Cómo detectar y actuar ante una brecha de seguridad

CECA MAGÁN
ABOGADOS

Febrero 2026

¿Qué es una brecha de seguridad?

Una **brecha de seguridad de datos personales** ocurre cuando la información se pierde, **se accede sin autorización, se altera o se** divulga de forma accidental o ilícita.

No es solo un ciberataque: también puede ser un error humano

Puedes estar ante una brecha si ocurre alguno de estos casos:

- Envío de correos con datos personales al **destinatario equivocado**
- **Uso** de credenciales por personas **no autorizadas**
- **Perdida o robo** de portátil, móvil o USB con información
- **Eliminación accidental** de datos sin copia de seguridad
- **Acceso** a carpetas o sistemas **sin permiso**
- **Sospecha** de **malware, phishing o acceso** extraño a sistemas

¿Por qué se debe avisar rápido?

Avisar a tiempo **permite al equipo técnico actuar de inmediato**, aplicar las medidas de seguridad necesarias y **prevenir daños mayores.**

La empresa dispone de **72 horas** desde que tiene conocimiento para informar a la autoridad de control, si existe riesgo para las personas.

¿Qué debes hacer si detectas una brecha?

1. **No intentes solucionarlo por tu cuenta**
2. **Informa de inmediato** al canal interno establecido
3. **Facilita toda la información que conozcas:**
   - **-Qué** ha ocurrido
   - **-Cuándo** lo detectaste
   - **-Qué datos** pueden estar afectados
   - **-A quién** afecta

Notificar a tiempo es proteger a las personas y a la organización.

¿Tienes dudas? Podemos ayudarte

Consúltalas con nuestro Delegado de Protección de Datos (DPD)

privacy@cecamagan.com

www.cecamagan.com