



Autodiagnóstico

¿Tu flota de dispositivos aguanta una fiscalización?

Endpoint compliance checklist.
Evalúa qué tan preparado estás
para la ley 21.719





Cómo usar este diagnóstico

Evalúa el estado del parque de dispositivos frente a las obligaciones de seguridad de la Ley 21.719.

No constituye una certificación ni reemplaza asesoría legal: cubre la dimensión técnica del cumplimiento, que suele ser la que queda sin revisar.



Quién lo completa:

TI / IT

Puede responderse desde TI, sin apoyo de legal ni de gerencia. Las quince preguntas son sobre capacidades técnicas del parque.



Tiempo estimado: 5 min.



Cómo responder:

Según lo que es cierto hoy, no según lo que indica la política ni lo que debería estar configurado. Un diagnóstico inflado no entrega información utilizable.



Sí

2 puntos

Puede hacerse ahora, para todo el parque, sin trabajo manual.



A Medias

1 punto

Puede hacerse solo para parte de los equipos, revisando uno por uno, o solicitando algo al usuario.



No

0 puntos

No puede hacerse, o no se sabe si puede hacerse.



En caso de duda entre dos opciones, corresponde la menor.



Cómo leer el resultado:

Los subtotales por bloque son más informativos que el total: dos organizaciones con el mismo puntaje pueden tener problemas distintos, y la prioridad depende de en qué bloque está el vacío. Los ítems marcados como “a medias” indican dónde hay avance sin cerrar.



Cuándo repetirlo:

Conviene reevaluar cada seis meses, o ante un cambio relevante: incorporación masiva de equipos, cambio de proveedor, incidente de seguridad o nueva regulación.

Endpoint Compliance Checklist



Inventario

El inventario es la base de cualquier medida de seguridad: ningún control puede aplicarse sobre un equipo que no está identificado. Este bloque evalúa la cobertura del inventario y su vigencia, no solo su existencia.

Pregunta	Sí (2)	A medias (1)	No (0)
1. ¿Se conoce cuántos equipos tratan datos personales en este momento?	☐	☐	☐
2. ¿Está identificado quién tiene cada equipo, con nombre y apellido?	☐	☐	☐
3. ¿El inventario se actualiza de forma automática, sin mantención manual de una planilla?	☐	☐	☐
4. ¿Está disponible el detalle del software instalado en cada equipo, sin solicitarlo al usuario?	☐	☐	☐

Subtotal:

/ 8

Protección de dispositivos

La Ley 21.719 exige medidas de seguridad apropiadas al riesgo. Este bloque distingue entre tener las medidas definidas y poder verificar su estado real en cada equipo sin revisión manual.



Pregunta	Sí (2)	A medias (1)	No (0)
5. ¿Se conoce qué equipos están cifrados hoy, sin revisarlos uno por uno?	☐	☐	☐
6. ¿El cifrado puede activarse en un equipo que no está físicamente disponible?	☐	☐	☐
7. ¿Puedes aplicar políticas mínimas de seguridad a todo el parque de dispositivos?	☐	☐	☐

Subtotal:

/ 6

Rastreo y monitoreo

La localización de equipos cumple una función operativa: permite actuar cuando un dispositivo sale de control. Se evalúan dos capacidades distintas, la de ubicar un equipo bajo demanda y la de detectar automáticamente cuando algo se desvía de lo esperado.



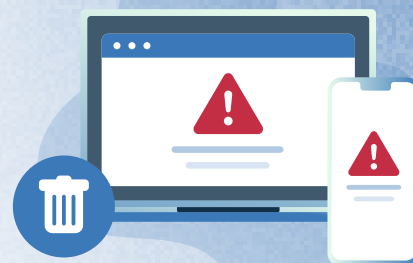
Pregunta	Sí (2)	A medias (1)	No (0)
8. ¿Puede ubicarse cualquier equipo del parque en este momento?	☐	☐	☐
9. ¿Se genera un aviso cuando un equipo sale de donde debería estar, sin que nadie lo reporte?	☐	☐	☐
10. ¿Existen controles de seguridad que se ejecuten automáticamente cuando eso ocurre, sin intervención manual?	☐	☐	☐

Subtotal:

/ 6

Respuesta ante incidentes

El intervalo entre la pérdida de un equipo y la primera acción determina el alcance del incidente. Este bloque evalúa la capacidad de intervenir en remoto dentro de ese intervalo, sin depender de la colaboración del usuario.



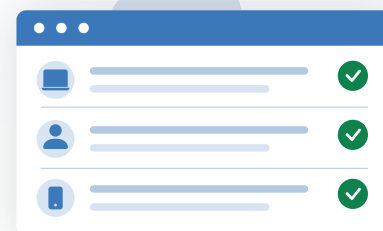
Pregunta	Sí (2)	A medias (1)	No (0)
11. Si un equipo desaparece hoy, ¿puede bloquearse dentro de la hora siguiente?	☐	☐	☐
12. ¿Pueden borrarse los datos en remoto, aunque el usuario no colabore?	☐	☐	☐

Subtotal:

/ 4

Trazabilidad y evidencia

El principio de responsabilidad exige acreditar el cumplimiento, no solo ejecutarlo. Este bloque evalúa si las acciones quedan documentadas de forma verificable y recuperable en el tiempo.



Pregunta	Sí (2)	A medias (1)	No (0)
13. ¿Queda registro automático de cada acción, con fecha y responsable?	☐	☐	☐
14. Si te preguntan qué pasó con un equipo hace seis meses, ¿puedes responder con documentos en vez de memoria?	☐	☐	☐

Subtotal:

/ 4

Offboarding

La desvinculación de personal cierra los accesos digitales, pero la devolución de equipos suele quedar fuera del procedimiento formal. Se evalúa el grado de conocimiento sobre los equipos que permanecen fuera de la organización.



Pregunta	Sí (2)	A medias (1)	No (0)
15. ¿Se conoce cuántos equipos no fueron devueltos por personas que ya dejaron la empresa?	☐	☐	☐

Subtotal:	/ 2
-----------	-----------------

 TOTAL:	/ 30
--	------------------

Interpretación de resultados

25 a 30 Estás cubierto.

Tienes visibilidad, control y evidencia. Lo que queda es mantenerlo: revisar el inventario cuando entra gente nueva y probar el borrado remoto antes de necesitarlo de verdad.



15 a 24 Vas encaminado, con puntos ciegos identificables.

Probablemente tienes las medidas instaladas pero no la forma de verificarlas ni de mostrarlas. Es la situación más común y también la más engañosa: en el papel todo está, y el día del incidente falta la mitad. Revisa dónde marcaste “a medias”: ahí está tu lista de trabajo.



0 a 14 Hay trabajo por delante, y es abordable.

El punto de partida es el inventario, porque sin él ninguna otra medida tiene sobre qué operar. Después el cifrado, que es lo que más protege por lo que cuesta. Con esos dos cubres el escenario más frecuente y el más caro.



Dónde mirar primero

Antes que el total, mira los subtotales. Un **18** que falla en inventario y un **18** que falla en evidencia son dos problemas distintos.

Si el bloque Inventario quedó bajo, empieza ahí y no sigas. Todo lo demás depende del inventario.

Si marcaste No en la pregunta **10**, tienes detección pero no respuesta. Las alertas que nadie alcanza a mirar cuentan lo mismo que no tenerlas.

Si el bloque Trazabilidad y evidencia quedó en cero pero el resto está alto, tu operación está bien y tu evidencia no. Es el escenario típico de los equipos que trabajan bien: hacen lo correcto y no queda registro de que lo hicieron. Frente a la Agencia, eso pesa igual que no haberlo hecho.

Si marcaste No en la pregunta **15**, ese número existe y conviene conocerlo antes de que lo pregunte alguien más.

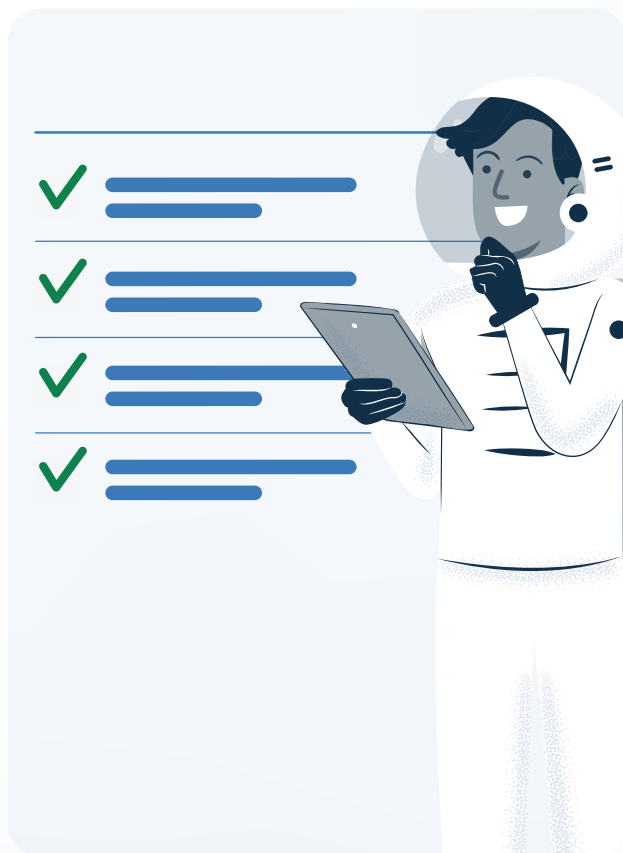


Cómo apoya Prey

Los bloques que hayan quedado con un resultado bajo suelen tener algo en común: no se cierran con más procedimiento, sino con la capacidad que tenga el equipo de TI de ver y actuar sobre los equipos.

En Prey, te ayudamos con:

Foco	Cómo apoya Prey
 Inventario	El inventario de hardware y software* se arma y se actualiza solo desde la instalación del agente, sin planillas que mantener
 Protección de dispositivos	El estado de cifrado queda visible equipo por equipo, y BitLocker puede activarse en remoto sobre los que falten
 Rastreo y monitoreo	Ubicación always-on de cada equipo y geofencing que avisan cuando uno sale de donde debería estar, sin que nadie tenga que reportarlo y con historial de ubicaciones para auditoría.
 Respuesta ante incidentes	Bloqueo y borrado remoto sin tener el equipo a mano ni depender de que el usuario colabore, además del reporte de pérdida para reunir la evidencia del caso.
 Trazabilidad y evidencia	Cada acción queda registrada con fecha y responsable, disponible cuando haya que acreditar qué se hizo y cuándo.
 Offboarding	El equipo que no fue devuelto puede borrarse en remoto, y la acción queda documentada para cerrar el proceso.



Siguientes pasos

Para revisar cómo proteger la flota de equipos frente a la Ley 21.719, el siguiente paso es una demo con nuestros especialistas. Son 20 minutos de conversación para entender el contexto de la organización y en qué puede apoyar Prey.

[Agenda una demo](#)

* Funcionalidades en desarrollo.

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