Checklist de seguridad y preparación

de fin de año con Prey

Prey Inc.

Checklist de seguridad y preparación de fin de año con Prey

Un año nuevo merece una flota igual de renovada. El inicio de año es el momento perfecto para ordenar tu cuenta, confirmar que todo funciona bien y asegurarte de que tus dispositivos estén listos para cualquier caos que traiga enero.

1. Salud general de la cuenta y la organización

Tu cuenta de Prey es el centro de mando de todo. Mantener ordenados los usuarios, permisos y accesos significa menos dolores de cabeza después. Este paso se asegura de que las personas correctas tengan el acceso correcto, que no queden sesiones antiguas dando vueltas y que tu cuenta esté protegida desde adentro hacia afuera.

Nombre	N° personas	Gestión de cuenta	Gestión de dispositivos	Acciones de dispositivos	Acciones
Owner	1	Todos los permisos	Todos los permisos	Todos los permisos	Todos los
Admin	0	Todos los permisos	Todos los permisos	Todos los permisos	Todos los
User	0	Sin permisos	Algunos permisos	Todos los permisos	Algunos

Seguridad de la cuenta

Tus dispositivos pueden estar repartidos por todas partes, pero tu cuenta de Prey es el corazón de la operación, y tiene que estar bien asegurada. Esta sección se trata de reducir errores humanos y cerrar la puerta principal a riesgos innecesarios.

- [ ] Verifica que cada usuario tenga **2FA** (autenticación en dos factores) activado.
  (Los usuarios deben activarla ellos mismos desde la configuración de su perfil.)
- [ ] Revisa y actualiza los **roles y permisos de usuario** (Owner, Admin, User o roles personalizados).
- [ ] Usa el **Registro de auditoría** (Full Suite) para revisar acciones recientes sobre dispositivos, cambios de administración y eventos críticos.
- [ ] (Opcional) Realiza una **rotación de contraseñas** para usuarios con permisos elevados.
  Consejo: Si un admin las cambia desde el Panel, avisa a los usuarios para que puedan volver a iniciar sesión.

2. Seguimiento y monitoreo de dispositivos

Si un dispositivo desaparece del mapa y nadie se da cuenta... ¿realmente pasó algo? Esta sección se asegura de que tu configuración de rastreo esté funcionando bien, para que no te tome por sorpresa cuando alguien deje un laptop en un taxi... o algo peor.

Configuración de Tracking

El rastreo solo sirve si realmente está rastreando. Suena obvio, pero es fácil asumir que todo está bien... hasta que deja de estarlo. Estos chequeos se aseguran de que los dispositivos hablen con el Panel, envíen ubicación y se actualicen con frecuencia, especialmente si dependes de Rastreo activo para mantener control.

- [ ] Confirma que estén activos todos los dispositivos usando los filtros del Panel.
- [ ] Valida que **el rastreo Activo** esté habilitado cuando se necesiten actualizaciones de ubicación continuas.

Visibilidad del Historial de Ubicación

Saber dónde está un dispositivo en estos momentos es útil; saber por dónde se ha movido es mucho más poderoso. Antes de empezar el año, date una vuelta por el historial de ubicaciones de tus equipos. Esto ayuda a detectar alertas tempranas, validar usos o simplemente confirmar que todo ha operado como es debido.

- [ ] Revisa y **exporta el Historial de Ubicación** para confirmar que los dispositivos reportan de forma regular.
- [ ] Marca los dispositivos que muestren largos periodos sin conexión o patrones extraños de movimiento.

3. Adopción y validación de geocercas

Las geocercas te avisan cuando un dispositivo sale del edificio, entra a una zona restringida o está donde no debería. Esta sección te ayuda a revisar si tus geocercas están correctamente configuradas y haciendo su trabajo: enviar alertas, ejecutar acciones y mantener tu flota dentro de los límites esperados.

- [ ] Verifica que las **Geocercas** para tus ubicaciones clave estén configuradas (oficinas, colegios, bodegas, etc.).
- [ ] Asegúrate de que los **dispositivos estén asignados** a las geocercas correctas.
- [ ] Valida que las **notificaciones por correo** estén configuradas para alertar entradas y salidas.
- [ ] Confirma que las acciones automáticas estén configuradas y probadas donde se necesiten.

Visibilidad de la flota

Mantener tu flota visible y conectada garantiza que las acciones remotas funcionen cuando más las necesitas. Estos chequeos ayudan a detectar problemas de conexión a tiempo, confirmar que los comandos de seguridad llegan a los equipos y evitar que estés “a ciegas” cuando algo sale mal.

- [ ] Verifica que el firewall, antivirus, proxy y otras herramientas de seguridad estén permitiendo el tráfico de Prey, evitando bloqueos en la comunicación del agente con los servidores de Prey.
- [ ] Confirma que todos los **dispositivos sean visibles** en la vista mapa y se hayan conectado recientemente al Panel.
- [ ] Revisa la **última conexión** y el **estado de conexión**, ayúdate usando los filtros de la página de Dispositivos.
- [ ] Revisa que **no tengas equipos duplicados** entre los que hayas reinstalado, y que no estén asociados a más de un grupo (a menos que lo necesites).
- [ ] Revisa si hay **patrones de ubicación inusuales** o dispositivos que permanezcan fuera de línea.

4. Seguridad y protección de dispositivos

Los dispositivos se pierdan y son robados, son cosas que pasan. Lo importante es qué tan preparado estás cuando sucede. Esta sección se enfoca preparar tus herramientas de seguridad antes de que algo salga mal, para que puedas actuar rápido, proteger datos sensibles y evitar un problema mayor.

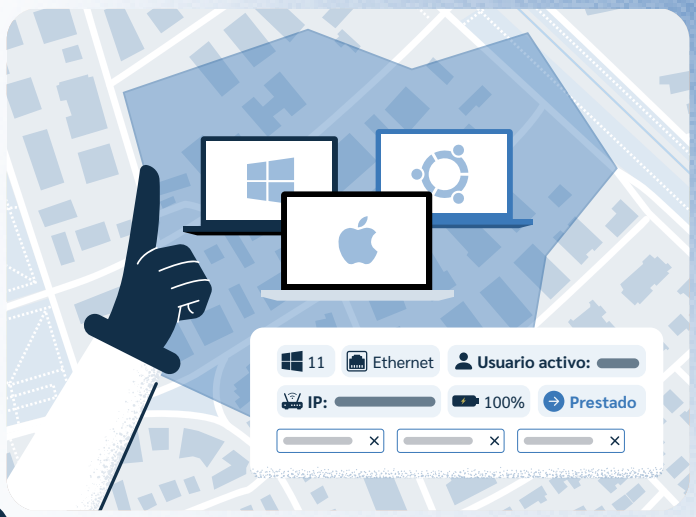
Protección de datos (dependiente del SO)

Algunos equipos almacenan datos sensibles, credenciales o acceso a otros sistemas. Estos pasos te ayudan a confirmar que el cifrado esté activado donde corresponde y que tengas la capacidad de borrar todo a distancia si hace falta. Mejor tener la red de seguridad y no usarla, que necesitarla y no tenerla.

- [ ] Prueba la funcionalidad de **Borrado** personalizado en un dispositivo de prueba.
- [ ] Usa el filtro de **Cifrado para identificar dispositivos que soportan cifrado** y aquellos que almacenan datos sensibles.
- [ ] Exporta el archivo **CSV con las llaves de recuperación de BitLocker** de los dispositivos Windows y guárdalo de forma segura.

5. Gestión de dispositivos

El objetivo central de la gestión de dispositivos es la organización; mantener todo actualizado y limpio. Asegúrate de no cargar con registros desactualizados o “equipos fantasma”.



Revisión de inventario

¿Cuándo fue la última vez que repasaste cuáles son los dispositivos que tienes en circulación? Esta es tu oportunidad para confirmar que cada equipo está registrado, que corre la última versión de Prey y que no haya máquinas olvidadas en algún cajón.

- [ ] Asegúrate de que **todos los dispositivos tengan instalada la última versión de Prey.**
- [ ] Exporta un CSV con el inventario completo de dispositivos para verificar la integridad de los datos de hardware y detectar anomalías.
- [ ] Elimina o archiva los **dispositivos dados de baja o inactivos** de la cuenta, liberando espacios en tu suscripción.

Organización y etiquetas

Agrupa los dispositivos para reflejar sus funciones dentro de la organización: por equipo humano, departamento, ubicación/oficina o programa de préstamo. Etiquetas y grupos bien pensados ahorran tiempo, reducen confusiones y evitan el scroll infinito.

- [ ] Confirma que las **etiquetas y grupos reflejen la estructura actual:** equipos, departamentos, locaciones como campus, facultad o bodega, y programas de préstamo.

Acciones masivas y Acciones automáticas (solo Full Suite)

¿Quieres bloquear 20 laptops de una sola vez sin sufrir en el proceso? Para eso están las **acciones masivas y automáticas**, ayudantes para eventos repetitivos como marcar dispositivos con batería baja o reaccionar cuando un equipo lleva días sin conectarse.

- [ ] Prueba las **Acciones masivas** como **Bloqueo y Desbloqueo de pantalla, Mensaje de alerta y Alarma remota en algunos dispositivos de prueba.**
- [ ] Valida que las **Acciones automáticas** estén correctamente programadas (marcar dispositivos como perdidos en horas exactas o tiempos sin conexión a Prey etc.).

6. Automatizaciones programadas

Las Acciones automáticas te permiten definir reglas inteligentes que se activan cuando pasa algo específico: desconexión con los servidores de Prey (periodos fuera de control) o cambios de hardware, para que nada se te escape. Una vez configuradas, trabajan en segundo plano por ti.

- [ ] Revisa y prueba las Acciones automáticas configuradas:
  - Marcar como perdido
  - Mensaje de alerta
  - Alarma remota
  - Bloqueo de pantalla

7. Gestión de préstamos de dispositivos (Full Suite)

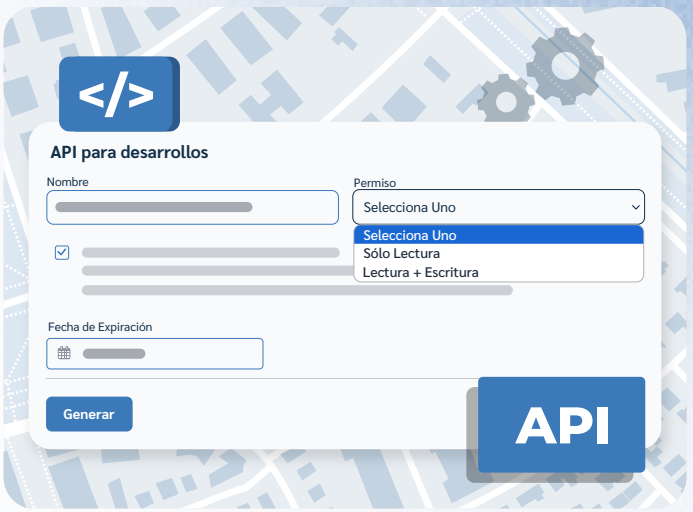
Esta sección se trata de mantener tu sistema de préstamos bajo control: fechas de devolución claras, dispositivos asignados correctamente y equipos atrasados que no pasan desapercibidos.

Administrador de Préstamos

El Administrador de Préstamos facilita asignar dispositivos, hacer seguimiento de las devoluciones y agregar un poco de automatización al proceso. Con alertas, acciones de seguridad para equipos atrasados y buena visibilidad, mantiene todo ordenado sin sumar carga extra al equipo.

- [ ] Revisa y ordena las **asignaciones de usuario**, asegurándote de que cada dispositivo tenga una persona usuaria establecida.
- [ ] Revisa todos los **préstamos activos** y confirma sus fechas de vencimiento.
- [ ] Asegúrate de que las **notificaciones** por dispositivos atrasados se estén enviando y recibiendo correctamente.

8. Integraciones para desarrolladores y API (Full Suite)



Si usas Prey junto a otras herramientas, como tu sistema de tickets o dashboards internos, esta sección es para asegurarte de que todo siga comunicándose entre sí. Un chequeo rápido ayuda a evitar flujos rotos, tokens vencidos o vacíos inesperados en tus integraciones.

Herramientas para desarrolladores

La API y las integraciones te dan más control y flexibilidad, pero también necesitan mantención de vez en cuando. Considera esto un recordatorio para revisar el estado de tus tokens, limpiar lo que ya no se usa y confirmar que los sistemas conectados sigan funcionando sin problemas.

- [ ] Rota / Desvincula cualquier **API Key** que no se esté utilizando.
- [ ] Si tienes integraciones habilitadas, **revisa su estado y verifica que estén funcionando como se espera.**

9. Breach Monitoring (bonus track)

Las credenciales tienen la mala costumbre de aparecer donde no deben, sobre todo cuando nadie está mirando. Si estás suscrito a Breach Monitoring de Prey, esta sección te ayuda a confirmar que tu servicio esté bien configurado, detectando correctamente y dándote la información necesaria para reaccionar rápido.

Conciencia de la exposición

Una mirada rápida al dashboard de Breach Monitoring puede decirte mucho: qué correos han aparecido en la dark web, qué tipo de datos se expusieron y con qué frecuencia está ocurriendo.

- [ ] Revisa el **Reporte de Breach Monitoring** para detectar credenciales expuestas, PII u otros datos relevantes.
- [ ] Descarga y archiva el **último reporte** para analizarlo o reportar temas de cumplimiento.
- [ ] Verifica si el **tu suscripción es la más conveniente para tu caso de uso, correos o dominio completo.** Tu necesidad puede haber cambiado desde que contrataste el servicio.

10. Preparación de fin de año

¡Casi llegas a la meta! Esta última sección es tu barrido final: cerrar pendientes, probar tus acciones de respuesta y dejarle a tu equipo un punto de partida limpio para comenzar el nuevo año con fuerza.

Chequeos finales

Antes de dar todo por cerrado, vale la pena confirmar que los dispositivos siguen reportando, que las acciones remotas funcionan bien y que tu equipo sabe qué hacer si algo sale mal. Un poco de tiempo ahora ahorra muchos dolores de cabeza después.

- [ ] Visita la página de **Dispositivos** para asegurarte de que toda tu flota haya registrado actividad durante los últimos 30 días.
- [ ] Ordena usuarios, geocercas, automatizaciones e inventario para **comenzar el año entrante con registros frescos.**
- [ ] Ejecuta una **prueba de acciones remotas** (bloqueo, desbloqueo, alarma, mensaje).
- [ ] Asegúrate de que todo el equipo conozca los procedimientos de emergencia (Borrado, Kill Switch, Restauración de fábrica).

Sobre Prey

Es una herramienta multi-plataforma para el **Rastreo y la Seguridad** de tus dispositivos remotos. Es un servicio que actualmente protege más de 8 millones de equipos y sus datos cada día, alrededor de todo el mundo.

Prey comenzó en 2009 como una pequeña compañía de tecnología que se propuso un solo objetivo: ayudar a las personas a mantener el control de sus dispositivos. 15 años más tarde, nuestro servicio ha evolucionado hasta convertirse en una confiable multi herramienta para personas y negocios. Somos expertos en localizar, proteger y administrar tus dispositivos tecnológicos para el ocio y el trabajo. Y un equipo de personas orgullosas de poder ofrecerte apoyo.

Prey para: **Personas** | **Organizaciones** | **Escuelas y Universidades**