UNIDAD 5

DETECCIÓN Y DOCUMENTACIÓN DE INCIDENTES DE CIBERSEGURIDAD

PROCEDIMIENTOS DE ACTUACIÓN PARA LA NOTIFICACIÓN DE INCIDENTES.

Estos procedimientos se refieren los controles y mecanismos de seguridad dentro y alrededor de las instalaciones de la organización, así como los medios de acceso remoto a la información.

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

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

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

Es preciso tener en cuenta que con frecuencia un incidente que tenga lugar en el ámbito de la seguridad física puede también tener repercusión en el contexto de la ciberseguridad y por

lo tanto en los tratamientos de datos personales, de ahí la necesidad de mantener cierto grado de coordinación entre los responsables de la seguridad física y la ciberseguridad.

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

· Notificaciones de usuarios: presencia de archivos con caracteres inusuales, recepción de correos electrónicos con archivos adjuntos sospechosos, comportamiento extraño de dispositivos, imposibilidad de acceder a ciertos servicios, extravío/robo de dispositivos de almacenamiento o equipos con información.

· Alertas generadas por software antivirus.

· Consumos excesivos y repentinos de memoria o disco en servidores y equipos.

· Anomalías de tráfico de red o picos de tráfico en horas inusuales.

· Alertas de sistemas de detección/prevención de intrusión (IDS/IPS).

· Alertas de sistemas de correlación de eventos.

· Análisis de registros de conexiones realizadas a través de proxys corporativos o conexiones bloqueadas en los cortafuegos.

· Análisis de registro de servidores y aplicaciones con intentos de acceso no autorizados.

· Análisis de registros en herramientas DLP (Data Loss Prevention).

También se debe considerar cualquier posible indicio de la ocurrencia de un incidente de seguridad en el futuro, como el análisis del resultado de un escáner de vulnerabilidades del sistema, el anuncio de un nuevo 'exploit' dirigido a atacar una vulnerabilidad que podría estar presente en el sistema o amenazas explícitas anunciando ataques a los sistemas de información de la organización7 .

NOTIFICACIÓN INTERNA DE INCIDENTES.

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

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

- Descripción objetiva del incidente.

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

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

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

NOTIFICACIÓN EXTERNA DE INCIDENTES.

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

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

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

Estas nuevas obligaciones para el responsable vienen a ampliar las previamente establecidas para operadores de servicios de comunicaciones electrónicas11 y prestadores de servicios de confianza12.

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

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

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

12 Artículo 19.2 del Reglamento 910/2014 del Parlamento Europeo y del Consejo 39

La existencia de una política de notificaciones de brechas de seguridad se debe tener en cuenta con el fin de disponer de un criterio común a todos los tratamientos de datos personales que consten en el registro de actividades de tratamiento de una organización. En cada caso se debe de valorar los umbrales bajo los cuales el responsable procederá a la notificación.

Proceso de notificación a la autoridad de control

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

El criterio a tener en cuenta para determinar si un incidente ha producido “una brecha de la seguridad de los datos personales” se recoge en el propio RGPD, e incluye “todas aquellas brechas de la seguridad que ocasionen la destrucción, pérdida o alteración accidental o ilícita

de datos personales transmitidos, conservados o tratados de otra forma, o la comunicación o acceso no autorizados a dichos datos."

Esta comunicación deberá contener la siguiente información:

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

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

- Naturaleza y contenido de los datos personales en cuestión.

- Resumen del incidente que ha causado la brecha de seguridad de datos personales (con indicación de la ubicación física y del soporte de almacenamiento).

- Posibles consecuencias y efectos negativos en los afectados.

- Medidas técnicas y organizativas que se hayan adoptado por parte del responsable del tratamiento según el apartado 33.2d) del RGPD.

- Categoría de los datos afectados y número de registros afectados.

- Categoría y número de individuos afectados.

- Posibles cuestiones de carácter transfronterizo, indicando la posible necesidad de notificar a otras autoridades de control.

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

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

Cuando la notificación inicial no sea posible en el plazo de 72 horas, la notificación deberá realizarse igualmente, y en ella deberán constar y justificarse los motivos de la dilación.

Las notificaciones deben ser sean claras, concisas y que incluyan la información necesaria para que puedan ser analizadas adecuadamente.

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

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

Canal de notificación a la AEPD

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

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

9.2.2 Proceso de comunicación al afectado

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

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

· Cuáles son las obligaciones legales y contractuales.

· Riesgos que comporta la pérdida de los datos: daños físicos, daños reputacionales, etc.

· Existe un riesgo razonable de suplantación de identidad o fraude (en función del tipo de información que se ha visto afectada y teniendo en cuenta si la información estaba seudonimizada o cifrada).

· Hasta qué punto la persona afectada puede evitar o mitigar posibles daños posteriores.

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

Esta comunicación, debería contener como mínimo:

· Datos de contacto del Delegado de Protección de Datos, o en su caso, del punto de contacto en el que pueda obtenerse más información.

· Descripción general del incidente y momento en que se ha producido.

· Las posibles consecuencias de la brecha de la seguridad de los datos personales.

· Descripción de los datos e información personal afectados.

· Resumen de las medidas implantadas hasta el momento para controlar los posibles daños.

· Otras informaciones útiles a los afectados para proteger sus datos o prevenir posibles daños.

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

La notificación indirecta, a través de avisos públicos en sitios web como blogs corporativos, o comunicados de prensa, se utilizará cuando para la notificación directa los costos sean

excesivos o cuando no sea posible contactar con las personas afectadas (por ejemplo porque se desconocen, o los datos de contacto no están actualizados).