prey

Checklist de cumplimiento Ley 21.719:

evalúa tu modelo por componente ✅

Prey Inc.

Cómo evaluar tu cumplimiento con la ley 21.719

Qué es este checklist (y qué no es)

Este checklist es una herramienta de autodiagnóstico para organizaciones que tratan datos personales en Chile.

No es una auditoría legal ni técnica,
pero sí te permite responder una pregunta clave:

¿Qué tan preparado estoy hoy para cumplir y demostrar cumplimiento con la Ley 21.719?

Cómo usarlo

- Marca cada ítem como: **Sí / No**
- Si tu respuesta es **“sí, pero...”**, considéralo como **“No”** para efectos de este diagnóstico.
- Si un componente queda mayoritariamente en **No**, revisa la señal de riesgo
- Usa los links sugeridos para profundizar y cerrar brechas

Componentes esenciales de un modelo de cumplimiento

1. Gobernanza y roles

Este componente evalúa la existencia de responsabilidades claras, de coordinación interna y de una toma de decisiones trazable en materia de protección de datos y ciberseguridad.

- [ ] ¿Existe un Delegado de Protección de Datos (DPO) designado y documentado?
- [ ] ¿El rol del DPO tiene funciones claras, autoridad y acceso a información relevante?
- [ ] ¿TI tiene responsabilidades explícitas en protección de datos (no solo “soporte”)?
- [ ] ¿Existe un comité o instancia de coordinación entre legal, TI, seguridad y negocio?
- [ ] ¿Las decisiones sobre datos personales quedan documentadas?

Señal de riesgo:
Cumplimiento huérfano: cuando nadie es realmente responsable, el riesgo se distribuye... y la sanción no.

Artículos relacionados:

Qué es la gobernanza de datos y por qué será clave para cumplir con la Ley 21.719

Cómo estructurar una gobernanza de datos efectiva en tu organización

2. Políticas y procedimientos

Este componente evalúa la existencia de reglas claras y aplicables que rigen el tratamiento de datos personales en el día a día.

- [ ] ¿Existe una política de privacidad actualizada y alineada con la ley?
- [ ] ¿Existe una política de protección de datos actualizada y alineada con la ley?
- [ ] ¿Hay procedimientos documentados para el tratamiento de datos?
- [ ] ¿Existe un procedimiento de respuesta a brechas?
- [ ] ¿Existe una política de retención y destrucción de datos?
- [ ] ¿Las políticas reflejan la operación real y no solo el “deber ser”?

Señal de riesgo:
Política declarativa: existe el documento, pero no gobierna la operación.

Artículos relacionados:

Políticas mínimas exigidas por la Ley 21.719

3. Registro de actividades de tratamiento (RAT)

Este componente evalúa la capacidad de la organización para saber qué datos trata, dónde, cómo y con quién.

- [ ] ¿Existe un RAT documentado y centralizado?
- [ ] ¿Incluye sistemas, procesos, bases de datos y responsables?
- [ ] ¿Incluye proveedores y encargados de tratamiento?
- [ ] ¿Está actualizado y refleja la operación real?
- [ ] ¿TI participó en su elaboración o validación?

Señal de riesgo:
RAT “para la foto”: sirve para mostrar, no para gestionar ni responder incidentes.

Artículos relacionados:

Cómo crear y mantener un RAT efectivo

4. Evaluaciones de impacto en protección de datos (DPIA)

Este componente evalúa la capacidad de identificar, evaluar y mitigar riesgos cuando el tratamiento de datos puede afectar los derechos de las personas.

- [ ] ¿La organización sabe cuándo corresponde realizar una DPIA?
- [ ] ¿Se han realizado DPIA en procesos de alto riesgo?
- [ ] ¿TI participa activamente en la evaluación?
- [ ] ¿Las medidas definidas se implementan efectivamente?
- [ ] ¿Se documenta el seguimiento de las medidas?

Señal de riesgo:
DPIA como trámite: se evalúa el riesgo, pero no se mitiga.

Artículos relacionados:

DPIA paso a paso según la Ley 21.719

5. Controles técnicos mínimos

Este componente evalúa la existencia de medidas técnicas efectivas para proteger datos personales.

- [ ] ¿Existen controles de acceso por usuario y por perfil en los sistemas de la empresa?
- [ ] ¿Existe un inventario actualizado de dispositivos que tratan datos personales?
- [ ] ¿Incluye proveedores y encargados de tratamiento?
- [ ] ¿Los dispositivos cuentan con políticas básicas de seguridad?
- [ ] ¿Los dispositivos cuentan con cifrado activo?
- [ ] ¿Hay capacidad de bloqueo o de borrado remoto en los dispositivos?
- [ ] ¿Existe un control técnico para actuar ante la pérdida, robo o comportamiento anómalo de dispositivos que contienen datos personales?
- [ ] ¿Hay capacidad para realizar respaldos periódicos?
- [ ] ¿Hay capacidad para cifrar los respaldos?
- [ ] ¿Existen alertas o mecanismos básicos para detectar accesos anómalos o dispositivos comprometidos?

Señal de riesgo:
Datos sin control en endpoints: el principal punto ciego del cumplimiento moderno.

6. Evidencia y documentación

Este componente evalúa la capacidad de demostrar cumplimiento ante una fiscalización o un incidente.

- [ ] ¿Se generan logs o registros técnicos de eventos relevantes en sistemas y dispositivos que tratan datos personales?
- [ ] ¿Los registros permiten identificar qué ocurrió, cuándo y en qué sistema o dispositivo?
- [ ] ¿Se generan registros específicos ante incidentes de seguridad?
- [ ] ¿Los logs se conservan por un período definido y son accesibles cuando se requieren?
- [ ] ¿Existen reportes periódicos de seguridad o cumplimiento?
- [ ] ¿Los incidentes y las acciones correctivas se documentan con fecha, responsable y medida aplicada?
- [ ] ¿Se conserva evidencia histórica de cumplimiento (registros, reportes, configuraciones, acciones ejecutadas)?

Señal de riesgo:
"Lo hacemos, pero no lo podemos probar": en fiscalización, eso equivale a no cumplir.

7. Monitoreo y mejora continua

Este componente evalúa si el cumplimiento es un proceso vivo que se revisa y ajusta en el tiempo.

- [ ] ¿El modelo de cumplimiento se revisa periódicamente?
- [ ] ¿Se ajusta ante cambios legales, técnicos u organizacionales?
- [ ] ¿Se revisan incidentes y casi-incidentes?
- [ ] ¿Existen responsables del seguimiento continuo?

Señal de riesgo:
Cumplimiento estático: funciona solo hasta el primer cambio o incidente.

8. Gestión de terceros y proveedores

Componente que evalúa el control sobre proveedores que acceden o tratan datos personales de la empresa.

- [ ] ¿Existe inventario de proveedores que tratan datos personales?
- [ ] ¿Los contratos incluyen cláusulas de protección de datos?
- [ ] ¿Se evalúa el riesgo de proveedores críticos?
- [ ] ¿Existen obligaciones de notificación de incidentes?
- [ ] ¿TI conoce qué proveedores acceden a datos desde dispositivos?

Señal de riesgo:
Brecha por terceros: el incidente ocurre fuera, la responsabilidad queda dentro.

9. Gestión de incidentes y notificación

Componente que evalúa la capacidad de detectar, contener, documentar y notificar incidentes de seguridad y datos personales.

- [ ] ¿Existe un plan formal de respuesta a incidentes?
- [ ] ¿Define roles, tiempos y responsables?
- [ ] ¿Incluye incidentes de datos personales?
- [ ] ¿Define criterios de notificación a la autoridad y titulares?
- [ ] ¿Existen herramientas o capacidades técnicas para contener incidentes (bloqueo, aislamiento, borrado, restauración)?
- [ ] ¿Se han realizado simulacros o ejercicios de respuesta a incidentes?

Señal de riesgo:
Reacción improvisada: se responde tarde, mal o sin evidencia.

10. Continuidad operacional y resiliencia

Componente que evalúa la capacidad de mantener o recuperar operaciones críticas ante incidentes de ciberseguridad.

- [ ] ¿Existen planes de continuidad operacional?
- [ ] ¿Incluyen sistemas que tratan datos personales?
- [ ] ¿Consideran pérdida o compromiso de dispositivos?
- [ ] ¿Se pueden aislar o recuperar endpoints críticos?
- [ ] ¿Se prueban escenarios de interrupción?

Señal de riesgo:
Cualquier incidente menor se transforma en una crisis mayor.

11. Capacitación y cultura de cumplimiento

Componente que evalúa el grado en que las personas conocen y aplican el modelo de cumplimiento.

- [ ] ¿El personal recibe capacitación en protección de datos?
- [ ] ¿TI recibe formación específica en incidentes y controles?
- [ ] ¿Se capacita ante cambios normativos o tecnológicos?
- [ ] ¿Existe evidencia de las capacitaciones realizadas?

Señal de riesgo:
Cumplimiento de cartón: el modelo existe, pero la gente no sabe cómo actuar.

Cumplimiento hoy: menos declaración, más control

El estándar regulatorio en Chile está cambiando. Ya no basta con decir **“cumplimos”**; ahora hay que **demostrarlo**, incluso bajo presión.

Este checklist es un primer paso para identificar brechas. Lo siguiente será cerrarlas con capacidades sostenibles, especialmente en los puntos de mayor riesgo.

Cómo ayuda Prey a fortalecer tu modelo de cumplimiento

Prey no reemplaza políticas, asesoría legal ni marcos de gobernanza. Prey te ayuda a convertir el control de dispositivos en una capacidad operativa, alineada con lo que hoy exigen las leyes.

Desde una perspectiva de cumplimiento, Prey permite:

- Visibilidad centralizada de dispositivos que tratan datos personales.
- Capacidad de reacción ante pérdida, robo o comportamiento anómalo.
- Acciones remotas como bloqueo o borrado para mitigar incidentes.
- Registro de acciones que puede usarse como evidencia operativa.
- Menos dependencia de procesos manuales en escenarios críticos.

En otras palabras, ayuda a que el cumplimiento no dependa solo de documentos, sino de controles reales.

Explora cómo Prey ayuda a recuperar visibilidad y control sobre los dispositivos que hoy ponen en riesgo tu cumplimiento.

Agendar demo

Sobre Prey

Nacimos en 2009 con una misión clara: devolverle a las personas el control sobre su tecnología. Hoy, Prey ha evolucionado en una **plataforma integral de gestión y seguridad para flotas globales**. Más allá del rastreo, empoderamos a las empresas con herramientas avanzadas para el manejo de software, cumplimiento de políticas y protección de datos.

Somos el aliado estratégico que ayuda a administrar y proteger entornos de trabajo remoto, facilitando el cumplimiento normativo. Un equipo comprometido con la continuidad de tu operación.

Prey para: **Personas** | **Organizaciones** | **Escuelas y Universidades**