



Marco Legal

# ¿Cómo implementar una política de prevención de riesgos?/Ley protección datos personales

● ○ ○ FICHA BÁSICA

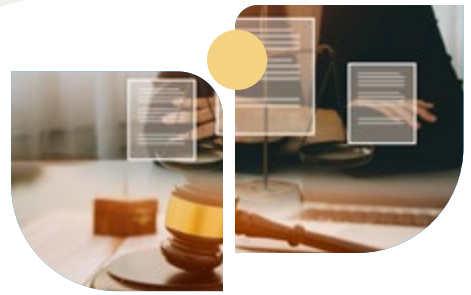
|                 |            |
|-----------------|------------|
| Fecha           | Julio 2025 |
| Tpo. de lectura | 10 min.    |

En el marco de la ley de protección de datos personales de Chile, la recomendación para las empresas, tanto grandes como pequeñas, es comprometerse con un manejo responsable y seguro de los datos de sus clientes, empleados y proveedores, evitando conductas de riesgo y fortaleciendo su reputación en el mercado.

Lo anterior a través de una política que fije:

- **Objetivo:** establecer las medidas preventivas que debe adoptar la empresa para evitar vulneraciones, filtraciones o uso indebido de los datos personales bajo su responsabilidad, en cumplimiento con la Ley de Protección de Datos Personales en Chile.
- **Alcance:** aplica a todos los trabajadores, colaboradores y proveedores que tengan acceso a datos personales en el contexto de sus funciones dentro de la empresa.

**FGE**



## Y que vele por el cumplimiento de las siguientes acciones:

### 1. Evaluación de riesgos

- Realizar un diagnóstico inicial y revisión anual de los datos que se recolectan, almacenan, comparten y procesan.
- Identificar los puntos vulnerables (archivos, accesos, canales digitales).

### 2. Acceso restringido

- Limitar el acceso a datos personales sólo a quienes los necesiten para su trabajo.
- Establecer claves de acceso seguras y personales.
- Prohibir el uso de cuentas compartidas para sistemas o plataformas.

### 3. Buenas prácticas digitales

- No compartir contraseñas.
- No enviar datos personales por canales inseguros (como WhatsApp o correos sin cifrar).
- Usar antivirus y mantener el software actualizado.
- Realizar copias de seguridad de forma regular.

### 4. Manejo de incidentes

- Ante una filtración, acceso no autorizado o pérdida de datos:
  - Notificar al encargado de datos de la empresa.
  - Detener el acceso indebido (cambio de clave, bloqueo de cuenta, etc.).
  - Registrar el incidente.
  - Informar a los afectados de forma clara y oportuna.

### 5. Capacitación

- Capacitar al personal nuevo sobre esta política durante su inducción.
- Reforzar anualmente el protocolo de manejo y seguridad de datos.

### 6. Revisión y actualización

- Esta política debe ser revisada al menos una vez al año o cada vez que cambie:
  - La tecnología utilizada.
  - La forma de recolectar o usar datos.
  - La estructura organizacional o de responsabilidades.

Este documento debe mantenerse accesible al personal y formar parte del manual interno de buenas prácticas de la empresa..

FUENTE: el contenido de esta ficha fue elaborado por FGE con el apoyo de inteligencia artificial.