Checklist de auditoría:

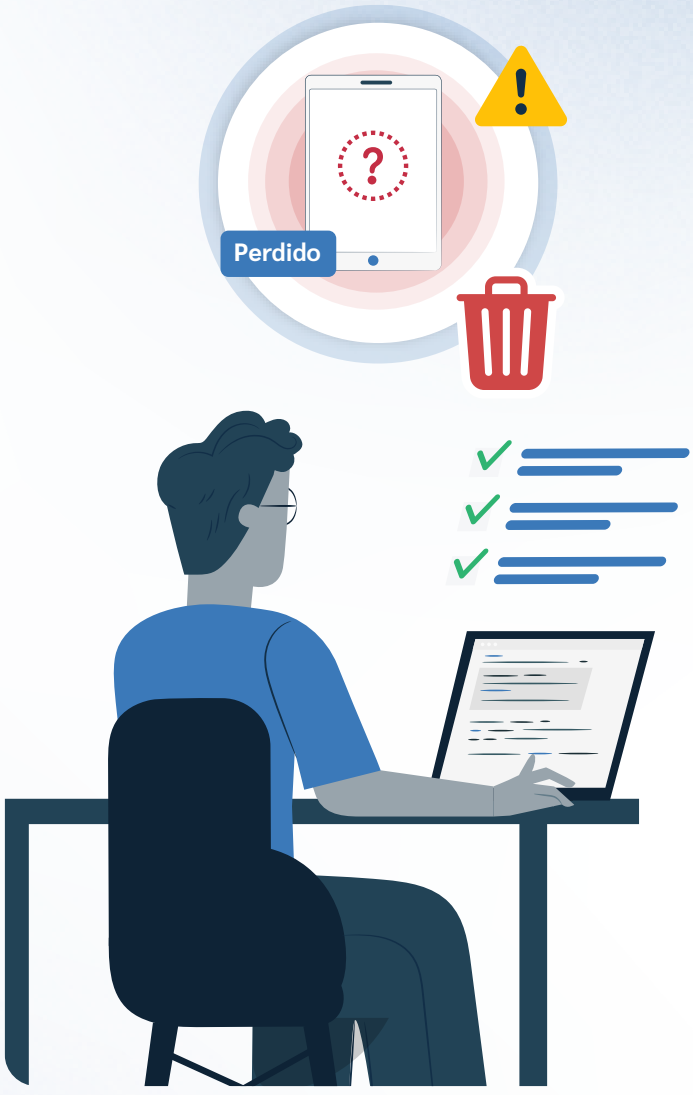
Gestión del ciclo de vida de dispositivos (DLM)

Prey Inc.

Checklist de auditoría: Gestión del ciclo de vida de dispositivos (DLM)

Evalúa si tu organización tiene control real sobre el ciclo de vida de sus dispositivos en menos de 10 minutos.

La gestión del ciclo de vida de los dispositivos se ha convertido en una capacidad crítica para los equipos de TI. Con el crecimiento del trabajo remoto, el uso de dispositivos móviles y las exigencias de cumplimiento normativo, cada laptop o smartphone corporativo representa tanto un activo operativo como un posible punto de riesgo para la organización.



En la práctica, muchas empresas creen tener control sobre sus dispositivos, pero cuando ocurre un incidente —como la pérdida de un equipo o una auditoría de seguridad— descubren que faltan elementos básicos: inventarios incompletos, procesos de offboarding poco claros o ausencia de controles como el bloqueo o borrado remoto.

Esta checklist te ayudará a evaluar rápidamente si tu organización tiene control real sobre el ciclo de vida de sus dispositivos. Incluye controles clave que los equipos de TI deberían poder demostrar, junto con la evidencia técnica que normalmente se solicita durante auditorías de seguridad o revisiones internas.

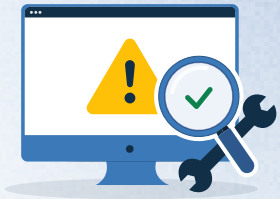
1. Inventario y visibilidad de dispositivos

Control	Evidencia esperada	Riesgo si no existe	Status	Próximos pasos
Inventario centralizado de todos los dispositivos corporativos	Export de inventario con ID del dispositivo, usuario, OS y última conexión	Dispositivos activos que TI no conoce	☐ Implementado ☐ Parcial ☐ No existe	
Cada dispositivo tiene usuario asignado u ownership definido	Registro de asignación de dispositivos	Imposible determinar quién tenía el dispositivo en caso de incidente	☐ Implementado ☐ Parcial ☐ No existe	
El inventario incluye tipo de dispositivo, sistema operativo y versión	Reporte de inventario actualizado	Falta de visibilidad sobre vulnerabilidades y estado del sistema	☐ Implementado ☐ Parcial ☐ No existe	
Existe visibilidad sobre la última actividad del dispositivo	Logs de check-in o conexión	Dispositivos que desaparecen operativamente	☐ Implementado ☐ Parcial ☐ No existe	
Los dispositivos que no reportan actividad generan alertas	Configuración de alertas de inactividad	Equipos comprometidos o perdidos pasan desapercibidos	☐ Implementado ☐ Parcial ☐ No existe	

2. Enrollment y configuración inicial

Control	Evidencia esperada	Riesgo si no existe	Status	Próximos pasos
Todos los dispositivos pasan por enrollment obligatorio	Registro de inscripción en la plataforma de gestión	Equipos fuera del control de TI	☐ Implementado ☐ Parcial ☐ No existe	
Se aplica una baseline de seguridad estándar a todos los dispositivos	Políticas de seguridad aplicadas	Configuraciones inconsistentes entre dispositivos	☐ Implementado ☐ Parcial ☐ No existe	
Los dispositivos nuevos utilizan automatización o zero-touch deployment	Configuración de despliegue automatizado	Procesos manuales lentos y propensos a errores	☐ Implementado ☐ Parcial ☐ No existe	
El cifrado de disco está habilitado desde el primer uso	Estado de cifrado activo	Exposición de datos en caso de robo o pérdida	☐ Implementado ☐ Parcial ☐ No existe	

3. Monitoreo y mantenimiento



Control	Evidencia esperada	Riesgo si no existe	Status	Próximos pasos
Se monitorea el estado de seguridad de los dispositivos	Reporte de compliance de dispositivos	Dispositivos vulnerables pasan desapercibidos	☐ Implementado ☐ Parcial ☐ No existe	
Los dispositivos reciben actualizaciones de seguridad periódicas	Logs de actualización del sistema	Vulnerabilidades explotables	☐ Implementado ☐ Parcial ☐ No existe	
Se detectan dispositivos fuera de cumplimiento de políticas	Alertas de desviación de políticas	Configuraciones inseguras sin remediación	☐ Implementado ☐ Parcial ☐ No existe	
Existe visibilidad del estado del sistema operativo y parches	Reporte de versión y patch level	Falta de control sobre vulnerabilidades	☐ Implementado ☐ Parcial ☐ No existe	

4. Gestión de incidentes de dispositivos

Control	Evidencia esperada	Riesgo si no existe	Status	Próximos pasos
Existe un procedimiento para dispositivos perdidos o robados	Procedimiento documentado	Respuesta improvisada ante incidentes	☐ Implementado ☐ Parcial ☐ No existe	
El equipo de TI puede localizar dispositivos cuando es necesario	Historial de ubicación o último check-in	Imposibilidad de recuperar equipos	☐ Implementado ☐ Parcial ☐ No existe	
Existe capacidad de bloqueo remoto del dispositivo	Logs de remote lock	Acceso no autorizado a información corporativa	☐ Implementado ☐ Parcial ☐ No existe	
Existe capacidad de borrado remoto de datos (remote wipe)	Registro de ejecución de wipe	Exposición de datos sensibles	☐ Implementado ☐ Parcial ☐ No existe	

5. Offboarding y retiro de dispositivos

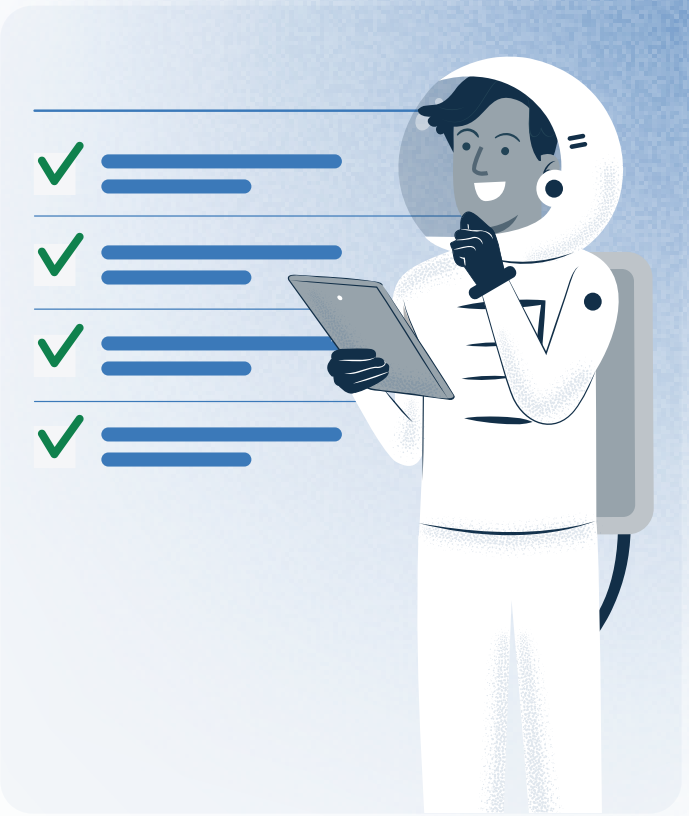
Control	Evidencia esperada	Riesgo si no existe	Status	Próximos pasos
Existe un proceso formal de offboarding de dispositivos	Procedimiento documentado	Equipos y accesos quedan activos	☐ Implementado ☐ Parcial ☐ No existe	
Los dispositivos de empleados que dejan la organización se recuperan o bloquean	Registro de recuperación o bloqueo	Riesgo de acceso persistente	☐ Implementado ☐ Parcial ☐ No existe	
Los dispositivos retirados pasan por borrado seguro de datos	Registro de wipe o destrucción de datos	Exposición de información corporativa	☐ Implementado ☐ Parcial ☐ No existe	
Los equipos retirados se eliminan del inventario activo	Registro de baja del dispositivo	Inventario inconsistente	☐ Implementado ☐ Parcial ☐ No existe	

Resultado rápido de la auditoría

Cuenta cuántos controles marcaste como **No existe.**

- **0–3:** Lifecycle bien controlado
- **4–8:** Existen brechas operativas relevantes
- **9 o más:** La organización probablemente no tiene control real del lifecycle de dispositivos

Cómo Prey puede ayudarte a cumplir este checklist



Las herramientas de gestión y seguridad de dispositivos juegan un rol importante para implementar muchos de los controles incluidos en esta checklist. Prey ayuda a los equipos de TI a mantener visibilidad y control sobre sus dispositivos corporativos, especialmente en entornos donde los equipos operan fuera de la red de la organización.

Algunas funcionalidades de Prey que pueden apoyar la gestión del ciclo de vida de dispositivos incluyen:

Visibilidad de la flota de dispositivos

Prey permite mantener un inventario centralizado de dispositivos y conocer información clave como el estado del equipo, el sistema operativo y la última actividad reportada.

Localización de dispositivos

En caso de pérdida o robo, los equipos de TI pueden localizar dispositivos para facilitar su recuperación o investigar incidentes.

Bloqueo remoto de dispositivos

Si un dispositivo se extravía o cae en manos no autorizadas, es posible bloquear el equipo para evitar accesos indebidos.

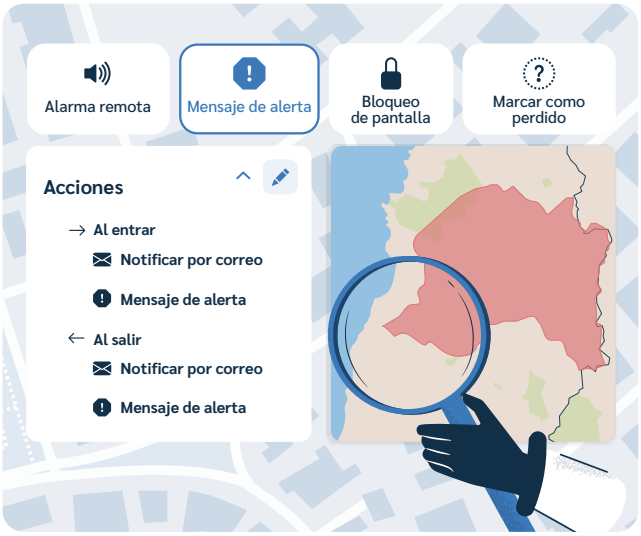
Borrado remoto de datos (remote wipe)

Cuando existe riesgo de exposición de información sensible, los administradores pueden eliminar datos del dispositivo de forma remota.

Alertas de seguridad y geofencing

Las alertas permiten detectar comportamientos inusuales o movimientos de dispositivos fuera de zonas definidas, lo que ayuda a responder más rápido ante posibles incidentes.

En conjunto, estas capacidades permiten a los equipos de TI fortalecer el control sobre sus dispositivos y responder de manera más rápida cuando ocurre un incidente de seguridad.



¿Quieres mejorar el control y la visibilidad sobre tus dispositivos corporativos?

Descubre cómo Prey puede ayudarte a proteger y gestionar tu flota de dispositivos.

Solicita tu demo personalizada

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**