Pridatect
POWERING PRIVACY COMPLIANCE

CÓMO PREPARARSE Y GESTIONAR UNA BRECHA DE SEGURIDAD

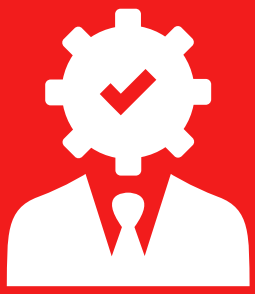
Contenido

1. Introducción

Las brechas de seguridad son una de las mayores preocupaciones para empresas y organizaciones, más aún teniendo en cuenta su repercusión mediática y los graves perjuicios reputacionales que pueden causar. Lo más importante para evitar que se produzca una brecha o violación de seguridad es adoptar las medidas preventivas adecuadas.

Aun así, la prevención de la empresa no garantiza la inmunidad ante brechas de seguridad, es por ello que las empresas deben tener una previsión de las medidas reactivas que deberían tomar en caso de sufrir un accidente de seguridad relacionado con el tratamiento de datos personales.

Si ocurre, el responsable del tratamiento debe ser capaz de detectar, afrontar y gestionar la crisis de seguridad lo antes posible para minimizar sus efectos.



2. Tipos de brecha de seguridad

Una vez detectada la brecha de seguridad y antes de proceder a la actuación, repasaremos los tipos de brecha de seguridad que pueden existir.

Conocer los tipos de brecha más común nos ayudará no solo a identificarlas, sino también a afrontarlas.

- **Brecha de confidencialidad:** supone un acceso no autorizado a la información.
- **Brecha de integridad:** se produce cuando se altera la información original y la sustitución de datos puede ser perjudicial.
- **Brecha de disponibilidad:** supone la imposibilidad de acceder a los datos, puede ser temporal o permanente, en función de si los datos se podrán recuperar o no.

Una vez detectada la brecha y su naturaleza, se podrán preveer sus consecuencias.
A continuación, veremos cuál es el proceso concreto a seguir cuando se detecta o se cree haber detectado un incidente de este tipo.

3. Los cuatro pasos a seguir

De acuerdo con los artículos 33 y 34 del Reglamento General de Protección de Datos, una organización que ha sufrido una brecha de seguridad deberá seguir los siguientes pasos:

a) Investigar la brecha

La organización responsable deberá investigar los hechos para poder describir el responsable o la causa, las características y las fechas de inicio y finalización de la brecha.

Necesitará, a su vez, conocer qué partes interesadas se ven afectadas o están relacionadas con la fuga, así como la naturaleza y las consecuencias de esta:

- La naturaleza de la fuga se refiere a la forma en la que se ocasionó el problema y qué tipo de datos están afectados.
- En cuanto a las consecuencias, se tendrá que definir qué daños ocasionará la brecha y a que individuos afectará.
- Por último, se deberán describir las medidas que la compañía está dispuesta a poner en marcha para reparar o evitar los daños.

b) Determinar la necesidad de notificación de la brecha

Las brechas de seguridad deben ser notificadas a la autoridad de control competente, a menos que sea improbable que dicha violación de la seguridad constituya un riesgo para los derechos y las libertades de las personas físicas.

Asimismo, deberá notificarse a los interesados cuando sea probable que la brecha de seguridad cause un alto riesgo para los derechos y libertades de los mismos, con algunas salvedades.

Lo más recomendable es notificar siempre a la autoridad competente y determinar correctamente la necesidad o no de notificar a los interesados.

c) Notificar a la autoridad competente

En **menos de 72 horas** la brecha debe ser notificada a la autoridad competente, que en el caso de España es la Agencia Española de Protección de Datos. Si no se notifica en el plazo de 72 horas, se deberá justificar el motivo.

La notificación deberá incluir la naturaleza de la brecha, con las categorías y número de datos y personas afectadas, los datos del DPO y una descripción de las consecuencias. Asimismo, se especificarán las medidas que se llevarán o se han llevado a cabo.

d) Notificar a los interesados

Por último, pero no menos importante, habrá que determinar si es necesario notificar a los interesados la brecha. Ello deberá realizarse cuando sea probable que haya un riesgo para sus derechos y libertades.

No será necesario notificar a los interesados cuando el responsable ha adoptado las medidas de protección técnicas y organizativas apropiadas que hagan ininteligible la información o que garanticen que no existe alto riesgo, así como cuando la comunicación suponga un esfuerzo desproporcionado.

4. Conclusión

La principal conclusión es la necesidad de contar con un plan de actuación en el caso de que ocurriera una brecha de seguridad, para ello es conveniente contar con un apoyo en la gestión del RGPD, ya sea contando con un DPO (incluso cuando no sea necesario) o con una plataforma como Pridatect

De este modo, no sólo se contarán con medidas para evitar las posibles brechas de seguridad, sino que, además, se estará preparado para afrontar las que puedan aparecer causando los mínimos daños de reputación a la empresa víctima del ataque.

Pridatect
POWERING PRIVACY COMPLIANCE

SIMPLIFICANDO LA PROTECCIÓN DE DATOS EN LAS EMPRESAS

Para más información:
pridatect.com

Contacto:
info@pridatect.com