GESTIÓN DE VIOLACIONES DE SEGURIDAD

¿Qué debo hacer cuando exista un incidente de seguridad que comprometa datos personales?

1. **Detección y Delimitación**: cuando se detecte una violación o brecha de seguridad, se debe informar inmediatamente al responsable de IT y/o a la Dirección.

2. **Comunicación interna:** si dentro de esa violación se han visto afectados datos personales (de empleados, clientes, proveedores, etc.), el responsable de IT/Dirección debe comunicárselo a la persona responsable de privacidad/Delegado de protección de datos, para que registre la incidencia y valore la gravedad de lo ocurrido para su notificación a la Autoridad de control.

3. **Notificación a la Autoridad de Control (AEPD):** la comunicación, en el caso de tener que realizarse, se deberá llevar a cabo dentro de las primeras 72 horas desde que se tuvo conocimiento del incidente, salvo imposibilidad justificada.

4. **Información a los afectados:** si la brecha supone una vulneración grave para los derechos y libertades de las personas en materia de privacidad (ej.: usurpación de identidad, daño para la reputación, perjuicio económico o social significativo, restricción de derechos, etc.), la empresa deberá también informar a esas personas sin demora.

Los datos personales son cualquier información relacionada con una persona identificada o identificable (por ejemplo, nombre, correo electrónico, teléfono, dirección, salud, datos profesionales, bancarios, etc.)

Ejemplos de violaciones de seguridad sobre datos personales:

Pérdida de Información

- El ordenador portátil, memoria USB, teléfono móvil corporativo o archivos en papel con datos personales se pierden o son robados.
- Desinstalación de aplicaciones informáticas.
- Extravío u olvido de soportes.
- No usar destructora de papel o de soportes digitales.
- Incencio, inundación u otras causas ajenas a la empresa

Acceso a datos no autorizado

- Acceso indiscriminado a impresoras, fotocopiadoras, etc.
- Encargado de Tratamiento sin el correspondiente contrato
- Acceso no autorizado a sistemas informáticos.
- Acceso no autorizado a información confidencial (ej.: datos de nóminas, CVs, imágenes de videovigilancia, etc.)

Comunicación de datos no autorizada

- Envío de correo electrónico a destinatario equivocado, con contenido incorrecto, o envío masivo sin ocultar destinatarios (copia oculta).
- Publicación de imágenes sin autorización del interesado.
- Vulneración de secreto profesional.
- Transmisión ilícita de datos a un destinatario

Ausencia de medidas de seguridad

- Antivirus, antispam, antimalware, cifrado, seudonimización, etc.
- Mecanismos de seguridad para acceder a mobiliario o departamentos con datos personales.
- Identificación y autenticación para acceder a sistemas informáticos.