



**Gestión de dispositivos remotos:**

# Riesgos y buenas prácticas frente a la Ley 21.719

Qué cambió cuando la flota de dispositivos salió de la oficina, y cómo se administra hoy.





## El perímetro de seguridad se expandió

---

Durante años, administrar dispositivos fue un problema con solución conocida. Los equipos estaban en un edificio, conectados a una red propia, al alcance del equipo de TI que podía caminar hasta el escritorio. El inventario se verificaba casi mirando. El soporte se hacía en persona. Un equipo que fallaba se reemplazaba por uno desocupado.

El trabajo híbrido dejó desfasado ese modelo. Lo dejó sin base. Las herramientas y los procedimientos con los que se administraba la flota asumían proximidad física, y esa proximidad desapareció sin que se rediseñara nada.

Hoy el mismo equipo de TI administra notebooks en casas, teléfonos en terreno, equipos que cambiaron de ciudad y computadores personales que se conectan al correo corporativo. Todo eso opera sobre redes que la organización no administra, con usuarios que resuelven solos lo que antes resolvía soporte.

# Qué se perdió en el camino

El problema no es una lista de amenazas nuevas. Son cuatro capacidades que se daban por sentadas y dejaron de funcionar.



## Visibilidad

En la oficina, el inventario se verificaba casi mirando. A distancia, no se sabe qué equipos siguen activos, en qué estado están ni dónde se encuentran. Y lo que no se ve, no se puede proteger.



## Trazabilidad

En la oficina, buena parte del registro era implícito: se sabía quién usaba qué porque se veía. A distancia, lo que no queda anotado deja de existir. Y casi nada queda anotado por su cuenta.



## Control físico

Cuando un equipo presentaba un problema, se llamaba a TI, alguien lo tomaba y lo resolvía. Ahora cada acción depende de que el usuario colabore, esté disponible y siga instrucciones por escrito. Lo que antes tomaba diez minutos hoy toma dos días de coordinación.



## Velocidad de respuesta

Un equipo perdido en la oficina era un problema acotado. Un equipo perdido en otra ciudad, con datos adentro y sin forma de intervenirlos, es un problema que crece con cada hora que pasa.

# Qué agrega la nueva regulación de protección de datos

Todo lo anterior ya era un problema operativo antes de que existiera cualquier ley. Lo que cambió con la Ley 21.719, que entra en vigencia en diciembre de 2026, es que ese desorden pasó a tener consecuencias formales.



La ley exige **aplicar medidas de seguridad apropiadas al riesgo**, que aseguren la confidencialidad e integridad de los datos personales y prevengan su pérdida o el acceso no autorizado. También obliga a reportar las vulneraciones sin dilaciones indebidas cuando existe riesgo razonable para las personas afectadas.

## Dos cosas importan de ese texto para quien administra equipos.

01



- **La primera:** la ley no distingue entre un equipo que está en la oficina y uno que está en una casa. El deber de protección es el mismo, aunque las condiciones para cumplirlo sean radicalmente distintas.

02



- **La segunda:** no entrega una lista cerrada de herramientas. Habla de medidas apropiadas al riesgo, lo que significa que la referencia es lo que hoy resulta razonable para una organización del mismo tamaño, y que hay que poder justificar las decisiones tomadas.

Ninguna de estas es novedosa. Lo que cambia en una flota distribuida de dispositivos es que dejan de ocurrir solas y necesitan quedar formalizadas.

## 01 Un inventario que se alimenta solo

El inventario mantenido a mano falla por diseño: depende de que alguien recuerde actualizarlo justo cuando está ocupado con otra cosa. En una flota remota, el inventario tiene que construirse desde el propio equipo y actualizarse sin intervención.



## 02 Cifrado activado antes de la entrega

El cifrado de disco es la medida con mejor relación entre esfuerzo y protección: convierte un equipo perdido en un problema de hardware en lugar de una exposición de datos. La práctica correcta es que ningún equipo salga sin él, verificado y registrado. Activarlo después de un incidente no sirve de nada.



## 03 Un responsable identificado por equipo

Cada dispositivo debe tener una persona asociada, con nombre, y esa asociación debe actualizarse cuando el equipo cambia de manos. Sin esto, la respuesta a cualquier incidente empieza por averiguar a quién llamar.



## 04 Una política de uso escrita, que incluya los equipos personales

El aparato personal que accede a datos corporativos existe en todas las organizaciones. Ignorarlo no lo elimina. La práctica correcta es definir qué está permitido, comunicarlo y dejar constancia de que fue aceptado.



## 05 Zonas y alertas de ubicaciones seguras configuradas antes de necesitarlas

Definir dónde debería estar cada grupo de equipos permite que el sistema avise cuando algo se sale de lo esperado, en lugar de depender de que alguien lo note. Una alerta configurada después del incidente no aporta nada.



## 06 Un procedimiento de incidente probado

Tener la capacidad de bloquear o borrar un equipo no equivale a poder hacerlo bajo presión. La práctica correcta es ensayarlo con un equipo de prueba, medir cuánto toma y dejar el procedimiento escrito, con responsables y pasos.



## 07 Offboarding con devolución del equipo como paso formal

El cierre de accesos suele estar automatizado; la devolución del equipo suele quedar como una coordinación informal que se pierde. Debe ser un paso con responsable, plazo y registro, igual que el cierre del correo.



## 08 Revisión periódica del parque completo

Un parque distribuido se desordena solo, sin que nadie haga nada mal. Sin una revisión programada, la diferencia entre lo registrado y lo real crece de forma silenciosa.



## Cómo se sostiene en el tiempo

La mayoría de las organizaciones ordena su flota una vez y lo deja correr. Seis meses después está igual que antes. Una cadencia mínima que funciona:



- **Cada mes:** contrastar altas y bajas de personal contra el inventario, estado de las configuraciones de cada dispositivo. Es el punto donde más rápido se desalinea todo.



- **Cada trimestre:** revisar el estado de cifrado del parque completo y las alertas que se generaron sin que nadie las atendiera.



- **Cada seis meses:** probar el procedimiento de incidente de punta a punta y revisar la lista de equipos que figuran sin responsable o sin actividad reciente.



**Ante cambios relevantes como incorporación masiva de nuevos equipos,** cambio de proveedor, fusión, incidente de seguridad o nueva regulación se recomienda hacer un chequeo exhaustivo de la flota.

# Cómo te apoya Prey

Las prácticas anteriores requieren una base técnica. Prey te acompaña en los distintos escenarios, independiente del tipo de flota que la empresa maneje.

## Estas son las funcionalidades detrás de cada una:

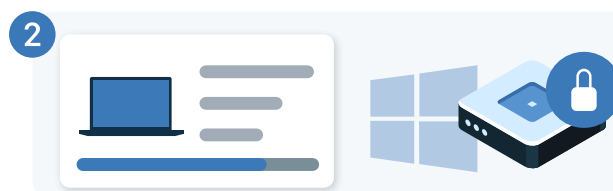
### Inventario de hardware y software

Cada equipo entra al inventario apenas se instala el agente, con su especificación y su software instalado\*. Se actualiza solo, sin que nadie tenga que mantener una planilla.



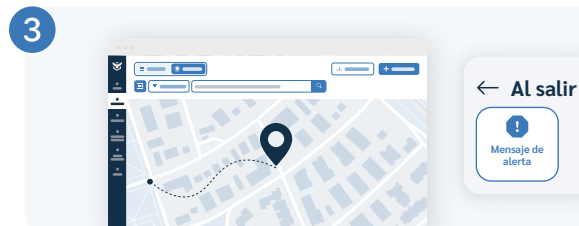
### Gestión de cifrado

Verificación y activación de BitLocker en Windows desde el mismo panel, con el estado de cada equipo a la vista en todo momento.



### Monitoreo continuo

Localización para cada equipo, con la ubicación siempre encendida y rastreando dónde se encuentran. Programa geocercas que te avisan cuando los dispositivos entran y salen de sus perímetros permitidos, y ejecutan acciones automáticas.



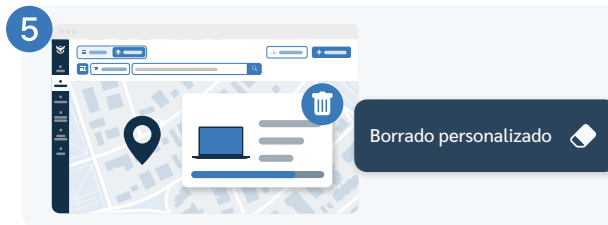
### Reporte de pérdida

Marcar un equipo como perdido o robado activa la recolección de evidencia y deja registrado el momento en que se detectó, que es el dato contra el cual después se mide el tiempo de respuesta.



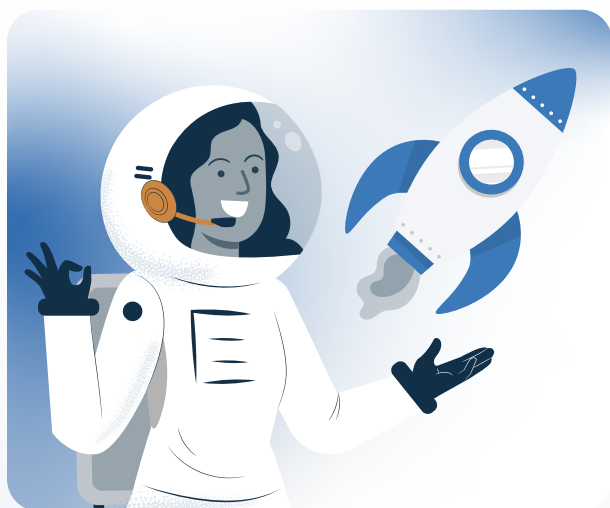
### Acciones remotas de seguridad

Bloqueo del equipo, borrado de datos y mensajes en pantalla, ejecutables sin tenerlo en la mano y sin que el usuario tenga que colaborar.



### Registro de actividad

Toda acción ejecutada queda con registro auditable. Es lo que responde por escrito cuando alguien pregunta qué se hizo y en qué momento.



## Próximos pasos

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 puede apoyarte.

[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