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)

Material de estudio

Módulo 1

Apunte descargable del estudiante

Contenido del módulo

1. **El nuevo escenario: Ley 21.719 y su alcance**
2. **Conceptos clave: datos, titulares y actores**
3. **Principios rectores I: licitud, lealtad, transparencia y finalidad**
4. **Principios rectores II: minimización y calidad**
5. **Principios de responsabilidad proactiva y seguridad**
6. **La Agencia de Protección de Datos Personales (APDP)**

La era digital ha transformado la forma en que las organizaciones interactúan con la información personal. En Chile, este nuevo escenario se regula con la entrada en vigencia de la **Ley N°21.719 sobre Protección de Datos Personales**. Esta normativa no es solo un conjunto de reglas, sino un cambio fundamental en cómo se gestionan los datos, pasando de una respuesta a incidentes a una **responsabilidad proactiva**. Como Encargado, Jefatura o profesional de Recursos Humanos, comprender sus bases es esencial para asegurar el cumplimiento y proteger tanto a las personas como a la organización.

1 El nuevo escenario: Ley 21.719 y su alcance

Imagina que lideras el área de cumplimiento en una empresa de servicios financieros con una robusta plataforma digital. El 1 de diciembre de 2026 marca un hito: la aplicación plena de la Ley 21.719. Desde esa fecha, cada operación que involucre datos personales deberá estar alineada con esta normativa. La Ley N°21.719 tiene como fin primordial **garantizar y proteger el derecho a la privacidad y a la protección de datos personales** de las personas naturales. Esto implica que las empresas y organismos públicos deben manejar la información personal con el debido resguardo.

El **ámbito de aplicación** de la ley es amplio. Se extiende a cualquier tratamiento de datos personales, ya sea total o parcialmente automatizado, así como al tratamiento no automatizado de datos contenidos o destinados a ser incluidos en registros. Esto abarca tanto al sector público (ministerios, servicios, municipalidades) como al privado (empresas de todo tipo, fundaciones, ONG), con excepciones muy específicas como tratamientos exclusivamente personales o domésticos, o aquellos relacionados con la seguridad nacional.

La entrada en vigencia ha sido gradual, pero la fecha clave para la aplicación plena de todas sus obligaciones es el **1 de diciembre de 2026**. Este plazo ha permitido a las organizaciones prepararse para adoptar un modelo de **responsabilidad proactiva**, un enfoque que exige anticipación y demostración de cumplimiento, en lugar de solo reaccionar a incidentes. Este paradigma se alinea con estándares internacionales avanzados como el Reglamento General de Protección de Datos (RGPD) de la Unión Europea.

Sector	Ejemplo de Entidad	Tipo de Datos Manejados
Privado	Empresas de retail	Datos de clientes (historial de compras, preferencias, direcciones)
Privado	Clínicas privadas	Datos de salud de pacientes, agendas médicas
Público	Municipalidades	Datos de registro civil, licencias de conducir, permisos
Público	Servicios de Impuestos Internos	Datos económicos, tributarios de contribuyentes

La Ley 21.719: Un escudo protector para los datos personales en el entorno digital y empresarial.

✔ Puntos clave

- La Ley 21.719 protege el derecho fundamental a la privacidad y a la protección de datos personales.
- Se aplica a todo tratamiento de datos, automatizado o no, en los sectores público y privado.
- La aplicación plena entró en vigencia el 1 de diciembre de 2026, estableciendo un modelo de responsabilidad proactiva.
- Existen excepciones específicas para tratamientos domésticos o de seguridad nacional.

💭 Para reflexionar

- ¿Cómo afectará la aplicación plena de la Ley 21.719 a los procesos de tu área o departamento?
- ¿Cuáles son los principales riesgos de no cumplir con el ámbito de aplicación de esta ley en tu organización?
- ¿Qué medidas proactivas podrías sugerir para asegurar la preparación de tu equipo ante esta normativa?

2 Conceptos clave: datos, titulares y actores

Para implementar eficazmente la Ley 21.719, es crucial dominar la terminología específica. Esto permite que todos en la organización, desde las jefaturas hasta los encargados de tratamiento, hablen el mismo lenguaje y comprendan sus roles y responsabilidades.

- **Dato personal:** Es cualquier información que permite identificar o hacer identificable a una persona natural. Ejemplos laborales incluyen el nombre completo de un empleado, su RUT, dirección particular, correo electrónico corporativo o personal, número de teléfono, información biométrica (huella dactilar para registro de asistencia), o incluso datos sobre su desempeño laboral que permitan su identificación.
- **Dato sensible:** Constituye una categoría especial de dato personal que, por su naturaleza, requiere una protección aún mayor debido al riesgo inherente que su tratamiento conlleva. Incluyen el origen étnico o racial, opiniones políticas, convicciones religiosas o filosóficas, afiliación sindical, datos genéticos, datos biométricos únicos para identificación, datos de salud, vida sexual u orientación sexual. En el ámbito de RRHH, la recopilación de certificados médicos o datos de género son ejemplos de datos sensibles que exigen un manejo extremadamente cuidadoso y justificado.
- **Titular:** Es la persona natural a quien se refieren los datos personales. En el contexto laboral, el titular es el empleado, candidato, ex-empleado, cliente o proveedor cuya información personal está siendo tratada por la organización.
- **Responsable del tratamiento:** Es la persona natural o jurídica (la empresa, el departamento de RRHH, la jefatura) que decide “qué” datos se van a tratar y “cómo” se van a tratar. Es quien determina los fines y los medios del tratamiento de datos personales. Por ejemplo, la gerencia de una empresa es la responsable de definir la política de tratamiento de datos de sus empleados.
- **Encargado del tratamiento:** Es la persona natural o jurídica que trata datos personales **por cuenta del responsable**, siguiendo sus instrucciones. Un proveedor externo que gestiona la nómina de la empresa o una plataforma de evaluación de desempeño contratada son ejemplos de encargados del tratamiento.
- **Tratamiento:** Cualquier operación o conjunto de operaciones realizadas sobre datos personales. Esto incluye desde la recolección inicial de un currículum vitae, el registro de datos en un sistema, la organización de expedientes, la conservación de contratos, hasta la modificación, consulta, comunicación o supresión de información personal.

✔ Puntos clave

- Un dato personal identifica a una persona natural, mientras que un dato sensible exige mayor protección.
- El titular es la persona a quien se refieren los datos.
- El responsable define los fines y medios del tratamiento; el encargado lo ejecuta siguiendo instrucciones.
- El tratamiento abarca cualquier operación realizada sobre los datos personales.

💭 Para reflexionar

- En tu rol, ¿qué tipo de datos personales y sensibles manejas regularmente?
- ¿Quién es el responsable del tratamiento de los datos de tus empleados y quiénes actúan como encargados?
- ¿Podrías identificar un ejemplo de 'tratamiento de datos' en tu día a día laboral y clasificar los datos involucrados?

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

La Ley 21.719 establece principios que actúan como la columna vertebral de cualquier operación de tratamiento de datos. Estos principios no son meras recomendaciones, sino directrices obligatorias que deben orientar cada decisión. Los primeros cuatro son fundamentales:

1. **Licitud:** Significa que todo tratamiento de datos debe tener una base legal válida. No basta con poseer los datos; se debe justificar su procesamiento bajo alguna de las causales establecidas por la ley. Estas pueden incluir el consentimiento del titular, la ejecución de un contrato (por ejemplo, el contrato de trabajo), el cumplimiento de una obligación legal (como el pago de impuestos), la protección de intereses vitales del titular, el interés público o el interés legítimo del responsable.
2. **Lealtad:** Implica que el tratamiento de datos debe realizarse de buena fe, sin prácticas engañosas o fraudulentas. La información no debe obtenerse por medios que vulneren la confianza del titular. Por ejemplo, no se puede recopilar información para un fin y luego usarla para otro sin informar ni obtener nuevo consentimiento.
3. **Transparencia:** El titular tiene el derecho fundamental a saber qué sucede con sus datos. Esto significa informarle quién los trata, para qué propósitos, durante cuánto tiempo, con quién se comparten y cuáles son sus derechos. Esta información debe ser clara, accesible y presentada en un lenguaje sencillo, usualmente a través de políticas de privacidad o avisos de tratamiento.
4. **Finalidad:** Los datos deben ser recolectados con propósitos específicos, explícitos y legítimos. Una vez definidos, no se pueden tratar posteriormente de manera incompatible con esos fines originales. Si los fines cambian, generalmente se requerirá un nuevo consentimiento o una justificación legal para la compatibilidad del nuevo propósito con el original. Por ejemplo, los datos recopilados para la selección de personal no deberían usarse para enviar publicidad sin un consentimiento adicional.

Responsable y Encargado: Roles clave en el ecosistema del tratamiento de datos bajo la Ley 21.719.

✔ Puntos clave

- El principio de licitud exige una base legal para todo tratamiento de datos.
- La lealtad garantiza que los datos se obtengan sin engaño ni abuso de confianza.
- La transparencia obliga a informar al titular sobre el tratamiento de sus datos de forma clara y accesible.
- La finalidad requiere que los datos se recojan para propósitos específicos y no se usen para fines incompatibles.

💭 Para reflexionar

- En un proceso de contratación, ¿cuál es la base legal (licitud) para solicitar el certificado de antecedentes de un candidato?
- ¿Cómo se asegura la transparencia en tu área cuando se recopilan datos personales de nuevos empleados?
- Si los datos de contacto de un cliente se obtuvieron para la entrega de un producto, ¿sería lícito usarlos para una campaña de marketing sin su consentimiento?

4 Principios rectores II: minimización y calidad

Además de los principios anteriores, la ley enfatiza la gestión eficiente y precisa de los datos. Los principios de minimización y calidad son clave para evitar el exceso de información y asegurar su veracidad.

- **Minimización (o Proporcionalidad):** Este principio establece que los datos personales deben ser **adecuados, pertinentes y no excesivos** en relación con los fines para los cuales son tratados. En la práctica, esto significa que una organización solo debe solicitar y conservar aquellos datos que sean estrictamente necesarios para cumplir con la finalidad declarada. Por ejemplo, si se está creando un formulario para una inscripción a un curso interno, ¿es realmente necesario solicitar el estado civil o el número de hijos del empleado si esos datos no guardan relación con el objetivo del curso? Si la respuesta es no, ese campo debe ser eliminado o marcado como opcional.
- **Calidad (o Exactitud):** Este principio exige que los datos personales sean exactos y, cuando sea necesario, actualizados. Las organizaciones 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. Esto es crucial en cualquier base de datos de empleados o clientes. Por ejemplo, un cambio de domicilio o de número de teléfono de un empleado debe poder ser actualizado con facilidad para que la empresa siempre maneje información correcta. Facilitar al titular el ejercicio de su derecho de rectificación es una manifestación directa de este principio.

✔ Puntos clave

- La minimización exige recolectar solo los datos estrictamente necesarios para el fin declarado.
- La calidad obliga a mantener los datos exactos y actualizados, facilitando su rectificación.
- Ambos principios buscan evitar la recolección excesiva y la inexactitud de la información personal.

💭 Para reflexionar

- ¿Qué información adicional se solicita en los formularios de tu organización que podría no ser estrictamente necesaria para su finalidad?
- ¿Cómo se asegura que los datos personales de los empleados se mantengan actualizados en tu departamento?
- Si un empleado solicita la corrección de un dato erróneo en su expediente, ¿cuál es el procedimiento para garantizar el principio de calidad?

5 Principios de responsabilidad proactiva y seguridad

El nuevo marco normativo de la Ley 21.719 se distingue por un enfoque particular en la responsabilidad de las organizaciones. Los principios de responsabilidad proactiva y seguridad son el pilar de este cambio de paradigma.

- **Responsabilidad Proactiva (Accountability):** Este es uno de los principios más innovadores. El responsable del tratamiento no solo debe cumplir con la ley, sino que debe ser capaz de **demostrar ese cumplimiento**. Esto va más allá de evitar infracciones; implica adoptar una cultura de cumplimiento documentada. Por ejemplo, una empresa debe implementar políticas internas de protección de datos, realizar evaluaciones de impacto sobre la privacidad (DPIA) para nuevos proyectos, mantener registros detallados de todas las actividades de tratamiento, capacitar continuamente a su personal y documentar todas estas acciones. La carga de la prueba recae en la organización, que debe poder justificar y evidenciar sus esfuerzos de protección.
- **Seguridad:** Tanto el responsable como el encargado del tratamiento tienen la obligación de implementar medidas técnicas y organizativas adecuadas para garantizar un nivel de seguridad que corresponda al riesgo de los datos que tratan. Esto implica proteger los datos contra el tratamiento no autorizado o ilícito, la pérdida accidental, la destrucción o el daño. Ejemplos de medidas incluyen el cifrado de datos, la implementación de controles de acceso robustos, la realización de copias de seguridad periódicas, la gestión de la identidad y el acceso, y la capacitación de los empleados en seguridad de la información.
- **Confidencialidad:** Todas las personas que, de alguna manera, intervengan en el tratamiento de datos personales, están obligadas a guardar secreto profesional sobre ellos. Esta obligación subsiste incluso después de que haya terminado su relación laboral o contractual con el responsable o encargado. Esto es fundamental en áreas como RRHH, donde el acceso a información sensible de los empleados debe ser estrictamente confidencial. Se materializa en acuerdos de confidencialidad, políticas internas de acceso a la información y sanciones disciplinarias en caso de incumplimiento.

✔ Puntos clave

- La responsabilidad proactiva exige no solo cumplir la ley, sino también demostrar ese cumplimiento de manera documentada.
- El principio de seguridad requiere implementar medidas técnicas y organizativas para proteger los datos de riesgos.
- La confidencialidad obliga a guardar secreto sobre los datos personales, incluso después de finalizar la relación laboral o contractual.

💭 Para reflexionar

- ¿Cómo podría tu equipo demostrar proactivamente el cumplimiento de la Ley 21.719 en la gestión de expedientes de personal?
- ¿Qué medidas de seguridad técnica y organizativa se aplican en tu organización para proteger la información de los empleados?
- ¿Existen acuerdos de confidencialidad o políticas internas que regulen el acceso a datos sensibles en tu área?

6 La Agencia de Protección de Datos Personales (APDP)

Finalmente, es fundamental conocer a la entidad encargada de velar por el cumplimiento de la Ley 21.719. La **Agencia de Protección de Datos Personales (APDP)** es la autoridad de control creada para supervisar, fiscalizar, sancionar y orientar a todas las organizaciones en Chile.

La APDP es un servicio público descentralizado, con autonomía funcional y patrimonio propio, y se relaciona con el Presidente de la República a través del Ministerio de Justicia y Derechos Humanos. Su existencia marca la formalización de un ente regulador especializado en privacidad, similar a otras agencias de datos personales a nivel internacional.

Entre sus **principales funciones** se encuentran:

- **Fiscalizar** el cumplimiento de la normativa sobre protección de datos personales, tanto de oficio (por iniciativa propia) como a petición de parte (tras una denuncia).
- **Instruir procedimientos sancionatorios** y aplicar multas que pueden ascender hasta 15.000 Unidades Tributarias Mensuales (UTM) en casos de infracciones graves.
- **Conocer y resolver los reclamos** que presenten los titulares de datos personales por la vulneración de sus derechos.
- **Emitir directrices, instrucciones y recomendaciones** que sirven para interpretar y aplicar correctamente la ley, actuando como una guía para las organizaciones.
- **Autorizar transferencias internacionales** de datos personales a países que no garanticen un nivel adecuado de protección, cuando sea necesario y bajo ciertas condiciones.

Es importante destacar que la APDP también tendrá un rol educativo y preventivo, buscando fomentar una cultura de protección de datos en el país.

✔ Puntos clave

- La APDP es la autoridad de control de la Ley 21.719, con funciones de fiscalización y sanción.
- Puede imponer multas significativas por incumplimiento de la normativa.
- Resuelve reclamos de titulares y emite directrices para la correcta aplicación de la ley.
- También tiene la facultad de autorizar transferencias internacionales de datos bajo ciertas condiciones.

💭 Para reflexionar

- ¿Cómo podría la existencia de la APDP influir en las políticas de privacidad de tu organización?
- ¿Qué acciones preventivas podrías tomar para evitar un procedimiento sancionatorio por parte de la APDP?
- ¿Dónde buscarías las directrices o recomendaciones de la APDP si tuvieras dudas sobre un tratamiento de datos específico?

🗺 Esquema Conceptual de la Ley 21.719

Objeto y Alcance	Garantizar la privacidad y protección de datos de personas naturales, aplicándose a todo tratamiento de datos en sectores público y privado.
Conceptos Clave	Dato personal, dato sensible, titular, responsable del tratamiento, encargado del tratamiento, tratamiento.
Principios Rectores Fundamentales	Licitud, Lealtad, Transparencia, Finalidad, Minimización, Calidad, Responsabilidad Proactiva, Seguridad, Confidencialidad.
Actores Principales	Titular de los datos, Responsable del Tratamiento, Encargado del Tratamiento, y la Agencia de Protección de Datos Personales (APDP).
Novedad del Modelo	Cambio de un enfoque reactivo a uno de responsabilidad proactiva y demostrable, alineado con estándares internacionales.

En síntesis. La Ley 21.719 no es solo una regulación más; es la base para construir una cultura organizacional donde la privacidad y la protección de datos sean pilares fundamentales. Al comprender sus fundamentos, conceptos y principios, no solo garantizas el cumplimiento legal, sino que también fortaleces la confianza de tus empleados, clientes y proveedores. La responsabilidad proactiva te invita a ser un agente de cambio, anticipando riesgos y aplicando las mejores prácticas para salvaguardar la información personal. Este conocimiento es el primer paso para liderar con éxito la implementación de esta normativa crucial en tu organización.