APUNTES DEL MÓDULO 1

Fundamentos, conceptos y principios de la Ley 21.719

Protección de Datos Personales (Ley 21.719) — Concientización (todo el personal)

Material de estudio

Módulo 1

Apunte descargable del estudiante

Contenido del módulo

La protección de datos personales es una preocupación creciente en el mundo digital. En Chile, la Ley N°21.719, cuya aplicación plena rige desde el 1 de diciembre de 2026, establece un marco legal robusto para salvaguardar la privacidad de las personas. Como parte del personal de una organización, es fundamental comprender sus fundamentos, conceptos clave y principios rectores para asegurar el cumplimiento y fomentar una cultura de protección de datos. Este apunte de estudio te proporcionará las herramientas necesarias para reconocer y aplicar las directrices de esta importante normativa.

1 El nuevo escenario: Ley 21.719 y su alcance

Imagina que diriges el área de *compliance* de una empresa de retail con plataforma digital. El 1 de diciembre de 2026 entra en vigencia la Ley 21.719, y necesitas entender exactamente qué protege y a quiénes obliga. Acompáñame en este recorrido para dominar los fundamentos de esta normativa.

La Ley N°21.719 sobre Protección de Datos Personales tiene por objeto **garantizar y proteger el derecho a la privacidad y a la protección de datos personales de las personas naturales**, ante su tratamiento por parte de organismos públicos y entidades privadas.

El **ámbito de aplicación** de la ley es amplio: se aplica a todo tratamiento de datos personales, total o parcialmente automatizado, y al tratamiento no automatizado de datos personales contenidos en registros o destinados a ser incluidos en ellos. Esto significa que tanto un sistema informático de gestión de clientes como un archivador físico con expedientes de personal están bajo su paraguas. Se aplica tanto al sector público como al privado, con ciertas excepciones, como los tratamientos exclusivamente personales o domésticos, o aquellos relacionados con la seguridad nacional.

La **entrada en vigencia** fue gradual, con su aplicación plena a partir del **1 de diciembre de 2026**. Desde esa fecha, todas las organizaciones deben cumplir íntegramente con sus obligaciones.

Esta normativa marca un cambio de paradigma: desde un modelo reactivo (esperar la denuncia o fiscalización) hacia uno de **responsabilidad proactiva**, alineado con estándares internacionales como el Reglamento General de Protección de Datos (RGPD) europeo.

Sector	Alcance	Ejemplo Laboral
Privado	Empresas, fundaciones, ONG que traten datos personales	Una empresa de logística que gestiona datos de envíos de clientes.
Público	Ministerios, servicios, municipalidades, empresas del Estado	Un hospital público que maneja historiales médicos de pacientes.

La Ley 21.719 protege la privacidad de las personas frente al tratamiento de sus datos personales, marcando un antes y un después en la seguridad de la información.

✔ Puntos clave

- La Ley 21.719 protege el derecho a la privacidad y la protección de datos personales de personas naturales.
- Se aplica a todo tratamiento de datos personales, automatizado o no, en el sector público y privado.
- La ley entró en plena vigencia el 1 de diciembre de 2026.
- Establece un modelo de responsabilidad proactiva, en línea con estándares internacionales.

💭 Para reflexionar

- ¿Por qué es importante para mi organización conocer la fecha de plena vigencia de la Ley 21.719?
- ¿Cómo impacta el cambio de un modelo reactivo a uno de responsabilidad proactiva en las operaciones diarias de mi equipo?
- ¿Qué tipo de datos en mi área podrían ser afectados por esta ley?

2 Conceptos clave: datos, titulares y actores

Para implementar la ley en tu organización, primero debes hablar el mismo idioma legal. Vamos a definir qué es un dato personal, qué lo hace sensible, y quiénes son los responsables y encargados del tratamiento. Comprender estos roles es fundamental para delimitar las responsabilidades dentro de tu equipo.

- **Dato personal:** Toda información concerniente a una persona natural identificada o identificable. Esto va más allá del nombre y RUT. Incluye, por ejemplo, una dirección IP si permite identificar a un usuario, una fotografía, o incluso preferencias de consumo si se asocian a una persona específica.
- **Dato sensible:** Aquellos datos personales que revelan origen étnico o racial, opiniones políticas, convicciones religiosas o filosóficas, afiliación sindical, datos genéticos o biométricos dirigidos a identificar unívocamente a una persona, datos de salud, vida sexual u orientación sexual. Su tratamiento exige mayores garantías y, en muchos casos, un consentimiento explícito y reforzado.
- **Titular:** La persona natural a quien se refieren los datos personales. Es el "dueño" de la información y quien ejerce los derechos que le confiere la ley.
- **Responsable del tratamiento:** Persona natural o jurídica, pública o privada, que, sola o conjuntamente con otras, determina los fines y medios del tratamiento de datos personales. Es quien **decide el "qué" y el "cómo"**. Por ejemplo, la empresa que decide recolectar datos de clientes para marketing.
- **Encargado del tratamiento:** Persona natural o jurídica que trata datos personales por cuenta del responsable. Actúa siguiendo las instrucciones del responsable. Un ejemplo común es una empresa de servicios en la nube que almacena bases de datos de clientes para otra compañía.
- **Tratamiento:** Cualquier operación o conjunto de operaciones realizadas sobre datos personales: recolección, registro, organización, estructuración, conservación, modificación, consulta, comunicación, supresión, etc. Prácticamente cualquier acción que se realice con los datos entra en esta definición.

✔ Puntos clave

- Dato personal es cualquier información que identifique o haga identificable a una persona natural.
- Dato sensible es un tipo de dato personal que requiere mayor protección por su naturaleza.
- El titular es la persona a la que pertenecen los datos.
- El responsable define los fines y medios del tratamiento; el encargado lo ejecuta por cuenta del responsable.
- Tratamiento abarca cualquier operación con datos personales.

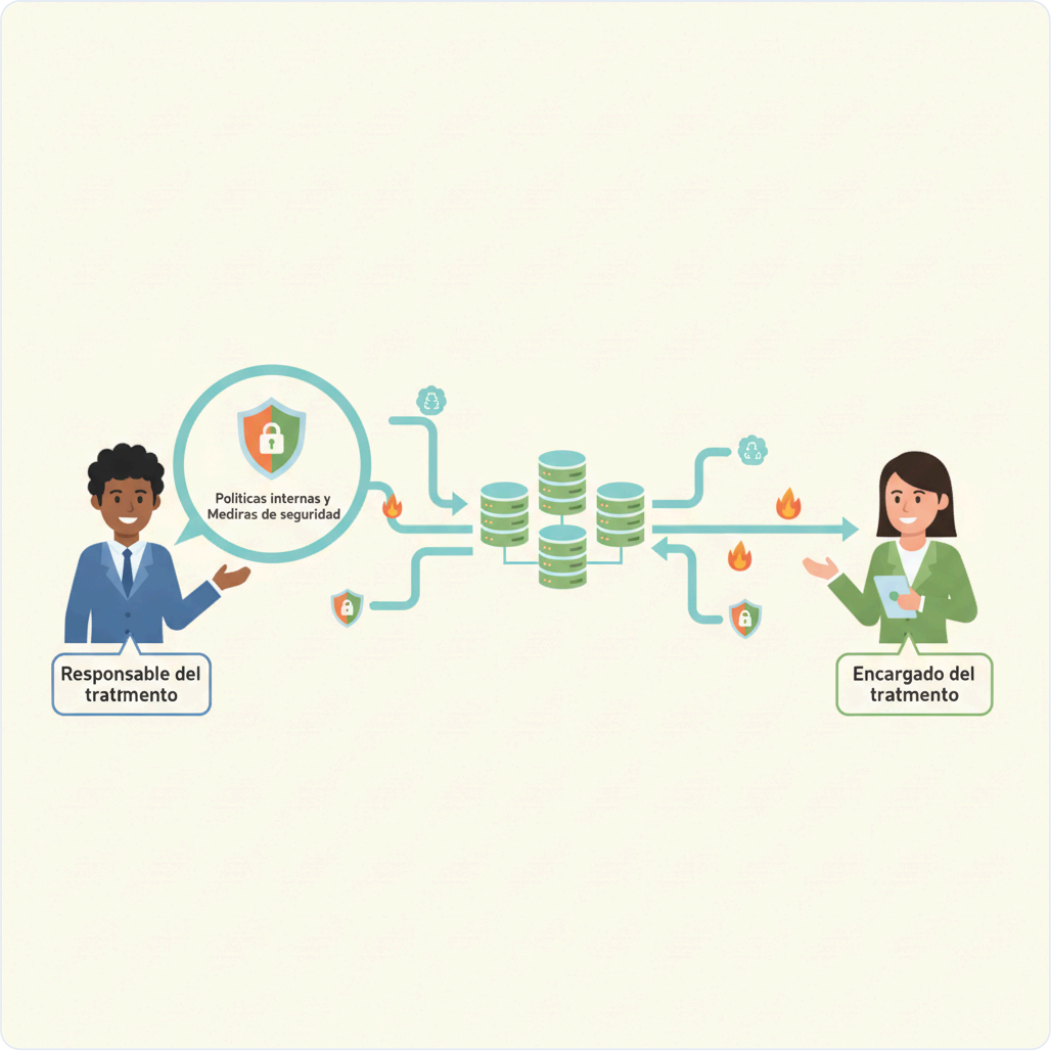
💭 Para reflexionar

- En mi rol, ¿qué tipo de datos personales y sensibles manejo regularmente?
- ¿Podría identificar si mi organización actúa como Responsable o Encargado del tratamiento en diferentes escenarios?
- ¿Con quiénes en mi equipo debería coordinar para identificar los datos sensibles que gestionamos?

3 Principios rectores I: licitud, lealtad, transparencia y finalidad

Ahora que conoces los actores, veamos las reglas del juego. La Ley 21.719 establece principios que deben orientar cada decisión de tratamiento de datos. Estos principios no son meras recomendaciones; son el corazón del cumplimiento y deben aplicarse en cada etapa del ciclo de vida del dato.

1. **Licitud:** Los datos personales deben tratarse de forma lícita, es decir, con fundamento en alguna de las bases de legitimación que establece la ley. Esto puede ser el consentimiento del titular, la ejecución de un contrato, el cumplimiento de una obligación legal, la protección de intereses vitales, el interés público, o el interés legítimo del responsable. No basta con tener los datos; es preciso tener una causa legal válida para procesarlos.
2. **Lealtad:** El tratamiento debe realizarse de manera leal, sin engaño ni abuso de confianza. Esto implica que los datos no pueden obtenerse mediante prácticas desleales, como engañar al titular sobre el propósito de la recolección, o a través de medios fraudulentos.
3. **Transparencia:** El titular tiene derecho a saber quién trata sus datos, para qué, durante cuánto tiempo, con quién se comparten y cuáles son sus derechos. La información debe ser clara, accesible y en lenguaje sencillo. Este principio se materializa en avisos de privacidad y políticas de tratamiento que deben ser fácilmente comprensibles.
4. **Finalidad:** Los datos deben ser recolectados con fines determinados, explícitos y legítimos, y no tratarse posteriormente de manera incompatible con dichos fines. Por ejemplo, si recolectas un correo electrónico para enviar una confirmación de compra, no puedes usarlo para enviar publicidad sin un nuevo consentimiento o una justificación legal para esa nueva finalidad. Si cambias el propósito original, en general deberás solicitar nuevo consentimiento o justificar la compatibilidad del nuevo fin con el original.



Comprender los roles de Responsable y Encargado es clave para una gestión eficiente y segura de los datos personales en cualquier organización.

✔ Puntos clave

- El tratamiento de datos debe basarse en una causa legal (licitud).
- Los datos deben obtenerse sin engaño o abuso de confianza (lealtad).
- El titular debe saber claramente cómo se usan sus datos (transparencia).
- Los datos solo deben usarse para los fines explícitos y legítimos para los que fueron recolectados (finalidad).

💭 Para reflexionar

- ¿Cómo aseguramos que el consentimiento que obtenemos de los clientes para el tratamiento de sus datos es lícito, leal y transparente?
- Si mi equipo decide reutilizar una base de datos de correos electrónicos para un nuevo fin, ¿qué pasos debemos seguir para cumplir el principio de finalidad?
- ¿Dónde puedo encontrar la política de privacidad de mi organización para entender cómo se aplica el principio de transparencia?

4 Principios rectores II: minimización y calidad

Continuamos con dos principios operativos esenciales: minimización y calidad. Ambos buscan que los datos tratados sean solo los necesarios, y que además sean exactos y estén actualizados. Aplicar estos principios eficientemente puede reducir riesgos y mejorar la eficiencia en la gestión de la información.

- **Principio de minimización (proporcionalidad):** Los datos personales deben ser adecuados, pertinentes y **no excesivos** en relación con los fines para los cuales son tratados. Solo debes solicitar y conservar aquellos datos que sean estrictamente necesarios para cumplir la finalidad declarada. Este principio también se conoce como «proporcionalidad» porque busca un equilibrio entre el dato solicitado y el objetivo.
  - *Implicancias prácticas:* Antes de diseñar un formulario o una base de datos para un nuevo proyecto (ej. registro de participantes para un evento), pregúntate: ¿realmente necesito este campo (p. ej., número de hijos, estado civil) para prestar el servicio o cumplir el contrato? Si la respuesta es no, elimínalo o hazlo opcional con consentimiento explícito y separado.
- **Principio de calidad (exactitud):** Los datos personales deben ser exactos y, cuando sea necesario, actualizados. Se deben adoptar medidas razonables para que los datos inexactos o incompletos, en relación con los fines para los que se tratan, sean suprimidos o rectificados sin dilación.
  - *Implicancias prácticas:* Implementa rutinas de verificación y actualización periódica de datos (p.ej., confirmar correo electrónico de clientes, validar dirección de envío en cada compra). Facilita al titular el ejercicio de su derecho de rectificación mediante un canal claro y accesible.

✔ Puntos clave

- Solo recolectar y conservar los datos estrictamente necesarios para la finalidad (minimización).
- Asegurar que los datos sean exactos y actualizados, rectificando o suprimiendo los incorrectos (calidad).

💭 Para reflexionar

- ¿Estamos recolectando datos excesivos en algún proceso actual de mi área? ¿Cuáles podrían ser?
- ¿Existen mecanismos en mi organización para que los titulares de los datos puedan solicitar la rectificación de su información?
- ¿Cómo podemos implementar un control de calidad para los datos que se registran diariamente en nuestros sistemas?

5 Principios de responsabilidad proactiva y seguridad

El corazón del nuevo modelo de protección de datos está en el principio de responsabilidad proactiva. Ya no basta con cumplir: ahora debes demostrar que cumples, anticiparte a los riesgos y aplicar medidas técnicas y organizativas robustas. Estos principios son fundamentales para construir una gestión de datos sólida y confiable.

- **Principio de responsabilidad proactiva (*accountability*):** El responsable del tratamiento es responsable del cumplimiento de los principios y debe ser capaz de **demostrarlo**. Esto implica adoptar políticas internas claras, implementar medidas técnicas y organizativas adecuadas, realizar evaluaciones de impacto de privacidad (DPIA), mantener registros de actividades de tratamiento, capacitar al personal y documentar todas estas acciones.
  - *Cambio de paradigma:* Se pasa de un modelo reactivo (esperar la denuncia o fiscalización) a uno **preventivo y documentado**. La carga de la prueba recae en la organización. Si hay una auditoría, la organización debe poder mostrar la evidencia de su cumplimiento.
- **Principio de seguridad:** El responsable y el encargado deben implementar medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo. Esto incluye proteger los datos contra tratamiento no autorizado o ilícito, pérdida, destrucción o daño accidental.
  - *Ejemplos de medidas:* Cifrado de datos, control de acceso basado en roles, copias de seguridad regulares, planes de continuidad de negocio y recuperación ante desastres, y auditorías de seguridad periódicas.
- **Principio de confidencialidad:** Toda persona que intervenga en cualquier fase del tratamiento de datos personales está obligada a guardar secreto respecto de estos, obligación que subsiste aun después de finalizada su relación con el responsable o encargado.
  - *Implicancias laborales:* Este principio se refuerza con acuerdos de confidencialidad en los contratos laborales, políticas internas claras sobre el manejo de información y sanciones disciplinarias para su incumplimiento.

✔ Puntos clave

- La organización debe demostrar activamente el cumplimiento de la ley (responsabilidad proactiva).
- Se deben aplicar medidas técnicas y organizativas para proteger los datos de riesgos (seguridad).
- El personal con acceso a datos debe guardar secreto sobre ellos, incluso después de su salida (confidencialidad).

💭 **Para reflexionar**

- ¿Qué documentos o registros existen en mi área que demuestren nuestro cumplimiento de la Ley 21.719?
- ¿Qué medidas de seguridad técnica y organizativa conozco que se apliquen a los datos que manejo?
- ¿Hemos firmado acuerdos de confidencialidad que incluyan la protección de datos personales?

6 La Agencia de Protección de Datos Personales (APDP)

Finalmente, conoce al nuevo guardián de la privacidad en Chile. La Agencia de Protección de Datos Personales (APDP) es la autoridad de control creada por la Ley 21.719 para fiscalizar, sancionar y orientar el cumplimiento. Su existencia consolida la protección de datos como un derecho fundamental.

La **Agencia de Protección de Datos Personales (APDP)** es un servicio público descentralizado, con personalidad jurídica y patrimonio propio, sometido a la supervigilancia del Presidente de la República a través del Ministerio de Justicia y Derechos Humanos. Es una entidad autónoma y técnica que tiene la misión de velar por el cumplimiento efectivo de la ley.

Entre sus **principales funciones** se encuentran:

- **Fiscalizar** el cumplimiento de la normativa sobre protección de datos personales, de oficio (por iniciativa propia) o a petición de parte (tras una denuncia).
- **Instruir procedimientos sancionatorios** y aplicar sanciones, que pueden ser multas de hasta 15.000 UTM en casos graves, o incluso la suspensión del tratamiento de datos.
- **Conocer y resolver reclamos** de titulares por vulneración de sus derechos, actuando como un mediador y garante de justicia.
- **Emitir directrices, instrucciones y recomendaciones** para interpretar y aplicar la ley, lo que es vital para las organizaciones que buscan cumplir con la normativa.
- **Autorizar transferencias internacionales** de datos a países que no posean un nivel adecuado de protección, asegurando que los datos chilenos estén protegidos incluso fuera del país.
- Llevar un **registro público de responsables y encargados** del tratamiento de datos, así como de las actividades de tratamiento que estos realizan, lo que aumenta la transparencia.
- **Promover la educación y concientización** sobre la protección de datos personales en la sociedad.

La APDP es un actor clave en el ecosistema de protección de datos, y su rol es fundamental para garantizar que los derechos de los titulares sean respetados y que las organizaciones operen dentro del marco legal.

✔ Puntos clave

- La APDP es la autoridad encargada de fiscalizar y aplicar la Ley 21.719.
- Tiene funciones de fiscalización, sanción, resolución de reclamos y emisión de directrices.
- Autoriza transferencias internacionales y promueve la concientización.
- Es un organismo descentralizado y autónomo.

💭 **Para reflexionar**

- ¿Cómo podría mi organización acceder a las directrices o recomendaciones que emita la APDP?
- Si un cliente presenta un reclamo ante la APDP, ¿cuál sería el procedimiento a seguir en mi organización?
- ¿Qué recursos educativos ofrece la APDP para concientizar al personal sobre la protección de datos?

🗺 Esquema del Módulo: Fundamentos de la Ley 21.719

El nuevo escenario	La Ley 21.719 protege el derecho a la privacidad de datos personales de personas naturales, aplicándose a todo tratamiento en el sector público y privado, con plena vigencia desde el 1 de diciembre de 2026. Establece un modelo de responsabilidad proactiva.
Conceptos clave	Define qué es un Dato Personal (identificable), Dato Sensible (mayor protección), Titular (dueño del dato), Responsable (define fines y medios), Encargado (trata por cuenta del Responsable) y Tratamiento (cualquier operación con datos).
Principios rectores I	Guían el tratamiento de datos: Licitud (base legal), Lealtad (sin engaño), Transparencia (informar al titular) y Finalidad (fines explícitos y legítimos).
Principios rectores II	Complementan la gestión de datos: Minimización (solo datos necesarios) y Calidad (datos exactos y actualizados).
Responsabilidad proactiva y seguridad	La organización debe demostrar cumplimiento (documentar, capacitar, DPIA), asegurar los datos (medidas técnicas/organizativas) y garantizar confidencialidad (secreto profesional).
Agencia de Protección de Datos Personales (APDP)	Autoridad de control con funciones de fiscalización, sanción, resolución de reclamos, emisión de directrices y promoción de la cultura de protección de datos en Chile.

En síntesis. La Ley N°21.719 no es solo una normativa, es un llamado a la responsabilidad y a la ética en el manejo de la información personal. Al reconocer su objeto, sus conceptos clave y sus principios rectores, cada miembro de la organización contribuye a un entorno más seguro y confiable. La protección de datos es una tarea continua que requiere compromiso y adaptación. Al internalizar estos fundamentos, estamos sentando las bases para construir una cultura organizacional que valora y respeta la privacidad de todos.