



**Antivirus:**

## ¿Alcanza para cumplir con la Ley 21.719?

Necesario pero insuficiente.  
El punto ciego está en el ciclo de vida de los equipos.



La Ley 21.719 no entrega una lista de herramientas para comprar. Exige medidas de seguridad apropiadas al riesgo y, sobre todo, exige **demostrar que estas medidas se aplicaron**.

Ahí aparece la diferencia. El antivirus puede demostrar una cosa: que el equipo estaba protegido frente a software malicioso. Un notebook, sin embargo, no es solo una vía de entrada. Es un destino vivo, lleno de datos personales que son **responsabilidad de la empresa**. Los equipos se mueven, cambian de manos y a veces no vuelven. De eso, el antivirus no sabe nada.

Esta guía recorre los puntos ciegos que enfrentan los equipos TI al gestionar dispositivos: cuando se entrega un equipo, durante su uso, cuando se pierde y cuando vuelve.



## ¿Qué cubre el antivirus?

Partamos por lo justo: el antivirus es una capa necesaria

Un antivirus protege el equipo de lo que puede traer el software: malware, ransomware, ejecución de código malicioso. Y eso importa para la ley, porque el ransomware es uno de los eventos que puede provocar una brecha de seguridad.

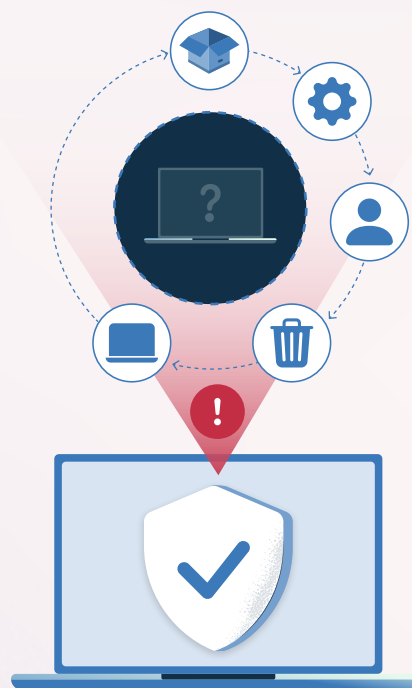
Pero responde una sola pregunta: ¿hay algún elemento malicioso corriendo en este equipo? La ley exige prevenir la pérdida y el acceso no autorizado a los datos personales. Para lograrlo con un equipo que sale de la oficina, hay otras cuatro preguntas que hay que poder responder:

- ¿Dónde está este equipo?
- ¿Los datos que almacena están cifrados?
- ¿Quién lo tiene hoy?
- ¿Qué se puede hacer si desaparece?



## ¿Dónde deja de cubrir?

Carece de visibilidad sobre el ciclo de vida del dispositivo, una gestión que en teoría parece sencilla pero que se complica al escalar a decenas o cientos de equipos. Con flotas heterogéneas (Windows, macOS, Linux, Android, ChromeOS e iOS), dispositivos adquiridos en diferentes momentos y distribuidos entre la oficina, el trabajo remoto y el terreno, **cada dispositivo tiene línea de tiempo propia**. Seguir las distintas etapas operativas de una flota sin registros automáticos de estas actividades es la receta para el desastre.



## Etapas operativas que requieren control

|                                                                                     |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|-------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|    | <p><b>Entrega y asignación</b></p> <p>Ingresa un nuevo miembro al equipo y se le asigna un notebook. Desde ese momento comienzan a operar datos personales dentro y fuera de la oficina, en un dispositivo que nadie vuelve a ver por meses. Si nadie anotó con qué configuración salió, cifrado activo y responsable asignado, después no hay manera de reconstruirlo. La protección de un equipo se define antes de entregarlo, no cuando aparece el problema.</p>                                                                                                |
|   | <p><b>Operación diaria</b></p> <p>Aunque no haya intención maliciosa, todos los días pasan cosas: alguien le presta el notebook a un compañero mientras espera el suyo, otro instala una app no autorizada, el equipo sale de la ciudad y nadie se entera. Esta es la normalidad de cualquier operación, no son “incidentes”. Pero aun así se debe responder a los distintos escenarios y establecer controles de protección con evidencia. El día que tengas que explicar qué pasó y cuál fue el protocolo de respuesta no basta la memoria de alguien.</p>        |
|  | <p><b>Incidentes</b></p> <p>Da lo mismo si fue un robo en el metro o si quedó en la mesa de un café. El equipo salió de tu control y la pregunta ahora es: qué se puede hacer en las próximas horas para proteger los datos personales y qué va a poder contar al fiscalizador después. Si no se logra ubicar, bloquear ni borrar el equipo, la única respuesta que queda es avisar y esperar.</p>                                                                                                                                                                  |
|  | <p><b>Devolución</b></p> <p>Esta es la etapa que más se subestima. Se acaba el contrato, la empresa tiene un protocolo de <b>offboarding</b>. Se cierra el correo del usuario, los accesos a la VPN y otras herramientas, todo en el mismo día, pero la devolución del notebook queda “por coordinar”. Aquí se pierde el control. Casi todas las empresas tienen equipos que nunca volvieron y que nadie registró ni alcanzó a borrar. Estos siguen siendo notebooks con datos personales de la organización, bajo su responsabilidad pero fuera de su control.</p> |

## ¿Qué te pide la Ley 21.719 en cada etapa?

| Etapa              | Qué exige la Ley 21.719                                                                                                                                                                                                                                                                                                                          | Qué debes demostrar                                                                                                                                                                                 | ¿Lo cubre tu antivirus?                                                                         |
|--------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------|
| Entrega del equipo | Implementar medidas de seguridad y controles de acceso desde el diseño, antes de asignar el dispositivo. Se debe garantizar la protección operativa previo al tratamiento de cualquier dato personal.                                                                                                                                            | Qué dispositivos tratan datos personales y con qué protecciones fueron configurados: cifrado activo, control de acceso, responsable asignado.                                                       | No. No sabe qué equipos existen ni cuáles son sus configuraciones de seguridad.                 |
| Operación diaria   | Adoptar medidas que aseguren confidencialidad, integridad, disponibilidad y resiliencia, proporcionales al riesgo, considerando el estado de la técnica y la gravedad de sus efectos (art. 14 quinquies).                                                                                                                                        | Que las medidas siguen activas hoy, no basta que las hayas instalado antes de la asignación. Qué equipos están operando con datos y en qué estado.                                                  | En parte. Cubre la prevención de software malicioso. No cubre saber qué equipos están en juego. |
| Pérdida o robo     | Prevenir la pérdida y el acceso no autorizado (art. 14 quinquies). Reportar a la Agencia en forma expedita y sin dilaciones indebidas cuando haya riesgo razonable para los titulares; comunicar también a los afectados si hay datos sensibles, de menores de catorce años o económicos, financieros, bancarios o comerciales (art. 14 sexies). | Qué equipo sufrió el incidente, qué datos tenía, qué acción fue tomada ante lo ocurrido y cuándo se tomó la acción. Registros comprobables de las comunicaciones en torno a la medida de seguridad. | No. Un equipo perdido no es un problema de malware.                                             |
| Devolución         | Aquí la ley no da un artículo dedicado, pero el deber del art. 14 quinquies no se suspende: mientras el equipo conserve datos y esté fuera de tu control, el riesgo de acceso no autorizado sigue abierto, y la responsabilidad por el cumplimiento sigue siendo tuya (art. 3 letra e).                                                          | Que el equipo volvió y fue comprobado, o la evidencia de que los datos se eliminaron. Con fecha y persona usuaria responsable.                                                                      | No. El antivirus no sabe que alguien dejó la empresa.                                           |

# Cómo te apoya Prey

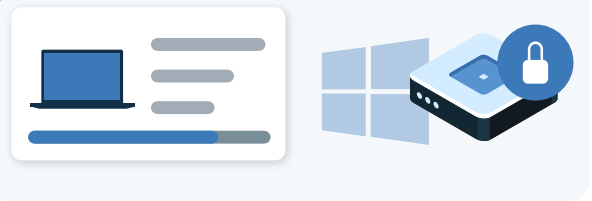


El antivirus cuida lo que entra al equipo. Prey se ocupa del equipo: dónde está, quién lo tiene, si sigue protegido y qué puedes hacer cuando desaparece. Si tu configuración inicial cambia, todo queda registrado

## En la entrega.

El equipo entra al inventario apenas instalas el agente, con su hardware, usuario y su software\*. Desde ahí activar el cifrado en Windows con BitLocker y definir políticas de seguridad ante incidentes. Queda registrado qué equipo es, quién lo tiene y en qué estado salió.

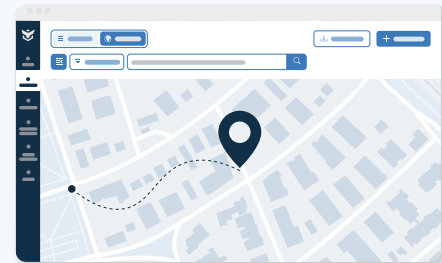
1



## En la operación.

El inventario se mantiene solo, sin necesidad de ingresar cambios. Con la ubicación de cada equipo siempre encendida rastreando dónde se encuentran y geocercas que te avisan cuando entran y salen de sus perímetros permitidos, sin que nadie tenga que reportarlo. Windows, macOS, Ubuntu, Android, iOS y ChromeOS conviven en una misma cuenta.

2



## En la pérdida o el robo.

Ubicas el equipo, lo bloqueas o borras los datos en forma remota. El reporte de pérdida reúne la evidencia del incidente, y cada acción que ejecutas queda con fecha y responsable. Ese es el insumo con el que después podrás notificar a la Agencia.

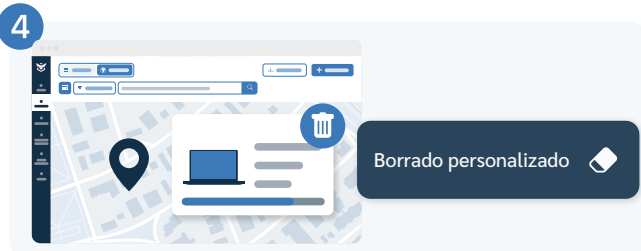
3



## En la devolución.

Borrado remoto del equipo que no volvió, con el registro completo de esta ejecución. El proceso de offboarding se cierra aunque el notebook nunca aparezca.

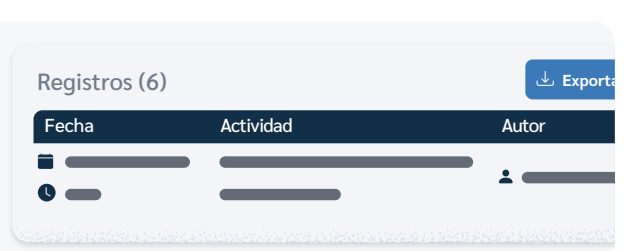
4

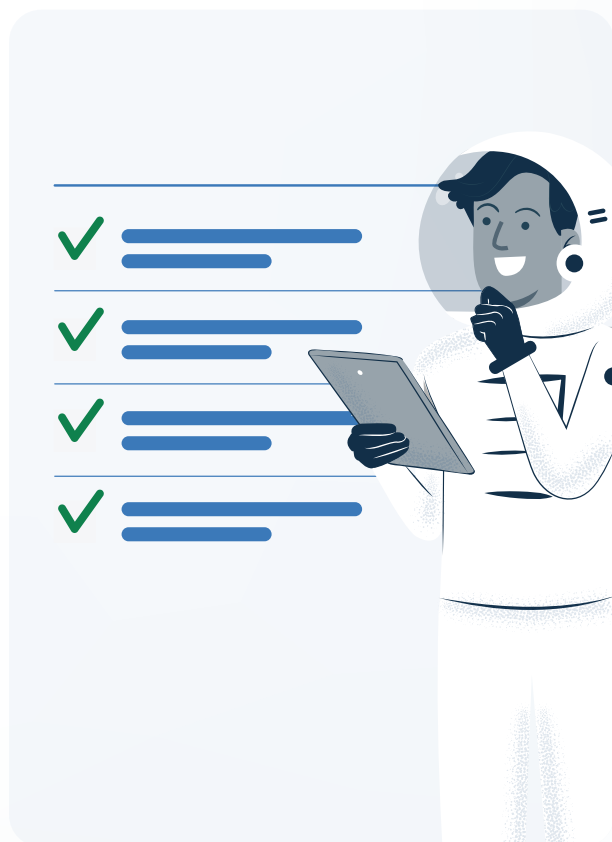


## Y transversal a los cuatro.

todo lo anterior queda en el registro de actividad. Una lista imborrable y personal para cada dispositivo. Cuando llegue la pregunta de qué hiciste y en qué momento, la respuesta no depende de que alguien se acuerde.

5





## ¡Hablemos!

Te ayudamos a revisar cómo proteger tu flota de equipos frente a la Ley 21.719. Cuéntanos sobre tu organización y en solo 20 minutos uno de nuestros especialistas te explicará cómo Prey te puede apoyar.

[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