

DÍA INTERNACIONAL DE LA PROTECCIÓN DE DATOS

Convenio 108 del Consejo de Europa

Cada 28 de enero se celebra el **Día Internacional de la Protección de Datos**, fecha en la que se firmó el Convenio 108 del Consejo de Europa, el primer instrumento internacional que estableció reglas para proteger la **privacidad de las personas frente al tratamiento automatizado de datos personales**.

Esta fecha nos recuerda que la protección de los datos personales es un derecho fundamental reconocido por nuestra Constitución y que, en el día a día, **todos compartimos la responsabilidad de cuidar la información personal que gestionamos en nuestras empresas**.

En ese contexto, queremos compartirles una guía práctica sobre **cómo actuar ante un incidente de seguridad**.



¿Qué es un incidente de seguridad?

Es toda vulneración que ocasione la destrucción, pérdida, alteración ilícita, o la comunicación/exposición no autorizada de datos personales.

Ejemplo: un acceso no autorizado a los datos, su modificación sin permiso o la eliminación de información personal.



Recuerda:

La protección de los datos personales es un derecho fundamental que asegura la autodeterminación informativa de las personas. Por ello, es importante contar con procedimientos internos claros para la notificación de incidentes, de modo que cada área sepa cómo actuar.

Ante cualquier incidente de seguridad, el responsable del tratamiento debe dejar constancia de lo ocurrido, sus efectos y las medidas adoptadas. Actuar con rapidez resulta clave para reducir su impacto.

¿Qué hacer ante un incidente de seguridad?

GUÍA PRÁCTICA

Si ocurre una filtración o incidente con datos personales, debemos actuar con rapidez siguiendo estos pasos:

1

Registrar e identificar

Detecta qué ocurrió, qué datos fueron comprometidos y el alcance. Documenta cada detalle desde el inicio.

2

Contener y mitigar el daño

Aísla los sistemas afectados inmediatamente para controlar la situación y evitar una mayor exposición de los datos.

3

Notificar a la autoridad (ANPDP)

Si hay alto riesgo, gran volumen o datos sensibles, el responsable debe notificar formalmente.

4

Comunicar a los afectados

Informar al titular en lenguaje claro y sencillo sobre el incidente y las medidas tomadas sin dilación.

5

Analizar y corregir

Evalúa las causas raíz del problema y refuerza las medidas de seguridad para evitar futuras filtraciones.

Proteger los datos es responsabilidad de todos.