APUNTES DEL MÓDULO 1

Fundamentos, conceptos y principios de la Ley 21.719

Protección de Datos Personales (Ley 21.719) — Aplicación por rol (Encargados, Jefaturas y RRHH) (imagen real)

Material de estudio

Módulo 1

Apunte descargable del estudiante

Contenido del módulo

La **Ley N°21.719 sobre Protección de Datos Personales** representa un cambio de paradigma en Chile: desde un modelo reactivo de protección a uno de **responsabilidad proactiva**, alineado con estándares internacionales como el RGPD europeo. A partir del **1 de diciembre de 2026**, todas las organizaciones —públicas y privadas— deben cumplir íntegramente con esta normativa, garantizando el derecho a la privacidad y protección de datos personales de las personas naturales. Este módulo te permitirá dominar los conceptos clave, principios rectores y alcance de la ley, para que puedas aplicarla correctamente en tu rol profesional, ya seas encargado de tratamiento, jefatura o parte del equipo de Recursos Humanos.

1 El nuevo escenario: objeto, alcance y entrada en vigencia de la Ley 21.719

La **Ley N°21.719** 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. Esta protección no es meramente declarativa: implica obligaciones concretas, controles y sanciones severas para quien incumpla.

Ámbito de aplicación: La ley se aplica a *todo tratamiento de datos personales*, sea total o parcialmente automatizado (bases de datos digitales, CRM, sistemas de nómina), y también al tratamiento *no automatizado* de datos contenidos en registros físicos o destinados a ser incluidos en ellos (archivadores, carpetas de personal). Se aplica tanto al **sector público** (ministerios, municipalidades, servicios públicos, empresas del Estado) como al **sector privado** (empresas, fundaciones, ONG, profesionales independientes que traten datos).

Excepciones: Quedan fuera del alcance de la ley los tratamientos exclusivamente personales o domésticos (tu agenda personal de contactos, álbum familiar), y aquellos vinculados a seguridad nacional, defensa o investigación criminal, que se rigen por normativas especiales.

Entrada en vigencia plena: La ley entró en vigor de manera gradual, con su **aplicación plena a partir del 1 de diciembre de 2026**. Desde esa fecha, todas las organizaciones deben cumplir íntegramente: tener políticas de privacidad actualizadas, registros de actividades de tratamiento, medidas de seguridad implementadas, y capacidad de atender derechos de los titulares.

Sector	Ejemplos de organizaciones obligadas	Tipos de datos que suelen tratar
Privado	Empresas de retail, plataformas digitales, clínicas, bancos, consultoras, startups	Datos de clientes, colaboradores, proveedores, usuarios web
Público	Ministerios, servicios públicos, municipalidades, hospitales públicos, universidades estatales	Datos de funcionarios, ciudadanos beneficiarios de programas, pacientes, estudiantes

Ejemplo laboral: Si diriges el área de compliance de una empresa de retail con plataforma digital, debes asegurar que tanto los datos recolectados en tienda física (programa de fidelización) como en el e-commerce (compras online, historial de navegación, cookies) cumplan con la ley desde el 1 de diciembre de 2026. Esto incluye revisar contratos con proveedores de servicios cloud, auditar bases de datos heredadas y capacitar a equipos de ventas y marketing.

Equipo de compliance revisando el cumplimiento de la Ley 21.719: la responsabilidad proactiva exige documentación, controles y capacitación continua en toda la organización.

✔ Puntos clave

- La Ley 21.719 protege el derecho a la privacidad y los datos personales de personas naturales, con aplicación plena desde el 1 de diciembre de 2026.
- Se aplica a todo tratamiento automatizado y no automatizado, en sectores público y privado, salvo excepciones específicas.
- Marca el paso de un modelo reactivo a uno de responsabilidad proactiva, alineado con estándares internacionales.

💭 **Para reflexionar**

- ¿Qué tipos de tratamientos de datos realiza mi organización: automatizados, no automatizados, o ambos?
- ¿Estamos preparados para demostrar cumplimiento desde el 1 de diciembre de 2026 en todas nuestras operaciones?
- ¿Existen tratamientos en mi área que podrían quedar fuera del alcance de la ley (excepciones) o todos están regulados?

2 Conceptos clave: datos, titulares y actores del tratamiento

Para implementar la ley, es fundamental dominar el **lenguaje técnico-jurídico** que establece. Estos conceptos son la base sobre la que se construyen las obligaciones y derechos.

Dato personal: Toda información concerniente a una *persona natural identificada o identificable*. No se limita a nombre y RUT: incluye correo electrónico, número de teléfono, dirección IP, huella digital, fotografía, geolocalización, matrícula de vehículo, preferencias de consumo, historial de compras, evaluaciones de desempeño. Si con esa información puedes identificar directa o indirectamente a una persona, es un dato personal.

Dato sensible: Categoría especial de datos personales que revelan **origen étnico o racial, opiniones políticas, convicciones religiosas o filosóficas, afiliación sindical, datos genéticos, datos biométricos dirigidos a identificar unívocamente a una persona, datos de salud, vida sexual u orientación sexual**. Su tratamiento exige **mayores garantías**: en general, consentimiento explícito del titular o una causa legal muy específica. Ejemplo laboral: si implementas control de acceso con huella dactilar (dato biométrico) o solicitas certificados médicos (datos de salud), estás tratando datos sensibles y debes extremar precauciones.

Titular: La persona natural a quien se refieren los datos personales. Es el **sujeto protegido** por la ley y titular de derechos (acceso, rectificación, supresión, portabilidad, oposición).

Responsable del tratamiento: Persona natural o jurídica, pública o privada, que **determina los fines y medios del tratamiento**. Es quien decide *qué datos recoger, para qué, cómo almacenarlos, con quién compartirlos y cuánto tiempo conservarlos*. Ejemplo: tu empresa es responsable del tratamiento de datos de empleados y clientes. **El responsable asume las obligaciones principales** de la ley: implementar medidas de seguridad, atender derechos, notificar brechas, etc.

Encargado del tratamiento: Persona natural o jurídica que **trata datos personales por cuenta del responsable**, siguiendo sus instrucciones. No decide los fines ni medios, solo ejecuta. Ejemplo: si contratas una empresa externa de nómina (payroll), esa empresa es encargada del tratamiento de datos de tus colaboradores; tú sigues siendo el responsable. La relación debe formalizarse mediante un **contrato de encargo** que detalle objeto, duración, obligaciones de seguridad y confidencialidad.

Tratamiento: Cualquier operación o conjunto de operaciones realizadas sobre datos personales: *recolección, registro, organización, estructuración, conservación, adaptación, modificación, extracción, consulta, utilización, comunicación por transmisión, difusión, interconexión, limitación, supresión o destrucción*. Desde que pides un correo electrónico en un formulario hasta que eliminas ese dato de tu servidor, estás realizando tratamiento.

Actor	Pregunta clave	Ejemplo laboral
Responsable	¿Quién decide el «qué» y el «cómo»?	Tu empresa decide recolectar CVs para selección de personal
Encargado	¿Quién ejecuta por instrucciones?	Plataforma de reclutamiento externa que almacena los CVs en tu nombre

Actor	Pregunta clave	Ejemplo laboral
Titular	¿De quién son los datos?	El postulante que envió su CV y tiene derechos sobre sus datos

Ejemplo integrado: En RRHH, tú (empresa) eres **responsable** del tratamiento de datos de postulantes y empleados. Si usas una plataforma cloud de gestión de talento, esa plataforma es tu **encargado**. Los postulantes y empleados son los **titulares**, y cada acción que realizas con sus datos (recibir CV, almacenar en sistema, revisar para evaluación, archivar por periodo legal) constituye **tratamiento**.

✔ Puntos clave

- Dato personal: toda información que identifica o hace identificable a una persona natural; dato sensible: categoría especial con mayores garantías.
- Responsable: decide fines y medios del tratamiento y asume obligaciones principales; encargado: ejecuta por cuenta del responsable.
- Tratamiento: cualquier operación sobre datos, desde recolección hasta supresión; la relación responsable-encargado debe formalizarse por contrato.

💭 Para reflexionar

- ¿Soy responsable o encargado del tratamiento en mi organización? ¿O ambos, según el caso?
- ¿Qué datos sensibles tratamos en mi área y qué garantías adicionales estamos implementando?
- ¿Tenemos contratos de encargo formalizados con todos nuestros proveedores que acceden a datos personales (cloud, outsourcing, consultoras)?

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

La Ley 21.719 establece **principios rectores** que deben orientar *cada decisión de tratamiento*. No son meras declaraciones: son mandatos vinculantes cuyo incumplimiento puede derivar en sanciones. Iniciamos con cuatro principios fundamentales.

1. Principio de licitud: Los datos personales deben tratarse de forma **lícita**, es decir, con fundamento en alguna de las **bases de legitimación** que establece la ley. No basta con tener acceso a los datos; debes tener una **causa legal válida** para procesarlos. Las bases de legitimación incluyen: *consentimiento del titular, ejecución de un contrato, cumplimiento de una obligación legal, protección de intereses vitales, ejercicio de función pública o interés público, interés legítimo del responsable (siempre que no prevalezcan derechos del titular)*. Antes de recoger o usar datos, pregúntate: **¿cuál es mi base legal?**

Ejemplo laboral: En RRHH, tratas datos de empleados con base en la *ejecución del contrato de trabajo* (nómina, evaluaciones) y en el *cumplimiento de obligaciones legales* (declaración de impuestos, cotizaciones previsionales). No necesitas consentimiento para estos tratamientos, pero sí debes informar al titular. En cambio, si quieres publicar la foto del empleado en la intranet para el directorio interno, necesitas su *consentimiento explícito* (base de legitimación distinta).

2. Principio de lealtad: El tratamiento debe realizarse de manera **leal**, sin engaño, manipulación ni abuso de confianza. No puedes obtener datos mediante prácticas desleales o fraudulentas. Ejemplo: no puedes ocultar en letra pequeña que los datos del formulario de contacto serán usados para marketing, o inducir al titular a dar consentimiento mediante patrones oscuros (dark patterns) en tu sitio web.

Ejemplo laboral: Si implementas un programa de bienestar y solicitas datos de salud de colaboradores, debes ser **transparente y leal**: explicar claramente que es voluntario, qué harás con esos datos, quién tendrá acceso, y que no habrá consecuencias laborales adversas por no participar.

3. Principio de transparencia: El titular tiene **derecho a saber** quién trata sus datos, para qué fines, durante cuánto tiempo, con quién se comparten, bajo qué medidas de seguridad, y cuáles son sus derechos (acceso, rectificación, supresión, portabilidad, oposición). La información debe ser **clara, accesible, en lenguaje sencillo y oportuna**. Este principio se materializa en **avisos de privacidad** (al momento de recoger datos) y **políticas de tratamiento** (documento general accesible).

Ejemplo laboral: Al contratar un nuevo empleado, debes entregarle un **aviso de privacidad laboral** que explique qué datos personales recogerás (datos de contacto, de dependientes para cargas familiares, cuentas bancarias, certificados de estudios, antecedentes laborales), para qué fines (gestión de contrato, nómina, capacitación, evaluación de desempeño), quiénes tendrán acceso (área RRHH, jefatura directa, proveedores de nómina), cuánto tiempo los conservarás (durante la relación laboral y según plazos legales posteriores), y cómo ejercer sus derechos.

4. Principio de finalidad: Los datos deben ser recolectados con **fines determinados, explícitos y legítimos**, y **no tratarse posteriormente de manera incompatible con dichos fines**. Si decides cambiar el propósito original del tratamiento, en general deberás solicitar **nuevo consentimiento** del titular o demostrar que el nuevo fin es compatible con el original.

Ejemplo laboral: Si recolectaste datos de clientes para procesar una compra (finalidad: ejecución de contrato), **no puedes** usarlos automáticamente para enviar publicidad de terceros (finalidad incompatible)

sin obtener consentimiento adicional. En cambio, usar esos datos para informar sobre el estado del pedido o políticas de devolución sí es compatible con la finalidad original.

- **Licitud:** ¿Tengo base legal válida para este tratamiento?
- **Lealtad:** ¿Estoy actuando de buena fe, sin engaño?
- **Transparencia:** ¿El titular sabe claramente qué hago con sus datos?
- **Finalidad:** ¿Para qué recolecté estos datos y estoy respetando ese propósito?

✔ Puntos clave

- Licitud: todo tratamiento requiere una base legal válida (consentimiento, contrato, ley, interés legítimo, etc.); identifica cuál aplica en cada caso.
- Lealtad y transparencia: informa al titular de manera clara, accesible y oportuna; no engañes ni manipules.
- Finalidad: define fines específicos y explícitos al recoger datos; no los uses para propósitos incompatibles sin nueva legitimación.

💭 Para reflexionar

- ¿Cuál es la base de legitimación para cada tipo de tratamiento que realizo en mi área (consentimiento, contrato, ley, interés legítimo)?
- ¿Nuestros avisos de privacidad y políticas de tratamiento son claros, accesibles y están actualizados con todos los elementos de transparencia?
- ¿Hemos cambiado alguna vez la finalidad del tratamiento de datos sin informar o solicitar nuevo consentimiento al titular?

4 Principios rectores II: minimización, calidad y limitación de plazo

Continuamos con tres principios **operativos** esenciales que determinan *qué datos recoger, cómo mantenerlos y cuánto tiempo conservarlos*.

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 obliga a un ejercicio riguroso de **autodisciplina**: antes de pedir un dato, justifica su necesidad.

Implicancias prácticas: Antes de diseñar un formulario de registro, un formato de postulación o una encuesta interna, pregúntate campo por campo: *¿realmente necesito este dato para prestar el servicio, cumplir el contrato o ejecutar el proceso?* Si la respuesta es no, **elimínalo** o hazlo **opcional** con consentimiento explícito y finalidad específica.

Ejemplo laboral (RRHH): Al reclutar, es legítimo pedir nombre, contacto, formación académica, experiencia laboral (datos pertinentes para evaluar idoneidad). **No es proporcional** exigir estado civil, número de hijos, religión o fotografía (salvo que el cargo lo justifique específicamente, como modelo o actor). Si incluyes estos campos, debes justificar su necesidad o hacerlos opcionales con consentimiento.

Ejemplo laboral (Marketing): Si ofreces un webinar gratuito, puedes pedir nombre, correo y empresa (datos mínimos para enviar acceso). **No debes exigir** teléfono, cargo, RUT, dirección postal, salvo que tengan relación directa con la finalidad (por ejemplo, envío de certificado físico posterior).

Principio de calidad (exactitud): Los datos personales deben ser **exactos y, cuando sea necesario, actualizados**. Debes 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**: confirmación de correo electrónico mediante doble opt-in, validación de dirección al enviar correspondencia, recordatorios anuales a empleados para actualizar datos de contacto y cargas familiares. Facilita al titular el **ejercicio de su derecho de rectificación** mediante canales sencillos (botón «actualizar mis datos», formulario web, correo de contacto).

Ejemplo laboral (RRHH): Cada año, solicita a los empleados que revisen y actualicen sus datos personales (dirección, teléfono, contacto de emergencia, cargas familiares para asignación familiar). Si un empleado notifica un cambio de domicilio y no actualizas el sistema, puedes enviar información confidencial a una dirección incorrecta (incumplimiento de calidad y seguridad).

Principio de limitación del plazo de conservación: Los datos personales deben conservarse **solo durante el tiempo necesario** para cumplir los fines para los cuales fueron recolectados, o durante los plazos legales de conservación exigidos por otras normativas (tributarias, laborales, etc.). Cumplido el plazo, los datos deben ser **eliminados o anonimizados**.

Implicancias prácticas: Define **plazos de retención** para cada categoría de datos: CVs de postulantes no seleccionados (ejemplo: 1 año, salvo consentimiento para mantenerlos en base de talentos), registros de clientes inactivos (ejemplo: 3 años sin compras), datos de empleados tras término de relación laboral

(según plazos legales tributarios y laborales: generalmente 5 a 10 años). Implementa **rutinas automáticas de eliminación** y documenta el proceso.

Ejemplo laboral (RRHH): Un postulante envió su CV para una vacante en 2022 y no fue seleccionado. Si no obtuviste su consentimiento para mantener sus datos en una base de talentos, debes **eliminar su CV y datos asociados** transcurrido un plazo razonable (por ejemplo, 1 año). Si lo conservas indefinidamente «por si acaso», incumples el principio de limitación de plazo.

Principio	Pregunta clave	Herramienta práctica
Minimización	¿Es estrictamente necesario este dato?	Revisión campo por campo de formularios; matriz de necesidad vs. finalidad
Calidad	¿Están los datos exactos y actualizados?	Validaciones automáticas; recordatorios periódicos de actualización; canal de rectificación
Limitación de plazo	¿Cuánto tiempo debo conservar estos datos?	Tabla de retención documental; rutinas automáticas de eliminación; logs de borrado

✔ Puntos clave

- Minimización: solo recoger datos adecuados, pertinentes y no excesivos; revisar formularios y eliminar campos innecesarios.
- Calidad: mantener datos exactos y actualizados; implementar verificaciones periódicas y facilitar la rectificación al titular.
- Limitación de plazo: conservar datos solo el tiempo necesario o legal; definir plazos de retención y eliminar o anonimizar al cumplirse.

💭 Para reflexionar

- ¿Hemos revisado nuestros formularios, contratos y sistemas para eliminar campos de datos que no son estrictamente necesarios?
- ¿Tenemos procedimientos para verificar y actualizar periódicamente los datos personales que tratamos?
- ¿Hemos definido plazos de retención claros para cada categoría de datos y contamos con procesos de eliminación al cumplirse esos plazos?

5 Principios de responsabilidad proactiva, seguridad y confidencialidad

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.

Principio de responsabilidad proactiva (accountability): El responsable del tratamiento es responsable del cumplimiento de todos los principios de la ley y debe ser capaz de **demostrarlo**. Esto implica adoptar **políticas internas** de protección de datos, implementar **medidas técnicas y organizativas** apropiadas, realizar **evaluaciones de impacto** en tratamientos de alto riesgo, mantener **registros de actividades de tratamiento**, **capacitar al personal**, designar un **delegado de protección de datos** (cuando corresponda), y **documentar todas estas acciones**.

Cambio de paradigma: Se pasa de un modelo *reactivo* (esperar la denuncia, fiscalización o sanción) a uno **preventivo y documentado**. La **carga de la prueba** recae en la organización: si la Agencia de Protección de Datos Personales (APDP) te fiscaliza, debes demostrar con evidencia documental que has cumplido. «No sabía» o «lo hacíamos de buena fe» no son excusas válidas.

Herramientas de accountability:

- **Registro de actividades de tratamiento:** inventario detallado de todos los tratamientos que realizas (qué datos, para qué, base legal, destinatarios, plazos de retención, medidas de seguridad).
- **Evaluaciones de impacto en privacidad (DPIA):** análisis de riesgos para tratamientos que puedan implicar alto riesgo para derechos y libertades (tratamiento masivo de datos sensibles, decisiones automatizadas, videovigilancia extensiva, etc.).
- **Políticas y procedimientos internos:** política de privacidad, política de seguridad de la información, protocolos de respuesta a brechas, guías para atender derechos de titulares.
- **Capacitación continua:** programas de formación para todos los colaboradores que traten datos, adaptados a su rol.
- **Auditorías y controles:** revisiones periódicas del cumplimiento, auditorías internas o externas, pruebas de seguridad.

Ejemplo laboral (Jefatura de TI): Implementas un nuevo CRM cloud para gestionar datos de clientes. Bajo accountability, debes: (1) evaluar el riesgo del tratamiento (DPIA si es masivo o sensible); (2) seleccionar un proveedor que ofrezca garantías de cumplimiento (certificaciones, cláusulas contractuales); (3) formalizar un contrato de encargo; (4) configurar el CRM con medidas de seguridad (cifrado, control de acceso por roles); (5) capacitar a ventas y marketing en uso seguro; (6) registrar esta actividad de tratamiento; (7) documentar todo el proceso. Si hay una brecha de seguridad, deberás demostrar que actuaste con diligencia.

Principio de seguridad: El responsable y el encargado deben implementar **medidas técnicas y organizativas apropiadas** para garantizar un **nivel de seguridad adecuado al riesgo**, protegiendo los datos contra tratamiento no autorizado o ilícito, pérdida, destrucción o daño accidental. Las medidas deben ser **proporcionales al riesgo**: mayor riesgo (datos sensibles, gran volumen, tratamiento automatizado), mayor nivel de protección.

Medidas técnicas: cifrado de datos en tránsito y en reposo, control de acceso basado en roles (RBAC), autenticación multifactor, firewalls, antivirus, copias de seguridad periódicas, anonimización o seudonimización cuando sea posible.

Medidas organizativas: políticas de seguridad, procedimientos de control de acceso físico, gestión de incidentes de seguridad, planes de continuidad del negocio, cláusulas de confidencialidad en contratos.

Ejemplo laboral (RRHH): Almacenas datos sensibles de empleados (certificados médicos, licencias médicas). Medidas de seguridad apropiadas incluyen: (1) carpeta física en archivador con cerradura, acceso restringido a jefatura RRHH; (2) versión digital en carpeta cifrada de servidor, acceso solo con credenciales autorizadas y registro de accesos (log); (3) contratos de confidencialidad firmados por todo el equipo RRHH; (4) protocolo de eliminación segura (destrucción física de papel, borrado seguro de archivos digitales).

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. El incumplimiento puede generar responsabilidad laboral (despido), civil (indemnización) y penal.

Implicancias prácticas: Incorpora **cláusulas de confidencialidad** en contratos de trabajo, contratos de prestación de servicios y acuerdos con encargados. Implementa **políticas internas** que establezcan claramente la obligación de confidencialidad y las consecuencias de su incumplimiento (sanciones disciplinarias). Capacita regularmente sobre la importancia de la confidencialidad y los riesgos de compartir datos personales sin autorización (por WhatsApp, correo personal, conversaciones informales).

Ejemplo laboral (Jefatura): Un colaborador de tu equipo comenta en una reunión social datos personales de un cliente («fulano compró tal producto, tiene tal problema»). Aunque no haya mala intención, es una **violación de confidencialidad**. Debes investigar, aplicar medidas disciplinarias según gravedad, reforzar capacitación y revisar controles para evitar repetición.

✔ Puntos clave

- Responsabilidad proactiva (accountability): no basta cumplir, debes demostrarlo con políticas, registros, evaluaciones de impacto, capacitación y documentación.
- Seguridad: implementar medidas técnicas (cifrado, control de acceso, copias de seguridad) y organizativas (políticas, procedimientos) proporcionales al riesgo.
- Confidencialidad: obligación de secreto para toda persona que intervenga en el tratamiento, que subsiste tras finalizar la relación; incumplimiento genera responsabilidad.

💭 Para reflexionar

- ¿Contamos con un registro de actividades de tratamiento actualizado y evaluaciones de impacto para tratamientos de alto riesgo?
- ¿Las medidas de seguridad implementadas (técnicas y organizativas) son proporcionales al nivel de riesgo de los datos que tratamos?
- ¿Todos los colaboradores y proveedores que acceden a datos personales han firmado cláusulas de confidencialidad y recibido capacitación sobre su obligación de secreto?

6 La Agencia de Protección de Datos Personales (APDP): el guardián de la privacidad

La Ley 21.719 crea una nueva **autoridad de control** en Chile: la **Agencia de Protección de Datos Personales (APDP)**. Es el órgano fiscalizador, sancionador y orientador del cumplimiento de la normativa, con amplias facultades y sanciones severas para quien incumpla.

Naturaleza jurídica: La 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. Esto le otorga **autonomía técnica** para ejercer sus funciones sin injerencia política directa.

Principales funciones de la APDP:

- **Fiscalizar** el cumplimiento de la normativa sobre protección de datos personales, de oficio (por iniciativa propia) o a petición de parte (por reclamo de un titular o denuncia de terceros).
- **Instruir procedimientos sancionatorios** y aplicar sanciones administrativas: *amonestación, multa de hasta 15.000 UTM en casos graves o reiterados* (más de 800 millones de pesos al valor actual), y en casos extremos, *clausura temporal o definitiva de bases de datos*.
- **Conocer y resolver reclamos** de titulares por vulneración de sus derechos (acceso, rectificación, supresión, portabilidad, oposición). La APDP puede ordenar al responsable o encargado adoptar medidas correctivas.
- **Emitir directrices, instrucciones y recomendaciones** para interpretar y aplicar la ley, facilitando el cumplimiento por parte de organizaciones y orientando sobre mejores prácticas.
- **Autorizar transferencias internacionales** de datos a países que no cuenten con un nivel adecuado de protección, mediante cláusulas contractuales tipo, normas corporativas vinculantes u otros mecanismos de garantía.
- **Llevar un Registro de Responsables y Encargados** de tratamiento (obligatorio para ciertos sectores o tipos de tratamiento), facilitando la transparencia y el control.
- **Promover la educación y difusión** de derechos y obligaciones en materia de protección de datos personales.

Procedimiento sancionatorio: Si la APDP detecta un incumplimiento (por fiscalización o reclamo), puede iniciar un procedimiento sancionatorio. El responsable o encargado tiene derecho a defensa y a presentar descargos. Si se confirma la infracción, la APDP graduará la sanción considerando: *naturaleza, gravedad y duración de la infracción; carácter sensible de los datos; daño causado; intencionalidad; medidas adoptadas para mitigar el daño; grado de responsabilidad; antecedentes de infracciones previas; grado de cooperación con la APDP*.

Infracciones graves: Tratamiento sin base legal, tratamiento de datos sensibles sin consentimiento o causa legal específica, no atender derechos del titular, no notificar brechas de seguridad, transferencia internacional ilícita, obstaculizar la fiscalización de la APDP. **Sanciones: multas elevadas, órdenes de cesación inmediata del tratamiento, clausura de bases de datos, publicación de la sanción (daño reputacional)**.

Ejemplo laboral (Director de Compliance): La APDP fiscaliza tu empresa y detecta que no has implementado medidas de seguridad adecuadas para proteger datos sensibles de empleados (certificados médicos en carpeta compartida sin cifrado, accesible por múltiples personas no autorizadas). Inicia un procedimiento sancionatorio. Tú presentas descargos, pero la APDP confirma la infracción. Sanción: multa de 5.000 UTM (más de 260 millones de pesos) y orden de implementar medidas correctivas en 30 días, bajo apercibimiento de clausura de la base de datos. Además, la sanción se publica en el sitio web de la APDP, generando daño reputacional para tu empresa.

Importancia de la cooperación con la APDP: Colaborar activamente con la Agencia, responder oportunamente sus requerimientos, adoptar medidas correctivas voluntarias y demostrar accountability puede **atenuar significativamente las sanciones**. En cambio, obstaculizar, ocultar información o reincid incurrir genera agravantes.

Recursos: Las resoluciones de la APDP pueden ser reclamadas ante los tribunales de justicia, pero la carga de la prueba recae en quien reclama (debes demostrar que la decisión de la APDP es ilegal o arbitraria).

Función de la APDP	Impacto para las organizaciones
Fiscalización	Auditorías sorpresa, requerimientos de información, inspecciones in situ
Sancionatoria	Multas de hasta 15.000 UTM, clausura de bases de datos, daño reputacional
Resolución de reclamos	Órdenes de rectificación, supresión, limitación; compensación al titular
Orientación	Directrices y recomendaciones que facilitan el cumplimiento y reducen incertidumbre

Recomendación final: Establece un **canal directo de comunicación con la APDP**, mantente informado sobre sus directrices y orientaciones, y adopta una postura de **cumplimiento proactivo y cooperación**. No esperes a ser fiscalizado: anticípate, implementa, documenta y mejora continuamente tus prácticas de protección de datos.

✔ Puntos clave

- La APDP es la autoridad de control con facultades de fiscalización, sanción (multas hasta 15.000 UTM), resolución de reclamos y emisión de directrices.
- Las infracciones graves (tratamiento ilícito, no atender derechos, brechas no notificadas) pueden derivar en multas millonarias, clausura de bases de datos y daño reputacional.
- La cooperación con la APDP, el cumplimiento proactivo y la demostración de accountability atenúan sanciones; obstaculizar genera agravantes.

💭 **Para reflexionar**

- ¿Estamos preparados para responder oportunamente a un requerimiento de fiscalización de la APDP con evidencia documental de cumplimiento?
- ¿Conocemos las directrices y recomendaciones emitidas por la APDP aplicables a nuestro sector o tipo de tratamiento?
- ¿Tenemos un plan de acción para atender una eventual sanción o reclamo ante la APDP, incluyendo capacidad de respuesta y medidas correctivas?

🗺 Mapa conceptual: Ley 21.719 – Fundamentos, conceptos y principios

Objeto y alcance de la Ley 21.719	Proteger privacidad y datos personales de personas naturales; aplicación plena desde 1/dic/2026 a sectores público y privado, tratamientos automatizados y no automatizados.
Actores y conceptos clave	Dato personal (identificación), dato sensible (categoría especial); titular (sujeto protegido); responsable (decide fines/medios); encargado (ejecuta por cuenta); tratamiento (toda operación sobre datos).
Principios rectores (I): licitud, lealtad, transparencia, finalidad	Base legal válida para tratar; buena fe sin engaño; información clara y accesible al titular; fines determinados, explícitos y legítimos.
Principios rectores (II): minimización, calidad, limitación de plazo	Datos adecuados, pertinentes, no excesivos; exactitud y actualización; conservación solo durante tiempo necesario o legal, luego eliminación.
Responsabilidad proactiva, seguridad y confidencialidad	Accountability: demostrar cumplimiento con políticas, registros, DPIA, capacitación; medidas técnicas/organizativas proporcionales al riesgo; obligación de secreto.
Agencia de Protección de Datos Personales (APDP)	Autoridad de control: fiscaliza, sanciona (multas hasta 15.000 UTM), resuelve reclamos, emite directrices, autoriza transferencias internacionales.

En síntesis. Has completado el recorrido por los **fundamentos, conceptos clave y principios rectores de la Ley N°21.719**. Ahora comprendes el objeto y alcance de la normativa, distingues entre datos personales y sensibles, identificas los roles de responsable y encargado, y conoces los principios que deben guiar cada decisión de tratamiento: licitud, lealtad, transparencia, finalidad, minimización, calidad, limitación de plazo, responsabilidad proactiva, seguridad y confidencialidad. También sabes que la **Agencia de Protección de Datos Personales (APDP)** fiscaliza y sanciona con rigor el incumplimiento. El siguiente paso es llevar este conocimiento a la práctica en tu rol específico: aplicar estos principios en tus procesos diarios, implementar controles, documentar tu

cumplimiento y desarrollar una **cultura de protección de datos** en tu organización. La Ley 21.719 no es solo una obligación legal: es una oportunidad para generar confianza, diferenciarte en el mercado y proteger los derechos fundamentales de las personas con quienes trabajas. **¡Adelante, el desafío es tuyo!**