



Marco Legal

Claves para implementar un protocolo básico/ Ley de ciberseguridad

● ○ ○ FICHABÁSICA

Fecha	Julio 2025
Tpo. de lectura	10 min.

En Chile existen dos cuerpos legales la Ley N° 21.663 (Ley Marco de Ciberseguridad) y la Ley N° 21.459 (Ley de Delitos Informáticos) cuya relación es de complementariedad absoluta, funcionando como las dos caras de una misma moneda para la protección del ecosistema digital.

- Mientras una se enfoca en la prevención técnica y organizativa,
- La otra castiga penalmente los ataques informática

FGE

La Ley Marco de Ciberseguridad contempla los siguientes aspectos:



- 1. Designación de responsable de ciberseguridad**
 - Nombrar a una persona encargada de supervisar el cumplimiento de este protocolo.
 - No es necesario que sea un experto, pero debe tener conocimientos básicos y acceso a información clave.
- 2. Buenas prácticas digitales**
 - Usar contraseñas seguras (mínimo 8 caracteres, con números y símbolos) y cambiarlas cada 6 meses.
 - No compartir cuentas de usuario entre trabajadores.
 - Cerrar sesión al terminar de usar un sistema.
 - No instalar programas sin autorización.
- 3. Protección de equipos y sistemas**
 - Tener antivirus actualizado en todos los computadores.
 - Actualizar los sistemas operativos y aplicaciones regularmente.
 - Usar conexiones seguras (evitar Wi-Fi públicas sin VPN).
- 4. Respaldo de información**
 - Realizar copias de seguridad (*backups*) al menos una vez por semana.
 - Guardar los respaldos en un lugar seguro, idealmente externo (nube o disco externo cifrado).
 - Probar regularmente que los respaldos funcionen.
- 5. Prevención de fraudes y engaños (phishing)**
 - Enseñar al equipo a reconocer correos falsos o sospechosos.
 - No hacer clic en enlaces dudosos ni abrir archivos de origen desconocido.
 - Verificar siempre la dirección del remitente antes de responder o pagar.
- 6. Manejo de incidentes de seguridad**
 - Si se detecta un ataque, virus, robo de información o filtración:
 - Avisar de inmediato al encargado de ciberseguridad.
 - Cambiar contraseñas si hay riesgo de acceso indebido.
 - Registrar qué ocurrió y cómo se respondió.
 - Si afecta a terceros o datos sensibles, evaluar informar a los afectados.
- 7. Capacitando al equipo**
 - Realizar al menos una sesión anual de capacitación básica en ciberseguridad.
 - Entregar este protocolo en formato físico o digital a todo el equipo.
- 8. Revisión periódica del protocolo**
 - Revisar y actualizar este protocolo al menos una vez al año.
 - También actualizarlo si hay cambios en sistemas, proveedores digitales o procesos internos.

Contenido desarrollado por FGE con base en la Ley N° 21.663 y la Ley N° 21.459

