Política de gestión de brechas e incidentes de seguridad

1.- Introducción y definición

El Esquema Nacional de Seguridad (ENS) define un "incidente o brecha de seguridad" como aquel "suceso inesperado o no deseado con consecuencias en detrimento de la seguridad del sistema de información". En la misma línea, la Directiva NIS define "incidente" como "todo hecho que tenga efectos adversos reales en la seguridad de las redes y sistemas de información".

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

Esta "violación" a la que se refiere el RGPD, aun siendo un tipo de incidente de seguridad, solo se aplica en la medida en que afecte a datos de carácter personal, y en consecuencia dicho incidente pueda comprometer al responsable del tratamiento en el cumplimiento de los principios del RPGD.

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

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

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

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

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

1.1 Figuras implicadas

Será necesaria la colaboración y actuación de las siguientes figuras para la gestión de los incidentes y brechas de seguridad acaecidos en la empresa:

Responsable del tratamiento: le corresponde aplicar las medidas técnicas y organizativas apropiadas a fin de garantizar y poder demostrar que el tratamiento es conforme con el RGPD. Deberá notificar

la brecha de seguridad a la autoridad de control competente, sin dilación indebida, y en su caso la comunicación con los afectados.

El responsable del tratamiento podrá contar con el asesoramiento de expertos en materia de seguridad o los servicios informáticos propios o que pueda tener subcontratados. Así mismo podrá delegar la gestión de brechas de seguridad en servicios informáticos externos y/o los encargados del tratamiento.

Delegado de Protección de Datos (DPO): en los casos en los que se haya designado un DPO (porque lo exija el RGPD o voluntariamente), éste ocupará un papel muy relevante liderando el plan de actuación en todos sus aspectos junto al responsable de seguridad.

Responsable de seguridad: responsable designado por la empresa a nivel interno para garantizar el seguimiento y cumplimiento efectivo de las medidas, políticas y procesos de seguridad de la información diseñados por el responsable del tratamiento y el DPO.

Jefes de departamentos: Quienes deberán facilitar toda la información que sea solicitada por el responsable de seguridad o el DPO.

Encargado del tratamiento: notificará, sin dilación indebida, al responsable del tratamiento las brechas de seguridad de los datos personales de las que tenga conocimiento, con indicación de toda aquella información mínima y necesaria para su comunicación.

El responsable puede delegar en el encargado la gestión de las brechas de seguridad, tanto en lo relativo a la respuesta como en lo relativo a la notificación, documentándose dicha delegación de funciones en el contexto de la relación contractual establecida. No obstante, el responsable debe asegurarse de que se están tomando las acciones de respuesta, notificación y comunicación oportunas, dado que la delegación de funciones no implica la delegación de responsabilidad.

Autoridad de control competente: se encargará de verificar que se cumple con el RGPD, y en este caso concreto en lo relativo a la gestión de la brecha de seguridad.

1.2 Clasificación incidentes de seguridad

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

- Tipo de amenaza: código dañino, intrusiones, fraude, etc. Se trata de una breve descripción del incidente en función de la información de la que se disponga.
- Contexto u origen de la amenaza: interna o externa.
- Categoría de seguridad de los sistemas y datos afectados.
- El perfil de los usuarios afectados.
- Número y tipología de los sistemas afectados.
- Impacto del incidente en la organización y en los derechos y libertades de los afectados.
- Requerimientos legales y regulatorios.
- Vector de ataque o método: ruta o medio por el que se ha materializado el incidente.

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

1. 0-day (vulnerabilidad no conocida): Vulnerabilidad que permite a un atacante el acceso a los datos en la medida en que es una vulnerabilidad desconocida. Esta vulnerabilidad estará disponible hasta que el fabricante o desarrollador la resuelva.

2. APT (ataque dirigido): Se refiere a diferentes tipos de ataques dirigidos normalmente a recabar información fundamental que permita continuar con ataques más sofisticados. En esta categoría se encuadraría por ejemplo una campaña de envío de email con software malintencionado a empleados de la empresa hasta conseguir que alguno de ellos lo instale en su equipo y proporcione una puerta de entrada al sistema.

3. Denegación de servicio (DoS/DDoS): Consiste en inundar de tráfico un sistema hasta que no sea capaz de dar servicio a los usuarios legítimos del mismo.

4. Acceso a cuentas privilegiadas: El atacante consigue acceder al sistema mediante una cuenta de usuario con privilegios avanzados, lo que le confiere libertad de acciones. Previamente deberá haber conseguido el nombre de usuario y contraseña por algún otro método, por ejemplo, un ataque dirigido.

5. Código malicioso: piezas de software cuyo objetivo es infiltrase o dañar un ordenador, servidor u otro dispositivo de red con finalidades muy diversas. Una de las posibilidades para que el código dañino alcance a una organización es que un usuario lo instale de forma involuntaria.

6. Compromiso de la información: Recoge todos los incidentes relacionados con el acceso y fuga, modificación o borrado de información no pública.

7. Robo y/o filtración de datos: Se incluye en esta categoría la pérdida/robo de dispositivos de almacenamiento con información.

8. Desfiguración (Defacement): Es un tipo de ataque dirigido que consiste en la modificación de la página web corporativa con la intención de colgar mensajes reivindicativos de algún tipo o cualquier otra intención. La operativa normal de la web queda interrumpida, produciéndose además daños reputacionales.

9. Explotación de vulnerabilidades de aplicaciones: Cuando un posible atacante logra explotar con éxito una vulnerabilidad existente en un sistema o producto consiguiendo comprometer una aplicación de la organización.

10. Ingeniería social: Son técnicas basadas en el engaño, normalmente llevadas a cabo a través de las redes sociales, que se emplean para dirigir la conducta de una persona u obtener información sensible. Por ejemplo, el usuario es inducido a pulsar sobre un enlace haciéndole pensar que es lo correcto.

1.3 Tipo de brecha de seguridad

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

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

2.- FASES DE GESTIÓN BRECHA DE SEGURIDAD

2.1-Detección e identificación

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

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

2.1.1 Formas de detección e identificación

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

2.1.2 Fuentes internas

Se refiere los controles y mecanismos de seguridad dentro y alrededor de las instalaciones de la empresa, así como los medios de acceso remoto a la información.

Desde el punto de vista de la seguridad física, la detección se produciría ante el incumplimiento o vulneración de las medidas de seguridad adoptadas, como, por ejemplo:

- Políticas específicas de mesas limpias, bloqueo de pantallas, accesos con usuario y contraseña, etc.
- Controles físicos como detección de intrusos, videovigilancia, control y registro de accesos a determinadas zonas, etc.

- Controles y procedimientos frente a daños ambientales o desastres naturales. En este sentido, cobra suma importancia la concienciación y formación de todo el personal de la organización para evitar situaciones de riesgo e incluso detectarlas y notificarlas.

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

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

Se pueden considerar las siguientes fuentes de información:

- Notificaciones de usuarios: presencia de archivos con caracteres la empresa, recepción de correos electrónicos con archivos adjuntos sospechosos, comportamiento extraño de dispositivos, imposibilidad de acceder a ciertos servicios, extravío/robo de dispositivos de almacenamiento o equipos con información.
- Alertas generadas por software antivirus. Consumos excesivos y repentinos de memoria o disco en servidores y equipos.
- Anomalías de tráfico de red o picos de tráfico en horas la empresa. Alertas de sistemas de detección/prevención de intrusión (IDS/IPS).
- Alertas de sistemas de correlación de eventos. Análisis de registros de conexiones realizadas a través de proxys corporativos o conexiones bloqueadas en los cortafuegos. Análisis de registro de servidores y aplicaciones con intentos de acceso no autorizados.
- Análisis de registros en herramientas DLP (Data Loss Prevention).

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

2.1.3 Fuentes externas

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

2.2 Identificación y registro

El análisis de las fuentes de información antes mencionadas permitirá determinar si se está ante un incidente de seguridad o no, así como su naturaleza, clase, tipo, si dicho incidente ha afectado a

datos de carácter personal y por tanto constituye una “brecha de los datos de carácter personal” descrita en el RGPD, y el nivel de riesgo al que se enfrenta la organización.

Desde los síntomas y mecanismos de detección que permitieron identificarlo hasta las acciones y medidas de control adoptadas en cada una de las fases de gestión del incidente. En particular, la empresa a través de su responsable de seguridad en coordinación con su DPO si este hubiera sido designado deberá mantener como mínimo un registro documental de los incidentes de seguridad que hayan afectado a los datos de carácter personal8, incluyendo el tipo de incidente, descripción del mismo, gravedad, estado y medidas adoptadas para su resolución.

Dicho registra seguirá el siguiente Modelo:

REGISTRO DE BRECHAS E INCIDENCIAS EN MATERIA DE SEGURIDAD DE DATOS	
Tipología de brecha de seguridad de datos	
Contexto de la brecha de seguridad	
Medio por el se ha materializado la brecha	
Categorías de datos afectados	
Volumen aproximado de registros afectados	
Colectivos afectados	
Volumen aproximado de intereses afectados	
Fecha de detección de la brecha de seguridad	
Fecha de inicio de la brecha	
Descripción de la brecha de seguridad	
Medidas de seguridad aplicadas	
Medidas correctoras posteriores	
Valoración del riesgo y de la necesidad de comunicación	
Fecha estimada de resolución de la brecha	

2.3. Valoración del alcance de la brecha de seguridad

La peligrosidad dependerá de los siguientes factores:

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

Naturaleza, sensibilidad y categorías de los datos personales afectados:

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

Datos legibles/ilegibles: Datos protegidos mediante algún sistema de seudonimización (por ejemplo, cifrado o hash)

Volumen de datos personales: expresados en cantidad (registros, ficheros, documentos) y/o en periodos de tiempo (una semana, un año, etc.)

Facilidad de identificación de individuos: facilidad con la que se puede deducir la identidad de los individuos a partir de los datos involucrados en la brecha

Severidad de las consecuencias para los individuos:

- Baja: Las personas no se verán afectadas o pueden encontrar algunos inconvenientes que superarán sin ningún problema (tiempo de reingreso de información, molestias, irritaciones, etc.).
- Media: Las personas pueden encontrar inconvenientes importantes, que podrán superar a pesar de algunas dificultades (costos adicionales, denegación de acceso a servicios comerciales, miedo, falta de comprensión, estrés, dolencias físicas menores, etc.).
- Alta: Las personas pueden enfrentar consecuencias importantes, que deberían poder superar, aunque con serias dificultades (malversación de fondos, listas negras de los bancos, daños a la propiedad, pérdida de empleo, citación judicial, empeoramiento de la salud, etc.).
- Muy alta: Las personas pueden enfrentar consecuencias significativas, o incluso irreversibles, que no pueden superar (exclusión o marginación social, dificultades financieras tales como deudas considerables o incapacidad para trabajar, dolencias psicológicas o físicas a largo plazo, muerte, etc.).

Características especiales de los individuos: Si afectan a individuos con características especiales o con necesidades especiales.

Número de individuos afectados: Dentro de una escala determinada, por ejemplo, más de 100 individuos.

Características especiales del responsable del tratamiento (de la entidad en sí): En base a la actividad de la entidad.

El perfil de los usuarios afectados, su posición en la estructura organizativa de la entidad y, en su consecuencia, sus privilegios de acceso a información sensible o confidencial.

El número y tipología de los sistemas afectados.

El impacto que la brecha puede tener en la organización, desde los puntos de vista de la protección de la información, la prestación de los Servicios, la conformidad legal y/o la imagen pública. Va a estar relacionado con la categoría o criticidad de los servicios afectados y personas afectadas. En este aspecto diferenciamos entre los siguientes impactos: Bajo (perjuicio limitado) Medio (perjuicio grave) Alto (perjuicio muy grave).

Los requerimientos legales y regulatorios: Notificación de la brecha a la autoridad de control y cualquier otra obligación de notificación, comunicación a Fuerzas y Cuerpos de Seguridad del Estado en caso de delito.

El responsable de seguridad deberá, una vez recibida e identificada la brecha de seguridad, calcular el nivel de criticidad conforme a la siguiente formula:

ESQUEMA PARA LA VALORACIÓN DE CRITICIDAD DE LA BRECHA DE SEGURIDAD

Parámetros de valoración: volumen, tipología de datos e impacto.

VOLUMEN (números de registros completos e identificativos afectados)

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

TIPOLOGÍA DE DATOS

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

IMPACTO (EXPOSICIÓN)

- Nulo (2)
- Interno (dentro de la empresa) - (4)
- Externo (perímetro proveedor, atacante, terceros relacionados o no con la entidad)
- (6)
- Pública (accesible en Internet) - (8)
- Desconocido (10)

_____

El cálculo del riesgo se obtiene de la siguiente forma:

- Riesgo = P x I
- Riesgo = P (Volumen) x Impacto (Tipología x Impacto)

- **Procede notificación a la autoridad de control si**:

- Riesgo con valor cuantitativo en un umbral superior a 20.
- Ante la coincidencia de dos circunstancias cualitativas (marcadas en negrita).

-**Procede comunicación a los afectados si**:

- Riesgo con valor cuantitativo superior a 40.
- Ante la coincidencia de dos circunstancias cualitativas (marcadas en negrita).

_____

Cálculo final:

Comunicación AEPD:

1. Riesgo = 6 x 1 x 2 = 12 (inferior a 20) – NO procede comunicación
2. No coinciden dos circunstancias cualitativas

Comunicación formal a afectados:

3. Riesgo = 6 x 1 x 2 = 12 (inferior a 40) – NO preceptiva comunicación
4. No coinciden dos circunstancias cualitativas

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

2.4 Proceso de respuesta

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

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

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

2.5 Proceso de notificación

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

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

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

En el caso de la empresa, en el caso de ser necesario realizar la notificación, de las brechas de seguridad de los datos personales a las autoridades de control y, en casos graves, a los afectados será el responsable de seguridad el encargado de dicha de notificación previa consulta con el DPO si este hubiese sido designado.

Tan pronto como el responsable de seguridad tenga conocimiento de que se ha producido una brecha de la seguridad de los datos personales debe, sin dilación y, a más tardar en las 72 horas siguientes a tener constancia, efectuar la correspondiente notificación a la Autoridad de Control. Se

considera que se tiene constancia de una brecha de seguridad cuando hay una certeza de que se ha producido y se tiene conocimiento suficiente de su naturaleza y alcance.

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

Esta comunicación se realizará con el modelo de registro de la brecha adjunto anteriormente, y deberá contener la siguiente información:

- Datos identificativos y de contacto de:
- Entidad / Responsable del tratamiento
- Delegado de Protección de Datos (si está designado) o persona de contacto.
- Indicación de si se trata de una notificación completa o parcial. En caso de tratarse de una notificación parcial indicar si se trata de una primera notificación o una notificación complementaria. Información sobre la brecha de seguridad de datos personales:
- Fecha y hora en la que se detecta.
- Fecha y hora en la que se produce el incidente y su duración.
- Circunstancias en que se haya producido la brecha de seguridad de datos personales (por ejemplo, pérdida, robo, copia, etc.)
- Naturaleza y contenido de los datos personales en cuestión.
    - Resumen del incidente que ha causado la brecha de seguridad de datos personales (con indicación de la ubicación física y del soporte de almacenamiento).
    - Posibles consecuencias y efectos negativos en los afectados.
- Medidas técnicas y organizativas que se hayan adoptado por parte del responsable del tratamiento según el apartado 33.2d) del RGPD.
- Categoría de los datos afectados y número de registros afectados.
- Categoría y número de individuos afectados.
- Posibles cuestiones de carácter transfronterizo, indicando la posible necesidad de notificar a otras autoridades de control.
- Si en el momento de la notificación, no fuese posible facilitar toda la información, podrá facilitarse posteriormente, de manera gradual en distintas fases. La primera notificación se realizará en las primeras 72h, y al menos se realizará una comunicación final o de cierre cuando se disponga de toda la información relativa al incidente.
- Cuando el responsable realice la primera notificación deberá informar si proporcionará más información a posteriori. También podrá aportar información adicional mediante comunicaciones intermedias a la autoridad de control bajo petición de esta, o cuando el responsable considere adecuado actualizar la situación de la misma.
- Cuando la notificación inicial no sea posible en el plazo de 72 horas, la notificación deberá realizarse igualmente, y en ella deberán constar y justificarse los motivos de la dilación.
- Las notificaciones deben ser sean claras, concisas y que incluyan la información necesaria para que puedan ser analizadas adecuadamente.

2.5.1 Identificación de la autoridad de control

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

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

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

2.5.2 Canal de notificación a la AEPD (ESPAÑA)

La notificación a la AEPD se realizará a través del formulario destinado a tal efecto publicado en la sede electrónica de la agencia, en https://sedeagpd.gob.es/sedeelectronica- web/

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

2.5.3 Proceso de comunicación al afectado

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

- Cuáles son las obligaciones legales y contractuales.
- Riesgos que comporta la pérdida de los datos: daños físicos, daños reputacionales, etc.
- Existe un riesgo razonable de suplantación de identidad o fraude (en función del tipo de información que se ha visto afectada y teniendo en cuenta si la información estaba seudonimizada o cifrada).
- Hasta qué punto la persona afectada puede evitar o mitigar posibles daños posteriores.
- Si después del análisis correspondiente es necesario realizar la notificación, pero se prevé que la comunicación a los afectados puede comprometer el resultado de una investigación en curso, la comunicación podría posponerse siempre bajo la supervisión de la autoridad de control.
- La comunicación a los afectados se realizará a la mayor brevedad posible, en un lenguaje claro y sencillo y siempre en estrecha cooperación con la autoridad de control y las autoridades policiales, de acuerdo con sus orientaciones. Esta comunicación, debería contener como mínimo:
    - Datos de contacto del Delegado de Protección de Datos, o en su caso, del punto de contacto en el que pueda obtenerse más información.
    - Descripción general del incidente y momento en que se ha producido.
    - Las posibles consecuencias de la brecha de la seguridad de los datos personales.
    - Descripción de los datos e información personal afectados.

- Resumen de las medidas implantadas hasta el momento para controlar los posibles daños.
- Otras informaciones útiles a los afectados para proteger sus datos o prevenir posibles daños.

- La notificación preferentemente se deberá realizar de forma directa al afectado, ya sea por teléfono, correo electrónico, SMS, a través de correo postal, o a través de cualquier otro medio dirigido al afectado que el responsable considere adecuado.
- La notificación indirecta, a través de avisos públicos en sitios web como blogs corporativos, o comunicados de prensa, se utilizará cuando para la notificación directa los costos sean excesivos o cuando no sea posible contactar con las personas afectadas (por ejemplo, porque se desconocen, o los datos de contacto no están actualizados).

2.5.4 Excepciones a la notificación / comunicación

No será necesaria la notificación a la Autoridad de Control cuando el responsable pueda demostrar, de forma fehaciente, que la brecha de la seguridad de los datos personales no entraña un riesgo para los derechos y las libertades de las personas físicas. Por ejemplo, si los datos ya se encontraban públicamente disponibles y su revelación no entraña ningún riesgo hacia el titular de los datos.

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

El responsable ha tomado medidas técnicas y organizativas adecuadas, como que los datos no sean inteligibles para personas o máquinas no autorizadas con anterioridad a la brecha de seguridad de datos personales (mediante el uso de: cifrados de datos de última generación, minimización, disociación de datos, acceso a entornos de prueba sin datos reales, etc.). Por ejemplo, es probable que no sea necesaria la notificación si se pierde un dispositivo móvil y los datos personales que contiene están cifrados.

Sin embargo, sí que es posible que se requiera de notificación si esta fuera la única copia de los datos personales, o, por ejemplo, la clave de cifrado en posesión del responsable estuviera comprometida.

El responsable ha tomado con posterioridad a la brecha de seguridad de datos personales las medidas de protección que mitiguen total o parcialmente el posible impacto para los afectados y garanticen que ya no hay posibilidad de que el alto riesgo se materialice. Por ejemplo, mediante la identificación y puesta en marcha inmediatamente de las medidas contra la persona que ha accedido a los datos personales antes de que pudieran hacer algo con ellos.

Cuando la notificación a los afectados suponga un esfuerzo desproporcionado a nivel técnico y organizativo. Por ejemplo, cuando los detalles de contacto se hayan perdido como resultado de la brecha, o aquellos casos en los que se tenga que desarrollar un nuevo sistema o proceso para realizar la notificación, o se requiera la dedicación excesiva de recursos internos para la identificación de los afectados.

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

Si el responsable todavía no ha comunicado al afectado la brecha de la seguridad de los datos personales considerando el alto riesgo potencial, la autoridad de control podrá exigirle: que lo comunique, podrá decidir que se cumpla alguna de las condiciones mencionadas para que la comunicación a los afectados no sea obligada.

2.6 Seguimiento

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

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

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

2. Valoración de adopción de medidas procesales.

Se valorará la oportunidad de iniciar un procedimiento judicial, a los fines de imputación de hechos y de reparación de daño. Pero también deberán analizarse los riesgos y las consecuencias que se pudieran derivar de los mismos, teniendo en cuenta que, en ocasiones, el daño derivado del proceso judicial podría incrementar el perjuicio en lugar de reducirlo.

Una brecha de seguridad puede ocasionar daños materiales muy importantes, pero una mala gestión de los mismos, puede ocasionar consecuencias reputacionales todavía más dañinas. En este sentido, se debe tener en cuenta la repercusión que un incidente de seguridad puede tener en el ramo de la actividad empresarial, sobre clientes, proveedores, accionistas, empleados, y, en definitiva, sobre la sociedad en general debiendo preverse los efectos de la difusión de la brecha.

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

La gestión diligente del incidente exige una correcta organización de la documentación recopilada en relación al suceso. la empresa comprobará que las medidas correctoras adoptadas por el Responsable de seguridad o del DPO si este hubiera sido designado, son adecuadas para la resolución de la brecha y para la minimización del riesgo en caso de que se produzca otra de similares características, que ha concluido el proceso de comunicación a la Autoridad de Control y, en su caso, a los posibles afectados.

A fin de cerrar la brecha de seguridad se elaborará un Informe final sobre la trazabilidad del suceso y su análisis valorativo, en particular, en cuanto al impacto final.

Dicho Informe final recopilará toda la información y documentación relativa a la brecha de manera que se facilite el estudio y revisión por terceros, incluida la dirección de la empresa.

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

2.7 Recuperación

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

Esto puede implicar la adopción no solo de medidas activas, sino también implementando controles periódicos y eficaces que permitan el seguimiento pormenorizado de los procesos de mayor riesgo. Identificación y análisis de soluciones (corto, medio, plazo): Se identificarán las distintas soluciones dirigidas a evitar nuevos incidentes de seguridad basados en la misma causa, así como a reducir el riesgo de los mismos.

Debe hacerse contraste con las medidas adoptadas para solventar el incidente en cuestión y garantizar un análisis pormenorizado de soluciones:

- Selección estrategia: Teniendo en cuenta el riesgo que quiera asumir la empresa, 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.

En Puerto del Rosario, a 10 de febrero de 2025.

Fdo.: D. Juan Salvador Rodríguez Ramírez
Consejero Delegado de CORORASA

42723481S JUAN SALVADOR RODRIGUEZ (R: A35091719)

Firmado digitalmente por 42723481S JUAN SALVADOR RODRIGUEZ (R: A35091719)
Fecha: 2025.02.14 09:26:43 Z