CAPACITACIÓN USACH
UNIVERSIDAD DE SANTIAGO DE CHILE

Nueva ISO 27701:2025
Sistema de Gestión de Información de Privacidad

¿Cómo se alinea con la Ley de Protección de Datos?

ALIGNMENT
SOLUCIONES ESTRATÉGICAS

DIPLOMADO
CIBERSEGURIDAD

Agenda

- Breve contexto de la Ley
- Alineamiento con Principios de Privacidad – ISO 29100
- Norma ISO 27701
- Plan de Implementación

Profesor

Carlos Lobos de Medina

Ingeniero Civil en Informática y Magister en Informática © de la Universidad de Santiago de Chile, Diplomado en Auditoría de Sistemas, Postitulado en Seguridad Computacional de la Universidad de Chile.

Especialista en gobernanza, gestión y control de tecnologías de información empleando modelos como COBIT, ITIL, ISO 27001 e ISO 22301. Posee certificaciones internacionales CISA, CISM, COBIT, ISO Lead Auditor 27001, ISO Lead Auditor BS 25599 e ITIL V3, entre otras.}

https://www.linkedin.com/in/clobos/

Breve Contexto Ley 21719

Rol y Alcance de la Agencia de Protección de Datos

1 Ente Autónomo con Carácter Fiscalizador

La Agencia será un **organismo público autónomo**, con personalidad jurídica y patrimonio propio, encargado de **supervisar y fiscalizar el cumplimiento de la** Ley 27719 de las normas sobre protección de datos personales en Chile.

2 Enfoque de Derechos Fundamentales

Su misión principal será **proteger los derechos de las personas respecto del tratamiento de sus datos personales**, promoviendo el equilibrio entre innovación tecnológica y respeto a la privacidad.

3 Facultades de Supervisión y Sanción

Podrá **investigar, requerir información, realizar auditorías, emitir instrucciones y aplicar sanciones** a organismos públicos y privados que infrinjan la normativa de protección de datos.

4 Capacidad Normativa y de Orientación

Emitirá **directrices, guías técnicas, criterios interpretativos y estándares sectoriales** para apoyar la correcta implementación de la ley en instituciones y empresas.

5 Promoción de la Cultura de Privacidad

Desarrollará programas de **capacitación, sensibilización y educación ciudadana** en el uso responsable de los datos personales y en derechos digitales.

6 Coordinación Interinstitucional

Tendrá atribuciones para **coordinar acciones con otras autoridades**, como el Consejo para la Transparencia, CSIRT, Ministerio de Ciencia, y organismos reguladores sectoriales, fomentando coherencia normativa.

7 Supervisión sobre el Sector Público

Fiscalizará también a **servicios y organismos del Estado**, asegurando que cumplan las obligaciones legales de tratamiento, resguardo, conservación y eliminación de datos personales.

8 Gestión de Reclamos y Denuncias

Actuará como **canal institucional para la recepción y tramitación de reclamos de los titulares**, promoviendo mecanismos ágiles y trazables de resolución de controversias.

9 Transparencia y Rendición de Cuentas

Deberá mantener **informes públicos, estadísticas, resoluciones y criterios técnicos**, fortaleciendo la confianza ciudadana mediante una gestión abierta y verificable.

10 Cooperación Internacional y Estándares Globales

Participará activamente en **redes internacionales de autoridades de protección de datos** (como la Red Iberoamericana y el Comité del Convenio 108 del Consejo de Europa), para armonizar estándares y promover interoperabilidad normativa.

10 Principios Claves de la Ley 21719

1 Licitud, Lealtad y Transparencia

El tratamiento de datos debe realizarse conforme a la ley, de manera honesta, transparente y conocida por el titular.

> *Ningún tratamiento puede basarse en el engaño, la omisión o el abuso de confianza.*

2 Limitación del Propósito

Los datos solo pueden recolectarse para fines determinados, explícitos y legítimos, y no usarse para objetivos distintos sin una nueva base legal o consentimiento.

> *Define el "para qué" del tratamiento.*

3 Minimización de Datos

Solo deben tratarse los datos estrictamente necesarios para cumplir la finalidad declarada.

> *Evita la sobre-recolección o el almacenamiento innecesario.*

4 Exactitud y Actualización

Los datos deben mantenerse exactos, completos y actualizados. El responsable debe corregir o eliminar los que resulten inexactos.

> *El dato debe reflejar la realidad del titular.*

5 Limitación del Plazo de Conservación

Los datos se conservarán solo durante el tiempo necesario para cumplir la finalidad que motivó su tratamiento.

> *Ningún dato debe guardarse indefinidamente.*

6 Integridad y Confidencialidad

El responsable debe proteger los datos mediante medidas técnicas y organizativas que eviten el acceso, uso o divulgación no autorizada.

> *Garantiza la seguridad del tratamiento.*

7 Responsabilidad Proactiva (Accountability)

El responsable no solo debe cumplir, sino también demostrar que cumple con la Ley y sus principios.

> *Cumplimiento verificable y trazable.*

8 Principio de Licitud del Tratamiento

El tratamiento requiere base legal o consentimiento expreso, salvo las excepciones autorizadas por ley.

> *Todo tratamiento debe fundarse en una causa legítima.*

9 Participación y Control del Titular

Las personas tienen derecho a acceder, rectificar, eliminar y oponerse al tratamiento de sus datos.

> *Empodera al ciudadano como dueño de su información.*

10 Supervisión y Cumplimiento Efectivo

El cumplimiento será fiscalizado por la Agencia de Protección de Datos, que garantizará su aplicación transversal.

> *Institucionaliza la confianza y la rendición de cuentas.*

Derechos ARCO

+

Principios ISO 29100

Sanciones en la Ley 21719

1 Facultad fiscalizadora y sancionadora de la Agencia

La **Agencia de Protección de Datos Personales (APDP)** podrá **investigar, instruir y sancionar** directamente tanto a entidades públicas como privadas, con autonomía y debido proceso.

2 Clasificación de infracciones

La ley distingue tres categorías:

- **Leves:** incumplimientos formales o por descuido.
- **Graves:** vulneraciones que afecten derechos o principios sustantivos.
- **Muy graves:** divulgaciones masivas, tratamiento ilícito o uso doloso de datos sensibles.

3 Escala de sanciones

- Leves: hasta **1.000 UTM**
- Graves: hasta **5.000 UTM**
- Muy graves: hasta **15.000 UTM** o **2% de las ventas anuales**, en el caso de empresas.
  Los servicios públicos no pagan multas, pero sí enfrentan **medidas correctivas obligatorias.**

4 Criterios de graduación

La Agencia ponderará el **tipo de datos comprometidos**, la **intencionalidad**, la **reincidencia**, el **tamaño del infractor** y su **colaboración en la investigación.**

5 Sanciones complementarias

Además de multas, podrá ordenarse:

- Suspensión o bloqueo del tratamiento.
- Eliminación de datos.
- Publicación de la resolución sancionatoria.

6 Incentivos al cumplimiento preventivo

La **autodenuncia, cooperación y corrección temprana** pueden reducir o incluso eximir la sanción.
Se premia la **proactividad y cultura de cumplimiento.**

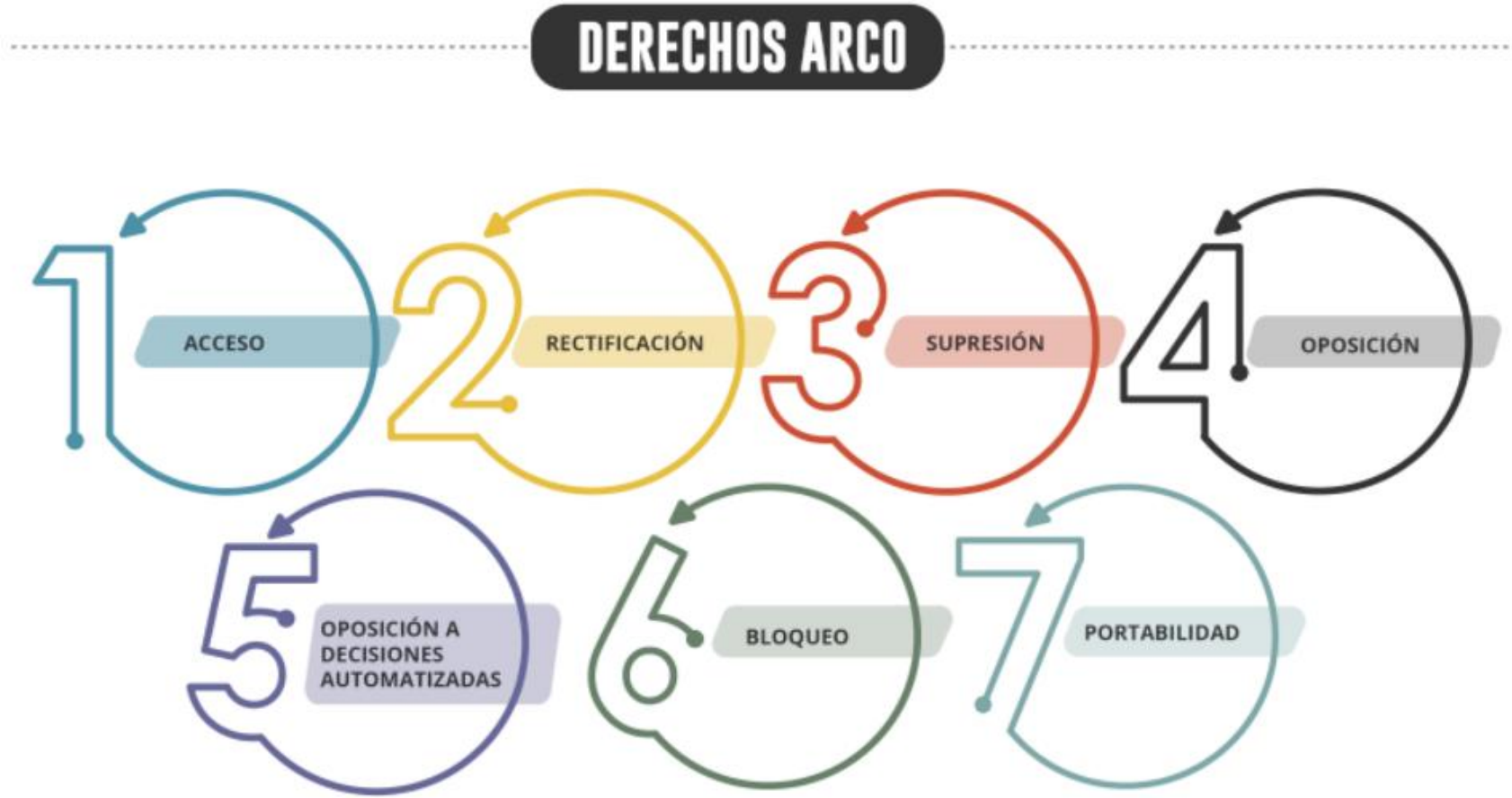
7 Responsabilidad del sector público

Los organismos del Estado serán fiscalizados y podrán recibir **requerimientos, auditorías y medidas correctivas**, aplicadas a sus autoridades responsables.

8 Transparencia y efecto reputacional

Las sanciones podrán hacerse **públicas por la Agencia**, impactando la **imagen institucional** y reforzando la rendición de cuentas ante la ciudadanía.

Derechos Arco



Derechos ARCO

- Acceso: conocer qué datos tiene el responsable.
- Rectificación: corregir información inexacta o incompleta.
- Cancelación/Supresión: solicitar eliminación de datos.
- Oposición: negarse a tratamientos no autorizados.
- Portabilidad: transferir datos a otro responsable.
- Limitación: restringir temporalmente el uso de los datos.
- Revocación: retirar el consentimiento previamente otorgado.
- Reclamación: posibilidad de acudir a la Agencia por vulneraciones.

Derechos ARCO

✅ Ejemplo Correcto – Aplicación de Derechos ARCO

> **Caso:** Ciudadano solicita la rectificación de su dirección en el registro de un servicio público.

Proceso seguido por la institución:

- 📩 El ciudadano presenta su solicitud por el canal oficial (formulario web o ventanilla única).
- 🕵️ El servicio verifica la identidad del solicitante mediante validación electrónica.
- 📋 El área responsable (protección de datos o transparencia) revisa la base de datos y confirma la modificación.
- ⏱️ En un plazo de 10 días hábiles se notifica al ciudadano la rectificación realizada.
- 🗂️ Se registra la solicitud, la acción ejecutada y el cierre del caso en un sistema de trazabilidad.

Características destacadas:

- ✔️ Procedimiento formal, trazable y documentado.
- ✔️ Respeto al principio de **exactitud** y **participación individual**.
- ✔️ Comunicación clara y dentro de los plazos establecidos.

❌ Ejemplo Incorrecto – Aplicación Deficiente de Derechos ARCO

> **Caso:** Ciudadana solicita eliminar sus datos de un registro en línea de beneficiarios.

Problemas observados:

- ✉️ La solicitud se recibe por correo electrónico sin procedimiento formal ni acuse de recibo.
- 🧩 No se verifica la identidad de la solicitante, generando riesgo de suplantación.
- 🕓 No se responde dentro del plazo, ni se entrega constancia del estado de la solicitud.
- 📁 No existe registro interno ni trazabilidad del requerimiento.
- ⚠️ Finalmente, la información permanece publicada, sin justificación documental ni respuesta al titular.

Consecuencias:

- ❌ Incumplimiento del derecho de **cancelación** y falta de **transparencia**.
- ❌ Vulneración del principio de **rendición de cuentas** y posibles sanciones.

Alineamiento con Principios de Privacidad – ISO 29100

Principios Claves de Privacidad – ISO 29100

1. Responsabilidad (Accountability)
2. Limitación de propósito
3. Minimización de datos
4. Calidad y exactitud de datos
5. Limitación de uso, retención y divulgación
6. Seguridad
7. Transparencia y apertura
8. Participación individual y acceso
9. Consentimiento y elección
10. Responsabilidad del tercero receptor
11. Cumplimiento y monitoreo

La ISO 29100 proporciona la arquitectura conceptual del tratamiento ético y legal de los datos personales: define los once principios universales que estructuran la rendición de cuentas, la legitimidad del propósito, la transparencia y la autodeterminación informativa. Su adopción permite traducir los derechos fundamentales de los titulares en políticas coherentes y verificables dentro de cualquier institución pública o privada

Responsabilidad

1. **Demostrabilidad** – Mostrar evidencia ante auditores o autoridad.
2. **Documentación** – Políticas, consentimientos, registros de tratamiento.
3. **Gobernanza** – Roles y responsabilidades definidos.
4. **Evaluaciones de impacto (PIA)** – Riesgos y mitigaciones documentadas.
5. **Mejora continua (PDCA)** – Revisar, medir, ajustar procesos.
6. **Capacitación** – Personal formado en privacidad.
7. **Gestión de incidentes** – Notificación, registro, lecciones aprendidas.
8. **Gestión de terceros** – Contratos con cláusulas de privacidad.
9. **Proporcionalidad** – Medidas acordes al riesgo del tratamiento.
10. **Trazabilidad** – Registro de qué, quién, cómo, cuándo y por qué.

"Cumplir no basta: hay que poder demostrarlo."

Principio ISO 29100	Artículo ISO 29100	Concepto central	Referencia Ley 21.719 (2024)	Referencia Ley 19.628 (1999)	Descripción del vínculo normativo
1. Responsabilidad (Accountability)	Art. 4.2	El responsable debe demostrar cumplimiento.	Art. 3 letra e), Art. 14 quinquies letra j)	Art. 11 (deber de diligencia del responsable)	Ambas leyes establecen que el responsable responde legalmente por las infracciones y debe mantener evidencia de cumplimiento.

Limitación del Propósito

1. **Finalidad definida:** Toda recolección de datos debe responder a un propósito claro y documentado.
2. **Legitimidad:** El propósito debe tener fundamento legal o consentimiento válido.
3. **Transparencia:** El titular debe conocer el objetivo del tratamiento en lenguaje simple.
4. **Coherencia:** El uso real de los datos debe coincidir con el propósito declarado.
5. **Prohibición de reutilización:** No se pueden usar los datos para fines distintos sin nueva base legal.
6. **Actualización de finalidades:** Cualquier cambio debe registrarse y comunicarse formalmente.
7. **Control interno:** Los sistemas deben vincular cada base de datos con su finalidad.
8. **Minimización del tratamiento:** Solo se recopilan los datos necesarios para cumplir el fin declarado.
9. **Supervisión:** El cumplimiento de la finalidad debe auditarse periódicamente.
10. **Rendición de cuentas:** La institución debe poder demostrar el respeto al propósito declarado.

Principio ISO 29100	Artículo ISO 29100	Concepto central	Referencia Ley 21.719 (2024)	Referencia Ley 19.628 (1999)	Descripción del vínculo normativo
2. Limitación de propósito	Art. 4.3	Los datos se tratan con fines específicos y legítimos.	Art. 3 letra b) y Art. 14 ter	Art. 12 (finalidad del almacenamiento y comunicación)	Chile exige que los datos se usen solo para los fines informados al titular.

Limitación del Propósito – Ejemplos

✅ Ejemplo Correcto – Buena Aplicación del Principio de Limitación del Propósito

> **Caso:** Un servicio público recolecta datos personales para gestionar postulaciones a subsidios habitacionales.

Proceso y características:

- 🏛️ En el formulario de postulación se informa claramente:
  "Los datos solicitados serán utilizados exclusivamente para la evaluación, asignación y seguimiento del subsidio habitacional. No se utilizarán con fines distintos."
- 📄 Los funcionarios solo acceden a la información necesaria para la evaluación.
- 🔒 Los datos no son compartidos con otras instituciones, salvo con organismos colaboradores autorizados mediante convenio formal.
- 🗑️ Una vez finalizado el proceso, los antecedentes son archivados y los no seleccionados son eliminados conforme a política de retención.

Buenas prácticas evidentes:

- ✔️ Propósito definido, legítimo y documentado.
- ✔️ Uso restringido al fin declarado.
- ✔️ Política de conservación y eliminación alineada a la finalidad.
- ✔️ Transparencia frente al ciudadano.

❌ Ejemplo Incorrecto – Mala Aplicación del Principio de Limitación del Propósito

> **Caso:** Un municipio utiliza la base de datos de beneficiarios de programas sociales para enviar propaganda electoral o encuestas políticas.

Problemas detectados:

- ⚠️ Los datos se recolectaron originalmente para fines sociales, no políticos.
- ❌ No existe consentimiento ni base legal que justifique el nuevo uso.
- ❌ No se informó al titular sobre este cambio de finalidad.
- ⚫ No hay registro de auditoría ni control interno sobre el uso posterior de la información.

Consecuencias:

- 🚫 Vulneración directa del principio de **finalidad y transparencia**.
- 🚫 Uso indebido de datos personales con riesgo reputacional y sancionatorio.
- 🚫 Falta de rendición de cuentas y trazabilidad del tratamiento.

Minimización de Datos

1. **Necesidad:** Recolectar únicamente los datos indispensables para el propósito definido.
2. **Pertinencia:** Asegurar que los datos sean relevantes y adecuados al fin declarado.
3. **Exactitud:** Evitar datos redundantes, excesivos o desactualizados.
4. **Evaluación previa:** Justificar la necesidad de cada dato antes de recolectarlo.
5. **Control de formularios:** Revisar campos innecesarios o de uso histórico sin valor actual.
6. **Limitación técnica:** Configurar sistemas para restringir la captura y almacenamiento excesivo.
7. **Revisión periódica:** Evaluar y eliminar información que ya no sea necesaria.
8. **Segmentación:** Separar datos personales de otros para reducir exposición.
9. **Responsabilidad compartida:** Las áreas usuarias deben justificar por qué cada dato es requerido.
10. **Evidencia:** Documentar los criterios utilizados para determinar la necesidad de cada dato.

Principio ISO 29100	Artículo ISO 29100	Concepto central	Referencia Ley 21.719 (2024)	Referencia Ley 19.628 (1999)	Descripción del vínculo normativo
3. Minimización de datos	Art. 4.4	Solo se recolectan los datos estrictamente necesarios.	Art. 3 letra c) y Art. 14 ter letra d)	Art. 10 (datos sensibles y límites de tratamiento)	Los datos deben ser adecuados, pertinentes y no excesivos en relación con su finalidad.

Minimización de Datos – Ejemplos

✅ Ejemplo Correcto – Buena Aplicación del Principio de Minimización de Datos

> **Caso:** Un servicio público implementa un formulario en línea para solicitar becas de capacitación laboral.

Proceso y características:

- 📄 El formulario solo solicita los datos estrictamente necesarios: nombre, RUT, edad, contacto y nivel educacional.
- 🔍 No se piden antecedentes sensibles (salud, ingresos familiares o estado civil) que no afectan la evaluación.
- 💻 El sistema valida automáticamente los campos obligatorios y bloquea la incorporación de datos adicionales.
- 🧹 Los registros se depuran anualmente, eliminando postulaciones no seleccionadas.

Buenas prácticas evidentes:

- ✔️ Recolección proporcional y pertinente al objetivo.
- ✔️ Validación técnica que impide el exceso de datos.
- ✔️ Política de retención y depuración periódica.
- ✔️ Alineamiento con principios de finalidad y exactitud.

Minimización de Datos – Ejemplos

❌ Ejemplo Incorrecto – Mala Aplicación del Principio de Minimización de Datos

> **Caso:** Un organismo público solicita antecedentes excesivos para inscribirse en un curso gratuito en línea.

Problemas detectados:

- ⚠️ El formulario exige información innecesaria: estado civil, número de hijos, situación laboral, ingresos, y nombre del cónyuge.
- ❌ No se explica por qué esos datos son relevantes para la inscripción.
- 📁 No existe política de eliminación de registros antiguos.
- 🧩 Los datos se comparten con otras unidades sin evaluación de pertinencia.

Consecuencias:

- 🚫 Vulneración del principio de **proporcionalidad y necesidad**.
- 🚫 Riesgo de exposición innecesaria de datos personales.
- 🚫 Falta de control interno y ausencia de revisión periódica de formularios.

Calidad y Exactitud de los Datos

1. **Exactitud:** Los datos deben reflejar la realidad del titular sin errores ni distorsiones.
2. **Integridad:** La información no debe estar incompleta ni fragmentada.
3. **Actualización:** Debe mantenerse vigente y revisarse periódicamente.
4. **Pertinencia:** Solo conservar datos que guarden relación con la finalidad declarada.
5. **Corrección:** Implementar mecanismos que permitan rectificar información inexacta.
6. **Validación:** Aplicar controles de verificación antes de registrar o utilizar datos.
7. **Responsabilidad compartida:** Las áreas que usan datos deben verificar su calidad antes de procesarlos.
8. **Control de versiones:** Evitar duplicidades o inconsistencias entre sistemas.
9. **Evidencia de revisión:** Mantener registro de actualizaciones o rectificaciones efectuadas.
10. **Prevención de errores:** Integrar controles automáticos que reduzcan fallas humanas o técnicas.

Principio ISO 29100	Artículo ISO 29100	Concepto central	Referencia Ley 21.719 (2024)	Referencia Ley 19.628 (1999)	Descripción del vínculo normativo
4. Calidad y exactitud de datos	Art. 4.5	Los datos deben ser exactos y actualizados.	Art. 3 letra d), Art. 14 quinquies letra i)	Art. 12 inciso 1°–3°	Ambas leyes obligan a mantener los datos correctos, completos y actualizados.

Calidad y Exactitud de los Datos - Ejemplos

✅ Ejemplo Correcto – Buena Aplicación del Principio de Calidad y Exactitud de los Datos

> **Caso:** Un servicio público mantiene actualizado su registro de beneficiarios de programas sociales.

Proceso y características:

- 📝 El sistema valida automáticamente que los datos ingresados (dirección, correo, teléfono) sean reales y estén completos.
- 🗓️ Se actualizan los registros anualmente mediante comunicación directa con los beneficiarios.
- 🕯️ Los ciudadanos pueden solicitar correcciones o actualizaciones mediante un formulario digital.
- 🔍 Cada modificación queda registrada con fecha, usuario responsable y motivo de cambio.

Buenas prácticas evidentes:

- ✔️ Datos precisos, actualizados y verificables.
- ✔️ Procedimiento formal de rectificación.
- ✔️ Control de versiones y trazabilidad.
- ✔️ Participación activa del titular en la actualización.

❌ Ejemplo Incorrecto – Mala Aplicación del Principio de Calidad y Exactitud de los Datos

> **Caso:** Un municipio utiliza bases de datos desactualizadas para enviar notificaciones de contribuciones.

Problemas detectados:

- ⚠️ Las direcciones no se revisan desde hace varios años.
- 📫 Los avisos se envían a domicilios erróneos o personas fallecidas.
- ❌ No existen procedimientos para que los ciudadanos actualicen su información.
- 🗂️ No hay registro de revisiones ni controles de consistencia entre sistemas.

Consecuencias:

- 🚫 Vulneración del principio de **exactitud y actualización**.
- 🚫 Riesgo de filtración o mal uso de datos personales.
- 🚫 Pérdida de confianza institucional y errores en la gestión pública.

Limitación de Uso, Retención y Divulgación

1. **Uso legítimo:** Los datos solo pueden emplearse para los fines originalmente declarados.
2. **Retención limitada:** Conservar la información únicamente durante el tiempo necesario.
3. **Eliminación o anonimización:** Implementar procesos seguros de eliminación cuando el dato pierde vigencia.
4. **Divulgación restringida:** Controlar toda transferencia o publicación de datos personales.
5. **Autorización previa:** Requerir base legal o consentimiento antes de divulgar información.
6. **Control de acceso:** Limitar internamente quién puede usar o consultar datos personales.
7. **Registro de uso:** Mantener evidencia de cuándo, quién y para qué se accede a la información.
8. **Procedimientos de borrado:** Establecer rutinas periódicas de depuración y destrucción de archivos.
9. **Supervisión continua:** Revisar que los sistemas no retengan datos obsoletos ni los compartan sin control.
10. **Responsabilidad documental:** Demostrar que las políticas de retención y divulgación están implementadas.

Principio ISO 29100	Artículo ISO 29100	Concepto central	Referencia Ley 21.719 (2024)	Referencia Ley 19.628 (1999)	Descripción del vínculo normativo
5. Limitación de uso, retención y divulgación	Art. 4.5	Los datos no deben conservarse más tiempo del necesario.	Art. 3 letra c), Art. 14 ter f)	Art. 18 (eliminación luego de cinco años)	Se limita el tiempo de conservación y la comunicación posterior del dato.

Limitación de Uso, Retención y Divulgación -Ejemplos

✅ Ejemplo Correcto – Buena Aplicación del Principio de Limitación de Uso, Retención y Divulgación

> **Caso:** Un servicio público administra una base de datos de postulantes a programas de becas estatales.

Proceso y características:

- 📋 Los datos se utilizan **únicamente** para la evaluación, asignación y seguimiento del beneficio.
- ⏱️ Se conservan por **cinco años**, según la política institucional de retención de documentos.
- 🗑️ Al concluir el período, los antecedentes se **anonimizan o eliminan** de forma segura.
- 🔒 Los datos solo se comparten con organismos públicos que participan directamente en el proceso, mediante convenios formales.
- 📑 Todo el ciclo de tratamiento queda documentado y es trazable.

Buenas prácticas evidentes:

- ✔️ Uso restringido al propósito declarado.
- ✔️ Retención temporal justificada y documentada.
- ✔️ Control de divulgación y convenios formales.
- ✔️ Eliminación o anonimización segura al cierre del proceso.

❌ Ejemplo Incorrecto – Mala Aplicación del Principio de Limitación de Uso, Retención y Divulgación

> **Caso:** Un organismo mantiene durante años una base de datos de antiguos beneficiarios y la utiliza para campañas de comunicación general sin autorización.

Problemas detectados:

- ⚠️ Los datos se usaron con fines distintos al propósito original (difusión institucional).
- 🗂️ No existen plazos de retención definidos ni procedimientos de depuración.
- ❌ La información se comparte con otros servicios sin convenio ni fundamento legal.
- 🧩 No hay evidencia de eliminación o control de acceso.
- ⚠️ Los titulares no fueron informados del nuevo uso ni del tiempo de conservación.

Consecuencias:

- 🚫 Vulneración del principio de **limitación del uso y finalidad**.
- 🚫 Riesgo de exposición de información personal y pérdida de confianza pública.
- 🚫 Falta de trazabilidad y control institucional sobre la información tratada.

Seguridad

1. **Protección integral:** Seguridad física, lógica y organizacional coordinadas entre sí.
2. **Confidencialidad:** Solo el personal autorizado puede acceder a los datos.
3. **Integridad:** Los datos no deben ser alterados o manipulados sin autorización.
4. **Disponibilidad:** Garantizar acceso oportuno cuando es legítimo y necesario.
5. **Autenticación y control de acceso:** Usuarios identificados, perfiles limitados y trazabilidad.
6. **Cifrado y resguardo:** Uso de técnicas de encriptación y almacenamiento seguro.
7. **Gestión de incidentes:** Procedimientos formales para detectar, reportar y mitigar brechas.
8. **Continuidad operativa:** Respaldo y recuperación ante desastres o fallas críticas.
9. **Supervisión de terceros:** Proveedores y encargados sujetos a controles y auditorías.
10. **Cultura de seguridad:** Capacitación permanente y concienciación institucional.

Principio ISO 29100	Artículo ISO 29100	Concepto central	Referencia Ley 21.719 (2024)	Referencia Ley 19.628 (1999)	Descripción del vínculo normativo
6. Seguridad	Art. 4.6	Los datos deben protegerse con medidas técnicas y organizativas.	Art. 3 letra f), Art. 14 quinquies letras c–f	Art. 11 (cuidado y responsabilidad del tratamiento)	Ambas leyes exigen medidas proporcionales a la naturaleza y riesgo del tratamiento.

Seguridad - Ejemplos

1️⃣ **DLP – *Data Loss Prevention***

🔍 Monitorea, detecta y bloquea la salida no autorizada de información sensible (por correo, nube, USB o impresiones).

💡 Ejemplo: *Symantec DLP, Forcepoint, Microsoft Purview DLP.*

2️⃣ **SIEM – *Security Information and Event Management***

📊 Consolida logs y eventos de seguridad para detectar patrones anómalos o incidentes.

💡 Ejemplo: *Splunk, IBM QRadar, Elastic SIEM.*

3️⃣ **IAM – *Identity and Access Management***

🔐 Controla la autenticación, permisos y trazabilidad de los usuarios sobre sistemas y datos.

💡 Ejemplo: *Okta, Azure AD, Oracle IAM.*

4️⃣ **MFA – *Multi-Factor Authentication***

🔑 Aumenta la seguridad en el acceso mediante doble o triple verificación (token, biometría, PIN).

💡 Ejemplo: *Google Authenticator, Duo Security, Microsoft Authenticator.*

5️⃣ **Backup y recuperación segura**

💾 Asegura la disponibilidad de los datos ante incidentes, ransomware o fallas técnicas.

💡 Ejemplo: *Veeam, Acronis, CommVault, Azure Backup.*

6️⃣ **Cifrado de datos (*Encryption*)**

🧩 Protege la confidencialidad tanto en tránsito como en reposo mediante algoritmos criptográficos robustos.

💡 Ejemplo: *BitLocker, VeraCrypt, OpenSSL.*

7️⃣ **CASB – *Cloud Access Security Broker***

☁️ Supervisa y regula el uso de aplicaciones en la nube, asegurando cumplimiento y control de acceso.

💡 Ejemplo: *Netskope, McAfee MVISION, Zscaler.*

8️⃣ **EDR / XDR – *Endpoint Detection & Response***

🖥️ Detecta y responde a amenazas avanzadas en equipos finales, con análisis de comportamiento.

💡 Ejemplo: *CrowdStrike Falcon, SentinelOne, Microsoft Defender for Endpoint.*

9️⃣ **Herramientas de gestión de vulnerabilidades**

🧠 Escanean sistemas y aplicaciones para identificar brechas y priorizar parches.

💡 Ejemplo: *Tenable Nessus, Qualys, Rapid7.*

🔟 **Plataformas de concienciación y simulación de phishing**

🎓 Fortalecen la cultura de seguridad capacitando al personal frente a ataques sociales.

💡 Ejemplo: *KnowBe4, Cofense, Terranova Security.*

Transparencia y apertura

1. **Claridad informativa:** Comunicar en lenguaje simple y comprensible el uso de los datos.
2. **Accesibilidad:** Facilitar el acceso del titular a las políticas y procedimientos de privacidad.
3. **Avisos de privacidad:** Mantener disponibles declaraciones sobre finalidades, derechos y contactos.
4. **Canales de consulta:** Disponer medios formales para solicitar información sobre el tratamiento.
5. **Publicidad activa:** Difundir políticas y normas internas en portales institucionales.
6. **Registro de tratamientos:** Mantener información pública o trazable sobre bases de datos gestionadas.
7. **Actualización continua:** Revisar periódicamente la información entregada a los titulares.
8. **Evidencia de cumplimiento:** Documentar que la institución entrega información cuando se solicita.
9. **Transparencia proactiva:** Anticipar comunicación ante cambios en finalidades o responsables.
10. **Cultura institucional:** Promover una gestión abierta y verificable frente a la ciudadanía.

Principio ISO 29100	Artículo ISO 29100	Concepto central	Referencia Ley 21.719 (2024)	Referencia Ley 19.628 (1999)	Descripción del vínculo normativo
7. Transparencia y apertura	Art. 4.7	Se debe informar al titular sobre el tratamiento.	Art. 3 letra g), Art. 14 ter	Art. 12 inciso 1°	Se obliga a informar política de privacidad y medios de ejercicio de derechos.

Participación Individual y Acceso

1. **Derecho de acceso:** Todo titular puede solicitar información sobre sus datos tratados.
2. **Derecho de rectificación:** Permite corregir errores o inexactitudes en los datos personales.
3. **Derecho de eliminación:** Autoriza a solicitar la supresión de información cuando sea procedente.
4. **Derecho de oposición:** Posibilita oponerse al tratamiento en casos sin fundamento legal.
5. **Mecanismos accesibles:** Deben existir canales simples, gratuitos y sin barreras para ejercer derechos.
6. **Plazos definidos:** Las instituciones deben responder en tiempos razonables y normativamente fijados.
7. **Identificación del solicitante:** El proceso debe garantizar la autenticidad del titular.
8. **Registro de solicitudes:** Llevar trazabilidad de peticiones, respuestas y tiempos de atención.
9. **Transparencia procesal:** Informar al titular el estado y resultado de su solicitud.
10. **Supervisión y mejora:** Analizar tendencias de reclamos para fortalecer la gestión de derechos.

Principio ISO 29100	Artículo ISO 29100	Concepto central	Referencia Ley 21.719 (2024)	Referencia Ley 19.628 (1999)	Descripción del vínculo normativo
8. Participación individual y acceso	Art. 4.8	Los titulares pueden acceder, rectificar o eliminar sus datos.	Art. 4–11 (Derechos ARCO+)	Art. 12 completo	Ambas leyes reconocen el derecho de acceso, rectificación y eliminación.

Participación Individual y Acceso

✅ Ejemplo Correcto – Buena Aplicación del Principio de Participación Individual y Acceso

> **Caso:** Un ciudadano solicita acceder a la información que mantiene un ministerio sobre él en un registro de programas sociales.

Proceso y características:

- 📥 El ministerio dispone de un **formulario en línea** y canal presencial para ejercer los derechos ARCO.
- 🧍 Se valida la identidad del solicitante mediante ClaveÚnica.
- ⏱️ En un plazo de 10 días hábiles, el ciudadano recibe una respuesta clara con copia de la información registrada.
- 🖍️ Se ofrece la posibilidad de **rectificar o eliminar** datos desactualizados.
- 🗂️ La solicitud queda registrada en una bitácora institucional con fecha, responsable y resolución.

Buenas prácticas evidentes:

- ✔️ Procedimiento formal, trazable y accesible.
- ✔️ Respuesta dentro de plazo legal.
- ✔️ Comunicación clara y lenguaje comprensible.
- ✔️ Participación del titular como parte del control ciudadano.

❌ Ejemplo Incorrecto – Mala Aplicación del Principio de Participación Individual y Acceso

> **Caso:** Una persona solicita a un servicio público conocer y corregir sus datos personales, pero no recibe respuesta.

Problemas detectados:

- ⚠️ No existe un canal formal para ejercer los derechos; solo se acepta por correo genérico.
- 🕓 La institución no responde dentro del plazo ni entrega constancia de recepción.
- 🧩 No hay registro interno ni trazabilidad del requerimiento.
- ❌ El ciudadano nunca es informado del estado ni del resultado de su solicitud.
- 📄 Los datos erróneos permanecen sin corrección ni justificación.

Consecuencias:

- 🚫 Incumplimiento del principio de **participación individual y transparencia**.
- 🚫 Riesgo de sanciones por falta de procedimiento.
- 🚫 Pérdida de confianza pública y debilidad en la rendición de cuentas.

Consentimiento y elección

1. **Libertad:** El consentimiento debe otorgarse sin coerción ni condicionamientos.
2. **Información:** El titular debe conocer claramente la finalidad y el uso de sus datos.
3. **Especificidad:** Debe referirse a un propósito concreto, no a autorizaciones genéricas.
4. **Expresividad:** Debe manifestarse de forma explícita (escrita, digital o equivalente verificable).
5. **Revocabilidad:** El titular puede retirar su consentimiento en cualquier momento.
6. **Registro de consentimiento:** La institución debe conservar evidencia verificable de la autorización.
7. **Transparencia:** La solicitud debe ser clara, destacada y sin lenguaje engañoso.
8. **Proporcionalidad:** No se deben exigir más datos que los necesarios para el fin autorizado.
9. **Excepciones legales:** El tratamiento sin consentimiento debe fundarse en norma expresa o función pública.
10. **Supervisión:** Se deben revisar periódicamente los procedimientos de obtención y gestión de consentimientos.

Principio ISO 29100	Artículo ISO 29100	Concepto central	Referencia Ley 21.719 (2024)	Referencia Ley 19.628 (1999)	Descripción del vínculo normativo
9. Consentimiento y elección	Art. 4.9	El tratamiento se basa en consentimiento libre e informado.	Art. 12 y 13	Art. 4 y 10	Requieren consentimiento previo, salvo excepciones legales.

Consentimiento y elección – Ejemplos

✅ Ejemplo de Consentimiento Válido (Correcto)

> **Formulario digital de un servicio público de salud:**

Texto mostrado al titular:

> "Autorizo al Servicio de Salud Metropolitana a utilizar mis datos personales de contacto (nombre, correo electrónico y teléfono) exclusivamente para comunicarme sobre mi cita médica y enviar recordatorios relacionados con mi atención.
> He sido informado/a de que puedo retirar esta autorización en cualquier momento escribiendo a datos@ssm.cl ↗."

Características del consentimiento:

- ✔ **Libre:** No es requisito para acceder a la atención médica.
- ✔ **Informado:** Explica claramente la finalidad y el uso de los datos.
- ✔ **Expreso:** Requiere acción afirmativa (check o firma).
- ✔ **Específico:** Limita el tratamiento a la comunicación de citas.
- ✔ **Revocable:** Indica el mecanismo para retirar la autorización.

❌ Ejemplo de Consentimiento Inválido (Incorrecto)

> **Formulario de inscripción genérico en un sitio institucional:**

Texto mostrado al titular:

> "Acepto los términos y condiciones del servicio y autorizo el uso de mis datos para cualquier fin institucional que la entidad estime conveniente."

Problemas del consentimiento:

- ❌ **Vago e impreciso:** No se especifican finalidades ni tipos de tratamiento.
- ❌ **No informado:** El titular desconoce cómo, quién y para qué usará los datos.
- ❌ **Amplio o genérico:** "Cualquier fin institucional" no cumple con especificidad ni proporcionalidad.
- ❌ **No revocable:** No se menciona cómo puede retirarse la autorización.
- ❌ **Condicionado:** Se impone como requisito para acceder al servicio.

Responsabilidad del tercero receptor

1️⃣ **Deber de confidencialidad:** El tercero debe proteger los datos con el mismo nivel de seguridad que el responsable original.
2️⃣ **Finalidad restringida:** Los datos solo pueden usarse para el propósito autorizado.
3️⃣ **Contrato formal:** Debe existir acuerdo o cláusula que establezca obligaciones y sanciones.
4️⃣ **Prohibición de cesión:** El tercero no puede transferir los datos a otros sin autorización expresa.
5️⃣ **Medidas de seguridad:** Debe aplicar controles técnicos y organizativos equivalentes o superiores.
6️⃣ **Supervisión del responsable:** El titular o responsable mantiene facultades de auditoría y control.
7️⃣ **Eliminación o devolución:** Los datos deben destruirse o devolverse al finalizar la relación contractual.
8️⃣ **Notificación de incidentes:** El tercero debe informar cualquier brecha o acceso no autorizado.
9️⃣ **Responsabilidad solidaria:** En caso de incumplimiento, ambos pueden ser responsables frente al titular.
🔟 **Evidencia contractual:** Se debe conservar documentación que acredite cumplimiento y supervisión.

Principio ISO 29100	Artículo ISO 29100	Concepto central	Referencia Ley 21.719 (2024)	Referencia Ley 19.628 (1999)	Descripción del vínculo normativo
10. Responsabilidad del tercero receptor	Art. 4.10	El receptor de datos debe cumplir los mismos principios.	Art. 15 bis (encargados y subencargados), Art. 26 (transferencias internacionales)	Art. 8 (comunicación a terceros)	Los encargados y receptores deben mantener los mismos estándares de protección.

Responsabilidad del tercero receptor - ejemplo

✅ Ejemplo Correcto – Buena Aplicación del Principio de Responsabilidad del Tercero Receptor

> **Caso:** Un ministerio contrata a una empresa externa para procesar datos de postulaciones a concursos públicos.

Proceso y características:

- 📜 El contrato establece cláusulas de **confidencialidad, finalidad exclusiva y prohibición de cesión** de los datos.
- 🔒 El proveedor aplica medidas de **seguridad equivalentes** a las del ministerio (cifrado, control de accesos, registro de incidentes).
- 🗑️ Se define un plazo de retención y obligación de **eliminar o devolver** los datos una vez finalizado el servicio.
- 🔍 El ministerio realiza auditorías periódicas para verificar cumplimiento.
- 🗂️ Todo el proceso está documentado con evidencias de control y supervisión.

Buenas prácticas evidentes:

- ✔️ Contrato formal y detallado.
- ✔️ Supervisión activa y trazabilidad.
- ✔️ Seguridad técnica y organizativa alineada.
- ✔️ Eliminación controlada de los datos al cierre.

❌ Ejemplo Incorrecto – Mala Aplicación del Principio de Responsabilidad del Tercero Receptor

> **Caso:** Un servicio público entrega a un proveedor de software una base de datos ciudadana para pruebas sin resguardo ni control contractual.

Problemas detectados:

- ⚠️ No existe contrato formal que defina deberes de confidencialidad ni límites de uso.
- 🗂️ El proveedor utiliza los datos para fines propios (pruebas y demostraciones comerciales).
- 🕳️ No se aplica cifrado ni control de acceso sobre la información compartida.
- ❌ No hay registros de supervisión ni de devolución o eliminación de los datos.
- 🚨 Se detecta que parte de la información terminó almacenada en servidores fuera del país.

Consecuencias:

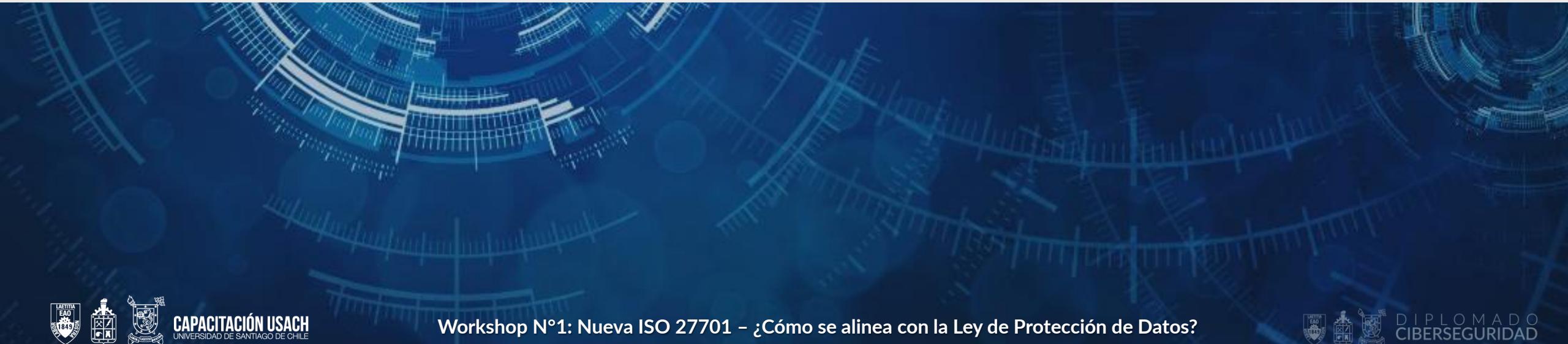
- 🚫 Vulneración de los principios de **confidencialidad y trazabilidad**.
- 🚫 Riesgo de filtración y responsabilidad solidaria del servicio público.
- 🚫 Falta de evidencia contractual y control institucional.

Cumplimiento y Monitoreo

1. **Gobernanza activa:** Designar responsables y definir roles claros de supervisión.
2. **Políticas vigentes:** Mantener normas internas actualizadas y comunicadas.
3. **Evaluaciones periódicas:** Realizar revisiones y autoevaluaciones de cumplimiento.
4. **Indicadores y métricas:** Medir avances y brechas mediante reportes cuantificables.
5. **Auditorías internas:** Ejecutar verificaciones planificadas con seguimiento de hallazgos.
6. **Planes de mejora:** Documentar y aplicar acciones correctivas y preventivas.
7. **Monitoreo continuo:** Usar herramientas o controles que detecten desviaciones en tiempo real.
8. **Comunicación institucional:** Reportar avances y brechas a la alta dirección.
9. **Evidencia documental:** Conservar actas, informes y registros de cumplimiento.
10. **Revisión externa:** Permitir auditorías o fiscalizaciones por entes competentes.

Principio ISO 29100	Artículo ISO 29100	Concepto central	Referencia Ley 21.719 (2024)	Referencia Ley 19.628 (1999)	Descripción del vínculo normativo
11. Cumplimiento y monitoreo	Art. 4.11	Deben existir mecanismos de control y auditoría.	Art. 14 quinquies j), Art. 29 (fiscalización de la Agencia)	Art. 11 y Título II (derechos de los titulares)	La Agencia de Protección de Datos y los responsables deben auditar y reportar cumplimiento.

ISO 27701:2025 SGIP



Características de la ISO 27701

1 Es un sistema de gestión certificable

Permite a las organizaciones obtener **certificación formal** de su cumplimiento en privacidad, mediante auditorías independientes, al igual que ISO 27001 en seguridad de la información.

> *Demuestra cumplimiento real, no solo declarativo.*

2 Alinea la gestión con el marco europeo (GDPR)

Recoge los **principios, derechos y obligaciones del Reglamento General de Protección de Datos (GDPR)**, asegurando equivalencia con estándares internacionales de privacidad.

> *Facilita interoperabilidad con Europa y otros mercados que reconocen el GDPR.*

3 Incorpora los principios universales de privacidad (ISO 29100)

Integra principios como **licitud, finalidad, minimización, exactitud, seguridad y responsabilidad demostrable**, transformándolos en políticas y controles concretos.

> *Conecta la ética de la privacidad con la gestión operativa.*

4 Establece roles y responsabilidades formales

Distingue y define los deberes del **responsable (PII Controller)** y del **encargado (PII Processor)**, creando claridad organizacional y fortaleciendo la rendición de cuentas.

> *Claridad de funciones = menos brechas y conflictos de control.*

5 Complementa, pero no depende, de ISO 27001 e ISO 27002

Aunque se origina en la familia de seguridad de la información, hoy actúa como **estándar autónomo**, manteniendo compatibilidad con sistemas de gestión de seguridad (SGSI).

> *Seguridad + Privacidad = Confianza digital institucional.*

6 Aporta trazabilidad y evidencia de cumplimiento (Accountability)

Exige **documentar políticas, evaluaciones de impacto, registros y decisiones**, asegurando que la organización pueda **probar cumplimiento** ante reguladores como la Agencia de Protección de Datos.

> *Lo que no se evidencia, no se cumple.*

7 Facilita la adecuación a leyes nacionales como la Ley 21.719

Sus controles y requisitos se alinean perfectamente con los **principios de la ley chilena**, proporcionando una **metodología estructurada** para implementarla de manera verificable.

> CL *La ISO 27701 es el puente entre la ley y la práctica.*

8 Es un estándar global y evolutivo

Reconocido a nivel internacional, su adopción demuestra **madurez institucional y compromiso con la privacidad**, y se actualiza para incorporar buenas prácticas emergentes (como IA y gobernanza de datos).

> *Garantiza competitividad y confianza en un ecosistema digital global.*

Principal cambio: La autonomía como un Sistema de Gestión

ANTES

- Extensión de la ISO 27001 y 27002, mas un conjunto de controles adicionales propios de la información de privacidad.
- Se analizaba cada clausula de la ISO 27001 y en caso de ser necesario se establecían extensiones para privacidad.
- Se analizaba cada control de la ISO 27002 y en caso de ser necesario se establecían extensiones para privacidad.
- Definía una serie de controles propios para la privacidad.

HOY Versión 2025

- Sistema de Gestión de Información de Privacidad ISO 27701, en total autonomía y alineado todos los principios de un Sistema de Gestión
- Todas las clausulas del Sistema de Gestión son independientes y relativas a privacidad.
- Define controles propios para la información de privacidad

Posee una estructura de un Sistema de Gestión Estándar

PLANIFICAR

- 4 CONTEXTO DE LA ORGANIZACIÓN
  - COMPRENSIÓN DE LA ORGANIZACIÓN Y SU CONTEXTO
  - COMPRENSIÓN DE LAS NECESIDADES Y EXPECTATIVAS DE LAS PARTES INTERESADAS
  - DETERMINACIÓN DEL ALCANCE DEL SISTEMA DE GESTIÓN DE INFORMACIÓN DE PRIVACIDAD
  - SISTEMA DE GESTIÓN DE INFORMACIÓN DE PRIVACIDAD
- 5 LIDERAZGO
  - LIDERAZGO Y COMPROMISO
  - POLÍTICA DE PRIVACIDAD
  - ROLES, RESPONSABILIDADES Y AUTORIDADES
- 6 PLANIFICACIÓN
  - ACCIONES PARA ABORDAR LOS RIESGOS Y OPORTUNIDADES
  - OBJETIVOS DE PRIVACIDAD Y PLANIFICACIÓN PARA LOGRARLOS
  - PLANIFICACIÓN DE LOS CAMBIOS

HACER

- 7 APOYO
  - RECURSOS
  - COMPETENCIA
  - CONCIENCIZACIÓN
  - COMUNICACIÓN
  - INFORMACIÓN DOCUMENTADA
- 8 OPERACIÓN
  - PLANIFICACIÓN Y CONTROL OPERACIONAL
  - EVALUACIÓN DE RIESGSO DE PRIVACIDAD
  - TRATAMIENTO DE RIESGOS DE PRIVACIDAD

VERIFICAR

- 9 EVALUACIÓN DE DESEMPEÑO
  - SEGUIMIENTO, MEDICIÓN ANÁLISIS Y EVALUACIÓN
  - AUDITORÍA INTERNA
  - REVISIÓN POR LA DIRECCIÓN

ACTUAR

- 10 MEJORA
  - MEJORA CONTINUA
  - NO CONFORMIDAD Y ACCIONES CORRECTIVAS

Anexos de la ISO 27701

Anexo A (Normativo)

Objetivos de control de referencia y controles del Sistema de Gestión de Información de Privacidad (PIMS) aplicables a **responsables del tratamiento (PII Controllers)** y **encargados del tratamiento (PII Processors).**

> Este anexo establece los **controles mínimos obligatorios** que las organizaciones deben implementar para gestionar de manera segura, legal y responsable la información de identificación personal (PII).
> Define objetivos de control específicos en materia de consentimiento, derechos del titular, transparencia, transferencias internacionales, tratamiento de datos sensibles y retención limitada.

Anexo B (Normativo)

Guía de implementación para responsables y encargados del tratamiento de información personal (PII Controllers y PII Processors).

> Entrega **orientaciones prácticas y operativas** para aplicar los controles del Anexo A según el rol que cumple cada organización, su contexto, tamaño y nivel de madurez en privacidad.
> Incluye ejemplos de procedimientos, políticas internas y mecanismos de verificación para asegurar **trazabilidad y cumplimiento demostrable (accountability).**

Anexo C (Informativo)

Correspondencia con la norma ISO/IEC 29100 – Marco de Privacidad.

> Describe la relación directa entre los **principios de privacidad definidos en ISO/IEC 29100** (como limitación de propósito, minimización y responsabilidad) y los **controles operativos del PIMS.**
> Permite a las organizaciones mantener **consistencia conceptual** entre la gestión estratégica de la privacidad y su implementación práctica.

Anexo D (Informativo)

Correspondencia con el Reglamento General de Protección de Datos (GDPR) de la Unión Europea.

> Muestra cómo los controles y requisitos del PIMS **responden a los principios, derechos y obligaciones establecidos por el GDPR**, facilitando la armonización con marcos regulatorios internacionales.
> Destaca correspondencias clave como: base legal, consentimiento, evaluación de impacto, portabilidad, privacidad desde el diseño y supervisión de terceros.

Anexo E (Informativo)

Relación con las normas ISO/IEC 27018 e ISO/IEC 29151.

> Explica la complementariedad del PIMS con las normas especializadas en **protección de datos personales en entornos de nube pública (ISO 27018)** y **protección de información de identificación personal (ISO 29151).**
> Refuerza que, aunque la ISO/IEC 27701 ahora es independiente, **mantiene compatibilidad técnica** con los marcos de seguridad y confidencialidad derivados de la familia 27000.

Anexo F (Informativo)

Correspondencia con la versión anterior ISO/IEC 27701:2019.

> Detalla los **cambios estructurales, nuevas definiciones y controles actualizados** en la versión 2024, que consolida al PIMS como un **sistema de gestión autónomo** e independiente de ISO 27001/27002.
> Incluye ajustes terminológicos (PII Controller / Processor), la incorporación de nuevos roles de supervisión, y la ampliación del enfoque hacia **cumplimiento normativo y evaluación de impacto en privacidad (PIA).**

Actividades Claves desde el Sistema de Gestión

1 Contexto de la organización y partes interesadas

Identificar el entorno interno y externo, los actores involucrados (titulares, proveedores, reguladores) y los factores que afectan la gestión de la privacidad.

> 🌐 *Permite alinear el PIMS con los riesgos, objetivos y obligaciones reales de la institución.*

2 Liderazgo y compromiso de la alta dirección

La dirección debe **asumir responsabilidad y demostrar apoyo activo**, asignando recursos, roles y autoridad al sistema.

> 🏛️ *Sin liderazgo, no hay cultura de privacidad ni sostenibilidad del sistema.*

3 Política de privacidad institucional

Definir una política formal que refleje el compromiso con los **principios de protección de datos**, la **Ley 21.719**, el **GDPR** y los estándares internacionales.

> 📜 *La política es la carta magna del PIMS.*

4 Planificación y gestión del riesgo de privacidad

Identificar riesgos, establecer objetivos de privacidad y definir acciones preventivas y de mitigación.

> ⚖️ *Alinea la gestión con el principio de proporcionalidad y la mejora continua.*

5 Roles, responsabilidades y estructura organizacional

Designar funciones clave como el **Encargado de Protección de Datos (EPD)** y los responsables de tratamiento, estableciendo jerarquías y dependencias formales.

> 👥 *Claridad organizacional = rendición de cuentas efectiva.*

6 Soporte y recursos

Asegurar que el sistema cuente con **recursos humanos, tecnológicos y financieros** adecuados, junto con mecanismos de concienciación y formación permanente.

> 💡 *La privacidad no se declara: se sostiene con recursos.*

7 Control documental y operacional

Mantener y gestionar la documentación del PIMS: políticas, procedimientos, inventarios, evaluaciones de impacto y registros de tratamiento.

> 🗂️ *Evidencia tangible del cumplimiento (Accountability).*

8 Evaluación del desempeño y auditoría interna

Medir la eficacia del sistema mediante **indicadores, revisiones periódicas y auditorías internas**, reportando resultados a la alta dirección.

> 📊 *La mejora continua se construye sobre datos verificables.*

9 Mejora continua y acciones correctivas

Implementar un ciclo PDCA (**Planificar–Hacer–Verificar–Actuar**) que permita identificar no conformidades, analizarlas y fortalecer el sistema.

> 🔄 *Privacidad como proceso evolutivo, no estático.*

10 Integración con otros sistemas de gestión

El PIMS puede integrarse con **ISO 27001 (seguridad)**, **ISO 9001 (calidad)** o **ISO 37301 (compliance)**, generando sinergias de gobernanza.

> 🔗 *Un enfoque integrado reduce costos, brechas y duplicidades.*

Actividades Claves desde la Privacidad

1 **Identificación de roles y responsabilidades**

Definir claramente quién es el **Responsable del Tratamiento (PII Controller)** y quién actúa como **Encargado (PII Processor)** dentro de la organización.

> 👥 *Claridad de funciones = trazabilidad y rendición de cuentas.*

---

2 **Elaboración del inventario de tratamientos de datos personales**

Registrar todas las actividades de tratamiento, bases de datos, finalidades y flujos de información (internos y externos).

> 📋 *Base esencial para cumplir con la transparencia y el principio de finalidad.*

---

3 **Evaluación de riesgos de privacidad (Privacy Risk Assessment)**

Analizar riesgos asociados al tratamiento de datos personales e implementar controles proporcionales.

> ⚖️ *Permite priorizar recursos y adoptar medidas efectivas.*

---

4 **Evaluación de impacto en privacidad (PIA/DPIA)**

Realizar evaluaciones preventivas cuando el tratamiento pueda generar **alto riesgo para los derechos de las personas.**

> 🔍 *Requisito clave del GDPR y la Ley 21.719 para tratamientos sensibles o masivos.*

---

5 **Definición de políticas y procedimientos de privacidad**

Documentar políticas sobre **consentimiento, derechos ARCO+, conservación, eliminación, transferencia y brechas de seguridad.**

> 📄 *Convierte la normativa en procedimientos concretos y auditables.*

---

6 **Gestión de derechos del titular (ARCO+)**

Implementar canales formales para atender solicitudes de **acceso, rectificación, cancelación, oposición y portabilidad** de datos.

> ✉️ *Demuestra respeto activo al principio de participación individual.*

---

7 **Implementación de medidas técnicas y organizativas**

Aplicar controles de seguridad y privacidad como cifrado, anonimización, control de accesos, registros de actividad y segregación de funciones.

> 🔒 *Integración efectiva entre seguridad y privacidad.*

---

8 **Gestión de incidentes y brechas de datos personales**

Definir procedimientos de **detección, reporte, análisis y notificación** de incidentes ante la Agencia y los titulares afectados.

> 🚨 *Obligación crítica en el marco de la Ley 21.719.*

---

9 **Monitoreo, auditoría y mejora continua**

Evaluar periódicamente la eficacia del PIMS mediante auditorías internas y planes de acción.

> 📊 *El ciclo PDCA (Planificar–Hacer–Verificar–Actuar) mantiene la madurez y mejora del sistema.*

---

10 **Concienciación y formación institucional**

Capacitar al personal en los principios, procedimientos y responsabilidades del PIMS.

> 🎓 *La cultura organizacional es el control más eficaz de todos.*

¿Por qué implementar la Ley 21719 con la ISO 27701?

1 Transforma el cumplimiento en gestión proactiva

ISO 27701 permite pasar del cumplimiento reactivo ante fiscalizaciones a un modelo **preventivo y medible**, basado en riesgos, políticas y evidencia verificable ante la Agencia de Protección de Datos.

2 Estructura la gobernanza de la privacidad

Incorpora roles, responsabilidades y procesos claros para la gestión de datos personales, alineando áreas jurídicas, tecnológicas y de negocio bajo un **modelo de control integrado**.

3 Asegura la trazabilidad y rendición de cuentas (accountability)

Provee los **registros, métricas y controles** que exige la Ley 21.719 para demostrar cumplimiento frente a auditorías o requerimientos de la Agencia.

4 Fortalece la gestión de riesgos de privacidad

Permite identificar, evaluar y tratar los riesgos sobre datos personales con criterios objetivos, fortaleciendo la **cultura de gestión preventiva** y la toma de decisiones informadas.

5 Integra la protección de datos al SGSI existente (ISO 27001)

Evita duplicidades al complementar el sistema de seguridad de la información con un **módulo de privacidad (PIMS)**, logrando eficiencia en gestión, auditoría y mejora continua.

6 Facilita la adaptación a la normativa nacional e internacional

Sus controles se alinean con los principios de la Ley 21.719, el GDPR y otros marcos globales, facilitando la **interoperabilidad normativa** y reduciendo costos de adecuación futura.

7 Mejora la confianza institucional y reputacional

Demostrar cumplimiento normativo mediante un estándar internacional **aumenta la credibilidad pública** y la confianza de los ciudadanos, socios y entes fiscalizadores.

8 Impulsa la mejora continua y la madurez organizacional

Incorpora el ciclo **Planificar–Hacer–Verificar–Actuar (PDCA)** aplicado a la privacidad, asegurando evolución sostenida del sistema y consolidando una **cultura organizacional de protección de datos.**

"Agrega un completo y robusto sistema de gestión para abordar la ley, basado en el ciclo PDCA, con enfoque en riesgos, que fortalece la gobernanza, trazabilidad y control interno, posibilitando la integración con otros sistemas de gestión"

Controles para los responsables del tratamiento de información personal

Cláusula ISO 27701	Descripción resumida del control	Ley 19.628 (vigente hasta 2026)	Ley 21.719 (vigencia desde 2026)
A.1.2.2	Identificar y documentar propósito	Art. 9: uso sólo para los fines para los cuales fueron recolectados.	Art. 3 b)–c): principio de finalidad y proporcionalidad.
A.1.2.3	Identificar base legal	Art. 4 inc. 1: sólo con ley o consentimiento.	Arts. 12–13: consentimiento u otras bases legales.
A.1.2.4	Cuándo y cómo obtener consentimiento	Art. 4 incisos 1–4: consentimiento escrito, informado y revocable.	Art. 12: consentimiento libre, informado, específico, inequívoco y revocable.
A.1.2.5	Obtener y registrar consentimiento	Art. 4: consentimiento escrito e informado.	Art. 12 inc. final: responsable debe probar licitud.
A.1.2.6	Evaluación de impacto en privacidad (EIPD)	No prevista expresamente.	Art. 14 quáter: protección desde el diseño y por defecto.
A.1.2.7	Contratos con encargados	Art. 8: mandato por escrito con condiciones de seguridad.	Art. 15 bis: encargado sólo puede tratar datos por instrucciones del responsable.
A.1.2.8	Corresponsables	No regulado.	Art. 15 bis: diferencia entre responsable y encargado; responsable define fines y medios.
A.1.2.9	Registros de tratamiento (ROPA)	Art. 5: debe dejarse constancia de requirente, motivo y tipo de datos transmitidos.	Art. 14 ter a), d), h), i): registro público de actividades de tratamiento.

Obligaciones frente a los titulares de la información personal

Cláusula ISO 27701	Descripción resumida del control	Ley 19.628 (vigente hasta 2026)	Ley 21.719 (vigencia desde 2026)
A.1.3.2	Obligaciones con titulares	Art. 12: derecho a información, rectificación, eliminación.	Art. 4: derechos ARCO+, personales e irrenunciables.
A.1.3.3	Información a titulares	Art. 3: informar carácter obligatorio y finalidad.	Art. 14 ter: política pública de tratamiento.
A.1.3.4	Proveer información accesible	Art. 12: informar procedencia, finalidad y destinatarios.	Art. 5: derecho de acceso con detalle de tratamiento.
A.1.3.5	Modificar o retirar consentimiento	Art. 4 inc. 4: revocable por escrito.	Art. 12: revocable en cualquier momento sin causa.
A.1.3.6	Derecho de oposición	Art. 3 inc. 2: oposición al uso para publicidad.	Art. 8: oposición general incluso en marketing directo.
A.1.3.7	Acceso, rectificación y supresión	Arts. 12–16: acceso, modificación, eliminación.	Arts. 4–11: acceso, rectificación, supresión, oposición, bloqueo, portabilidad.
A.1.3.8	Informar a terceros cambios	Art. 12 final: aviso a quienes recibieron datos.	Art. 6 inc. 2: comunicar rectificación a destinatarios.
A.1.3.9	Proveer copia / portabilidad	Art. 12: copia gratuita del registro.	Art. 9: derecho a portabilidad electrónica.
A.1.3.10	Gestionar solicitudes de derechos	Art. 16: respuesta en 2 días hábiles.	Arts. 10–11: respuesta en 30 días + prórroga; reclamo ante Agencia.
A.1.3.11	Decisiones automatizadas	No regulado.	Art. 8 bis: derecho a no ser objeto de decisiones automáticas.

Obligaciones frente a los titulares de la información personal

Cláusula ISO 27701	Descripción resumida del control	Ley 19.628 (vigente hasta 2026)	Ley 21.719 (vigencia desde 2026)
A.1.4.2	Limitación de recolección	Art. 9.	Art. 3 b)–c) y 14 quáter: minimización y privacidad por diseño.
A.1.4.3	Limitación del tratamiento	Art. 9.	Art. 3 b).
A.1.4.4	Exactitud y calidad	Art. 6: corrección de datos inexactos.	Art. 3 d): principio de calidad.
A.1.4.5	Minimización / seudonimización	Art. 6 y 9.	Art. 3 c) y f), 14 quinquies: seudonimización y cifrado.
A.1.4.6	Eliminación / anonimización	Art. 6.	Art. 3 c): supresión o anonimización al finalizar propósito.
A.1.4.7	Archivos temporales	Art. 6 (bloqueo).	Art. 8 ter (derecho de bloqueo).
A.1.4.8	Retención	Art. 6.	Art. 3 c) y 14 ter i): período de conservación.
A.1.4.9	Destrucción segura	Art. 6.	Art. 3 c).
A.1.4.10	Controles de transmisión	Art. 5.	Art. 14 quinquies: cifrado y trazabilidad.

Intercambio, transferencia y divulgación de información personal

Cláusula ISO 27701	Descripción resumida del control	Ley 19.628 (vigente hasta 2026)	Ley 21.719 (vigencia desde 2026)
A.1.5.2	Base para transferencias internacionales	Art. 5.	Art. 14 ter h): informar nivel de protección o garantías.
A.1.5.3	Países / organizaciones destino	Art. 5.	Art. 14 ter h): identificar destinatarios extranjeros.
A.1.5.4	Registro de transferencias	Art. 5.	Art. 14 ter d), h): registro público.
A.1.5.5	Divulgaciones	Art. 5.	Art. 26: transferencias internacionales.

Obligaciones frente a los titulares de la información personal

Cláusula ISO 27701	Descripción resumida del control	Ley 19.628 (vigente hasta 2026)	Ley 21.719 (vigencia desde 2026)
A.2.2.2	Acuerdo con cliente (responsable)	Art. 8: mandato por escrito con condiciones de seguridad.	Art. 15 bis: obligación contractual entre responsable y encargado.
A.2.2.3	Fines del encargado	Art. 8: actuar según mandato.	Art. 15 bis: sólo bajo instrucciones del responsable.
A.2.2.4	Uso para marketing	No previsto.	Art. 8: requiere consentimiento del titular.
A.2.2.5	Instrucción ilícita	Implícito.	Art. 15 bis inc. 2: informar instrucciones ilícitas del responsable.
A.2.2.6	Obligaciones del cliente	Implícito.	Art. 15 bis y 14 quáter: corresponsabilidad y seguridad desde el diseño.
A.2.2.7	Registros del tratamiento	Art. 5: constancia de requirente y propósito.	Art. 14 ter: registro público y documentación del tratamiento.
A.2.3.2	Atender derechos de titulares	Art. 12: derecho a información y eliminación.	Arts. 4–11 y 15 bis: el encargado asiste al responsable.
A.2.4.2	Archivos temporales	Art. 6 (bloqueo).	Art. 8 ter: suspensión temporal del tratamiento.
A.2.4.3	Eliminación al término del contrato	Art. 6: eliminación de datos caducos.	Art. 3 c) y 14 quinquies d): eliminación segura al finalizar el servicio.
A.2.4.4	Controles de transmisión	Art. 5.	Art. 14 quinquies: cifrado y trazabilidad.

Intercambio, transferencia y divulgación de información personal

Cláusula ISO 27701	Descripción resumida del control	Ley 19.628 (vigente hasta 2026)	Ley 21.719 (vigencia desde 2026)
A.2.5.2	Transferencias internacionales	Art. 5.	Art. 26: sólo con nivel adecuado o garantías.
A.2.5.3	Países destino	Art. 5.	Art. 26: identificación del destinatario.
A.2.5.4	Registro de divulgaciones	Art. 5.	Art. 26.
A.2.5.5	Notificación de requerimientos legales	Implícito.	Art. 14 quinquies: informar incidentes o requerimientos de acceso.
A.2.5.6	Divulgaciones legalmente vinculantes	Implícito.	Art. 26 inc. final: sólo si la ley extranjera lo exige y se informa a la Agencia.
A.2.5.7	Divulgación de subencargados	No previsto.	Art. 15 bis inc. 3: informar subencargados.
A.2.5.8	Contratación de subencargados	No previsto.	Art. 15 bis inc. 3: autorización previa y mismas obligaciones.
A.2.5.9	Cambios de subencargados	No previsto.	Art. 15 bis inc. 3: informar cambios al responsable.

Consideraciones de seguridad para los responsables y encargados del tratamiento

Cláusula ISO 27701	Descripción resumida del control	Ley 19.628 (vigente hasta 2026)	Ley 21.719 (vigencia desde 2026)
A.3.3	Política de seguridad de la información	Art. 11: responsable debe adoptar medidas de seguridad adecuadas.	Art. 14 quinquies: políticas de seguridad técnicas y organizativas basadas en riesgos.
A.3.4	Roles y responsabilidades de seguridad	Art. 11: deber general del responsable.	Art. 14 quinquies letras a)–b): roles y medios para mantener confidencialidad e integridad.
A.3.5	Clasificación de la información	No explícito (principio de proporcionalidad Art. 9).	Art. 14 quinquies: medidas acordes al riesgo; Art. 17: mayor protección a datos sensibles.
A.3.6	Etiquetado de información	No regulado.	Art. 14 quinquies letras a) y d): confidencialidad, integridad y disponibilidad.
A.3.7	Transferencia de información segura	Art. 5: registro del requirente y propósito.	Art. 14 quinquies letras c)–d): cifrado, trazabilidad y canales seguros.
A.3.8	Gestión de identidades y accesos	Implícito en Art. 11.	Art. 14 quinquies letras c)–f): autenticación, control de acceso y prevención de accesos no autorizados.
A.3.9	Revisión de derechos de acceso	Art. 11.	Art. 14 quinquies letra f): acceso restringido y revisiones periódicas.
A.3.10	Seguridad con proveedores y terceros	Art. 8: mandato por escrito con condiciones de seguridad.	Art. 15 bis inc. 3: encargado y subencargados deben cumplir medidas equivalentes.
A.3.11	Planificación de gestión de incidentes	No específico; se asume bajo Art. 11.	Art. 14 sexies: plan de respuesta y registro de vulneraciones.

Consideraciones de seguridad para los responsables y encargados del tratamiento

Cláusula ISO 27701	Descripción resumida del control	Ley 19.628 (vigente hasta 2026)	Ley 21.719 (vigencia desde 2026)
A.3.12	Respuesta a incidentes y brechas	No regulado.	Art. 14 sexies: obligación de notificar a la Agencia y a titulares.
A.3.13	Cumplimiento legal y contractual	Art. 11 y 16.	Art. 14 quinquies letras g)–i): cumplimiento, supervisión y registro de medidas.
A.3.14	Protección de registros (logs)	No regulado expresamente.	Art. 14 quinquies: mantener registros seguros y protegidos.
A.3.15	Revisión independiente de seguridad	No previsto.	Art. 14 quinquies letra j): revisión periódica de eficacia de medidas.
A.3.16	Cumplimiento con políticas internas	Implícito en deber de diligencia.	Art. 14 quinquies letra j): evaluación continua y auditorías.
A.3.17	Concientización y capacitación	No regulado.	Art. 14 quinquies letra k): programas de capacitación en protección de datos.
A.3.18	Acuerdos de confidencialidad	Art. 7: obligación de confidencialidad.	Art. 14 quinquies letra b): obligación de confidencialidad permanente.
A.3.19	Escritorio y pantalla limpia	No regulado.	Art. 14 quinquies letras d)–f): medidas físicas y organizativas de resguardo.
A.3.20	Seguridad en almacenamiento	Art. 11: medidas de seguridad adecuadas.	Art. 14 quinquies letras d) y f): seguridad de almacenamiento, cifrado y control de soportes.
A.3.21	Eliminación o disposición segura	Art. 6: eliminación de datos caducos.	Art. 3 c) y Art. 14 quinquies letra d): disposición segura de medios.

Consideraciones de seguridad para los responsables y encargados del tratamiento

Cláusula ISO 27701	Descripción resumida del control	Ley 19.628 (vigente hasta 2026)	Ley 21.719 (vigencia desde 2026)
A.3.22	Seguridad en dispositivos endpoint	No regulado.	Art. 14 quinquies letra f): evitar accesos no autorizados.
A.3.23	Autenticación segura	No regulado.	Art. 14 quinquies letra f): control de acceso y autenticación segura.
A.3.24	Respaldos y restauración	No regulado.	Art. 14 quinquies letra e): disponibilidad y resiliencia de sistemas.
A.3.25	Registro de eventos	No regulado.	Art. 14 quinquies letra i): trazabilidad de operaciones sobre datos.
A.3.26	Uso de criptografía	No regulado.	Art. 14 quinquies letra c): cifrado y seudonimización.
A.3.27	Desarrollo seguro de sistemas	No regulado.	Art. 14 quinquies letra j): revisión continua y control de cambios.
A.3.28	Requisitos de seguridad en aplicaciones	No regulado.	Art. 14 quinquies letra j): pruebas de eficacia de medidas.
A.3.29	Arquitectura e ingeniería segura	No regulado.	Art. 14 quáter: privacidad desde el diseño y por defecto.
A.3.30	Desarrollo tercerizado	Art. 8: condiciones contractuales al mandatario.	Art. 15 bis inc. 3: subencargados bajo mismas obligaciones.
A.3.31	Protección de información de pruebas	No regulado.	Art. 14 quinquies letras d) y f): proteger PII en entornos de prueba.

Plan de Acción – Revisión en 20 pasos

Plan tentativo: Desafíos para las SP

1️⃣ Sensibilización estratégica y compromiso institucional

Objetivo: Obtener respaldo político y compromiso del nivel directivo.
Acciones clave:

- Exponer al jefe de servicio los impactos de la Ley 21.719 y sus sanciones.
- Explicar la relación entre datos personales, gobierno digital y ciberseguridad.
- Alinear el tema con metas de modernización y transparencia.
- Designar un patrocinador ejecutivo del proyecto.
- Incorporar el plan en la planificación anual institucional (PAI o PMG).
  Entregables: Minuta de compromiso, resolución de inicio, presentación ejecutiva.
  Ley: Art. 1–3, 27.
  ISO: Cláusula 5.1, A.3.3.

2️⃣ Formación del Grupo Institucional de Datos y Privacidad

Objetivo: Crear un grupo de trabajo interdisciplinario.
Acciones clave:

- Integrar representantes de Jurídico, TI, Transparencia, RRHH y Gestión.
- Nombrar un líder provisional de privacidad y seguridad.
- Capacitar al grupo en principios de la Ley 21.719 y la ISO 27701.
- Definir frecuencia de reuniones y actas.
- Coordinar con la División de Gobierno Digital o Ministerio del Interior.
  Entregables: Acta constitutiva, plan de trabajo interno.
  Ley: Art. 18 (encargado de datos).
  ISO: A.3.4 (roles y responsabilidades).

3️⃣ Capacitación general y cultura de protección de datos

Objetivo: Introducir el tema a todos los funcionarios públicos.
Acciones clave:

- Desarrollar cápsulas e-learning sobre datos personales, privacidad y ciberseguridad.
- Realizar talleres presenciales en lenguaje no técnico.
- Incorporar la materia en inducciones de nuevos funcionarios.
- Publicar material en intranet institucional.
- Evaluar conocimientos antes y después.
  Entregables: Programa de capacitación, presentaciones y evaluación de impacto.
  Ley: Art. 14 quinquies k).
  ISO: A.3.17 (concientización).

4️⃣ Diagnóstico institucional de madurez en privacidad

Objetivo: Evaluar brechas de cumplimiento frente a la Ley y la norma.
Acciones clave:

- Aplicar una autoevaluación ISO 27701 y Ley 21.719.
- Identificar riesgos críticos (bases legales, brechas de seguridad, incidentes).
- Elaborar matriz de brechas y prioridades.
- Definir responsables y plazos para su cierre.
- Presentar informe ejecutivo a la dirección.
  Entregables: Informe de madurez, matriz de riesgos.
  Ley: Art. 3, 14 ter, 14 quinquies.
  ISO: A.1.2.2, A.3.15.

Plan tentativo: Desafíos para las SP

5 Definición del Encargado de Protección de Datos (EPD)

Objetivo: Nombrar formalmente al responsable institucional de privacidad.
Acciones clave:

- Seleccionar un funcionario con perfil jurídico/tecnológico.
- Definir sus atribuciones en reglamento interno.
- Establecer canal oficial de contacto público.
- Coordinar con la Agencia de Protección de Datos.
- Incorporar la función al organigrama.
  Entregables: Resolución de nombramiento y funciones.
  Ley: Art. 18.
  ISO: A.3.4.

6 Creación del Marco Normativo Interno

Objetivo: Formalizar políticas y procedimientos internos.
Acciones clave:

- Elaborar Política de Protección de Datos Personales.
- Aprobar por resolución y publicar en web institucional.
- Definir procedimientos de derechos ARCO+, gestión de incidentes y reclamos.
- Integrar con reglamento de seguridad digital y ciberseguridad.
- Alinear con la Ley 21.180 (Transformación Digital).
  Entregables: Política aprobada y procedimientos asociados.
  Ley: Art. 14 ter, Art. 14 quinquies.
  ISO: A.3.3, A.3.11.

7 Inventario y Registro de Actividades de Tratamiento

Objetivo: Identificar todas las operaciones con datos personales.
Acciones clave:

- Levantar registros de tratamiento en cada unidad.
- Documentar bases legales, finalidades, sistemas y transferencias.
- Clasificar según sensibilidad (datos personales/sensibles).
- Consolidar el registro institucional y mantenerlo actualizado.
- Establecer una versión pública de transparencia activa.
  Entregables: ROPA institucional.
  Ley: Art. 14 ter letras a), d), h).
  ISO: A.1.2.9, A.2.2.7.

8 Implementación de Controles Básicos de Seguridad de la Información

Objetivo: Alinear protección técnica con ciberseguridad estatal.
Acciones clave:

- Adoptar controles mínimos del CSIRT de Gobierno.
- Definir responsables de seguridad en TI.
- Implementar contraseñas, accesos, respaldos y cifrado básico.
- Coordinar con División de Gobierno Digital.
- Documentar los controles y revisarlos semestralmente.
  Entregables: Manual de seguridad y registro de medidas.
  Ley: Art. 14 quinquies letras a–f.
  ISO: A.3.8–A.3.26.

Plan tentativo: Desafíos para las SP

8 Implementación de Controles Básicos de Seguridad de la Información

Objetivo: Alinear protección técnica con ciberseguridad estatal.
Acciones clave:

- Adoptar controles mínimos del CSIRT de Gobierno.
- Definir responsables de seguridad en TI.
- Implementar contraseñas, accesos, respaldos y cifrado básico.
- Coordinar con División de Gobierno Digital.
- Documentar los controles y revisarlos semestralmente.
  Entregables: Manual de seguridad y registro de medidas.
  Ley: Art. 14 quinquies letras a–f.
  ISO: A.3.8–A.3.26.

9 Procedimiento de Atención de Derechos Ciudadanos (ARCO+)

Objetivo: Garantizar el ejercicio de derechos por los titulares.
Acciones clave:

- Crear formulario digital y correo institucional.
- Definir plazos y responsables.
- Registrar solicitudes y respuestas.
- Asegurar lenguaje claro y respuesta dentro de 30 días.
- Incorporar métricas en transparencia activa.
  Entregables: Procedimiento ARCO+, registro de solicitudes.
  Ley: Arts. 4–11.
  ISO: A.1.3.10, A.2.3.2.

10 Protocolo de Gestión de Incidentes y Brechas

Objetivo: Asegurar respuesta oportuna ante incidentes.
Acciones clave:

- Redactar protocolo de detección, registro y notificación.
- Integrar con CSIRT o Departamento TI.
- Establecer responsables y escalamiento.
- Simular un incidente al año.
- Notificar a la Agencia y titulares según la Ley.
  Entregables: Protocolo de incidentes y registro anual.
  Ley: Art. 14 sexies.
  ISO: A.3.11–A.3.12.

11 Evaluación de Impacto en Privacidad (EIPD)

Objetivo: Prevenir riesgos antes de nuevos proyectos.
Acciones clave:

- Diseñar plantilla simplificada de EIPD.
- Aplicarla a nuevos sistemas o convenios de datos.
- Revisar por EPD y Jurídico antes de implementación.
- Archivar informes y mitigaciones.
- Integrar con análisis de riesgos tecnológicos (ISO 27001).
  Entregables: EIPD institucional.
  Ley: Art. 14 quáter.
  ISO: A.1.2.6, A.3.29.

12 Incorporación de Cláusulas en Contratos y Licitaciones

Objetivo: Extender el cumplimiento a proveedores.
Acciones clave:

- Revisar bases de licitación y convenios vigentes.
- Incorporar cláusulas de confidencialidad, seguridad y tratamiento.
- Mantener registro de encargados y subencargados.
- Verificar cumplimiento por informes de avance.
- Aplicar medidas correctivas ante incumplimiento.
  Entregables: Modelo de cláusulas y registro de proveedores.
  Ley: Art. 15 bis.
  ISO: A.2.5.8, A.3.10.

13 Gestión de Transferencias de Datos

Objetivo: Regular el intercambio nacional e internacional.
Acciones clave:

- Identificar flujos entre instituciones del Estado y terceros.
- Formalizar convenios con condiciones de seguridad.
- Registrar transferencias internacionales.
- Aplicar medidas de cifrado y trazabilidad.
- Publicar listado de convenios vigentes.
  Entregables: Registro de transferencias, convenios actualizados.
  Ley: Art. 26.
  ISO: A.1.5, A.2.5.

Plan tentativo: Desafíos para las SP

1 4 Integración con Política Nacional de Ciberseguridad

Objetivo: Alinear seguridad de datos con ciberdefensa institucional.
Acciones clave:

- Mapear cumplimiento con el marco CSIRT y la Política Nacional 2023–2028.
- Implementar controles técnicos de resiliencia.
- Vincular ciberincidentes con gestión de privacidad.
- Establecer plan de continuidad digital.
- Reportar a la autoridad competente (Ministerio del Interior/CSIRT).
  Entregables: Plan de Ciberseguridad y continuidad.
  Ley: Art. 14 quinquies.
  ISO: A.3.24–A.3.26.

1 5 Política de Gobierno de Datos y Calidad

Objetivo: Integrar privacidad con gobernanza institucional de datos.
Acciones clave:

- Crear Comité de Gobierno de Datos.
- Definir roles de custodios y propietarios de datos.
- Integrar calidad, disponibilidad y privacidad.
- Alinear con la Estrategia Nacional de Datos Abiertos.
- Coordinar con la Secretaría de Modernización del Estado.
  Entregables: Política y modelo de gobierno de datos.
  Ley: Art. 14 ter; Ley 21.180.
  ISO: A.1.2.2, A.3.3.

1 6 Transparencia y comunicación ciudadana

Objetivo: Fortalecer la confianza pública.
Acciones clave:

- Crear sección “Protección de Datos Personales” en el sitio institucional.
- Publicar políticas, derechos y contacto del EPD.
- Incluir avisos en formularios digitales y presenciales.
- Difundir campañas informativas.
- Medir percepción de confianza ciudadana.
  Entregables: Portal de privacidad, material educativo.
  Ley: Art. 14 ter.
  ISO: A.1.3.3–A.1.3.4.

1 7 Coordinación interinstitucional y con la Agencia

Objetivo: Vincular la gestión de datos con otras instituciones del Estado.
Acciones clave:

- Coordinar con el Consejo para la Transparencia y CSIRT.
- Participar en mesas técnicas sectoriales.
- Compartir buenas prácticas y lecciones aprendidas.
- Enviar reportes de avance a la Agencia.
- Promover interoperabilidad con seguridad.
  Entregables: Reportes de coordinación, actas de mesa interinstitucional.
  Ley: Art. 27.
  ISO: Cláusula 7.5.

Plan tentativo: Desafíos para las SP

18 Auditoría interna de cumplimiento

Objetivo: Evaluar la eficacia de las políticas y controles.
Acciones clave:

- Diseñar plan anual de auditoría en privacidad.
- Aplicar listas de verificación basadas en ISO 27701 y Ley 21.719.
- Incluir seguridad y ciberseguridad en la revisión.
- Elaborar informe de hallazgos y plan de mejora.
- Presentar a la dirección y al EPD.
  Entregables: Informe de auditoría y plan de mejora.
  Ley: Art. 14 quinquies j).
  ISO: A.3.15–A.3.16.

19 Monitoreo, indicadores y mejora continua

Objetivo: Asegurar sostenibilidad del cumplimiento.
Acciones clave:

- Definir KPIs (porcentaje de respuestas ARCO, incidentes, brechas cerradas).
- Implementar tablero de seguimiento mensual.
- Revisar políticas anualmente.
- Integrar métricas en el Sistema de Gestión Institucional.
- Publicar informe de cumplimiento anual.
  Entregables: Cuadro de indicadores y reporte anual.
  Ley: Art. 27.
  ISO: Cláusula 10 (mejora continua).

20 Certificación y madurez avanzada

Objetivo: Consolidar la institucionalización del sistema.
Acciones clave:

- Validar cumplimiento con auditoría externa ISO 27701.
- Participar en programas públicos de acreditación.
- Evaluar adopción de ISO 27001 y 37301 (Compliance).
- Promover interoperabilidad segura con otras instituciones.
- Difundir logros y cultura de protección de datos.
  Entregables: Certificación ISO, informe final de madurez.
  Ley: Art. 28 (fomento del cumplimiento).
  ISO: A.3.15, A.3.16, Cláusulas 9–10.

CAPACITACIÓN USACH
UNIVERSIDAD DE SANTIAGO DE CHILE

Nueva ISO 27701:2025
Sistema de Gestión de Información de Privacidad

¿Cómo se alinea con la Ley de Protección de Datos?

ALIGNMENT
SOLUCIONES ESTRATÉGICAS

DIPLOMADO
CIBERSEGURIDAD