Checklist

Diagnóstico de Postura de Seguridad y Cumplimiento Regulatorio

Prey Inc.

Diagnóstico de Postura de Seguridad y Cumplimiento Regulatorio

Conoce el estado real de tu seguridad y descubre cómo fortalecer el cumplimiento frente a la Ley Marco de Ciberseguridad y la Ley de Protección de Datos.

Cómo usar este diagnóstico

Este checklist es una herramienta de autoevaluación práctica para organizaciones que necesitan entender qué tan preparadas están hoy en materia de ciberseguridad y protección de datos.

No es una auditoría formal, pero sí te permite responder tres preguntas clave:

- ¿Dónde estoy realmente parado?
- ¿Qué riesgos tengo hoy frente a fiscalizaciones o incidentes?
- ¿Qué debo priorizar primero?

Instrucciones

- ✕ No implementado = 0pts
- ◐ Parcialmente en desarrollo = 3pts
- ✓ Completamente operativo = 5pts

Al final, suma los puntos y revisa tu **nivel de madurez.**

Total máximo: 30 preguntas × 5 puntos = **150 puntos**

1. Gobernanza y liderazgo

Evaluación de la estructura organizacional de ciberseguridad

Una buena gobernanza permite responder rápido ante auditorías o incidentes.

	Pregunta	No implementado	Parcial	Operativo
1	¿Tu organización ha designado formalmente un Encargado de Ciberseguridad o CISO con autoridad ante la ANCI?	☐	☐	☐
2	¿Existe una política de ciberseguridad aprobada y comunicada a toda la organización?	☐	☐	☐
3	¿El área TI presenta reportes de seguridad y cumplimiento periódicos a la alta dirección?	☐	☐	☐
4	¿Cuentas con un mapa de roles y responsabilidades de ciberseguridad documentado?	☐	☐	☐

2. Gestión de activos y visibilidad 

Control y seguimiento de dispositivos y activos críticos

	Pregunta	No implementado	Parcial	Operativo
1	¿Mantienes un inventario actualizado de todos los dispositivos conectados a la red?	☐	☐	☐
2	¿Tienes identificados los activos críticos que procesan datos personales o confidenciales?	☐	☐	☐
3	¿Utilizas una plataforma MDM o equivalente para gestionar políticas de seguridad?	☐	☐	☐
4	¿Puedes localizar dispositivos y saber quién es el responsable asignado?	☐	☐	☐

3. Protección de datos personales

Cumplimiento de la Ley de Protección de Datos

	Pregunta	No implementado	Parcial	Operativo
1	¿Cuentas con un DPO o responsable de protección de datos formalmente designado?	☐	☐	☐
2	¿Mantienes un registro actualizado de tratamientos y consentimientos?	☐	☐	☐
3	¿Existen mecanismos de borrado seguro o remoto ante pérdida de equipos?	☐	☐	☐
4	¿Los accesos a datos personales están restringidos por rol y necesidad?	☐	☐	☐

4. Controles técnicos y protección de red

Infraestructura y seguridad perimetral

	Pregunta	No implementado	Parcial	Operativo
1	¿Tu red está segmentada por zonas y niveles de acceso?	☐	☐	☐
2	¿Cuentas con firewall o IDS/IPS activos y configurados correctamente?	☐	☐	☐
3	¿Utilizas VPN segura o Zero Trust para accesos remotos?	☐	☐	☐
4	¿Routers y switches tienen firmware actualizado y credenciales únicas?	☐	☐	☐

5. Identidades, contraseñas y autenticación

Infraestructura y seguridad perimetral

	Pregunta	No implementado	Parcial	Operativo
1	¿Usas MFA/2FA para accesos críticos?	☐	☐	☐
2	¿Existe una política formal de contraseñas?	☐	☐	☐
3	¿Utilizas un gestor de contraseñas corporativo?	☐	☐	☐
4	¿Se desactivan cuentas inactivas o de ex empleados oportunamente?	☐	☐	☐

6. Protección de endpoints y respaldo

Seguridad de dispositivos y continuidad operativa

	Pregunta	No implementado	Parcial	Operativo
1	¿Todos los dispositivos cuentan con antivirus o EDR activo?	☐	☐	☐
2	¿Realizas respaldos periódicos de sistemas críticos?	☐	☐	☐
3	¿Los respaldos están cifrados y protegidos?	☐	☐	☐
4	¿Existe gestión de parches y actualizaciones automáticas?	☐	☐	☐
5	¿Los dispositivos portátiles tienen cifrado de disco completo?	☐	☐	☐

7. Respuesta ante incidentes y monitoreo continuo

Preparación y reacción ante amenazas

Un buen plan de respuesta ante incidentes puede reducir el impacto de un ataque en hasta un 80%.

	Pregunta	No implementado	Parcial	Operativo
1	¿Existe un plan formal de respuesta ante incidentes (IRP)?	☐	☐	☐
2	¿Monitoreas logs y alertas de sistemas críticos?	☐	☐	☐
3	¿Usas herramientas de detección de credenciales filtradas o dark web monitoring?	☐	☐	☐
4	¿Tienes definido el proceso de notificación a ANCI y autoridad de datos?	☐	☐	☐
5	¿Realizas simulacros de incidentes al menos una vez al año?	☐	☐	☐

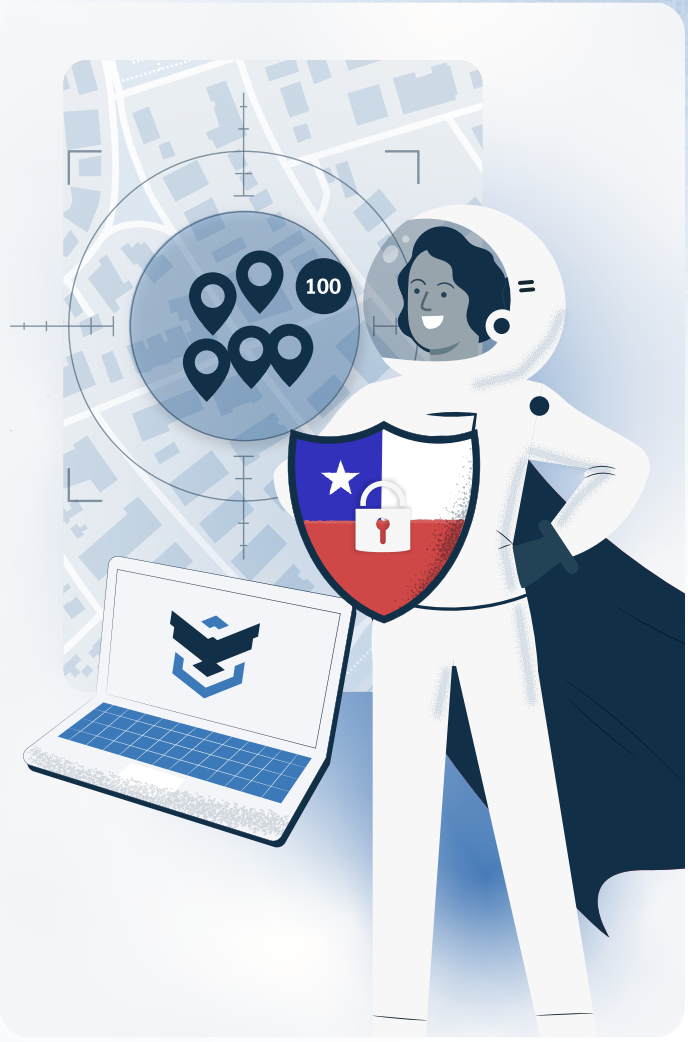
Niveles de madurez

Nivel	Nombre	Puntaje	Estado
1	Bombero digital	0 – 60	Reactivo / Vulnerable
2	Arquitecto en construcción	61 – 90	Medidas aisladas
3	Guardián de datos	91 – 120	Estable, poco automatizado
4	Orquestador cibernético	121 – 135	Sólido y coordinado
5	Maestro de la resiliencia	136 – 150	Ejemplar

Cómo interpretar tu resultado

- **Nivel 1–2:** Alto riesgo regulatorio y operativo. La organización depende de personas y reacción.
- **Nivel 3:** Cumplimiento básico, pero con brechas de visibilidad y evidencia.
- **Nivel 4:** Buen control, foco en eficiencia y automatización.
- **Nivel 5:** Seguridad integrada al negocio y preparada para fiscalización real.

Cómo Prey te ayuda a fortalecer tu postura de seguridad y cumplimiento



Este diagnóstico te permitió identificar brechas reales en tu postura de ciberseguridad y de protección de datos. El siguiente paso es cerrarlas de forma práctica, medible y demostrable.

Las organizaciones deben demostrar control operativo, especialmente sobre los dispositivos que acceden, almacenan o procesan datos personales.

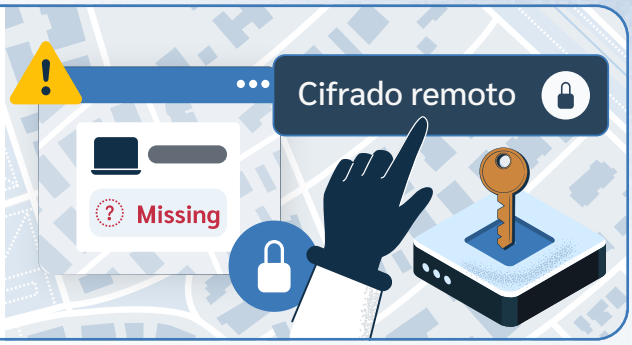
Prey es una plataforma de seguridad y control de dispositivos que ayuda a las organizaciones a cumplir con ambas leyes, especialmente desde TI.

Visibilidad y control de activos

- Inventario centralizado de dispositivos
- Identificación de responsables por equipo
- Ubicación y estado de dispositivos en tiempo real

Protección de datos desde el endpoint

- Bloqueo remoto y borrado seguro ante pérdida, robo o comportamiento errático
- Cifrado de dispositivos (según sistema operativo)
- Reducción del riesgo de fuga de información



Evidencia operativa de cumplimiento

- Acciones de seguridad registradas
- Controles aplicables a auditorías y fiscalizaciones
- Soporte para demostrar medidas técnicas activas

Cumplimiento sin complejidad

- Implementación rápida
- Sin infraestructura pesada
- Diseñado para equipos TI con recursos limitados

Evalúa Prey como parte de tu estrategia de 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**

Prey Spa. © Santiago, RM Chile

Todos los derechos reservados. La aplicación Prey, el logo y su marca son marcas registradas de Prey Inc.