



Los dispositivos:

El punto ciego de la Ley 21.719

Guía para profesionales de TI que gestionan flotas diversas.

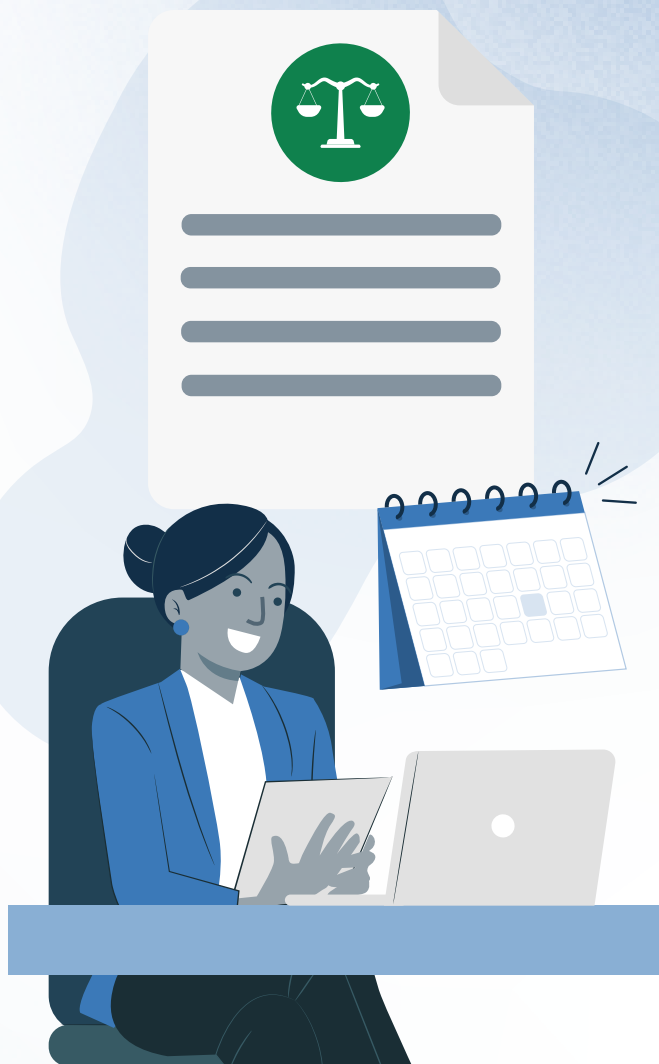


Esta guía es para TI, no para tu abogado

Casi todo lo que se ha publicado sobre la Ley 21.719 está escrito para abogados. Tiene sentido: es un texto legal, y en la mayoría de las empresas el proyecto nace en legal o en gerencia. Esa parte del trabajo está razonablemente cubierta.

El problema viene después. Cuando el proyecto avanza y hay que ejecutar, buena parte de las tareas **recae en tu equipo**. Y ahí se acaba el material de apoyo. Nadie explica qué significa “medidas técnicas apropiadas al riesgo” cuando hay doscientos notebooks repartidos entre oficinas, casas y terreno, con cuatro sistemas operativos conviviendo y un inventario que se armó en una planilla hace ocho meses.

Esta guía fue creada para llenar ese vacío. Qué dice la ley sobre los equipos que administra TI, qué riesgos ya existen, y qué capacidades hacen falta antes de que la ley entre en vigencia en diciembre de 2026.



¿Qué dice la ley sobre los dispositivos?

La Ley 21.719 no menciona notebooks ni teléfonos. Habla de datos personales y de las medidas que se deben tomar para protegerlos. Pero los datos no flotan: están en aparatos que usan y gestionan manos humanas. Tres artículos impactan directamente:



01



Proteger antes, no después (art. 14 quáter)

La ley obliga a aplicar medidas técnicas y organizativas adecuadas desde el diseño, con anterioridad y durante el tratamiento. Traducido a la operación: la protección de un equipo se define antes de entregarlo. Un notebook que sale sin cifrar no se arregla después del incidente.

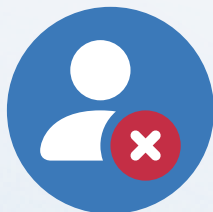
02



Prevenir la pérdida y el acceso no autorizado (art. 14 quinquies)

Este es el artículo central. Exige medidas que aseguren confidencialidad, integridad, disponibilidad y resiliencia, y que prevengan la alteración, destrucción, pérdida, tratamiento o acceso no autorizado a los datos. Un notebook robado es, literalmente, las dos cosas al mismo tiempo. Infringir este deber está tipificado como infracción grave, con multas de hasta 10.000 UTM.

03



Poder contar lo que pasó (art. 14 sexies)

Cuando ocurre una vulneración con riesgo razonable para las personas, hay que reportarla a la Agencia por los medios más expeditos posibles y sin dilaciones indebidas. Si además hay datos sensibles, de menores de catorce años o económicos, financieros, bancarios o comerciales, también hay que comunicarlo a los afectados. Del lado de TI eso implica algo muy concreto: para reportar hay que saber qué equipo era, qué datos tenía y qué se alcanzó a hacer.



La ley no entrega una lista de herramientas para comprar. Habla de medidas apropiadas al riesgo, tipo de tratamiento de datos y tamaño de la empresa. Eso significa que no existe una checklist de buenas prácticas que cubra la mayoría de estos.

Los riesgos que ya tienes en tu flota



Ninguno de estos escenarios son hipotéticos. Si administras una flota de equipos, reconoces al menos tres:

01 El equipo que nadie sabe que existe

Compras que hizo otra área, notebooks heredados de un proyecto que terminó, la máquina de reemplazo que se prestó y quedó circulando. No está en ninguna lista, así que tampoco está en ningún plan de protección. Es el más difícil de detectar porque simplemente nadie lo mira.



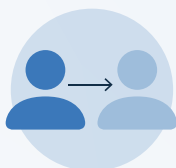
02 El equipo sin cifrar

Salió de TI a la rápida y el cifrado nunca se verificó, o alguien lo desactivó. La consecuencia es concreta: si este equipo se pierde, cualquiera que saque el disco y lo conecte a otra máquina lee los datos. El cifrado es lo que convierte un robo en un problema de hardware en vez de una brecha de datos personales.



03 El equipo cambió de manos

En los registros figura asignado a alguien que ya no lo usa. El día que pase algo, el aviso va a la persona equivocada y la búsqueda apunta donde el equipo no está. Y si hay que explicar quién tenía acceso a qué datos, la respuesta va a ser incorrecta.



04 El equipo personal que toca datos corporativos

Correo de la empresa configurado en un teléfono personal, archivos compartidos abiertos en un notebook familiar, una sesión que quedó sin cerrar. No está en el inventario porque el aparato no es de la empresa, pero los datos sí lo son, y la responsabilidad también.



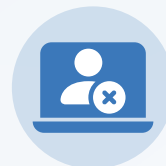
05 El equipo que no está en el lugar declarado por su usuario

Alguien se llevó el notebook de viaje, o cambió de ciudad, o el equipo lleva semanas sin aparecer y nadie lo notó porque tampoco había forma de notarlo. No es sospechoso por sí solo. Lo preocupante es enterarse tarde.



06 El equipo que no volvió del offboarding

El día que la persona deja la empresa se cierra el correo del usuario, los accesos la VPN y otras herramientas, pero la devolución del notebook queda “por coordinar”. Casi todas las empresas tienen dos o tres equipos como este, y se catalogan como merma. Pero ante la ley siguen siendo responsabilidad de la empresa tanto los equipos como los datos personales que almacenan.



07 El equipo que se pierde o roban

Es el único caso de la lista en que la velocidad de respuesta es clave. Cuando un notebook se sale del alcance, la ley deja de preguntarte por tus políticas y pasa a preguntarte qué alcanzaste a hacer: si pudiste ubicarlo, si los datos estaban cifrados, si lograste bloquearlo o borrarlo antes de que alguien lo abriera. Y es el momento en que los seis riesgos anteriores se cobran juntos, porque el equipo que desapareció puede ser justo el que no estaba en el inventario o el que nunca se cifró.

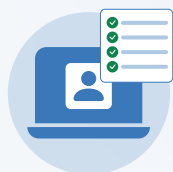


Las capacidades que necesitas

No son productos ni suscripciones, son ejemplos del control que tienes que tener para poder responder en cualquier momento, incluso frente a equipos apagados o desaparecidos.

01 Saber qué equipos pertenecen a la empresa, y quién tiene cada uno.

Es la base de todo lo demás. No se puede proteger, cifrar ni borrar lo que no se conoce. Y sin este control, ninguna de las otras cuatro capacidades tiene sobre qué operar.



02 Saber si siguen cifrados, hoy.

No basta con saber que fueron cifrados cuando se configuró la política. Si la medida no se puede verificar, tampoco se puede demostrar, y para efectos prácticos es como si no existiera.



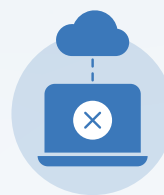
03 Saber dónde están.

No para vigilar a nadie: para poder actuar cuando un equipo desaparece, y para detectar que algo se salió de lo esperado antes de que se transforme en incidente.



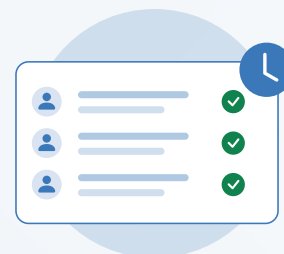
04 Poder actuar en forma remota.

Bloquear el equipo y borrar los datos sin tenerlo físicamente. Esta es la diferencia entre responder en minutos y responder con una notificación de que se perdió información y no se pudo hacer nada.



05 Llevar registros de todo lo anterior.

La más difícil, y la que la ley pide con más claridad. El principio de responsabilidad significa que no basta con haber actuado bien: hay que poder demostrarlo, con fecha y usuario responsable. Si la evidencia depende de que alguien se acuerde, no es evidencia.



Cómo te apoya Prey

Las cinco capacidades anteriores son las que Prey resuelve, en un solo lugar, independiente del tipo de flotas 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.



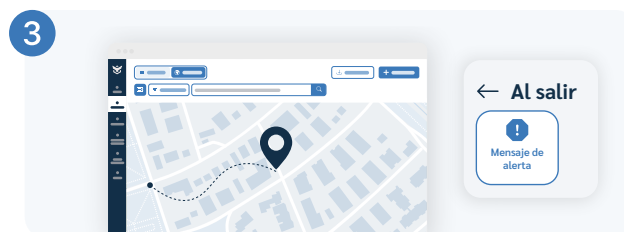
Gestión de cifrado

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.



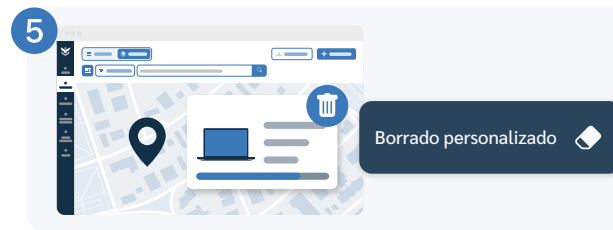
Reporte de pérdida

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.



Windows, macOS, Ubuntu, Android, iOS y Chromebook conviven en la misma cuenta, que en la práctica es lo que permite mantener el inventario completo.



Comencemos

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