaciones)	Menos de 100	1.000	Más de 100.000
Inform. Temporal	Momento en el que se conoció	Temprana	Temprana	Temprana	Temprana	Temprana
Inform. Temporal	Actuación ante la brecha	Temprana y diligente	Temprana y diligente	Temprana y diligente	Temprana y diligente	Temprana y diligente
Resultado	Comunicar a la autoridad de control	No - No es una brecha de datos personales	Si	Si	Si	Si
	Comunicar a los afectados	No	Si	No	Si	Si

Empleado que se lleva la base de datos de clientes a la competencia

Se incluye este caso práctico, ya que puede parecer más habitual de lo que debería, sobre todo en sectores ligados a servicios, telcos, banca, etc.

Uno de los motivos que hacen que estas situaciones se produzcan es la ausencia de medidas de preventivas, como la implantación de herramientas de DLP (prevención de fuga de datos), una incorrecta identificación y clasificación de la información o la ausencia de medidas de seguridad acordes al nivel de dicha información.

Si bien está muy extendida la firma de acuerdos de confidencialidad y deber de secreto de forma indefinida entre empresas y sus empleados o sus proveedores cuando actúan como encargados del tratamiento, la verdad es que en muchas ocasiones no hay controles automáticos que de verdad limiten las acciones que se pueden hacer sobre esos documentos, bases de datos, etc. Controles como aquellos asociados a la posibilidad de impresión, el rastreo de documentos o el control de los envíos de correos serían parte de dichos controles automáticos que permitirían prevenir este tipo de situaciones nada deseables y que complementaría esos controles asociados al compromiso de confidencialidad y deber de secreto que se tornan insuficientes a día de hoy.

Descripción del caso práctico

Tras reiteradas llamadas de clientes de la compañía que indican que están siendo contactados por una empresa de la competencia con datos de contacto e información sobre los servicios prestados por la nuestra y su coste, se llega a la conclusión de que un comercial que ha abandonado la compañía se ha llevado la base de datos de clientes a su nueva empresa, de la competencia, y la está utilizando.

La cronología de lo ocurrido sería la siguiente:

- 01 de noviembre: el servicio de Atención al cliente avisa al DPD de la compañía sobre el tipo de quejas que se están recibiendo.

El DPD solicita reenvío de los casos y comienza a contactar con los afectados para obtener más información y contrastar si lo que dicen es coherente y sólido para empezar el análisis de riesgo de si este hecho es brecha de datos personales notificable o no a la Autoridad de Control. Los clientes le confirman que se les ha llamado por su nombre y que tenían sus datos de domicilio, teléfono, etc.

- 05 de noviembre: se detecta que todos los clientes están en una misma área geográfica, tienen productos muy parecidos y se supervisa el código de agente que los grabó en el sistema.
- 10 de noviembre: se localiza que hay un agente que ya está de baja de la compañía y que está detrás de algunos casos de clientes contactados. Además, tras diversas investigaciones se confirma que dicho agente trabaja ahora para otra compañía de la competencia, mismo sector.

- 11 de noviembre: el DPD vuelve a ponerse en contacto con alguno de los clientes que notificaron el hecho a fin de obtener más información de detalle así como alguna evidencia que pudiera servir de base al hecho ocurrido.
- 30 de noviembre: se consigue una llamada que proporciona uno de los clientes, tras haber ejercido el derecho de acceso a la compañía que supuestamente había utilizado los datos, y se ratifica que ese comercial tenía los datos de los clientes y que no ha habido ningún tipo de virus o ataque informático que los haya manipulado, cifrado, etc.

Adicionalmente, se consigue disponer de la información necesaria para poder realizar la valoración de riesgo asociada.

En función de los resultados obtenidos de dicho análisis podrían producirse distintos tipos de situaciones que se detallan a continuación:

Situación 1: se trata de datos de contacto mínimos (nombre, teléfono, email), y empieza a haber varias quejas muy consecutivas. No se localiza el contrato firmado entre la empresa y ese agente o está obsoleto y sin actualizar en la parte de protección de datos. Se trata de un agente de baja que llevaba poco tiempo realmente.

Situación 2: se notifica que, entre los datos, además de datos de contacto, hay datos como fechas de nacimiento y DNI. Era un agente con mucha antigüedad en la compañía. Hay un contrato, pero no está actualizado. Se han recibido ya más de 5 quejas por este hecho en apenas una semana. No se sabe el número de registros realmente afectados. El agente ha sido despedido por la compañía.

Situación 3: se comprueba que, entre los datos, hay datos completos de la ficha de ese cliente (edad, sexo, nombre completo, profesión, DNI, teléfono, email, domicilio, cuenta bancaria, si era VIP o no, su propensión a fuga, etc..) incluso posiblemente valoraciones y juicios de opinión o datos de estado de salud en campos de Observaciones que se han encontrado. Era un agente con mucha antigüedad y que ha sido despedido, y amenaza con seguir realizando llamadas si no se le paga una indemnización. Se detecta en un análisis forense que había un log de su actividad, pero nadie lo estaba mirando.

Situación 4: entre los datos están todos los de la ficha de ese cliente (hay más de 20 tipologías de datos) incluso se han podido exportar datos de estado de salud, perfilados comerciales, juicios de opinión, etc. Se ha podido sacar una base de datos completa con más de 1.000 referencias. Entre los datos puede haber clientes que ya estaban en baja en la compañía pero que seguían activos y sin bloquear. También hay datos de leads/referencias de personas que aún no eran clientes, pero cuyos datos se habían obtenido de diversas fuentes. Puede haber datos de menores ya que se ha llevado datos de familiares y amigos. No se sabe exactamente el alcance ya que los sistemas no contaban con el nivel de monitorización necesario para obtener esta información y no es posible confirmar que realmente todas las quejas estén asociadas al agente que causó baja.

Aspectos relevantes en la valoración de la brecha

A la hora de valorar este tipo de brechas, el primer aspecto a tener en consideración es que la relación contractual con los empleados y agentes esté correctamente firmada y actualizada, las políticas de privacidad y seguridad firmadas, cursos de formación superados y los accesos a los sistemas concedidos siguiendo los protocolos para ello.

Otro tema muy importante es el perfil de la base de datos que se ha podido llevar de la compañía. No es lo mismo el perfil de un cliente, que el de un menor o un colectivo de discapacitados, que un excliente o que un mero lead/referencia que solicitó información en su momento. Si además se detecta que ese cliente había ejercido su derecho de oposición, supresión o limitación, el problema se agrava.

Las medidas de seguridad que hubiese desplegadas antes de ocurrir el incidente también son relevantes, tanto limitaciones de control de acceso de ese agente a las plataformas de CRM o transaccional, como el log de su actividad y monitoreo y su persistencia, pues si el agente causó baja hace tiempo pueden haberse borrado los journals y/o haber copias de seguridad de esa directiva.

Por último, en cuanto a las consecuencias de la brecha, hay que tener en consideración si la brecha no supone más que pequeñas molestias a las personas que están siendo contactadas o, por el contrario, están sufriendo spam telefónico, llamadas fuera de horario y/o en festivos o si están siendo extorsionadas en cierto modo.

Resumen de la valoración

A partir de la información anterior se realiza la valoración de la brecha a fin de confirmar la situación:

PARÁMETROS EVALUADOS		SITUACIÓN 1	SITUACIÓN 2	SITUACIÓN 3	SITUACIÓN 4
Sobre la brecha	Como ha sido el incidente	Intencionado	Intencionado	Intencionado	Intencionado
	Origen del incidente	Interno	Externo	Interno	Interno
	Consec. de ciberinciden.	Si	Si	Si	Si
Sobre las consecuencias	Consec. del incidente	Algunos clientes están siendo llamados y se les identifica claramente	Varias decenas de clientes se han quedado	Se está llamando a exclientes, leads y otros interesados, no solo clientes de la entidad	Las quejas no paran de llegar por diversas vías, son llamadas molestas, persistentes, no hay un patrón claro y no se tiene identificado quién o cómo ha podido pasar
Sobre las consecuencias	Se ha recuperado la disponibilidad de datos personales	N/A - No afecta a disponibilidad	N/A - No afecta a disponibilidad	Sí, se detecta que el agente ha manipulado ciertos datos de la base de datos después de copiárselos	Sí, se detecta que el agente eliminó datos de la base de datos después de copiárselos
	Grado en el que podría afectar	Los individuos pueden tener inconvenientes que ellos seguro que son capaces de superar a pesar de algunas dificultades	Los individuos pueden tener inconvenientes que ellos seguro que son capaces de superar a pesar de algunas dificultades	Los individuos pueden tener inconvenientes importantes pero que pese a las dificultades conseguirán superar con el tiempo (ie citaciones judiciales, intento de estafas, daños a la propiedad, etc.	Los individuos pueden tener inconvenientes importantes pero que pese a las dificultades conseguirán superar con el tiempo (ie citaciones judiciales, intento de estafas, daños a la propiedad, etc.
	Se ha materializado alguno de los daños	No	Si	Si	Si
	Probabilidad de que el daño anterior se materialice	Baja	Media	Alta	Muy alta
Categoría de datos	Tipos de datos afectados en personas físicas	Datos básicos y datos habituales en acceso a áreas privadas de cliente	Datos básicos y datos financieros	Todos los datos de la ficha de cliente CRM.	Datos de salud actual o futura, juicios de valor, perfilados, valor de cliente
Personas afectadas	Hay menores o vulnerables	No	Improbable	Probable	Si
	Volumen de personas afectadas por la brecha	Hasta 10	Hasta 100	Más de 1.000	Realmente se desconoce el volumen pero es de un tratamiento a gran escala
Inform. Temporal	Momento en el que se conoció	Temprana	Temprana	Tardía	Tardía
Inform. Temporal	Actuación ante la brecha	Temprana y diligente	Temprana y diligente	Temprana y diligente	Temprana y diligente
Resultado	Comunicar a la autoridad de control	No – pero sí es una brecha de datos personales	Aconsejable a modo preventivo – es una brecha y ya es probable que tenga afección para los afectados	Si, ya es probable	Si, es altamente probable que tenga afección
	Comunicar a los afectados	Si a modo preventivo	Si	Si	Si

Descripción del caso práctico

Una compañía de distribución de ropa [CLIENTE] ha renovado su página de comercio electrónico para adaptarse a las nuevas necesidades y oportunidades de negocio y, sobre todo, incluir el pago con tarjeta de crédito. Para ello ha contratado a un [PROVEEDOR], especialista en desarrollo de software. El proyecto comienza en el mes de enero y el objeto es tener la nueva web completamente operativa para la campaña navideña de ese mismo año.

El proyecto se ha gestionado siguiendo las mejores prácticas en los proyectos de desarrollo de software, incluyendo la participación de las áreas de Ciberseguridad y de Protección de Datos del [CLIENTE] desde el inicio del proyecto para definir sus requisitos y con puntos de control sobre estos a lo largo de su desarrollo. También se ha contado con un equipo de testing propio del [CLIENTE].

Sin embargo, a lo largo del proyecto surgieron varios problemas relacionados, fundamentalmente, con la reutilización de desarrollos de la web anterior, de baja calidad, así como de la tecnología de bases de datos del [CLIENTE], ya obsoleta.

La presión del proyecto y cuestiones internas del [PROVEEDOR] le llevaron a cambiar en varias ocasiones al equipo del proyecto, y a incorporar en su fase final, para llegar a la fecha prevista, a desarrolladores no familiarizados con el proyecto ni con las tecnologías que se habían visto obligados a utilizar.

- 27 de noviembre: el [PROVEEDOR] realiza la subida a producción de los desarrollos
- 01 de diciembre : el DPD del [CLIENTE] recibe un correo electrónico de un cliente quejándose de que, tras realizar su compra, en el correo electrónico con los datos de la compra, se le adjunta un PDF con datos de compra de otro cliente.

Se escala inmediatamente al [PROVEEDOR] que confirma a las pocas horas el incidente reportado por el cliente, y que tras comprobar otras 10 ventas descubre que en dos de ellas se ha producido el mismo error. Los procesos de envío de datos al almacén para preparar el pedido, el proceso de cobro y contabilización parecen funcionar correctamente, y solo se detecta incidencia en la generación del PDF de confirmación que se adjunta para el cliente.

Desde la puesta a producción de esta nueva web se han producido 10.000 ventas aproximadamente.

- 02 de diciembre: el DPD solicita al [PROVEEDOR] el análisis completo de todas las ventas realizadas para identificar todos los casos afectados.

Ese mismo día se reciben más quejas por casos similares en el Servicio de Atención al Cliente, así como otro correo al DPD similar al primero. Se reúne de urgencia el Comité de Protección de Datos y se decide:

- Paralizar el proceso de envío del correo electrónico que confirma la venta.

- Finalizar el análisis de las 10.000 ventas para identificar en cuáles de ellas se envió un email con información errónea.

- Involucrar al departamento de Ciberseguridad para descartar que el error se ha producido debido a la introducción de un código malicioso en la aplicación, o a un acto de sabotaje interno.

- Realizar un análisis más detallado por parte del [PROVEEDOR] para determinar si la incidencia es debida a un error en la aplicación.

- 03 de diciembre: el [PROVEEDOR] presenta su análisis forense preliminar realizado y de él se extrae la información suficiente para conocer la causa del incidente y también su alcance.

A partir de este momento se pueden producir distintas situaciones, en función de las cuales, la valoración de la brecha puede ser diferente. Así como las acciones posteriores a acometer por parte de la compañía.

Situación 1: En el análisis realizado se detecta que, debido a un error en el paso a producción, al no haberse actualizado correctamente, uno de los componentes es reutilizado. Esto provocaba que en las consultas que se realizan a las bases de datos no utilizaran el nuevo campo identificador de cliente, por lo que los nuevos clientes no eran encontrados en la base de datos y se les generaba un PDF con los datos de la siguiente venta en el tiempo. El departamento de Ciberseguridad considera, en base a esta conclusión, que no se ha producido ninguna intrusión.

Las facturas no contenían datos bancarios, sólo datos identificativos del cliente y la venta asociada. Y la situación ha afectado a 500 ventas, las cuales han recibido un PDF de una venta que no les correspondía.

El Comité de Protección de Datos decide:

- Solicitar al [PROVEEDOR] la corrección de la incidencia, así



como un informe detallado de la incidencia producida, así como los motivos por los que se produjo.

- Enviar un correo electrónico a las personas que recibieron erróneamente estas 500 ventas, informándoles de que debido a una incidencia informática recibieron un correo electrónico con información de otros clientes, e instándoles a que lo borren.

El 04 de diciembre se realiza un análisis de las respuestas recibidas:

- De las 500 personas que recibieron información que no era suya: un 85% no han contestado, un 12% han contestado que han suprimido los datos que no eran suyos y un 3% se niegan a borrarlos.

El Comité de Protección de Datos decide:

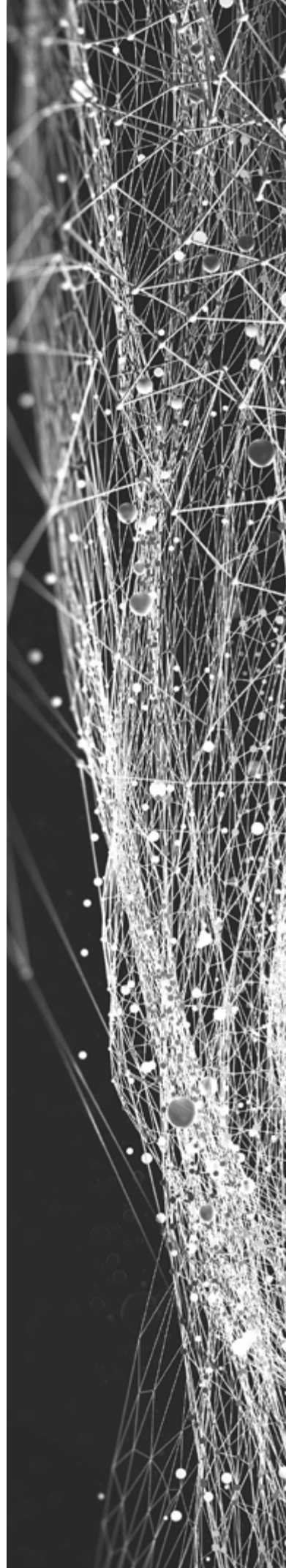
- Comunicar a la AEPD, basándose en el número de afectados, la tipología de datos afectadas, la rápida respuesta, las medidas adoptadas para reducir el impacto en la privacidad de los afectados, y el desarrollo de un plan para evitar que incidencias similares vuelvan a pasar.
- Crear un grupo de trabajo que se encargue de hacer seguimiento de las respuestas a los correos enviados.
- Crear un grupo de trabajo que se encargue de analizar la metodología de desarrollo, identificando un plan de acción con posibles mejoras.

Situación 2: En el análisis realizado se detecta que, debido a una incorrecta generación del último fichero de envío, se produjo un error que derivó en que determinados clientes tuvieran incorrectamente asignadas las facturas. El departamento de Ciberseguridad considera, en base a esta conclusión, que no se ha producido ninguna intrusión.

Las facturas no contenían datos bancarios, sólo datos identificativos del cliente y la venta asociada. Y el caso ha afectado únicamente a 20 clientes frente a los 10.000 que en principio parecía que podrían haberse visto afectados.

El Comité de Protección de Datos decide:

- Solicitar al [PROVEEDOR] la corrección de la incidencia, así como un informe detallado de la incidencia producida, así como los motivos por los que se produjo.





- Enviar un correo electrónico a las personas que recibieron erróneamente estas 20 ventas, informándoles de que debido a una incidencia informática recibieron un correo electrónico con información de otros clientes, e instándoles a que lo borren.
- Proceder a recabar de todos ellos confirmación del borrado del fichero recibido, así como que no se había realizado un uso no autorizado.

El 04 de diciembre se realiza un análisis de las respuestas recibidas. De las 20 personas que recibieron información que no era suya se ha conseguido respuesta de todos ellos. Al ser un volumen pequeño se determina la necesidad de contactar incluso telefónicamente con ellos para confirmar la situación. Tras contactar con todos ellos, se confirma que ninguno había realizado un uso de la información y que habían procedido al borrado del correo.

El Comité de Protección de Datos decide:

- No comunicar ni a la AEPD ni a los afectados, al haber podido concluir que, con las acciones llevadas a cabo, lo ocurrido no suponía un impacto alto para los derechos y libertades de los sujetos afectados.
- Crear un grupo de trabajo que se encargue de analizar la metodología de desarrollo, identificando un plan de acción con posibles mejoras.

Situación 3: similar a la Situación 1 pero en este caso no sólo había datos identificativos, sino que también había información de detalle de los datos bancarios que se habían utilizado en la compra, información que el [PROVEEDOR] decidió incluir en el PDF en el último momento sin el conocimiento del Departamento de Protección de Datos, y que podrían ser utilizados de manera incorrecta.

Además, a partir de una de las reclamaciones recibidas por parte de uno de los clientes, se confirma que dicho uso no autorizado por parte de un tercero se había materializado. De este modo, por la tipología de los datos afectados, el volumen de los datos y la probabilidad de ocurrencia, se considera que es una brecha que puede suponer un impacto alto para los derechos y libertades de los afectados.

El Comité de Protección de Datos decide:

- Solicitar al [PROVEEDOR] la corrección de la incidencia, así como un informe detallado de la incidencia producida, así como los motivos por los que se produjo.
- Enviar un correo electrónico a las personas que recibieron erróneamente estas

500 ventas, informándoles de que debido a una incidencia informática recibieron un correo electrónico con información de otros clientes, e instándoles a que lo borren y no hagan uso de esta información.

- Enviar un correo electrónico a las personas que realizaron las 500 ventas, informándoles de que debido a una incidencia informática a otros clientes los datos de su compra fueron enviados a otro cliente, y que ya se han tomado medidas para proceder a su borrado.
- Crear un grupo de trabajo que se encargue de hacer seguimiento de las respuestas a los correos enviados.
- Crear un grupo de trabajo que se encargue de analizar la metodología de desarrollo, identificando un plan de acción con posibles mejoras para evitar que esta incidencia vuelva a producirse en el futuro.
- Comunicar a la AEPD, basándose en el número de afectados, la tipología de datos afectadas, la rápida respuesta, las medidas adoptadas para reducir el impacto en la privacidad de los afectados, y el desarrollo de un plan para evitar que incidencias similares vuelvan a pasar.

Aspectos relevantes en la valoración de la brecha

Se identifican los siguientes aspectos relevantes en la valoración de la brecha del ejemplo:

- Origen del incidente: primer aspecto relevante a la hora de valorar la brecha, y que en este caso es interno y accidental.

En el caso de que el origen del incidente sea externo y deliberado, generalmente amplía el impacto de la brecha, ya que en estos casos el atacante lo que busca es realizar el mayor impacto posible.

- Afectación de la brecha: en este caso se ha visto afectada la confidencialidad de los datos de ciertos clientes. Si bien dado que a los datos solo tuvo acceso a una persona, su severidad es mucho menor con una afectación menor a la confidencialidad que en el caso que estos hubiesen sido accesibles desde internet, o si hubiese permitido su modificación irregular.

Otra afectación diferente que hubiera podido provocar el error en la subida a producción hubiese sido la disponibilidad de la web. En este caso habrá que analizar el servicio prestado por la mismas para conocer el impacto de su indisponibilidad. No siendo lo mismo una web de venta de ropa, como en el ejemplo, que una organización que presta un servicio esencial, como determinadas administraciones públicas.

- Momento en el que se conoció la brecha: en el ejemplo dado, la brecha fue conocida tras el aviso de varios de los afectados, al poco de producirse.

Hay que destacar que el [CLIENTE] disponía de canales ágiles que permitieron que los afectados les informaran rápidamente, lo que permitió actuar rápidamente para mitigar el impacto.

En caso de que el paso a producción hubiera dejado al descubierto alguna vulnerabilidad que hubiera permitido accesos no autorizados desde internet, el conocimiento de la brecha hubiera estado supeditado a las herramientas instaladas por el departamento de Ciberseguridad para monitorizar los accesos.

- Actuación ante la brecha: en el ejemplo dado, el [CLIENTE] actuó rápidamente una vez conocido el aviso del primero de los afectados, tomándose decisiones diligentemente, según se iba teniendo cada vez más conocimiento de lo acontecido.
- Tipo de datos (severidad): en el ejemplo dado, los datos afectados son datos identificativos (nombre y apellidos), datos de contacto (dirección postal), y los datos de la compra.

Puede considerarse que en la Situación 2 los afectados no se verán perjudicados, o se podrían encontrar con algunos inconvenientes que superarán sin problema. Por el contrario, en la Situación 3, las personas pueden encontrar inconvenientes importantes, produciendo un daño limitado que podrán superar (como, por ejemplo, que sus datos sean utilizados para realizar compras no autorizadas por ellos).

En caso de que los datos afectados fueran datos de salud como por ejemplo informes médicos, el impacto sería mucho mayor. A fin de que se pueda ver este aspecto en el resumen de valoración (aunque en un supuesto de este tipo de compra de ropa no sería de difícil aplicación) se incluye una Situación 4 que hace referencia a este aspecto.

Igualmente, en el caso de que los datos afectados sean de menores o de colectivos vulnerables, el impacto sería mucho mayor.

- Medidas de seguridad en vigor: en el ejemplo dado, diversas medidas técnicas y organizativas permitieron al [CLIENTE] actuar con diligencia:
 - Disponer de un Comité de Protección de Datos formalizado con las principales áreas de la organización (Clientes, Comunicación, Tecnología, Operaciones, Ciberseguridad, Protección de Datos, DPD), permitió el rápido entendimiento de la



gravedad de la situación, y la agilidad en la toma de decisiones.

-Los distintos sistemas implicados disponían de logs que permitieron realizar una investigación de lo sucedido, determinar las causas e identificar los datos afectados.

-El departamento de Ciberseguridad disponía de herramientas que permitieron descartar que la incidencia fuera debido a un ataque externo.

-La participación del DPD durante el proyecto permitió, por ejemplo, que el PDF con la carta no incluyera los datos de tarjeta de crédito, salvo en la Situación 3, que sí aparecían dichos datos por una decisión tomada por el [PROVEEDOR] sin conocimiento del DPD.

- Número de afectados: el volumen de afectados, si son muchos o pocos, sólo podrá determinarse conjuntamente con otros parámetros como por ejemplo el tipo de datos afectados. Por ese motivo, en la mayoría de los casos, este parámetro debería ser el último en analizarse.

En el ejemplo dado, en función de la situación que se ha producido, nos encontraríamos con 500 datos o 20.

En cualquier caso, aunque los 500 afectados puede parecer muchos, no debe dejarse de valorar teniendo en consideración el resto de parámetros (tipología de datos, rápida detección de la brecha, mitigación, etc.), puede minimizar la valoración.

Resumen de la valoración

Se identifican los siguientes aspectos relevantes en la valoración de la brecha del ejemplo:

PARÁMETROS EVALUADOS		SITUACIÓN 1	SITUACIÓN 2	SITUACIÓN 3	SITUACIÓN 4
Sobre la brecha	Como ha sido el incidente	Accidental	Accidental	Accidental	Accidental
Sobre la brecha	Origen del incidente	Interno	Interno	Interno	Interno
Sobre las consecuencias	Consec. del incidente	Afectación a la confidencialidad – a los clientes a los que se enviaron los datos de su compra a otros	Afectación a la confidencialidad – a los clientes a los que se enviaron los datos de su compra a otros	Afectación a la confidencialidad – a los clientes a los que se enviaron los datos de su compra a otros	Afectación a la confidencialidad – a los clientes a los que se enviaron los datos de salud a otros
Sobre las consecuencias	Grado en el que podría afectar	Pueden encontrar inconvenientes importantes	No se verán afectadas, o serán afectados por algunos inconvenientes que superarán sin problema	Pueden encontrar inconvenientes importantes	Pueden encontrar inconvenientes importantes
Sobre las consecuencias	Se ha materializado alguno de los daños	No	No	Si	No
Sobre las consecuencias	Probabilidad de que el daño anterior se materialice	Baja	Baja	Alta	Baja
Categoría de datos	Tipos de datos afectados en personas físicas	Identificativos, datos de contacto, datos de la compra	Identificativos, datos de contacto, datos de la compra	Identificativos, datos de contacto, datos de la compra incluyendo datos bancarios	Identificativos, datos de contacto, datos de la compra y de salud
Personas afectadas	Hay menores o vulnerables	No	No	No	No
Personas afectadas	Volumen de personas afectadas por la brecha	500	20	500	20
Inform. Temporal	Momento en el que se conoció	A los 3 días	A los 3 días	A los 3 días	Al mes de producirse
	Actuación ante la brecha	Temprana y diligente	Temprana y diligente	Temprana y diligente	Tardía
Resultado	Comunicar a la autoridad de control	Si	No	Si	Si
	Comunicar a los afectados	No	No	Si (para minimizar el impacto)	Si

Descripción del caso práctico

La operadora de Telecomunicaciones ha incluido entre los servicios que oferta a sus clientes la compra de terminales móviles a plazos, incluyendo los pagos dentro de su factura de Telecomunicaciones, y a unos precios especiales en función de los servicios contratados. La compra de estos equipos puede realizarse vía telefónica, sin más que identificarse unívocamente como cliente.

- 10 de enero: una persona [SUPLANTANTE] llama haciéndose pasar por el cliente reclamante y solicitando que se modifique su dirección postal y su dirección de e-mail.

Se autentica al cliente solicitándole número de DNI, fecha de nacimiento y domicilio actual. El SUPLANTANTE, posee esa información específica de un CLIENTE, ya que son tres datos que se encuentran en un DNI que ha obtenido del propio cliente. Este ha facilitado una copia de su DNI cuando el SUPLANTANTE ha intentado vender en una web no oficial un dorsal para la maratón de Madrid, ya que dijo que este lo necesitaba para poder ir a recoger el dorsal. Tras enviar la copia del DNI, el SUPLANTANTE decide cancelar la operación de compraventa del dorsal.

- 30 de enero: vuelve a llamar el SUPLANTANTE y contrata a nombre del cliente suplantado un terminal móvil de alta gama.

La autenticación del cliente se realizada de nuevo con los tres datos anteriores: número de DNI, fecha de nacimiento y domicilio. Y se envía al mail del SUPLANTANTE el contrato de compra-venta, para que el supuesto cliente lo envíe firmado y con copia de DNI. Este lo hace en una versión escaneada a través del mail.

- 27 de febrero: un cliente llama al Servicio de Atención al Cliente porque ha visto en su factura un cargo relacionado con la compra de un terminal móvil de alta gama que no reconoce haber realizado. Habiendo comprobado también en su espacio privado de cliente que sus datos de contacto han sido modificados sin su conocimiento.
- 28 de febrero: el equipo de Atención al Cliente de la Operadora ha comprobado que efectivamente se ha producido una suplantación a través de los logs de modificaciones en los registros de datos del cliente reclamante y escuchando las grabaciones de las llamadas recibidas.

Adicionalmente a lo anterior, hay una serie de aspectos que impactan en la valoración de la brecha y que proporcionan información adicional a la anterior. Por este motivo a continuación procederemos a indicar dichas situaciones para mostrar como un mismo hecho puede variar sustancialmente en función de cómo se haya producido y fruto del análisis y valoración de la brecha:

Situación 1: el CLIENTE SUPLANTADO detecta el problema antes de la emisión de la factura y lo comunica a la empresa de telecomunicaciones quien rápidamente revierte la situación y procede a analizar si se han producido

situaciones similares y si el SUPLANTANTE pudiera haber actuado de la misma manera con otros clientes. Confirma que se trata de un hecho que ha afectado a otra persona más y procede a avisarla preventivamente.

Además, por protocolos internos, la compañía de telecomunicaciones en la web del cliente incluye los datos financieros truncados a fin de que no puedan ser utilizados por terceros no autorizados.

En cualquier caso, la compañía, procede a revertir la situación del CLIENTE SUPLANTADO e informar al otro afectado a fin de alertarle de la situación y poder proceder a regularizar también la situación asociada a dicho cliente antes de que venza el mes.

Situación 2: El CLIENTE SUPLANTADO detecta el problema al mes siguiente, cuando ve en su domiciliación bancaria que el importe de la factura de la empresa de comunicaciones es superior al habitual y, comprueba que aún no se le ha remitido la factura, por lo que ingresa en su perfil de la web y, ve que sus datos han sido modificados y que en el detalle de su última factura se ha comprado también un terminal.

El CLIENTE SUPLANTADO por tanto se pone en contacto con la empresa de telecomunicaciones quien se da cuenta que ha habido una suplantación de identidad y revierte el cambio de datos que se ha realizado en la base de datos cancelando asimismo la compraventa realizada.

Además, por protocolos internos, la compañía de telecomunicaciones en la web del cliente incluye los datos financieros truncados a fin de que no puedan ser utilizados por terceros no autorizados.

Mientras tanto, se ha producido la emisión de la factura, que ha llegado al SUPLANTANTE y donde se incluye información financiera relevante que puede afectar significativamente al CLIENTE SUPLANTADO.

Tras un análisis de la situación, por parte de la empresa de telecomunicaciones, se detecta que este hecho no solo ha afectado a este CLIENTE SUPLANTADO, sino que se ha producido en 20 casos más.

Situación 3: se trata de un caso similar a la Situación 1 con la diferencia en que, en este caso, los datos bancarios del CLIENTE SUPLANTADO sí estaban disponibles para el SUPLANTANTE lo que significa que dispone de información que puede utilizar y que el impacto puede ser mayor.

Además, la compañía, tras analizar el hecho, detecta que este no es un caso aislado y que ha afectado a otros 3 clientes más por lo que determina ponerse en contacto con todos ellos a fin de poder revertir la situación cuanto antes y alertarles del hecho ocurrido.

Los principales aspectos asociados a esta brecha y que impactan en el análisis de la misma son los siguientes:

- Origen de la brecha: ha sido consecuencia de un incidente externo. El origen del mismo deviene de que el cliente ha proporcionado ciertos datos de carácter personal sin ser lo suficientemente diligente y, además, que el procedimiento de identificación que tiene la empresa de telecomunicaciones no es lo suficientemente robusto, en tanto que debería tener medidas adicionales para la rectificación de los datos de los interesados, principalmente de aquellos que pueden tener una consecuencia en la operativa, solicitando un doble factor de autenticación, es decir además de proporcionar información que nos identifica, tendría que haber solicitado información que nos autentique, por ejemplo una contraseña única del cliente que este haya creado o, enviándole a su dispositivo móvil una clave de confirmación, para poder comprobar que el cliente es quien dice ser.
- Consecuencias del incidente: las consecuencias del incidente dependen de la situación que se haya producido porque puede ser desde un caso aislado y que ha podido gestionarse a tiempo y sin que se haya tenido acceso a información financiera, a otros casos donde el impacto puede haber sido mayor al haberse detectado pasado el tiempo y al haber afectado a un colectivo mayor de personas.

En todos los casos se ha materializado el daño en tanto que se han utilizado los datos del CLIENTE para su perjuicio, en este caso, la compraventa de un bien. Asimismo, en tanto que la empresa de telecomunicaciones le ha enviado una factura al e-mail proporcionado por el SUPLANTANTE, este ha podido recibir otros datos del Cliente y, en función de dicho detalle, el impacto ser mayor.

- Los datos afectados: los datos afectados son datos identificativos como el número de teléfono. Adicionalmente, en función de la situación, puede haber implicado también datos financieros (datos de la cuenta bancaria en los casos en los que dicha información no aparecía truncada, como ocurría en la Situación 3). Respecto al volumen de los datos, estos han sido o 2 personas o 20, en función de la situación descrita. En cualquier caso, no se encontraban implicados colectivos vulnerables.
- La información temporal de la brecha: la brecha se ha detectado cuando el cliente ha realizado una consulta antes de vencer el tiempo para la emisión de la factura o en la Situación 2 y 3 que se ha producido cuando ha recibido la factura domiciliada en su cuenta bancaria, siendo el inicio de la misma cuando se ha remitido la factura electrónica al correo modificado por el SUPLANTANTE.

Resumen de la valoración

PARÁMETROS EVALUADOS		SITUACIÓN 1	SITUACIÓN 2	SITUACIÓN 3
Sobre la brecha	Como ha sido el incidente	Intencionado	Intencionado	Intencionado
	Origen del incidente	Externo	Externo	Externo
Sobre las consecuencias	Consec. del incidente	Acceso no autorizado a los datos y alteración de los datos del cliente	Acceso no autorizado a los datos y alteración de los datos del cliente	Acceso no autorizado a los datos y alteración de los datos del cliente
	Grado en el que podría afectar	Pueden encontrar inconvenientes limitados y reversibles (se gestiona rápidamente el hecho y se restaura la situación)	Pueden encontrar inconvenientes importantes – costes adicionales	Pueden encontrar inconvenientes importantes – costes adicionales
	Se ha materializado alguno de los daños	Si	Si	Si
	Probabilidad de que el daño anterior se materialice			
Categoría de datos	Tipos de datos afectados en personas físicas	Identificativos, datos de contacto, datos de la compra sin cuenta bancaria	Identificativos, datos de contacto, datos de la compra sin cuenta bancaria	Identificativos, datos de contacto, datos de la compra con cuenta bancaria
Personas afectadas	Hay menores o vulnerables	No	No	No
	Volumen de personas afectadas por la brecha	2	20	2
Inform. Temporal	Momento en el que se conoció	Antes del mes	Al mes	Al mes
	Actuación ante la brecha	Tan pronto como se tiene conocimiento	Tan pronto como se tiene conocimiento	Tan pronto como se tiene conocimiento
Resultado	Comunicar a la autoridad de control	No	SI	SI
	Comunicar a los afectados	Sí (Para minimizar riesgo)	SI	SI

Dstrucción soportes de información

Descripción del caso práctico

La compañía [CLIENTE], inmobiliaria que cuenta con una serie de fincas en el país y que tiene como una de sus principales actividades la administración de fincas, decide abrir una nueva sucursal en Valladolid. Para ello desplaza a uno de los gerentes más cualificados a dicha ciudad, con el objetivo de coordinar la apertura y los primeros meses de funcionamiento.

Se contratan dos administrativos especialistas en gestión de fincas, un comercial, y un técnico informático como Responsable de Soporte Local. Este último será la persona que realizará la implantación de los sistemas y redes de la sucursal, apoyados desde el Dpto. de Tecnología de Central.

La empresa cuenta con una persona encargada de la Protección de Datos.

- Mayo: tras cuatro meses de duro trabajo, la sucursal está prácticamente lista. Se han obtenido nuevos locales a gestionar, algunos de ellos pertenecientes a los últimos bloques de viviendas construidos en la ciudad.

La apertura no ha estado exenta de problemas técnicos.

La conexión de red de la nueva sucursal con Central no tenía la estabilidad deseada, por lo que se optó por que la aplicación “GestiónFincas”, utilizada para la gestión de la actividad principal de la compañía y que contiene, entre otros, información de los vecinos, los contactos realizados con ellos, información económica, etc., estuviera en un servidor de la propia sucursal, en lugar de utilizar una instancia del mismo de Central, como utilizaban el resto de las sucursales.

Adicionalmente, el Dpto. de Tecnología tuvo que encargarse de diversos proyectos estratégicos, y no tuvo capacidad para dar asistencia al Soporte Local.

- 28 de julio: se decide retirar uno de los servidores enviados desde Central en febrero utilizado para la implantación inicial, y que ya no era utilizado, para lo que se decide contratar una empresa especializada en destrucción de soportes. El Responsable de Soporte Local tramita la gestión identificando el servidor a destruir.
- 01 de agosto: a última hora de la tarde, la empresa especializada se presenta en la sucursal, y el administrativo le indica por error el servidor incorrecto, en parte porque las instrucciones del Responsable de Soporte Local fueron dadas por teléfono sin demasiado detalle.

Todas las personas de la sucursal, a excepción de un administrativo, han comenzado su periodo de vacaciones.

El servidor retirado por la empresa especializada es el que contenía la aplicación de “GestiónFincas”.

Únicamente se hacía copia de seguridad semanal de dicho servidor y se almacenaba en el mismo, ya que se estaba a la espera de solucionar los problemas de conexión con Central para utilizar los servicios de backup prestados desde allí.

- 02 de agosto: el administrativo acude a la sucursal para realizar unas últimas gestiones antes de irse de vacaciones, pero no se percató de que no está funcionando, por lo que al final de la jornada cierra la sucursal y se va de vacaciones.

La empresa especializada realiza un borrado seguro del servidor que contenía la aplicación de “GestiónFincas”, así como de la única copia de seguridad.

- 31 de agosto¹⁴: el Responsable de Soporte Local, aprovechando que tiene la tarde libre, se desplaza a la sucursal para comprobar que todo está en orden. Al intentar acceder con su usuario a la aplicación de “GestiónFincas”, se percató de que algo no va bien. Comprueba que el servidor no responde, por lo que accede a la sala técnica para comprobar que el servidor está encendido, y descubre que el servidor no está.

Inmediatamente llama al Gerente de la sucursal para notificarle lo ocurrido, barajándose la posibilidad de que fuera un robo. Se decide ir a la mañana siguiente a la sucursal a primera hora para aclarar con el resto de los empleados qué ha podido pasar.

- 01 de septiembre: a primera hora se convoca reunión de urgencia con todos los empleados para informarles de la situación. El administrativo que estuvo los primeros días de agosto comenta la hipótesis de que la empresa especializada hubiera podido llevarse el servidor erróneo.

El Responsable de Soporte Local comprueba que el servidor, que en realidad tenía que haberse retirado, sigue allí, y verifica en su correo electrónico que efectivamente tiene un certificado de destrucción de la empresa especializada.

Se decide informar al Dpto. de Coordinación Territorial, así como al Dpto. de Tecnología de Central. El Dpto. de Tecnología involucra al Responsable de Protección de Datos.

La sucursal gestionaba actualmente 10 edificios, con un total de 1.000 vecinos.

Se mantiene reunión entre todos ellos y se decide:

- Contactar con la empresa especializada, por si debido a un error la destrucción no se hubiera llevado a cabo, o por si hubiera forma de recuperar la información.
- En caso de que alguno de los vecinos contacte con la Sucursal, informarles de que se ha producido una incidencia informática, y que están trabajando en solucionarla.
- Instalar la aplicación “GestiónFincas” en alguno de los servidores disponibles, y activar la copia de seguridad en los servidores de ficheros de Central, los cuales se encontraban fuera de la Sucursal.
- Realizar una revisión de las aplicaciones y datos de la sucursal de los que no se está realizando copia de seguridad externalizada y regularizarlo.
- Notificar a Central para que realice una revisión similar en el resto de las sucursales.
- Elaborar un Plan de recuperación de la información, basado en:

-El volumen y la tipología de datos que se ha podido perder.

-La información que tuvieran los empleados de la sucursal en los emails o archivos de los servidores de ficheros.

-Contactar, en caso de necesidad, con cada uno de los vecinos, informarles del problema, y pedirles la información que tuvieran que pudieran necesitar (gestiones abiertas, relación de vecinos, etc.).

- 02 de septiembre: la empresa especializada confirma que el servidor fue destruido físicamente, y que la información no se puede recuperar.

Durante el análisis para la realización del Plan de recuperación se concluye que gran parte de la información está en correos electrónicos, y que puede ser volcada manualmente a la aplicación de “GestiónFincas”. De esta forma únicamente se perderían las gestiones realizadas telefónicamente con los vecinos, ya que estas únicamente se registraban en la aplicación.

En este momento se pueden dar distintas situaciones que pueden afectar de un modo u otro a la valoración del hecho ocurrido:

Situación 1: el volumen de datos personales afectados era de aproximadamente 1.000 interesados, con datos básicos de contacto, así como las gestiones realizadas pero todo ello se puede recuperar y mecanizar de nuevo sin apenas impacto para las personas.

En base todo lo anterior, se decide no comunicar a los afectados ni declarar brecha ante la AEPD.

Situación 2: el volumen de datos personales afectados era de aproximadamente 10.000 interesados, con datos básicos de contacto, así como las gestiones realizadas, pero al igual que el caso anterior, se puede proceder a la mecanización de nuevo de la información sin apenas impacto ya que se ha aprobado la contratación de una persona para agilizar este proceso.

En base todo lo anterior, se decide no comunicar a los afectados (vecinos) ni declarar brecha ante la AEPD.

Situación 3: el volumen de datos personales afectados era de aproximadamente 100.000 interesados, con datos básicos de contacto, así como las gestiones realizadas, pero en este caso no se disponía de información y era necesario proceder a contactar con cada uno de los vecinos para recopilar de nuevo la información asociada.

En base a todo lo anterior, se decide comunicar a los afectados (vecinos) y declarar brecha de disponibilidad ante la AEPD.

Situación 4: el volumen de datos personales afectados era de aproximadamente 1.000 interesados, con datos básicos de contacto, así como las gestiones realizadas.

Algunos de los datos contienen datos de salud, debido a que alguna de las fincas eran residencias de ancianos y, aparte de las gestiones tradicionales, realizaban otra serie de tratamientos, para lo que utilizaban la misma aplicación y que conllevaba el tratamiento de datos de salud.

Debido a la tipología de datos afectados, se decide comunicar a los afectados que pudieran tener datos de salud, haciendo hincapié en la rápida respuesta y las medidas adoptadas para reducir el impacto en los afectados, así como en el desarrollo de un plan para evitar que incidencias similares vuelvan a pasar.

Aspectos relevantes en la valoración de la brecha ocurrida

Se identifican los siguientes aspectos relevantes en la valoración de la brecha del ejemplo:

- Origen del incidente: en el ejemplo dado, el origen es interno y accidental.
- Afectación: en el ejemplo dado, la brecha afecta a la disponibilidad de la información. Pero la pérdida definitiva de ciertos datos, como pagos ya realizados por los vecinos, podría llegar a “constituir un riesgo para los derechos y las libertades de las personas físicas”.

Y también a la integridad, ya que, durante el Plan de recuperación de la información, es imposible garantizar que la información volviera a ser la misma que antes de suceder la brecha.

En este caso la brecha no tiene una afectación a la confidencialidad de la información, salvo por el hecho de que las dos personas de apoyo enviadas por Central accedieran a información personal, que de otra forma no habrían tenido que acceder.

- Momento en el que se conoció la brecha: en el ejemplo dado, la brecha fue conocida casi un mes después de producirse. El que haya transcurrido tanto tiempo puede ser considerado que ha debido ser por una fatalidad, ya que se produjo justo antes de un periodo, el vacacional, en el que ninguna de las personas que podrían haberla detectado estaban trabajando.
- Actuación ante la brecha: en el ejemplo dado, el cliente actuó rápidamente una vez conocida la brecha, tomándose decisiones diligentemente, y realizando un plan de acción para que una brecha similar no se volviera a producir.
- Tipo de datos (severidad): en el ejemplo dado, los datos afectados son datos identificativos (nombre y apellidos), datos de contacto (dirección postal), datos económicos del vecino, así como las solicitudes realizadas por el vecino.
Puede considerarse que, en términos generales, los afectados no se verán afectados, o serán afectados por algunos inconvenientes que superarán sin problema.

No obstante, en algunos casos excepcionales, podrían darse inconvenientes más importantes como costes adicionales para los afectados. Por ejemplo, si el afectado tiene una urgencia que no es atendida por no encontrarse sus datos en el sistema, o bien si la solicitud del afectado se ha perdido por haberla realizado telefónicamente.

En caso de que los datos afectados fueran datos de salud como en la Situación 4, como por ejemplo informes o pruebas médicas, el impacto sería mucho mayor, máxime si los datos no se pudieran recuperar.

Igualmente, en el caso de que los datos afectados sean de menores o de colectivos vulnerables, el impacto sería mucho mayor.

- Medidas de seguridad en vigor: en el ejemplo dado, la principal medida técnica que debía estar implantada (copia de seguridad externalizada) no estaba conforme.
- Número de afectados: el volumen de afectados, si son muchos o pocos, sólo podrá determinarse conjuntamente con otros parámetros como por ejemplo el tipo de datos afectados.

Por ese motivo, en la mayoría de los casos, este parámetro debería ser el último en analizarse.

En el ejemplo dado, 1.000 afectados puede parecer muchos, pero conjuntamente con el resto de parámetros (tipología de datos, rápida detección de la brecha, mitigación, etc.), puede minimizar la valoración.

Resumen de la valoración

Se identifican los siguientes aspectos relevantes en la valoración de la brecha del ejemplo:

PARÁMETROS EVALUADOS	SITUACIÓN 1	SITUACIÓN 2	SITUACIÓN 3	SITUACIÓN 4
Afectación a la confidencialidad	No	No	No	No
Afectación a la disponibilidad	No	No	No	No
Afectación a la integridad	No	No	No	No
Tipo de dato (severidad)	Identificativos, datos de contacto, gestiones con la comunidad (baja)	Identificativos, datos de contacto, gestiones con la comunidad (baja)	Identificativos, datos de contacto, gestiones con la comunidad (baja)	Identificativos, datos de contacto, datos de salud (alta)
Momento en el que se conoció la brecha	Al mes de producirse	Al mes de producirse	Al mes de producirse	Al mes de producirse
Actuación ante la brecha	Temprana y diligente	Temprana y diligente	Temprana y diligente	Temprana y diligente
Número de afectados	1.000	10.000	100.000	10.000
COMUNICAR AL REGULADOR	NO	NO	SI	SI
COMUNICAR A AFECTADOS	NO	NO	SI	SI

Descripción del caso práctico

La empresa ACME se dedica al transporte nacional de pasajeros, su forma jurídica es la de entidad pública empresarial, organismo público de los previstos en el artículo 103 de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público y se halla adscrito al Ministerio de Transportes, Movilidad y Agenda Urbana (MITMA). Tiene personalidad jurídica propia y diferenciada de la del Estado, plena capacidad jurídica y de obrar para el cumplimiento de sus fines, patrimonio y tesorería propios.

Tiene datos de más de dos millones de clientes que han viajado con ACME en los últimos dos años y cerca de 5 millones de registros de clientes históricos (de hasta ocho años atrás). Principalmente, el conjunto de datos se encuentra en la plataforma de Gestión de Relaciones con los clientes o en por sus siglas en inglés CRM.

El CRM tiene conexión con la plataforma de venta y con la plataforma de marketing. En el CRM se almacenan datos tales como: Identificación de cliente (nombre y apellidos, DNI, fecha nacimiento), identificación de tarjeta de fidelización (ID de la tarjeta), datos de contacto (teléfono, email), compras realizadas, operaciones con puntos e interacciones con postventa y preventa, gustos (ventanilla o pasillo) y necesidades relacionadas con el viaje (necesidades especiales de comida o de accesibilidad).

La empresa ACME contrató hace once meses a la compañía PROVEEDOR1 para que substituyera la plataforma CRM existente a una nueva en formato XaaS (Todo como servicio), es decir no sólo el CRM como PaaS (Plataforma como Servicio), sino todos los servicios TIC relacionados con la provisión del CRM (sistemas, comunicaciones, seguridad, soporte, etc.).

PROVEEDOR1 como parte de su oferta y en respuesta a las especificaciones técnicas de ACME, decidió diseñar el servicio a su cliente mediante servicios de sistemas de información en la nube; en concreto en una arquitectura de plataforma redundada multinube. Eligió esta arquitectura, apoyándose en los proveedores NUBE1 y NUBE2 a fin de garantizar tanto la disponibilidad, como la reducción de parte del riesgo de costes asociados a procesamiento y almacenamiento.

El cliente ACME, en el acto de firma del contrato, aceptó como encargado del tratamiento a PROVEEDOR1 y, como subencargados del tratamiento, tanto a NUBE1, como a NUBE2.

ACME había realizado tanto en el momento de definir las especificaciones técnicas como en el del diseño definitivo de la solución a implantar por PROVEEDOR1, los análisis de riesgos de seguridad y evaluación de impacto. Tomó y también exigió a PROVEEDOR1, las adecuadas medidas organizativas, procedimentales, humanas y técnicas derivadas de su análisis. Entre ellas, y no limitadas a ellas, se encuentran:

- **Directamente en ACME**
 - o Comité de privacidad, con representación de partes de interés en esta materia (DPD, comercial, postventa, legal, RRHH, Responsable de Seguridad, comunicación -externa e interna-).

- o Comité de Seguridad de la Información, con vocales de las partes con interés en ciberseguridad (Responsable de seguridad, legal, DPD, Dirección TIC, representantes diferentes área de negocio).
- o Delegado de Protección de Datos (DPD) y su oficina de apoyo
- o Responsable de Seguridad (de la información, RSEG) y su oficina de apoyo.
- o Identificación de obligaciones legales en materia de información RGPD y LOPDyGDD, así como el Esquema Nacional de Seguridad (por estar en el ámbito subjetivo del RD 40/2015).
- o Servicio interno de CERT (Grupo de respuesta a ciberincidentes). Incluye especialistas en gestión de incidentes, analistas de información -interna y fuentes públicas- y analistas de malware entre otros perfiles profesionales.
- o Cuerpo normativo: Política de Seguridad, normas, procedimientos e instrucciones de seguridad.
- o Procedimientos de Gestión de incidentes de seguridad (Detección, tratamiento, reacción, recuperación y comunicación a autoridades de control) que incluyen la cooperación con autoridades de control, fuerzas y cuerpos de seguridad del estado y cadena de suministro. En este procedimiento se contempla en qué circunstancias se deben enviar las comunicaciones por correo con copia a tercera parte para certificación de contenidos.
- o Está en posición de un Ciberseguro, con una franquicia de 300.000 euros y una cobertura en servicios profesionales (técnicos de sistemas, de gestión de incidentes, legales, ...) de hasta 30 millones de euros.

- **Requerido a PROVEEDOR1**

- o Debe disponer formalmente de un Marco Normativo en materia de ciberseguridad.
- o Debe disponer de las certificaciones de seguridad: ISO 27001:2017 y del ENS nivel alto o medio, para el alcance del conjunto de los servicios que le preste el PROVEEDOR1 (consecuencia del segundo párrafo del apartado segundo de la disposición adicional primera de la LOPDyGDD).
- o Debe realizar su propio análisis de riesgo a su arquitectura técnica y evaluación de impacto a los tratamientos de carácter personal que deberán llevar a cabo conforme a las especificaciones técnicas, todo ello como paso previo a la oferta (y así considerar en la misma los gastos de los controles y tratamientos). Posteriormente, una vez firmado el contrato y definido todos los “flecós” previos a la implantación, deberá realizar un nuevo análisis de riesgo y evaluación de impacto.
- o Debe aplicar las medidas de seguridad derivadas de los análisis. Entre ellas, y sin limitarse a las mismas:
 - ☐ Trazabilidad en sus servicios.
 - ☐ Auditorías por un tercero acreditado, cada dos años.
 - ☐ Posibilidad de ser auditado por ACME (muy excepcionalmente).
 - ☐ Colaboración en incidentes de seguridad con ACME (Inmediata notificación a ACME -menos de 24 horas de tener indicios claros de brecha-, aportación de cuanta información le sea requerida por ACME, sus autoridades de control y fuerzas y cuerpos de seguridad del estado).
- o Debe designar un Punto de contacto de seguridad, como responsable de todos los aspectos de seguridad de la provisión de servicios que le han sido contratados.
- o Debe identificar al DPD de PROVEEDOR1.
- o Debe identificar a los subencargados del tratamiento y hacerles partícipes efectivos de las mismas obligaciones que le han sido impuestas en el contrato con ACME.

- **01 de agosto¹⁵**: se hace público, en un grupo de Telegram y a través de la publicación de un empleado de una compañía de servicios que trabaja para el proveedor de servicios en la nube NUBE1, que dicho proveedor ha tenido una importante brecha de seguridad. El área de ciberinteligencia del CERT de ACME notifica al Responsable de Seguridad (en adelante RSEG ACME) esta información sin confirmar.

De inmediato, RSEG ACME se pone en contacto telefónico con el punto de contacto de seguridad de PROVEEDOR1 (en adelante POCSEG PROVEEDOR1) para verificar o desmentir la información indirecta que ha recibido. El proveedor indica, que se está investigando la incidencia a fin de identificar si se trata de un mal funcionamiento del sistema o si es un incidente (de seguridad).

- **03 de agosto**: POCSEG PROVEEDOR1 comunica telefónicamente que su proveedor de infraestructura en la nube NUBE1, ha sufrido la explotación de una vulnerabilidad crítica en los gestores de máquinas virtuales. Por los logs se determina que la IP origen del incidente, son externas a la organización y el incidente se produjo a las 03:45 del día anterior. La explotación de la vulnerabilidad ha podido provocar el robo de un conjunto de credenciales de acceso de cuentas de administrador de los gestores de virtualización. Probablemente, entre el listado de credenciales exfiltradas figuran las credenciales de los administradores de PROVEEDOR1 de las máquinas virtuales y servicios de base de datos alojados en NUBE1 y que forman parte de la infraestructura con la que presta servicio ACME.

POCSEG PROVEEDOR1 confirma que NUBE2 dispone de otra tecnología de virtualización y no se ha visto afectada. Han tomado la acción de resetear todas las cuentas de administrador, bloqueando las no esenciales y disponiendo de nuevas alertas de uso de dichas credenciales en la plataforma.

POCSEG PROVEEDOR1 informa que se han puesto en conocimiento de la Policía Nacional los hechos.

RSEG ACME indica en la llamada telefónica con POCSEG PROVEEDOR1 que la comunicación y posteriores acciones se haga conforme al procedimiento acordado de notificación y gestión de incidentes en PROVEEDOR1 y/o en su cadena de suministro.



¹⁴Se inicia el proceso de gestión de la brecha

POCSEG PROVEEDOR1 envía un email con certificación de contenido por tercera parte a RSEG ACME, conteniendo un breve informe de lo ya comunicado verbalmente. Esa información contiene un ID de referencia, una descripción del incidente, información temporal del momento de descubrimiento, una evaluación de impacto global y particularmente de impacto para ACME. Detalla las medidas de contención y las acciones que emprende para remediar y en cuanto sea posible recuperar los servicios de ACME1, si estos han sido afectados. También aporta los datos de contacto de POCSEG NUBE1.

El informe, como suele ser habitual en las primeras horas, es vago y no afirma, ni desmiente con rotundidad si ha habido uso o no de las credenciales y mucho menos si ha habido exfiltración de las mismas y de los datos de clientes. Tampoco se ha identificado el vector de entrada, si bien el vector de explotación parece que se confirma (la vulnerabilidad crítica citada).

RSEG ACME, inicia su procedimiento de gestión de incidentes, particularizándose su gestión en incidentes de la cadena de suministro con probable afectación de sistemas en los que se tratan datos de carácter personal.

Registra en la plataforma de gestión de incidentes de ACME (RTIR) tanto la información recibida por correo, como la telefónica, así como la información que sea de interés para la gestión; la cual esta identificada en el procedimiento de gestión: contratos, detalle de arquitecturas, análisis, etc. Responde a POCSEG por el mismo medio (correo certificado por tercera parte) indicándole que se realizarán reuniones telemáticas de puesta al día y toma de decisiones, a las 10 AM y a las 18 PM todos los días, hasta que se determine una cadencia diferente de seguimiento.

También se harán reuniones fuera de las programadas si la situación lo requiere. Las reuniones serán grabadas.

RSEG ACME informa preventivamente al DPD y ambos convocan a una reunión telemática a los Comités de Privacidad y Seguridad, para informarles de una posible situación de incidente de nivel medio o alto, con afectación de datos de carácter personal. También informa al proveedor del ciberseguro, todo como medida preventiva.

RSEG ACME abre incidente con el CCN-CERT, pues con independencia del acceso a datos de carácter personal, se dan las circunstancias que aconsejan informar del incidente al CCN, si bien en su comunicación no se valora ni la extensión ni el impacto y se queda a la espera de actualizaciones de situación.

El DPD decide no comunicar a la AEPD; pues no es que aún no tenga confirmación de acceso no autorizado a las BBDD de clientes, sino tan siquiera PROVEEDOR1 tiene indicios de ese posible acceso no autorizado a las BBDD.

A partir de este momento y en función de los distintos resultados que se van obteniendo y/o produciendo, se pueden dar distintas situaciones que afectarán de manera directa a la valoración de la brecha y que procedemos a detallar:

Situación 1: las Especificaciones Técnicas de ACME del servicio a ofertar por PROVEEDOR1 y el posterior contrato de prestación de servicios, indicaban que los servicios de Negocio objeto del contrato se proveerán desde una plataforma dedicada a ACME, sin compartición ni HW, ni SW de la misma con otros clientes.

Situación 2: el contrato estipulaba que la plataforma que presta directamente el servicio de Negocio a ACME por PROVEEDOR1, es una plataforma pública, compartida por NUBE1 con otros clientes.

- 04 de agosto: POCSEG PROVEEDOR1 informa sin concretar si sus cuentas de administración (las de PROVEEDOR1) han sido reveladas al atacante. También informa de las medidas de gestión del incidente que están adoptando (análisis de registros, reseteo de contraseñas, habilitación de doble factor o generación de alertas, entre otras). Es aquí donde habrá diferencias de actuación para las dos situaciones descritas como Situación 1 y Situación 2.

En la Situación 1, tanto PROVEEDOR1 como ACME podrán ejercer una mayor dirección y gestión del incidente.

- o ACME ejercerá el liderazgo de seguimiento del incidente y lo hará directamente sobre el proveedor que ha tenido la hipotética brecha; es decir, sobre PROVEEDOR1.
- o PROVEEDOR1 podrá realizar directamente un forense de los sistemas y de los registros de los ficheros de logs de la plataforma dedicada a ACME. Lo que facilitará conocer si ha habido accesos no permitidos a la base de datos de clientes y, en ese caso, si se ha producido una exfiltración masiva de los mismos.
- o Incluso ACME a través de su ciberseguro, o con los medios propios de su CERT, podrán colaborar en los trabajos de gestión del incidente en la plataforma de PROVEEDOR1 o incluso si el contrato se lo permite, verificar los mismos con trabajo de campo con recursos puestos a disposición por la aseguradora.

En Situación 2, la gestión y comunicación se complica al ser un incidente de la cadena de suministro de nuestro proveedor; el cual, es el tomador y cliente del contrato con NUBE1.

- o En el escenario de Situación 2 nos solemos encontrar que la instancia que da servicio a ACME comparte registros con otras instancias de otros clientes. En este caso, la toma de decisiones que favorezcan la agilidad, concreción y dedicación a PROVEEDOR1 por NUBE1, será mucho menor que en Situación 2.
 - o Cuestiones como migraciones de versiones para solventar otras vulnerabilidades que pudieran extender el problema pueden verse comprometidas por necesidades e intereses diferentes de los diferentes clientes que comparten infraestructuras.
 - o En este caso el liderazgo de las gestiones sobre el proveedor de la plataforma afectada le corresponde a PROVEEDOR1.
- 06 de agosto: PROVEEDOR1 en la Situación 1 confirma que:
 - o El vector de entrada fue un phishing a un Administrador de la infraestructura global suya.
 - o Con las credenciales reveladas accedieron por VPN y explotaron la vulnerabilidad crítica ya citada.
 - o Mediante dicha explotación lograron acceder y exfiltrar el conjunto de credenciales del grupo de Administradores de la infraestructura.
 - o Con rotundidad manifiestan que, tras la revisión de los sistemas de trazabilidad, las credenciales de los administradores que administran la plataforma dedicada para ACME, no han sido utilizadas en los sistemas de dicha plataforma.
 - o El sistema de identidad de usuarios dentro del CRM no ha sido violentado.



o Se han verificado los accesos a las bases de datos (BBDD) de clientes de ACME y tan sólo se han realizado desde la aplicación CRM, por usuarios finales de ACME, desde las IPs de ACME y que en ningún caso el análisis de comportamiento ha identificado anomalías en el acceso a las BBDD desde CRM, el Sistema o sistemas auxiliares como copias de seguridad o sistemas de transferencia de ficheros.

Ese mismo día, el RSEG informa al DPD de que no ha existido brecha de datos de carácter personal de clientes y ambos comunican a los respectivos comités el cierre de actuaciones.

06 de agosto: PROVEEDOR1 en Situación 2, a través del POCSEG informa a RSEG que NUBE1 sigue investigando y que debe entender que hacen todo lo posible, pero NUBE1 tiene a más de cien clientes en una situación similar a ACME y están desbordados. NUBE1 ha identificado el acceso no autorizado al repositorio de credenciales del grupo de administradores, pero no le es posible confirmar ni desmentir el acceso no autorizado a la BBDD de ACME.

Ese mismo día RSEG y DPD, junto con los respectivos comités en sesión conjunta, intercambian opiniones y valoraciones de la situación. El DPD decide, como medida de transparencia, comunicar a la AEPD con la información que tienen hasta el momento y sin poder valorar el impacto a los datos de los interesados.

- 15 de agosto: a pesar de las reuniones diarias, no hay avances hasta el día 15 de agosto, en el que el PROVEEDOR1 en Situación 2, indica que NUBE1 por la estructura compartida de fichero de registros de accesos que tiene, junto por la arquitectura de acceso común de clientes, no puede, ni podrá, confirmar o desmentir un acceso ilegítimo a la BBDD de clientes de ACME a raíz del ciberincidente.

RSEG informa al DPD y estos a sus comités, decidiendo:

- o DPD comunicará a la AEPD de las circunstancias apuntadas por NUBE1 a PROVEEDOR1, aportando el informe del RSEG.
- o RSEG comunicará al CCN-CERT la situación actualizada y las medidas que se adoptarán.
- o Se decide habilitar el comité de crisis y abordar desde este la comunicación a los clientes de ACME de la brecha y de las acciones emprendidas, así como de los cauces de comunicación y reclamación.

- o Entre otras medidas, se realizará un reseteo masivo de credenciales de clientes y se forzará al uso de doble factor de verificación.
- o Dado que no se puede saber el alcance de cuentas y datos exfiltrados, se asumirá que ha sido al conjunto global de datos de clientes activos, así como históricos: 12 millones de clientes en total.
- o Con el apoyo de jurídico se notifica el siniestro al tenedor del ciberseguro.

Aspectos relevantes en la valoración de la brecha

Se identifican los siguientes aspectos relevantes en la valoración de la brecha del ejemplo:

- Origen del incidente: el origen del incidente es externo e intencionado. Lo que habitualmente se traduce en una motivación económica. Ahora bien, el autor del incidente puede intentar rentabilizar directamente la intrusión o bien revenderla a un tercero para que sea este el que lo explote. Esto implica que la intrusión puede haberse producido mucho antes del descubrimiento de actividad maliciosa, lo que suele conducir a un impacto alto. Este no ha sido por los registros del servicio explotado, entre la intrusión y el descubrimiento de la misma, no ha transcurrido más que un día.
- Afectación a la confidencialidad, disponibilidad e integridad:

En la Situación 1 no se ha producido pérdida de confidencialidad, disponibilidad o integridad de los datos de carácter personal.

En la Situación 2 con las medidas técnicas adoptadas, la disponibilidad no se ha visto comprometida. Ahora bien, la confidencialidad e integridad si se han visto comprometidas pues no se ha podido garantizar que no hayan sido utilizadas las credenciales de los administradores PROVEEDOR1 y en consecuencia no se puede garantizar que las credenciales de los administradores de la aplicación del CRM no hayan sido utilizadas o las de administración de la base de datos.

- Momento en el que se conoció la brecha: extraoficialmente a través un mensaje en un grupo de Telegram y oficialmente a través del adjudicatario PROVEEDOR1.
- Actuación ante la brecha: en este caso, la empresa ACME responsable del tratamiento, por el tipo de servicio en el que se realiza el tratamiento de los datos, tiene muy mermadas las capacidades de poder actuar directamente en la contención, investigación y remediación. Sus capacidades de gestión del incidente estarán en la capa de supervisión, las operativas y de dirección de las operaciones les corresponden en la Situación 1 a PROVEEDOR1, mientras que en Situación 2 ese papel le corresponde a NUBE1.

Las condiciones puestas en la licitación permitirán a ACME, en el caso extremo representado por Situación 2, actuar operativamente en la instalación de NUBE1 para realizar un forense que le permita reducir el grado de incertidumbre en relación con el acceso.

En el ejemplo dado, los datos afectados son datos identificativos (nombre y apellidos), datos de contacto (dirección postal), datos de la compra, así como, por ejemplo, posiblemente datos de salud derivados de las solicitudes de ayuda a personas con dificultades de movimiento o incluso de religión por cuestiones tan indirectas como por la posibilidad de seleccionar comida kosher.

En la Situación 1 las personas físicas no se verán afectadas, mientras que en la Situación 2, aunque sea por las acciones que deben ser tomadas de forma preventiva, ante la incertidumbre de lo que realmente ha pasado, si tienen una afectación grave.

En cualquier caso, es necesario indicar que, obviamente, ACME estará sometido a un grave impacto reputacional y económico.

- Medidas de seguridad en vigor:

En el ejemplo dado, en la Situación 1, las diversas medidas técnicas y organizativas implementadas por ACME o exigidas al proveedor del servicio, permitieron a ACME gestionar adecuadamente el incidente:

- o Disponer de un Comité de Protección de Datos formalizado con las principales áreas de la organización (Clientes, Comunicación, Tecnología, Operaciones, Ciberseguridad, Protección de Datos, DPD), permitió el rápido entendimiento de la gravedad de la situación, y la agilidad en la toma de decisiones.
- o Tener las exigencias plasmadas en el contrato.
- o Disponer del procedimiento de Gestión de incidentes y capacidades adecuadas para dicha gestión.
- o Disponer de logs en los distintos sistemas implicados que permitieron realizar una investigación de lo sucedido, determinar las causas, e identificar los datos afectados.
- o Actuar, por parte de los equipos de Ciberseguridad, con prontitud, eficacia y determinación.
- o Disponer de la participación por parte del DPD durante el proyecto permitió, por ejemplo, que el PDF con la carta no incluyera los datos de tarjeta de crédito.

En la Situación 2, la falta de exigencia de infraestructura dedicada, junto con una clara falta de supervisión de la cadena de suministro y unas deficiencias en la misma, avocaron a que el incidente fuera finalmente un incidente grave.

- Número de afectados:

En la Situación 1: ninguno.

En la Situación 2: 12 millones de clientes.

Resumen de la valoración

Se identifican los siguientes aspectos relevantes en la valoración de la brecha del ejemplo:

PARÁMETROS EVALUADOS		SITUACIÓN 1	SITUACIÓN 2
Sobre la brecha	Como ha sido el incidente	Intencionado	Intencionado
	Origen del incidente	Externo	Externo
Sobre las consecuencias	Consec. del incidente	Afectación a la confidencialidad de las cuentas de usuarios privilegiados de la plataforma. Descartado acceso a datos de carácter personal de clientes	Alcance del impacto desconocido. Lo que a efectos prácticos de notificación implica considerar que se ha producido en una exfiltración total.
	Grado en el que podría afectar	Bajas, a pesar de la gravedad potencial del incidente	Graves
	Se ha materializado alguno de los daños	No	No se sabe a ciencia cierta y en consecuencia debe interpretarse como que SI se han materializado.
	Probabilidad de que el daño anterior se materialice	Baja	Alta
Categoría de datos	Tipos de datos afectados en personas físicas	-	Identificativos, datos de contacto, datos de la compra y salud.
Personas afectadas	Hay menores o vulnerables	No	SI
	Volumen de personas afectadas por la brecha	-	12 millones
Inform. Temporal	Momento en el que se conoció	Menos de 48 horas	Se desiste a los 15 días
	Actuación ante la brecha	Temprana y diligente	Tardía
Resultado	Comunicar a la autoridad de control	No	Si
	Comunicar a los afectados	No	SI (para minimizar el impacto)

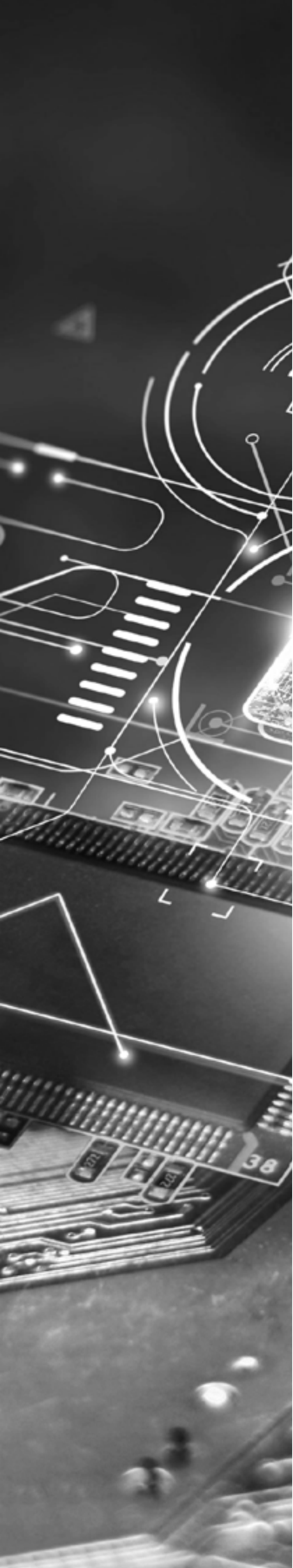
Brecha relacionada con el papel

Descripción del caso práctico

Se analiza la situación en el que se ha producido la pérdida o robo de un porta- documentos de un médico con información personal / expedientes / valoraciones médicas/etc.

En general, el sector médico-asistencial, tanto grandes centros médicos como médicos que también dan soporte a aseguradoras privadas, todavía sigue moviendo grandes cantidades de papel y en ocasiones su manipulación y su destrucción no son las adecuadas en los centros médicos donde prestan el servicio.

En este caso práctico se abordan distintas situaciones, desde la pérdida de una documentación que hace difícilmente identificable al paciente hasta el caso de robo de esa información claramente personal por otro paciente mientras



Se analiza la situación en el que se ha producido la pérdida o robo de un portadocumentos de un médico con información personal / expedientes / valoraciones médicas/etc.

En general, el sector médico-asistencial, tanto grandes centros médicos como médicos que también dan soporte a aseguradoras privadas, todavía sigue moviendo grandes cantidades de papel y en ocasiones su manipulación y su destrucción no son las adecuadas en los centros médicos donde prestan el servicio.

En este caso práctico se abordan distintas situaciones, desde la pérdida de una documentación que hace difícilmente identificable al paciente hasta el caso de robo de esa información claramente personal por otro paciente mientras estaba en el box de un médico esperando a ser atendido tras anestesia local, pasando por situaciones como que la impresora está fácilmente accesible al alcance de terceros o por problemas técnicos se llena el buffer de memoria e imprime los documentos en varios momentos, quedando accesible dicha documentación sin recoger:

Situación 1: el médico envía la información a la administrativa para que la imprima porque no tiene impresora en su puesto de trabajo. La administrativa la imprime y la deja en su mesa. El médico utiliza la información para una valoración con el paciente y luego la deja en un contenedor para que un proveedor la destruya. El proveedor en su manipulación no la destruye adecuadamente y es recuperada en el vertedero por un operario que procede a denunciarlo a la AEPD.

Situación 2: el médico imprime la información de salud del paciente, la consulta y posteriormente la deja en la papelera normal, no destructora. El personal de limpieza de una empresa externa vacía las papeleras en un contenedor de la calle, el contenedor del papel está lleno y lo deja apoyado fuera en la acera. Un viandante ve los portadocumentos, entra a nuestro centro médico y nos pone una queja sin más por nuestra acción, pero nos confirma que no va a realizar ningún uso de los datos.

Situación 3: el médico imprime la información de salud del paciente y, tras la consulta, el paciente solicita que le envíe esa y otra información sobre su historia clínica a su domicilio para tener una copia. El médico prepara toda la información y la deja depositada para su envío por el proveedor de mensajería habitual. Este por un error la deja en el buzón de otro vecino que no dice nada. Meses más tarde el paciente vuelve a solicitar la información. El centro médico no entiende qué ha podido suceder y lo vuelve a enviar sin más.

Situación 4: el médico imprime la información de salud de varios pacientes que va a visitar a lo largo de la mañana y los deja sobre su mesa. En su box atiende a varios pacientes citados de forma simultánea, mientras va a atender a uno y ponerle anestesia, el otro avezado se hace con información médica de terceros pacientes

que estaban citados ese día. El médico detecta que faltan papeles impresos. El infractor contacta con la compañía aseguradora para la que trabaja ese médico y amenaza con publicar la información si no se le paga el dinero que solicita.

Situación 5: el médico imprime toda la información médica que le ha solicitado el paciente. Al ser archivos pesados y numerosos la impresora imprime una primera tanda, se llena el bufer y posteriormente imprime la segunda tanda. El médico no se da cuenta de esa segunda parte. La impresora está en una zona de paso y, uno de los que estaban en espera de ser atendidos en recepción, se percata de que de repente esa impresora empieza a sacar documentación por su bandeja y la recoge. Tras visualizar la información, se la deja en recepción avisando de lo

Aspectos relevantes en la valoración de la brecha

Los principales aspectos asociados a esta brecha y que impactan en el análisis de la misma son los siguientes:

- Controles durante el proceso de destrucción: cuando una información con datos sensibles es impresa, quien lo hace a continuación debe preocuparse por cómo se destruye, en su completitud.
- El por quién te enteras de que has tenido una posible brecha, así como quiénes son los actores implicados: una negligencia del proveedor que se dedica exclusivamente a destruir los datos, un error no intencionado del personal de limpieza, la visualización por un tercero ajeno (recordemos que la mera visualización ya es tratamiento en el RGPD), un acto ilícito por otro paciente o un fallo en la impresora entrañan distintas evaluaciones de riesgo. En los proveedores deberemos ver si los contratos reflejan bien este tipo de fallos y sus consecuencias. En el caso de la impresora es un riesgo probable fruto de un envío importante de documentación, ahí por tanto ya debemos tomar otras medidas.
- La buena o mala intencionalidad de quien se hace con esa información es relevante: no es lo mismo que la persona que detecta un fallo lo comunique para que se subsane, que otra persona te extorsione a cambio de su devolución.

Resumen de la Valoración

PARÁMETROS EVALUADOS		SITUACIÓN 1	SITUACIÓN 2	SITUACIÓN 3	SITUACIÓN 4	SITUACIÓN 5
Sobre la brecha	Como ha sido el incidente	No Intencionado	No Intencionado	No Intencionado	Intencionado	No Intencionado
	Origen del incidente	Externo	Externo	Interno	Externo	Interno

PARÁMETROS EVALUADOS		SITUACIÓN 1	SITUACIÓN 2	SITUACIÓN 3	SITUACIÓN 4	SITUACIÓN 5
Sobre las consecuencias	Consec. del incidente	Acceso no autorizado a datos concretos sobre prueba médica	Acceso no autorizado a datos concretos sobre prueba médica	Acceso no autorizado a todo el historial médico de un paciente, por un conocido suyo/ vecino.	Acceso no autorizado a datos de pruebas médicas sobre una especialidad de otros pacientes	Acceso no autorizado a datos parciales sobre historial clínico de un paciente
	Grado en el que podría afectar	BAJA (Los clientes no se verán afectados o si se ven lo superarán rápidamente sin más consecuencias para ellos (irritación, ansiedad, disconfort, molestias del tipo recibir información varias veces...))	Media (Los individuos pueden tener inconvenientes que ellos seguro que son capaces de superar a pesar de algunas dificultades (costes adicionales, miedo, stress, no acceso a ciertos servicios temporalmente, pequeños daños o problemas físicos, etc..))	Alta (Los individuos pueden tener inconvenientes importantes pero que pese a las dificultades conseguirán superar con el tiempo (ie citaciones judiciales, empeoramiento o agravación de enfermedades o dolencias))	Alta (Los individuos pueden tener inconvenientes importantes pero que pese a las dificultades conseguirán superar con el tiempo (ie citaciones judiciales, empeoramiento o agravación de enfermedades o dolencias))	BAJA (Los clientes no se verán afectados o si se ven lo superarán rápidamente sin más consecuencias para ellos (irritación, ansiedad, disconfort, molestias del tipo recibir información varias veces...))
	Se ha materializado alguno de los daños	No	No	Si	Si	No
	Probabilidad de que el daño anterior se materialice	Baja	Baja	Media	Muy alta	Baja
Categoría de datos	Tipos de datos afectados en personas físicas	datos identificativos, datos de número de póliza/ transaccionales, datos de estado de salud real o inferida	datos identificativos, datos de número de póliza/ transaccionales, datos de estado de salud real o inferida	datos identificativos, datos de número de póliza/ transaccionales, datos de estado de salud real o inferida	datos identificativos, datos de número de póliza/ transaccionales, datos de estado de salud real o inferida	datos identificativos, datos de número de póliza/ transaccionales, datos de estado de salud real o inferida
Personas afectadas	Hay menores o vulnerables	No	No	No	No	Si
	Volumen de personas afectadas por la brecha	1	1	10	1	1
Inform. Temporal	Momento en el que se conoció	A la semana	Al mes	Al día siguiente	Al día siguiente	Al día siguiente
	Actuación ante la brecha	Tan pronto como se tiene conocimiento	Tan pronto como se tiene conocimiento	Tan pronto como se tiene conocimiento	Tan pronto como se tiene conocimiento	Tan pronto como se tiene conocimiento
Resultado	Comunicar a la autoridad de control	No (ya nos viene dado el requerimiento)	No	No	No	No
	Comunicar a los afectados	Sí	No	Si, recomendable	Sí	Si, recomendable

Descripción del caso práctico

La empresa SEGUROS es una mediadora de seguros que a través de sus gestores ayuda a sus clientes a gestionar diferentes seguros con diferentes compañías.

- 13 de marzo: un cliente, CLIENTE1, solicita por teléfono a su gestor el envío de toda la documentación contractual relacionada con su seguro a su correo electrónico.
- 21 de marzo: tras varios días reclamándoselo el gestor, que tiene una elevada carga de trabajo, busca al cliente en la base de datos de la entidad por su nombre y apellidos. Pero, a causa de las prisas, selecciona el correo electrónico de otro cliente de la compañía, con el mismo nombre, aunque distinto documento de identificación, CLIENTE2, remitiendo la documentación solicitada por el CLIENTE1 al correo electrónico del CLIENTE2.
- 28 de marzo¹⁶: el empleado tiene conocimiento del error una semana después ante la notificación del CLIENTE2. Ante esta situación:
 - o Le indica a dicho cliente que proceda a eliminar la documentación enviada.
 - o Notifica la incidencia a su superior quien pone en conocimiento del DPD esta circunstancia.
 - o Envía la documentación a la dirección correcta del solicitante.

Situación 1: el cliente solicitante tiene contratado un seguro de automóvil y el empleado remite por correo electrónico sus condiciones particulares y generales a otro cliente.

En las condiciones particulares de la póliza se contienen los siguientes datos: nombre y apellidos, DNI, fecha de nacimiento, número de teléfono, email, dirección, datos del vehículo (matrícula y marca), precio y coberturas de la póliza, cuenta bancaria de cargo.

Situación 2: el cliente solicitante tiene contratado un seguro de salud y el empleado remite por error sus condiciones particulares y cuestionario de salud a otro cliente.

En el cuestionario de salud se contienen datos de salud del cliente y en las condiciones particulares las exclusiones de la póliza derivadas de las patologías notificadas en el cuestionario de salud, así como nombre y apellidos, DNI, fecha de nacimiento, número de teléfono, email, dirección, precio de la póliza y cuenta bancaria de cargo.

Situación 3: el empleado ante solicitudes muy similares de otros clientes, decide remitirle a toda su cartera, compuesta por 1.000 clientes, la información contractual por correo electrónico.

El empleado enlaza erróneamente la documentación con los clientes de tal forma que envía de forma errónea la comunicación correspondiente a 1.000 clientes.

Por error envía la documentación asociada a un seguro de salud (cuestionario y condiciones particulares) de un mismo cliente a toda su cartera.

Situación 4: El empleado ha recibido formación en privacidad por lo que tiene claro que para enviar documentación contractual con datos de salud por correo electrónico debe hacer uso de un canal seguro.

Así incluye la documentación en el repositorio Owncloud de la Entidad y envía un correo electrónico que contiene el enlace al repositorio indicándole que para acceder deberá incluir la contraseña enviada a su número de teléfono. El correo electrónico es enviado de forma errónea a otra cliente, sin embargo, este no puede acceder al repositorio y por extensión a la documentación, puesto que la contraseña ha sido enviada de forma correcta al móvil del solicitante.

Aspectos relevantes en la valoración de la brecha ocurrida

Se identifican los siguientes aspectos relevantes en la valoración de la brecha del ejemplo:

- Origen del incidente: el incidente ha sido accidental y con origen interno.
- Tipología: uno de los parámetros más importantes a la hora de evaluar el nivel de riesgo de una brecha de datos personales es determinar con exactitud su tipología, es decir determinar a qué dimensión de seguridad de los datos personales ha afectado la brecha (confidencialidad, disponibilidad, integridad).

Cualquiera de las situaciones descritas afecta a la confidencialidad, puesto que los datos personales han sido accedidos por terceros no autorizados.

En la Situación 4, los datos fueron enviados de forma segura mediante cifrado de tal forma que en este caso las consecuencias de la brecha quedan prácticamente mitigadas anulando los riesgos derivados del incidente.

- Categoría de los datos afectados: se han visto afectados datos básicos, datos de contacto, medios de pago, datos económicos y, en algunos casos, datos de salud.

En cuanto al perfil de las personas físicas, en este caso son clientes. Un aspecto importante a tener en cuenta como agravante del riesgo potencial es si el tratamiento que ha sufrido la brecha se realiza sobre datos de personas que pertenecen a un colectivo especialmente vulnerable, como pueden ser menores de edad, supervivientes de violencia de género, de acoso o situaciones similares. En la situación expuesta no se ha visto afectado el perfil de personas físicas especialmente vulnerables.

- Volumen de clientes afectados: la brecha ha afectado en función de la situación o simplemente a 1 cliente o en otros casos a 1.000 clientes.
- Consecuencias para los afectados: en este caso, la brecha podría tener como consecuencia para los afectados la pérdida de control sobre sus datos personales y el riesgo de usurpación de identidad.

¹⁵Comienza la gestión de la brecha

- Nivel de seguridad: a su vez para determinar el nivel de seguridad debe tenerse en cuenta el daño que se puede producir al materializarse las consecuencias identificadas. En este caso el nivel de severidad asociado al riesgo identificado de usurpación de identidad es medio (las personas pueden enfrentar inconvenientes importantes, produciendo un daño limitado).
- Probabilidad de ocurrencia: se calificaría como improbable en la Situación 4, baja en la Situación 1 y 2 pues los datos erróneos se han comunicado a un solo cliente y alta en la Situación 3 pues los datos se han comunicado erróneamente los datos de 1000 clientes.

Resumen de la valoración

Se identifican los siguientes aspectos relevantes en la valoración de la brecha del ejemplo:

PARÁMETROS EVALUADOS		SITUACIÓN 1	SITUACIÓN 2	SITUACIÓN 3	SITUACIÓN 4
Sobre la brecha	Como ha sido el incidente	Accidental	Accidental	Accidental	Accidental
	Origen del incidente	Interno	Interno	Interno	Interno
Sobre las consecuencias	Consec. del incidente	Pérdida de confidencialidad y riesgo de usurpación de identidad	Pérdida de confidencialidad y riesgo de usurpación de identidad	Pérdida de confidencialidad y riesgo de usurpación de identidad	Pérdida de confidencialidad y riesgo de usurpación de identidad
	Grado en el que podría afectar	Las personas pueden encontrar inconvenientes importantes produciendo un daño limitado	Las personas pueden encontrar inconvenientes importantes produciendo un daño limitado	Las personas pueden encontrar inconvenientes importantes produciendo un daño limitado	Las personas pueden encontrar inconvenientes importantes produciendo un daño limitado
	Se ha materializado alguno de los daños	No	No	No	No
	Probabilidad de que el daño anterior se materialice	Baja	Baja	Alta	Improbable
Categoría de datos	Tipos de datos afectados en personas físicas	Datos básicos, datos de contacto, número del DNI, medios de pago.	Datos básicos, datos de contacto, número del DNI, medios de pago, datos de salud	Datos básicos, datos de contacto, número del DNI, medios de pago, datos de salud	Datos básicos, datos de contacto, número del DNI, medios de pago, datos de salud
Personas afectadas	Hay menores o vulnerables	No	No	No	No
Personas afectadas	Volumen de personas afectadas por la brecha	1	1	1000	1
Inform. Temporal	Momento en el que se conoció	1 semana	1 semana	1 semana	Al mes de producirse
Inform. Temporal	Actuación ante la brecha	Temprana y diligente	Temprana y diligente	Temprana y diligente	Temprana y diligente
Resultado	Comunicar a la autoridad de control	No	No	Si	No
Resultado	Comunicar a los afectados	Si (mitigar riesgo)	Si (mitigar riesgo)	Si	No

Descripción del caso práctico

La cadena de supermercados COMIDA se dedica desde hace más de 100 años al negocio de los pequeños supermercados de barrio. En los últimos años ha crecido mucho en toda España gracias a su especialización en productos gourmet y veganos de calidad. No cuenta con ningún tipo de servicio de venta online para clientes ni tampoco con gestión informatizada remota de las tiendas. De sus más de 3.000 empleados, solo utilizan los sistemas de información de la compañía los 300 de servicios centrales, salvo por las cuentas de correo corporativas que se facilitan desde RRHH a todos los empleados para sus gestiones con ellos, incluyendo el envío de la nómina en formato PDF mensualmente.

Aunque no cuentan con personal interno para cuestiones de ciberseguridad, sí tienen contratada una empresa externa que les da soporte y operación en las medidas básicas que tienen implantadas.

- 02 de enero: los empleados de una gran cadena de supermercados reciben a través de una red social una noticia relacionada con un supuesto expediente de regulación de empleo en su compañía, que incluye una URL con más información. La web a la que eran enviados a través de este enlace incluía un código malicioso que infectaba los terminales móviles de los usuarios y les instalaba un software espía.

Con este método los ciberdelincuentes logran hacerse con las credenciales de las cuentas de correo electrónico de 200 empleados.

- 09 de enero: tras hacerse con las contraseñas, el atacante pudo entrar en las cuentas de correo de los empleados y reglas sobre los correos electrónicos de dichos empleados de tal forma que se reenviaban a una cuenta de correo externa correos con palabras claves tales como “cuenta bancaria, “Pago”, etc.
- 17 de febrero: el atacante tuvo acceso a correos electrónicos del área de facturación y así tuvo conocimiento sobre ciertos proveedores periódicos de la cadena de supermercados, además de datos identificativos clave de los mismos. Usando esta información suplantó la identidad de uno de estos proveedores y notificó a la cadena de supermercados un cambio en su cuenta de pago.

Simultáneamente, el atacante pone a la venta en la Deep web los datos económicos de 100 de los 200 empleados, a los que ha tenido acceso a través de la intranet corporativa: nombre completo, DNI, cuenta de pago, dirección y sueldo.

- 02 de marzo: al proceder al pago mensual al proveedor suplantado, la cadena de supermercados realizó un ingreso de 75.000€ en la cuenta del atacante.
- 07 de marzo: el proveedor suplantado se pone en contacto con la cadena de supermercados ante el impago de sus facturas, comprobándose entonces que había habido un cambio de cuenta de pago que no había sido solicitada por el proveedor.

- 07 de marzo: la cadena de supermercados contacta con su proveedor de ciberseguridad, ya que lo tiene todo externalizado y le comunica lo acontecido. Estos inician inmediatamente una investigación partiendo del correo electrónico, supuestamente desde el proveedor suplantado, en el que se cambiaba la cuenta bancaria de pago.
- 10 de marzo: tras acabar el informe forense se concluye que ha habido un incidente de seguridad causado por el robo de las credenciales de 200 empleados. Además, han encontrado en sus búsquedas en la Deep web sobre la compañía, que se estaba vendiendo información de estos empleados.

Se procede a la contención del incidente siguiendo las instrucciones del proveedor de ciberseguridad:

- o Reseteo de todas las credenciales de acceso de todos los empleados de la empresa en todos los sistemas.
- o Eliminación automática de todas las reglas de reenvío de correo a la cuenta maliciosa detectada.
- o Información a los afectados de la filtración de sus datos para que procedan a cambiar sus datos bancarios.
- 20 de marzo: se establece un plan de actuación para evitar que vuelva a darse una situación similar y que incluye doble factor de autenticación para los recursos corporativos, cambios en el procedimiento de pagos y de cambio de datos de proveedores, plan de formación en ciberseguridad a todos los empleados.

Aspectos relevantes en la valoración de la brecha ocurrida

- Origen del incidente: el incidente ha sido intencionado con origen externo.
- Tipología del incidente:

La brecha ha afectado a la confidencialidad, puesto que los datos personales han sido accedidos por terceros no autorizados.

También ha habido una afectación a la integridad, pero en este caso afectando únicamente a datos de un proveedor, persona jurídica, por lo que se sale del alcance de una evaluación en cuanto a brechas de protección de datos. Pero sí debería ser tenida en cuenta esta tipología en la gestión de riesgos global de la entidad afectada.

- Categoría de los datos afectados: datos básicos, datos de contacto, DNI, medios de pago y datos económicos.

En cuanto al perfil de las personas físicas en este caso son empleados y proveedores.

En la situación expuesta no se ven perfiles de personas físicas especialmente vulnerables.

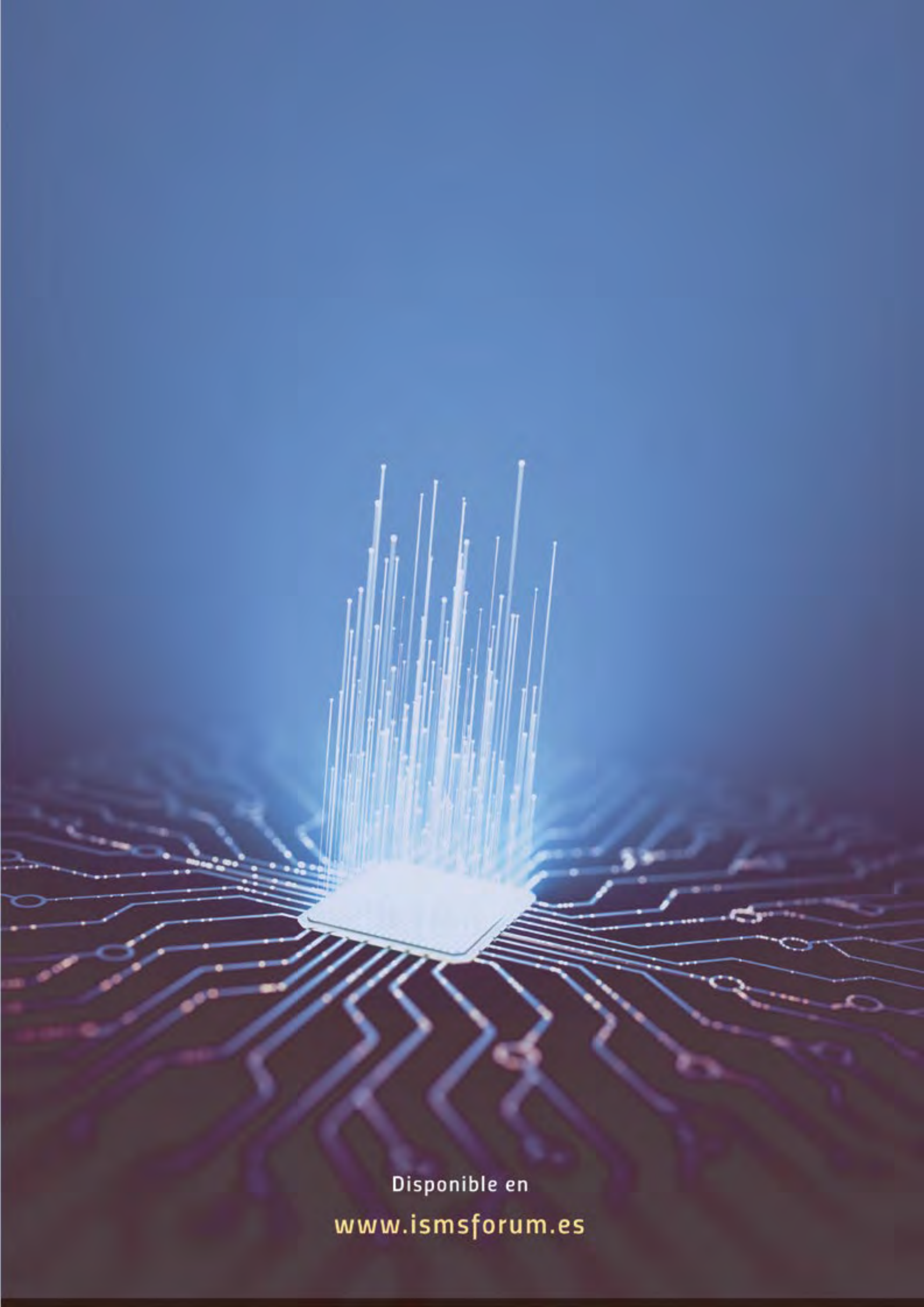
- Volumen de terceros afectados: la brecha ha afectado a 200 empleados.
- Consecuencias para los afectados:
 - o Pérdida de control sobre sus datos personales.
 - o Riesgo de usurpación de identidad.

- Nivel de seguridad: a su vez para determinar el nivel de seguridad debe tenerse en cuenta el daño que se puede producir al materializarse las consecuencias identificadas. En este caso el nivel de severidad asociado al riesgo identificado de usurpación de identidad es alto (Las personas pueden enfrentar consecuencias significativas que deberían poder superar).
- Probabilidad: por lo que se refiere a la probabilidad, dado que en este caso se ha tenido conocimiento de que se ha materializado un daño concreto, no sería necesario determinar dicho nivel.

Resumen de la valoración

Se identifican los siguientes aspectos relevantes en la valoración de la brecha del ejemplo:

PARÁMETROS EVALUADOS		SITUACIÓN A
Sobre la brecha	Cómo ha sido el incidente	Intencionado
Sobre la brecha	Origen del incidente	Externo
Sobre las consecuencias	Consec. del incidente	Pérdida de confidencialidad y riesgo de usurpación de identidad
Sobre las consecuencias	Grado en el que podría afectar	Las personas pueden enfrentar consecuencias significativas que deberían poder superar.
Sobre las consecuencias	Se ha materializado alguno de los daños	SI
Sobre las consecuencias	Probabilidad de que el daño anterior se materialice	NA
Categoría de datos	Tipos de datos afectados en personas físicas	Datos básicos, datos de contacto,, medios de pago, datos financieros.
Personas afectadas	Hay menores o vulnerables	No
Personas afectadas	Volumen de personas afectadas por la brecha	200
Inform. Temporal	Momento en el que se conoció	2 meses
Inform. Temporal	Actuación ante la brecha	Tardía
Resultado	Comunicar a la autoridad de control	SI
Resultado	Comunicar a los afectados	SI



Disponible en
www.ismsforum.es