APUNTES DEL MÓDULO 1

Fundamentos, conceptos y principios de la Ley 21.719

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

Material de estudio

Módulo 1

Apunte descargable del estudiante

Contenido del módulo

La entrada en vigencia plena de la **Ley N°21.719 sobre Protección de Datos Personales** el 1 de diciembre de 2026 marca un punto de inflexión para todas las organizaciones en Chile. Este módulo te permitirá comprender el objeto de la ley, dominar los conceptos esenciales que estructuran la normativa y reconocer los principios rectores que deben guiar cada tratamiento de datos personales en tu ámbito laboral. Pasaremos de un enfoque reactivo a uno de **responsabilidad proactiva**, donde demostrar el cumplimiento es tan importante como cumplir.

1 El objeto y alcance de la Ley 21.719: un nuevo paradigma de protección

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. Esta normativa representa un cambio de paradigma desde un modelo reactivo —donde se actuaba tras denuncias o fiscalizaciones— hacia uno de **responsabilidad proactiva**, alineado con estándares internacionales como el Reglamento General de Protección de Datos (RGPD) de la Unión Europea.

Ámbito de aplicación: La ley 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 incluye desde bases de datos digitales de clientes hasta archivos físicos de fichas de personal.

Sector	Alcance y ejemplos
Privado	Empresas de retail, clínicas, bancos, plataformas digitales, fundaciones, ONG que traten datos personales de clientes, trabajadores o beneficiarios.
Público	Ministerios, servicios públicos, municipalidades, empresas del Estado que gestionen datos de ciudadanos, funcionarios o usuarios.

Excepciones relevantes: La ley no se aplica a tratamientos realizados por personas naturales en el ejercicio de actividades exclusivamente personales o domésticas (por ejemplo, tu agenda personal de contactos), ni a aquellos vinculados a seguridad nacional o defensa, que se rigen por normativa especial.

Entrada en vigencia: La ley entró en vigor gradualmente, con su aplicación plena desde el **1 de diciembre de 2026**. A partir de esa fecha, todas las organizaciones deben cumplir íntegramente con sus obligaciones, incluyendo la implementación de políticas internas, registros de actividades de tratamiento y medidas de seguridad.

Ejemplo laboral: Si trabajas en el área de recursos humanos de una empresa manufacturera, a partir de diciembre de 2026 deberás asegurar que el tratamiento de datos de postulantes, trabajadores activos y ex trabajadores (fichas médicas, evaluaciones de desempeño, registros de asistencia) cumpla con todos los principios y obligaciones de la ley, y que puedas demostrar ese cumplimiento ante la Agencia de Protección de Datos Personales.

La Ley 21.719 protege los datos personales mediante principios rectores y un modelo de responsabilidad proactiva, resguardando la privacidad de las personas naturales en todos los tratamientos.

✔ Puntos clave

- La Ley 21.719 protege el derecho a la privacidad y a la protección de datos personales de personas naturales.
- Se aplica a tratamientos automatizados y no automatizados en registros, tanto en el sector público como privado.
- Su vigencia plena desde el 1 de diciembre de 2026 exige cumplimiento integral y demostrable.
- Representa un cambio hacia la responsabilidad proactiva, alineado con estándares internacionales.

💭 Para reflexionar

- ¿Qué tratamientos de datos personales realiza tu área o departamento actualmente?
- ¿Tu organización cuenta con políticas documentadas para demostrar el cumplimiento de la ley desde diciembre de 2026?
- ¿Existen tratamientos en tu trabajo que puedan calificar como excepciones a la ley?

2 Conceptos clave: datos, titulares y actores del tratamiento

Para implementar la ley en tu organización, es fundamental dominar el lenguaje jurídico que estructura la normativa. A continuación, definimos los conceptos esenciales.

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, preferencias de consumo, historial de compras, datos de navegación web, entre muchos otros. Una persona es identificable si puede ser identificada directa o indirectamente, en particular mediante un identificador.

Ejemplo laboral: En una empresa de logística, los datos personales incluyen el nombre y RUT del conductor, pero también la geolocalización en tiempo real de su vehículo (que permite identificarlo indirectamente), su registro de entregas, fotografías de firma de clientes, y datos de contacto de emergencia.

Dato sensible: Aquellos datos personales que revelan **origen étnico o racial, opiniones políticas, convicciones religiosas o filosóficas, afiliación sindical**, así como datos **genéticos, biométricos** dirigidos a identificar unívocamente a una persona, datos de **salud, vida sexual u orientación sexual**. Su tratamiento exige garantías reforzadas, como consentimiento explícito o una base legal específica, debido al riesgo elevado de discriminación o vulneración de derechos fundamentales.

Ejemplo laboral: Si tu empresa implementa un sistema de control de acceso por huella dactilar o reconocimiento facial, estás tratando datos biométricos (sensibles). Si gestionas licencias médicas en RRHH, tratas datos de salud (sensibles). Ambos casos requieren medidas adicionales de protección y bases legales sólidas.

Titular: La persona natural a quien se refieren los datos personales. Es el sujeto de derecho protegido por la ley, quien puede ejercer derechos de acceso, rectificación, cancelación, oposición y portabilidad (derechos ARCO+).

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 *para qué* y *cómo* se tratan los datos, y asume la responsabilidad principal ante la ley.

Encargado del tratamiento: Persona natural o jurídica que trata datos personales **por cuenta del responsable**, siguiendo sus instrucciones. El encargado no decide los fines ni los medios esenciales, sino que ejecuta operaciones específicas delegadas por el responsable.

Tratamiento: Cualquier operación o conjunto de operaciones realizadas sobre datos personales, por medios automatizados o no: **recolección, registro, organización, estructuración, conservación, modificación, consulta, comunicación por transmisión, difusión, interconexión, limitación, supresión o destrucción**.

Actor	Rol	Ejemplo laboral
Responsable	Decide el «qué» y el «cómo» del tratamiento	Tu empresa (empleador) que gestiona datos de trabajadores

Actor	Rol	Ejemplo laboral
Encargado	Ejecuta el tratamiento por instrucciones del responsable	Proveedor externo de nómina o plataforma cloud que procesa datos por cuenta de tu empresa
Titular	Persona natural a quien se refieren los datos	El trabajador, cliente o proveedor persona natural

Ejemplo laboral: Una clínica (responsable) contrata a una empresa de tecnología (encargado) para administrar su sistema de fichas electrónicas. La clínica define qué datos se almacenan, quién puede acceder y por cuánto tiempo; la empresa de tecnología solo ejecuta el alojamiento y mantenimiento según las instrucciones de la clínica. El paciente es el titular de los datos.

✔ Puntos clave

- Dato personal: toda información sobre una persona natural identificada o identificable.
- Dato sensible: datos que revelan características íntimas (salud, biometría, ideología) y requieren protección reforzada.
- Responsable: quien decide los fines y medios del tratamiento; Encargado: quien ejecuta por cuenta del responsable.
- Tratamiento: cualquier operación sobre datos, desde la recolección hasta la supresión.

💭 Para reflexionar

- ¿Puedes identificar quién es el responsable y quién el encargado en los tratamientos de datos de tu área?
- ¿Qué datos sensibles trata tu organización y qué garantías adicionales se han implementado?
- ¿Conoces los procedimientos para que los titulares ejerzan sus derechos en tu empresa?

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

La Ley 21.719 establece **principios rectores** que deben orientar cada decisión de tratamiento de datos personales. Estos principios son vinculantes y su incumplimiento puede generar responsabilidad y sanciones. Comenzamos 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** establecidas en la ley: consentimiento del titular, ejecución de un contrato, cumplimiento de una obligación legal, protección de intereses vitales del titular, cumplimiento de una misión de interés público, o interés legítimo del responsable (cuando no prevalezcan los derechos del titular). **No basta con tener los datos; es necesario tener una causa legal válida para procesarlos.**

Ejemplo laboral: Una empresa de telecomunicaciones puede tratar los datos de facturación de sus clientes con base en la ejecución del contrato de servicios; puede tratar datos de registro de llamadas con base en obligaciones legales tributarias y regulatorias; y puede enviar publicidad de nuevos servicios únicamente si cuenta con consentimiento del titular o puede justificar un interés legítimo (y el cliente no se ha opuesto).

2. Principio de lealtad: El tratamiento debe realizarse de manera leal, **sin engaño ni abuso de confianza**. No se pueden obtener datos mediante prácticas desleales, fraudulentas o que aprovechen la falta de información del titular.

Ejemplo laboral: Sería desleal que una tienda online, al solicitar el correo electrónico para enviar el comprobante de compra, lo utilice sin informar al cliente para enviarle publicidad de terceros o lo venda a intermediarios de datos. La lealtad exige coherencia entre lo informado y lo ejecutado.

3. Principio de 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, en lenguaje sencillo y comprensible. Este principio se materializa en **avisos de privacidad, políticas de tratamiento y notificaciones** que deben entregarse al momento de la recolección o antes del tratamiento.

Ejemplo laboral: En el proceso de selección de personal, antes de solicitar datos a un postulante, debes informarle mediante un aviso de privacidad claro: quién es el responsable (tu empresa), qué datos se recopilarán (CV, certificados, referencias), con qué finalidad (evaluación de candidatura), cuánto tiempo se conservarán (durante el proceso y, si es contratado, durante la relación laboral), si se compartirán (con empresas de verificación de antecedentes, si corresponde) y cómo puede ejercer sus derechos (contacto del responsable o del delegado de protección de datos).

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 cambias el propósito original del tratamiento, en general deberás solicitar nuevo consentimiento o demostrar que el nuevo fin es compatible con el original.

Ejemplo laboral: Una empresa de retail recopila datos de clientes para gestionar ventas y entregas. Si posteriormente desea utilizar esos datos para realizar análisis de mercado y segmentación comercial (finalidad distinta), debe evaluar la compatibilidad o solicitar nuevo consentimiento. No puede, sin más, compartir esos datos con terceros para fines publicitarios ajenos al servicio original.

Principio	Pregunta clave de cumplimiento	Herramienta práctica
Licitud	¿Tengo base legal válida para este tratamiento?	Matriz de legitimación por tratamiento
Lealtad	¿Estoy actuando de buena fe, sin engaño?	Revisión de comunicaciones y formularios
Transparencia	¿El titular sabe qué hago con sus datos?	Avisos de privacidad, políticas publicadas
Finalidad	¿Para qué recolecté estos datos originalmente?	Registro de finalidades por base de datos

La Agencia de Protección de Datos Personales (APDP) fiscaliza el cumplimiento, resuelve reclamos, aplica sanciones y orienta a las organizaciones en la implementación de la normativa de protección de datos.

✔ Puntos clave

- Licitud: todo tratamiento requiere una base legal válida (consentimiento, contrato, ley, interés legítimo, etc.).
- Lealtad: prohibición de prácticas engañosas o abusivas en la obtención y uso de datos.
- Transparencia: el titular debe recibir información clara, accesible y completa sobre el tratamiento.
- Finalidad: los datos se recopilan para fines determinados y explícitos; cambios requieren justificación o nuevo consentimiento.

💭 Para reflexionar

- ¿Qué base legal sustenta cada tratamiento de datos en tu área de trabajo?
- ¿Los avisos de privacidad de tu organización son claros y accesibles para todos los titulares?
- ¿Se ha evaluado la compatibilidad de finalidades cuando se reutilizan datos para nuevos propósitos?

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

Continuamos con tres principios operativos esenciales que buscan que los datos tratados sean **solo los necesarios, exactos, actualizados y conservados por el tiempo estrictamente requerido**.

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» y exige una evaluación previa de necesidad.

Implicancias prácticas: Antes de diseñar un formulario, una base de datos o un proceso de recolección, pregúntate: *¿realmente necesito este campo para prestar el servicio o cumplir el contrato?* Si la respuesta es no, elimínalo o hazlo opcional, requiriendo consentimiento específico. Por ejemplo, para contratar un servicio de internet residencial, es pertinente solicitar dirección de instalación y datos de facturación, pero no es necesario solicitar el estado civil o la cantidad de hijos del titular, salvo que exista una finalidad legítima y específica.

Ejemplo laboral: En un proceso de inscripción a un evento corporativo, el formulario debe limitarse a nombre, correo y empresa del participante. Solicitar fecha de nacimiento, género, religión o nivel de ingresos sería excesivo y violaría el principio de minimización, salvo que exista una finalidad legítima claramente justificada (por ejemplo, restricciones de edad para ciertos talleres).

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: confirmar correo electrónico mediante doble opt-in, validar dirección al enviar comunicaciones, solicitar actualización de datos de contacto en cada interacción relevante. Facilita al titular el ejercicio de su derecho de rectificación mediante canales simples y accesibles. Si un dato ha perdido vigencia o exactitud y no puede corregirse, debe eliminarse si ya no es necesario.

Ejemplo laboral: Una empresa de seguros debe revisar periódicamente los datos de contacto de sus asegurados (dirección, teléfono, correo) para garantizar que las comunicaciones lleguen correctamente. Si un asegurado informa un cambio de domicilio, la empresa debe actualizar el dato en todos los sistemas relevantes sin dilación.

Principio de limitación de conservación: Los datos personales deben ser mantenidos de forma que permitan la identificación de los titulares **durante no más tiempo del necesario** para los fines del tratamiento. Cumplida la finalidad, o transcurrido el plazo legal de conservación (cuando exista obligación legal), los datos deben ser eliminados o anonimizados.

Implicancias prácticas: Define plazos de conservación para cada tipo de dato o tratamiento, documentados en políticas internas o calendarios de retención. Por ejemplo, datos de postulantes no seleccionados pueden conservarse solo por el tiempo del proceso de selección más un plazo razonable

por si surge una nueva vacante similar (por ejemplo, seis meses), salvo que el postulante haya consentido expresamente su conservación en una base de datos de talentos.

Ejemplo laboral: En el área de ventas, los datos de clientes deben conservarse mientras dure la relación comercial y durante el plazo legal de prescripción de obligaciones tributarias o contractuales (usualmente entre cuatro y seis años desde la última factura, según la normativa aplicable). Transcurrido ese plazo, si no existe otra base legal, los datos deben eliminarse o anonimizarse para análisis estadísticos.

- **Minimización:** Formularios con campos estrictamente necesarios; evaluación de pertinencia antes de recopilar.
- **Calidad:** Procedimientos de validación (ej. verificación de correo, actualización de domicilio); protocolos de rectificación ágiles.
- **Limitación de conservación:** Calendarios de retención de datos; supresión automática o revisión periódica; anonimización post-plazo.

✔ Puntos clave

- Minimización: solo recopilar datos adecuados, pertinentes y no excesivos para la finalidad específica.
- Calidad: garantizar que los datos sean exactos, completos y actualizados; facilitar la rectificación.
- Limitación de conservación: eliminar o anonimizar datos una vez cumplida la finalidad o el plazo legal.
- Estos principios operativos exigen diseño previo, procedimientos documentados y revisión periódica.

💭 Para reflexionar

- ¿Los formularios y bases de datos de tu área solicitan únicamente datos necesarios para la finalidad declarada?
- ¿Existen procedimientos para verificar y actualizar la exactitud de los datos personales que tratas?
- ¿Tu organización cuenta con un calendario de retención y eliminación de datos personales?

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 las normas: 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 la privacidad cuando el tratamiento presente riesgos elevados, mantener **registros de actividades de tratamiento**, capacitar al personal, designar (cuando corresponda) un **delegado de protección de datos**, y documentar todas estas acciones.

Cambio de paradigma: Se pasa de un modelo reactivo (esperar la denuncia, la fiscalización o el incidente) a uno **preventivo, documentado y auditable**. La carga de la prueba del cumplimiento recae en la organización. Si la Agencia de Protección de Datos Personales te fiscaliza, deberás demostrar con evidencia documental y técnica que has implementado y mantenido un sistema de gestión de protección de datos.

Ejemplo laboral: Una empresa de comercio electrónico debe contar con: un registro actualizado de todas sus bases de datos y tratamientos; políticas de privacidad y seguridad aprobadas y difundidas; evaluaciones de impacto para tratamientos de alto riesgo (por ejemplo, perfilado automatizado de clientes); contratos con encargados de tratamiento (proveedores cloud, couriers, plataformas de pago); programa de capacitación anual para personal; procedimientos documentados para atender derechos ARCO; y un plan de respuesta ante brechas de seguridad. Todo esto debe estar documentado y disponible para demostrar 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, protegiendo los datos contra tratamiento no autorizado o ilícito, pérdida, destrucción o daño accidental. El nivel de seguridad debe ser proporcional al riesgo: tratamientos de datos sensibles o de alto volumen requieren medidas más robustas.

Medidas técnicas: Cifrado de datos en tránsito y en reposo, control de acceso basado en roles y privilegios mínimos, autenticación multifactor, sistemas de detección de intrusiones, copias de seguridad periódicas y planes de recuperación ante desastres, anonimización o seudonimización cuando sea posible.

Medidas organizativas: Políticas de seguridad de la información, procedimientos de gestión de incidentes y brechas, auditorías periódicas, control de acceso físico a servidores y archivos, destrucción segura de documentos y dispositivos, cláusulas de confidencialidad en contratos laborales y con terceros.

Ejemplo laboral: Un hospital que trata datos de salud (sensibles) debe implementar cifrado de fichas electrónicas, control estricto de acceso (solo personal autorizado según su función), auditoría de logs de acceso, capacitación en confidencialidad médica, protocolos de respuesta ante brechas, y contratos de confidencialidad con todo el personal clínico y administrativo.

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. Este deber de confidencialidad debe formalizarse mediante acuerdos escritos (cláusulas en contratos de trabajo, acuerdos de confidencialidad con proveedores) y reforzarse con capacitación y sanciones disciplinarias en caso de incumplimiento.

Ejemplo laboral: Un trabajador del área de cobranzas que accede a datos financieros de clientes tiene la obligación de no divulgar esa información a terceros, ni siquiera a familiares o amigos, ni utilizarla para fines personales. Esa obligación persiste incluso si deja de trabajar en la empresa. La empresa debe hacerle firmar un acuerdo de confidencialidad y capacitarlo en el manejo seguro y reservado de datos personales.

Principio	Herramientas y acciones clave
Responsabilidad proactiva	Registro de tratamientos, evaluaciones de impacto (DPIA), políticas documentadas, capacitación continua, auditorías internas, contratos con encargados.
Seguridad	Cifrado, control de acceso, autenticación, copias de seguridad, planes de continuidad, gestión de incidentes, destrucción segura.
Confidencialidad	Acuerdos de confidencialidad (NDA), cláusulas en contratos laborales, políticas internas, sanciones disciplinarias, cultura de privacidad.

✔ Puntos clave

- Responsabilidad proactiva: demostrar cumplimiento mediante políticas, registros, evaluaciones de impacto y documentación auditable.
- Seguridad: implementar medidas técnicas y organizativas proporcionales al riesgo (cifrado, control de acceso, copias de seguridad).
- Confidencialidad: obligación de secreto para toda persona que trate datos, formalizada y exigible incluso tras finalizar la relación.
- El nuevo modelo exige anticiparse, documentar y auditar continuamente el cumplimiento.

💭 Para reflexionar

- ¿Tu organización cuenta con un registro actualizado de todas las actividades de tratamiento de datos personales?
- ¿Qué medidas técnicas y organizativas de seguridad se han implementado para proteger los datos que tratas?
- ¿Todo el personal ha firmado acuerdos de confidencialidad y recibido capacitación en protección de datos?

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

Finalmente, es fundamental conocer 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, orientar y promover el cumplimiento de la normativa de protección de datos.

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. Goza de autonomía en el ejercicio de sus atribuciones, lo que le permite actuar con independencia técnica y funcional.

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 (reclamos de titulares).
- **Instruir procedimientos sancionatorios** y aplicar sanciones administrativas, que pueden alcanzar multas de hasta 15.000 UTM en casos graves de infracción (por ejemplo, tratamiento ilícito de datos sensibles, incumplimiento grave de medidas de seguridad que cause daño, obstaculización de la fiscalización).
- **Conocer y resolver reclamos** presentados por titulares por vulneración de sus derechos (acceso, rectificación, cancelación, oposición, portabilidad), actuando como instancia administrativa previa a la vía judicial.
- **Emitir directrices, instrucciones, recomendaciones y guías** para interpretar y aplicar la ley, orientando a responsables y encargados en el cumplimiento de sus obligaciones.
- **Autorizar transferencias internacionales** de datos personales a países o territorios que no cuenten con un nivel adecuado de protección, evaluando garantías apropiadas (cláusulas contractuales tipo, normas corporativas vinculantes, etc.).
- **Llevar y mantener el Registro de Sanciones**, que es público y permite consultar las infracciones y multas aplicadas a responsables y encargados.
- **Promover la educación y la cultura de protección de datos** mediante campañas de difusión, capacitaciones y publicaciones dirigidas a ciudadanos, organizaciones y sector público.

Ejemplo laboral: Si un cliente de tu empresa considera que se le ha negado injustificadamente el acceso a sus datos personales, puede presentar un reclamo ante la APDP. La Agencia solicitará información a tu empresa, evaluará los antecedentes y podrá ordenar que se entregue la información al titular, aplicar una multa si corresponde, o rechazar el reclamo si la negativa estaba justificada. Por ello es crucial contar con procedimientos documentados y ágiles para atender derechos de los titulares, y demostrar que se han ejercido de buena fe.

¿Qué significa esto para tu trabajo diario? La existencia de la APDP implica que el cumplimiento de la Ley 21.719 ya no es opcional ni depende solo de la voluntad de la organización. Existe una autoridad con facultades de fiscalización, sanción y orientación, que puede realizar auditorías, requerir documentación, acceder a sistemas y aplicar multas significativas. Esto refuerza la importancia de implementar un modelo de **responsabilidad proactiva**, donde cada área y cada trabajador asume su rol en la protección de datos

personales, bajo la coordinación de un responsable interno (o delegado de protección de datos, según corresponda).

Recomendación práctica: Familiarízate con el sitio web de la APDP, consulta sus directrices y guías sectoriales, y establece un canal de comunicación interno para reportar dudas o incidentes relacionados con protección de datos. La APDP es un aliado en el cumplimiento, no solo un fiscalizador.

✔ Puntos clave

- La APDP es un servicio público descentralizado, autónomo, encargado de fiscalizar y hacer cumplir la Ley 21.719.
- Puede iniciar fiscalizaciones de oficio, recibir reclamos de titulares, aplicar multas de hasta 15.000 UTM y autorizar transferencias internacionales.
- Emite directrices, guías y recomendaciones vinculantes para orientar el cumplimiento de responsables y encargados.
- Su existencia refuerza la necesidad de un modelo de responsabilidad proactiva y cumplimiento demostrable en toda la organización.

💭 Para reflexionar

- ¿Tu organización ha designado un responsable interno o delegado de protección de datos para interactuar con la APDP?
- ¿Conoces el procedimiento interno para atender un reclamo de un titular o una fiscalización de la APDP?
- ¿Se han revisado las directrices y guías emitidas por la APDP aplicables a tu sector o actividad?

🗺 Mapa conceptual: Ley 21.719 sobre Protección de Datos Personales

Objeto y alcance	Garantizar privacidad y protección de datos personales ante tratamientos automatizados y no automatizados en sector público y privado; vigencia plena desde 1 de diciembre de 2026; cambio hacia responsabilidad proactiva.
Conceptos clave	Dato personal (información sobre persona identificada/identificable); dato sensible (salud, biometría, ideología); titular (persona natural); responsable (decide fines y medios); encargado (ejecuta por cuenta del responsable); tratamiento (cualquier operación sobre datos).
Principios rectores fundamentales	Licitud (base legal válida); lealtad (sin engaño); transparencia (información clara al titular); finalidad (fines determinados y explícitos); minimización (solo datos necesarios); calidad (exactitud y actualización); limitación de conservación (eliminar cumplida finalidad).

Responsabilidad proactiva y seguridad	Demostrar cumplimiento (políticas, registros, evaluaciones de impacto, auditorías); medidas técnicas y organizativas de seguridad proporcionales al riesgo; confidencialidad obligatoria para toda persona que trate datos.
Agencia de Protección de Datos Personales (APDP)	Autoridad de control autónoma; fiscaliza cumplimiento, resuelve reclamos, aplica sanciones (hasta 15.000 UTM), autoriza transferencias internacionales y emite directrices vinculantes.
Modelo de cumplimiento	Registro de tratamientos, avisos de privacidad, procedimientos ARCO, contratos con encargados, capacitación continua, gestión de incidentes, cultura organizacional de privacidad y documentación auditable.

En síntesis. Has completado el recorrido por los fundamentos, conceptos y principios de la Ley N°21.719. Ahora comprendes el objeto de la normativa, dominas el lenguaje técnico-jurídico esencial (datos, titulares, responsables, encargados) y reconoces los principios rectores que deben guiar cada tratamiento en tu ámbito laboral. Este conocimiento es la base para implementar un modelo de **responsabilidad proactiva**, donde demostrar el cumplimiento es tan importante como cumplir. En los próximos módulos profundizaremos en las bases de legitimación, los derechos de los titulares, las obligaciones específicas de responsables y encargados, y las mejores prácticas para gestionar la protección de datos en tu organización. **La protección de datos personales es responsabilidad de todos.**