

PROTECCIÓN DE DATOS

La Ley N° 21.719, vigente desde el **1 de diciembre de 2026**, establece un nuevo estándar obligatorio para la protección de datos personales en Chile, reemplazando la obsoleta Ley 19.628. Su cumplimiento no solo requiere buenas intenciones, sino **evidencia documentada, roles claros y procesos operativos trazables**.

1. ALCANCE Y DEFINICIONES CLAVE

- **Dato personal:** cualquier información que identifique o haga identificable a una persona natural, incluyendo nombre, RUT, correo, teléfono, dirección, datos de salud, situación económica, hábitos de consumo y datos biométricos.
- **Tratamiento de datos:** cualquier operación sobre datos personales: recolección, almacenamiento, uso, comunicación, transferencia o eliminación.
- **Dato sensible:** categoría especial que requiere mayor cuidado, incluyendo salud, origen étnico, afiliación sindical, creencias, vida sexual, biometría y situación socioeconómica.

2. BASES LEGALES PARA EL TRATAMIENTO

- 2.1. **Consentimiento informativo, libre y específico** salvo otras bases legales permitidas.
- 2.2. **Finalidad:** los datos deben tratarse solo para los fines declarados.
- 2.3. **Transparencia:** informar sobre qué datos se recolectan, el propósito, el plazo de retención y con quién se comparten.

3. ROLES Y RESPONSABILIDADES

- **Responsable del Tratamiento:** decide para qué y cómo se tratan los datos. En la mayoría de los casos, la propia organización.
- **Encargado del Tratamiento:** ejecuta el tratamiento por cuenta del responsable (interno o externo).
- **Delegado de Protección de Datos (DPO):** recomendable en organizaciones con tratamiento de datos a gran escala o datos sensibles; coordina la estrategia, evalúa riesgos y supervisa cumplimiento.

4. DERECHOS DE LOS TITULARES

La Ley refuerza los derechos ARCO más **portabilidad** y bloqueo temporal:

- 4.1. **Acceso:** conocer qué datos existen y cómo se usan.
- 4.2. **Rectificación:** corregir información incorrecta.
- 4.3. **Cancelación/Supresión:** eliminar datos cuando proceda.
- 4.4. **Oposición:** negarse a ciertos usos.
- 4.5. **Portabilidad:** recibir datos en formato utilizable y transferible.
- 4.6. **Bloqueo:** suspender temporalmente el tratamiento.

5. DOCUMENTACIÓN Y EVIDENCIA OBLIGATORIA

El cumplimiento debe **demostrarse** ante la Agencia de Protección de Datos:

- **Registro de Actividades de Tratamiento (RAT):** qué datos se tratan, finalidad y medidas de seguridad aplicadas.
- **Políticas internas de protección de datos:** normas de manejo, acceso y resguardo.
- **Procedimientos para ejercer derechos ARCO.**
- **Protocolos para gestión de incidentes y brechas de seguridad.**
- **Contratos con proveedores** que manejen datos, incluyendo transferencias internacionales con cláusulas de protección.

6. MEDIDAS TÉCNICAS Y ORGANIZACIONALES

- **Seguridad:** cifrado, anonimización, control de accesos y segmentación.
- **Monitoreo:** backups regulares, planes de recuperación, ciberseguridad y supervisión de dispositivos.
- **Evaluación de Impacto en Privacidad (DPIA):** obligatoria para tratamientos de alto riesgo, sensibles, masivos o con nuevas tecnologías.

7. GESTIÓN DE INCIDENTES

- 7.1. Detectar, contener y evaluar impacto.
- 7.2. Notificar a la **Agencia de Protección de Datos** y a los titulares afectados.
- 7.3. Registrar evidencia y ejecutar corrección rápida.
- 7.4. Realizar simulacros periódicos y seguimiento de acciones correctivas.

8. TRANSFERENCIAS DE DATOS A TERCEROS

- Solo se permiten con **contratos DPA** que aseguren cumplimiento legal.
- Cumplimiento específico en transferencias internacionales según requisitos de la ley.

9. SANCIONES

- **Leves:** hasta 100 UTM. Ej.: errores formales o falta de información mínima.
- **Graves:** hasta 5.000 UTM. Ej.: tratar datos sin base legal, no atender derechos ARCO.
- **Gravísimas:** hasta 20.000 UTM (aprox. 1.400 millones de pesos) y posibles sanciones adicionales sobre ingresos anuales. Ej.: uso indebido de datos sensibles o transferencias ilegales, no notificar brechas críticas.

10. HOJA DE RUTA DE CUMPLIMIENTO

Fase 1: Diagnóstico (Meses 1–3)

- Inventario de datos, evaluación de brechas, análisis de proveedores y determinación de necesidad de DPIA.

Fase 2: Planificación y Estrategia (Meses 4–6)

- Definir políticas, responsabilidades, controles técnicos y flujos de evidencia.
- Implementar canales para derechos ARCO.
- Plan de respuesta a incidentes y capacitación del personal.

Fase 3: Implementación y Monitoreo (Meses 7–12)

- Ejecución de controles técnicos y organizativos.
- Supervisión continua y actualización de políticas.
- Auditorías internas y preparación para fiscalización.

11. BUENAS PRÁCTICAS

- Documentar decisiones y mantener registro actualizado.
- Integrar protección de datos con contabilidad, contratos y procesos internos.
- Preparar evidencias para auditorías.
- Capacitar de manera continua al personal, especialmente sobre derechos de los titulares y riesgos de seguridad.

CONCLUSIÓN



OFICINA: Cooperación Internacional y Gestión Digital
N° DE EXPEDIENTE: **PD-CIGD-2026-001**
APROBACIÓN: 29 sept 2026/
REVISIÓN: 29 sept 2027

El cumplimiento de la Ley 21.719 exige **gestión proactiva, documentación y trazabilidad**, combinando **roles claros, medidas técnicas y organizativas, y seguimiento riguroso de los derechos de los titulares**. Ignorar estos requisitos puede derivar en multas significativas, daños reputacionales y consecuencias legales de alto impacto.

Referencia Legal Única: Ley N° 21.719 sobre Protección de Datos Personales, Chile (publicada 13 de diciembre de 2024, vigente 1 de diciembre de 2026).

