BRECHAS DE SEGURIDAD

¿Qué es una violación o brecha de seguridad?

Es un incidente de la seguridad que afecta a datos personales. Puede ser tanto accidental como intencionado, y darse tanto a datos tratados de forma digital como en documentos en papel.

¿Qué tipos hay?

- **Confidencialidad:** Sucede cuando alguien que no tenía autorización para conocer dichos datos personales ha accedido a los mismo.
- **Integridad:** Es cuando los datos han sido corrompidos y ya no son precisos o coherentes. Un ejemplo sería cuando dos expedientes de personas distintas se mezclan.
- **Disponibilidad:** Cuando no es posible acceder a los datos personales que necesitamos para poder realizar nuestro trabajo.

¿Por qué es importante detectar las brechas de seguridad?

Las brechas u obligaciones de seguridad pueden causar daños en los derechos y libertades de las personas. La Protección de Datos Personales es un derecho fundamental y está conectado con la intimidad de las personas. Además, también pueden causar perjuicios económicos o reputacionales.

Ejemplos de incidentes de seguridad.

- Hemos enviado un correo con datos personales por error a la persona que no era.
- Hemos tirado documentación a la papelera sin haber pasado por la destructora de papel. Cuidado: cualquier persona puede denunciar a la AEPD que los datos estaban en el contenedor de basura. Los Cuerpos y Fuerzas de Seguridad informan siempre a la Agencia si encuentran este tipo de información sin custodia.
- Queremos hacer una comunicación general para todos los usuarios por correo electrónico pero no hemos usado la opción de "copia oculta" del correo electrónico. Ahora, todos los destinatarios tienen todos los correos electrónicos de los usuarios de la entidad.
- Hemos descuidado un expediente sobre la mesa y ha desaparecido.
- Hemos puesto nuestro usuario y contraseña en una nota adhesiva. Cualquier puede usarlo y entrar en el sistema apareciendo yo como responsable de todo lo que se haga con esas credenciales. Las contraseñas son individuales y no deben ser compartidas.
- Hemos abierto un correo sin comprobar el destinatario del mismo y hemos descargado el documento adjunto. Podría ser un virus, por lo tanto, debemos tener especial cuidado si no conocemos el remitente del correo.
- Se han inundado las instalaciones y se ha perdido todos los documentos en papel, de los cuales no había copia digital.
- Ha desaparecido un expediente o documentos del servidor o servicio de almacenamiento y no sabemos qué ha pasado.

¿Qué debo hacer si detecto una brecha de seguridad?

1. Mantener la calma y ver qué ha podido pasar. Recaba toda la información que puedas.
2. Comunicar al superior jerárquico y al Delegado de Protección de Datos / Responsable de Seguridad lo que ha sucedido de forma inmediata. Debes comunicarlo lo antes posible para poder reaccionar y tomar medidas que mitiguen los riesgos o que puedan causar daños a los titulares de los datos personales y, en su caso, notificar la brecha a la AEPD.
3. Colabora con el Delgado de Protección de Datos / Responsable de Seguridad. Puede que necesite más información para proporcionárselo y es tu obligación colaborar con él.

PRODAT
LIDERES EN PROTECCION DE DATOS