¿Cómo implementar una política de prevención de riesgos? Ley de ciberseguridad

Marco Legal

FICHA BÁSICA

Fecha	Julio 2025
Tpo. de lectura	10 min.

En el marco de la ley de ciberseguridad de Chile, la recomendación para las empresas, tanto grandes como pequeñas, es proteger su información, garantizar la continuidad de sus operaciones y dar cumplimiento a los principios de esta norma.

Lo anterior a través de una política que fije:

- **Objetivo**: establecer principios y acciones preventivas para proteger la información, los sistemas digitales y la continuidad operativa de la empresa, en cumplimiento con la Ley Marco de Ciberseguridad en Chile.
- **Alcance**: esta política se aplica a todos los trabajadores, colaboradores, socios y proveedores que utilicen recursos digitales o manejen información dentro de la empresa.

Y que vele por el cumplimiento de las siguientes acciones:

1. Identificación de riesgos

- Identificar los activos digitales críticos (computadores, servidores, sistemas contables, plataformas de ventas, etc.).
- Evaluar posibles amenazas como virus, acceso no autorizado, robo de información o caída de sistemas.
- Registrar y actualizar los riesgos al menos una vez al año.

2. Medidas preventivas obligatorias

- Uso de contraseñas seguras y personales.
- Antivirus actualizado en todos los dispositivos.
- Copias de seguridad periódicas.
- Control de acceso a sistemas (solo usuarios autorizados).
- Uso responsable del correo electrónico y navegación.

3. Procedimiento ante incidentes

- Todo trabajador debe reportar de inmediato cualquier situación sospechosa al responsable de ciberseguridad.
- Se deberá:

→ Contener el incidente.
→ Proteger los datos expuestos.
→ Documentar lo ocurrido.
→ Informar a los afectados si corresponde.

4. Designación de responsables

- La empresa designa un encargado/a de ciberseguridad (puede ser interno o externo) responsable de aplicar esta política y coordinar las acciones preventivas.

5. Concientización y capacitación

- Todo el personal recibirá al menos una vez al año una sesión básica sobre buenas prácticas digitales y seguridad informática.
- Esta política se entregará también en la inducción de nuevos trabajadores.

6. Revisión y mejora continua

- Esta política será revisada anualmente o cuando cambien:

→ Los sistemas digitales utilizados.
→ Las amenazas conocidas.
→ La estructura organizacional o de funciones.

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