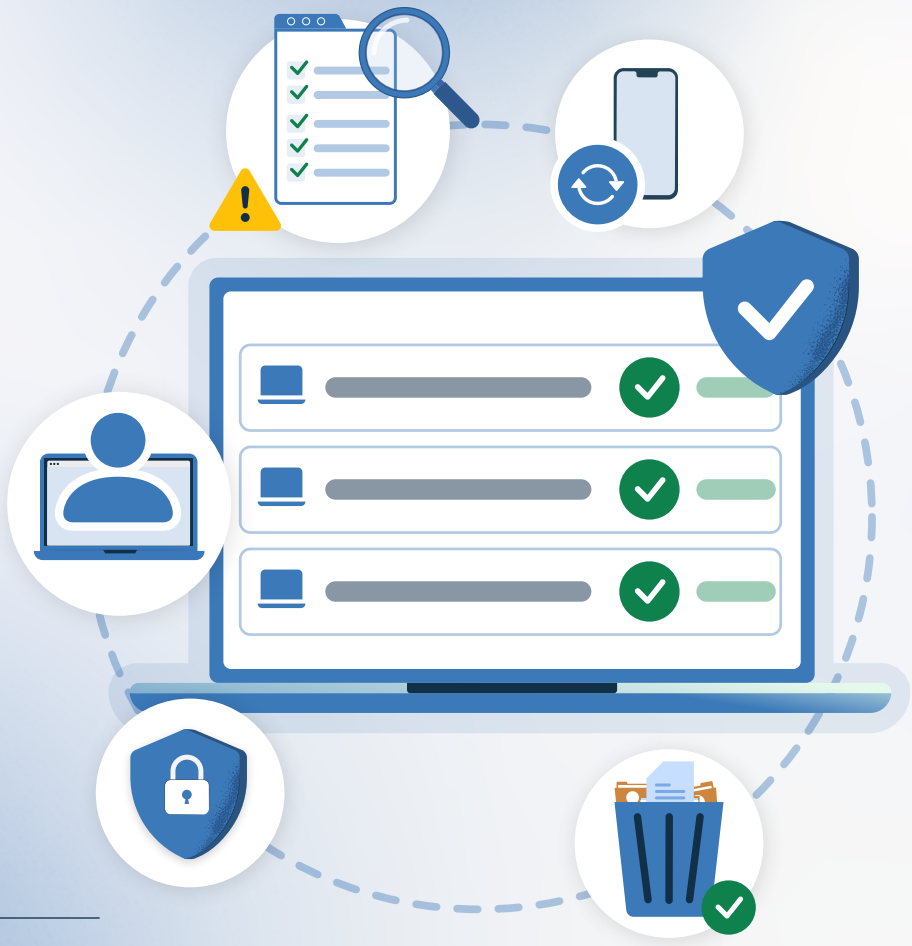


Checklist de evidencia de dispositivos:

Cómo demostrar control de endpoints (Ley 21.719)

Prey Inc.

Checklist de evidencia de dispositivos:

Cómo demostrar control de endpoints (Ley 21.719)

Este checklist permite a los equipos de TI verificar si cuentan con la evidencia mínima de control y seguridad de los dispositivos (endpoints) exigida por las buenas prácticas de ciberseguridad y por el principio de responsabilidad activa de la Ley 21.719 de protección de datos personales.

Aplica para:

- Laptops corporativas
- Dispositivos móviles de trabajo
- Tablets corporativas
- Dispositivos BYOD autorizados

1. Inventario y ownership

El primer requisito para demostrar control es saber qué dispositivos existen y quién los utiliza.

- [ ] Inventario actualizado de todos los dispositivos corporativos
- [ ] Campos mínimos: dispositivo/ID, usuario asignado, tipo (laptop/móvil/tablet), OS/versión, estado (activo/inactivo), ubicación/área (si aplica)
- [ ] Ownership definido: corporativo / BYOD / compartido
- [ ] Dueño interno del inventario (rol/área)
- [ ] Evidencia de altas/bajas de dispositivos (onboarding/offboarding de equipos)
- [ ] El inventario se revisa periódicamente (mensual o trimestral)

Evidencia recomendada:
Exportación mensual, registro de cambios (changelog) y responsable.

2. Historial de asignación del dispositivo

Para incidentes de seguridad o auditorías, es clave poder demostrar quién utilizó un dispositivo y cuándo.

- [ ] Existe historial de usuarios asignados por dispositivo
- [ ] Se registran fechas de entrega y devolución
- [ ] Los dispositivos se limpian (wipe) antes de reasignarse
- [ ] Existe registro de estado del equipo al ser devuelto

Evidencia recomendada:
Registro de asignaciones, wipe logs y registros de entregas

3. Provisión segura del dispositivo (onboarding)

Todo dispositivo debe ingresar al entorno corporativo con controles de seguridad activos desde el inicio.

- [ ] Todos los dispositivos se enrolan en una plataforma de gestión (MDM/UEM)
- [ ] Se aplica una baseline de seguridad automática
- [ ] El cifrado del disco se verifica antes de entregar el equipo
- [ ] Las políticas de seguridad se aplican automáticamente
- [ ] Capacidad de localización remota habilitada desde el enrolamiento*

Evidencia recomendada:
Logs de enrollment y baseline aplicada

***Nota:**
La localización del dispositivo solo debe utilizarse con fines de seguridad o de recuperación de activos, por ejemplo, cuando un equipo es reportado como perdido o robado.

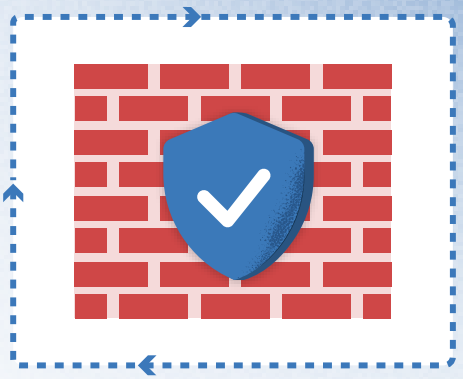
4. Controles básicos de seguridad del endpoint

Estos controles reducen el riesgo de exposición de datos personales.

- [ ] Cifrado habilitado (por dispositivo) con reporte de cumplimiento
- [ ] Bloqueo/pin/passcode obligatorio + timeout configurado
- [ ] Protección de pantalla (auto-lock) aplicada por política
- [ ] Política de dispositivos no conformes (qué pasa si no cumple: bloqueo, cuarentena, etc.)
- [ ] (Si aplica) Secure boot / protección adicional documentada

Evidencia recomendada:
Reporte de cifrado, reporte de passcode/lock, lista de “non-compliant” y acciones tomadas.

5. Postura de seguridad



El estado de seguridad del endpoint debe ser verificable.

- [ ] Reporte de OS/patch level (actualizaciones)
- [ ] Detección de root/jailbreak y estado (móvil)
- [ ] Estado de antimalware o EDR (si aplica)
- [ ] Configuraciones de firewall activa
- [ ] Cumplimiento de políticas de seguridad verificable

Evidencia recomendada:
Reportes de posture/compliance e historial de cambios de políticas.

6. Acceso y control de identidad asociado al dispositivo

Los dispositivos suelen ser el punto de acceso a sistemas que contienen datos personales.

- [ ] Evidencia de MFA aplicado a accesos críticos
- [ ] Control de cuentas administrativas locales
- [ ] Registro de cambios de privilegios
- [ ] Revocación de accesos en offboarding
- [ ] (Si aplica) Conditional access / acceso condicionado por compliance del dispositivo
- [ ] Registro de excepciones (quién aprueba, por cuánto tiempo, y por qué)

Evidencia recomendada:
Reporte de MFA, listado de excepciones, registro de cambios de privilegios.

7. Capacidad de respuesta ante incidentes

(acciones remotas con trazabilidad)

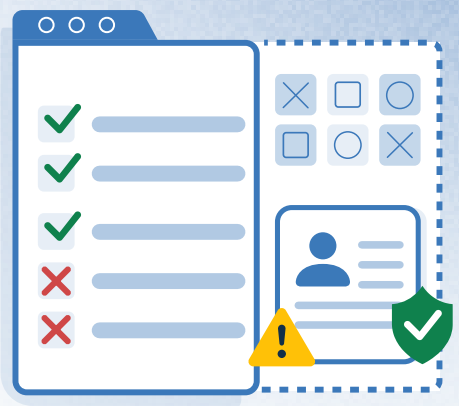
Los dispositivos afectados por algún incidente de seguridad son una de las principales fuentes de brechas de datos.

- [ ] Capacidad de remote lock
- [ ] Capacidad de remote wipe (full wipe) + selective wipe (BYOD)
- [ ] Capacidad de localización del dispositivo (si aplica)
- [ ] Flujo documentado de pérdida/robo (quién ejecuta qué, en qué orden)
- [ ] Logs de acciones remotas (quién, cuándo, qué acción, resultado)

Evidencia recomendada:
Logs/export de acciones y tickets/registro del incidente.

8. Apps, configuración y datos corporativos

(cuando aplica)



El control de aplicaciones ayuda a prevenir la exposición de datos.

- [ ] Lista de apps corporativas autorizadas (whitelist)
- [ ] Restricciones de instalación de software (blacklist)
- [ ] Distribución centralizadas de apps corporativas
- [ ] Separación de datos personales y corporativos (BYOD)
- [ ] Reporte/historial de cambios de configuración aplicados

Evidencia recomendada:
Reporte de apps instaladas/gestionadas, políticas aplicadas e historial de cambios.

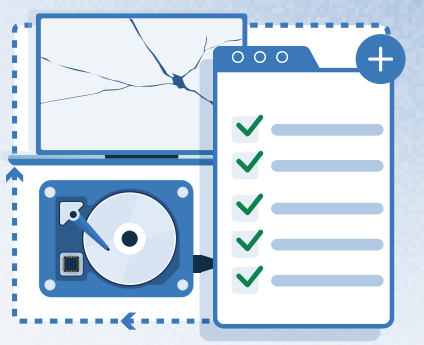
9. Logs y evidencia de auditoría

La evidencia técnica debe poder demostrar que los controles realmente existen y funcionan.

- [ ] Definición de qué logs se almacenan
- [ ] Política de retención de logs (por cuánto tiempo y dónde)
- [ ] Centralización o export “audit-ready” (no screenshots)
- [ ] Control de integridad (evitar edición manual)
- [ ] Evidencia de revisiones periódicas (mensual/trimestral) del cumplimiento

Evidencia recomendada:
Política de retención de logs, evidencia de export/centralización y actas de revisión.

10. Fin de vida del dispositivo



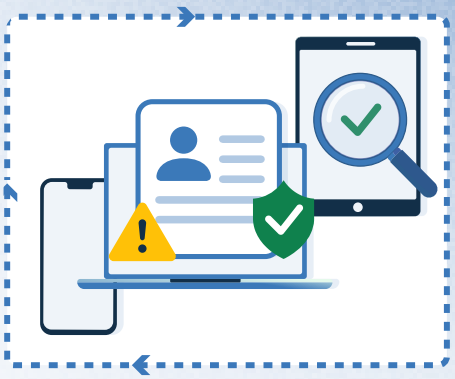
La gestión del ciclo de vida del dispositivo evita exposición de datos al retirar equipos.

- [ ] Procedimiento de baja de dispositivos
- [ ] Wipe completo antes de retiro
- [ ] Eliminación segura de datos
- [ ] Capacidad de selective wipe
- [ ] Registro de dispositivos retirados

Evidencia recomendada:
Registro de wipes e inventario actualizado

11. Gestión de dispositivos BYOD

(cuando aplica)



Cuando se permiten dispositivos personales para el trabajo, se requieren controles específicos.

- [ ] Existe política BYOD documentada
- [ ] Separación de datos corporativos y personales
- [ ] Requisitos mínimos de seguridad para BYOD
- [ ] Capacidad de selective wipe
- [ ] Registro de dispositivos BYOD autorizados

Evidencia recomendada:
Política de BYOD e inventario BYOD

¿Puedes demostrar control real sobre tus dispositivos?

En muchas auditorías de seguridad o cumplimiento, el problema no es la falta de controles.
El problema es la falta de evidencia clara de esos controles.

Cuando un dispositivo se pierde, un empleado deja la empresa o ocurre un incidente de seguridad, los equipos de TI deben poder responder preguntas como:

- ¿Dónde estaba el dispositivo por última vez?
- ¿Quién lo tenía asignado?
- ¿Se bloquearon los accesos?
- ¿Se protegieron los datos corporativos?

Tener visibilidad sobre tus endpoints no es solo una buena práctica de operaciones de TI.
Es una forma concreta de reducir el riesgo de exposición de datos personales y demostrar control operativo.

Con Prey, los equipos de TI pueden:

- **Mantener** inventario actualizado de dispositivos
- **Aplicar** políticas de seguridad
- **Localizar** dispositivos perdidos
- **Gestión** de préstamos de dispositivos
- **Ejecutar** remote lock o wipe
- **Ejecutar** acciones de seguridad basadas en eventos.
- **Mantener** historial de acciones y auditoría

Agendar demo y descubre cómo Prey puede ayudarte a obtener visibilidad real sobre tu flota de dispositivos.

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**