UNIVERSIDAD DE EL SALVADOR

FACULTAD MULTIDISCIPLINARIA PARACENTRAL

DEPARTAMENTO DE INFORMÁTICA

CICLO I/2025

CATEDRA: SEGURIDAD INFORMÁTICA - SIF175

CATEDRÁTICO: ING. ELISEO EULISES ROMERO AYALA

Tarea: Implementación de una Solución MDM en una Empresa

ESTUDIANTES:

BR. KARLA BEATRIZ AGUILLAR MARTINEZ AM20072

BR. JOSEPH ALEXIS GRANADOS OCHOA GO19004

CIUDAD DE SAN VICENTE, 17 DE NOVIEMBRE 2025

Introducción

En la actualidad, el uso de dispositivos móviles dentro de las empresas se ha convertido en una necesidad indispensable para realizar tareas diarias, comunicarse con los equipos de trabajo y acceder a información corporativa desde cualquier lugar. Sin embargo, esta misma facilidad trae consigo nuevos riesgos que antes no eran tan comunes, especialmente cuando no existe un control centralizado sobre los dispositivos que se integran al entorno laboral.

En el caso de TechSolutions S.A., una empresa dedicada al desarrollo de software, el incremento del uso de smartphones, tablets y laptops ha generado desafíos importantes relacionados con la seguridad de la información. La ausencia de políticas claras para la gestión de estos dispositivos ha provocado situaciones como la pérdida de equipos con datos sensibles, accesos no autorizados a correos y aplicaciones internas, así como falta de control sobre las actualizaciones y configuraciones de seguridad.

Ante esta situación, la Dirección de TI ha solicitado la implementación de una solución de Mobile Device Management (MDM), con el propósito de administrar, proteger y monitorear todos los dispositivos móviles utilizados por los empleados. Este informe responde a dicha solicitud y se enfoca en analizar la situación actual de la empresa, investigar y comparar diferentes soluciones MDM, seleccionar una herramienta adecuada y simular su implementación.

Como estudiantes, este trabajo nos permite comprender de manera práctica la importancia de la seguridad móvil dentro del ámbito empresarial, así como la necesidad de contar con herramientas que permitan gestionar dispositivos de forma centralizada y eficiente. Además, el proyecto nos da la oportunidad de familiarizarnos con normativas internacionales como ISO 27001, que juegan un papel clave en la creación de políticas de seguridad alineadas con estándares globales.

En este informe se desarrollan los siguientes puntos principales:

- Instalación y configuración de un sistema MDM.
- Definición de políticas de seguridad aplicables a dispositivos móviles.
- Identificación de riesgos y sus respectivas mitigaciones y contramedidas.
- Relación de las políticas implementadas con los controles de la norma ISO 27001.

A través de este análisis y de la implementación simulada, se busca proponer una solución que aporte seguridad, control y eficiencia a la gestión de dispositivos dentro de TechSolutions S.A., demostrando la importancia del MDM como una herramienta fundamental para la protección de los activos digitales en las organizaciones modernas.

1. Análisis de la Situación Actual

Riesgos de Seguridad Identificados

- Pérdida o robo de dispositivos con información sensible.
- Acceso no autorizado a correos corporativos y aplicaciones internas.
- Falta de control sobre actualizaciones de seguridad.
- Instalación de apps no autorizadas (malware, apps de baja reputación).
- Riesgo por uso de redes Wi-Fi públicas o inseguras.
- Ausencia de cifrado o respaldo adecuado de los datos corporativos.

Requerimientos de TechSolutions S.A.

- Administración centralizada mediante un dashboard MDM.
- Capacidad de forzar el cifrado obligatorio en todos los dispositivos.
- Control de aplicaciones (listas blancas y listas negras).
- Capacidad de borrado remoto (total y selectivo).
- Monitoreo del estado de seguridad y cumplimiento (compliance).
- Generación de reportes y auditorías de inventario.
- Soporte multiplataforma: Android, iOS, Windows.
- Alineación con el marco de cumplimiento ISO 27001.

2. Investigación de Soluciones MDM

Se compararon tres herramientas populares en el mercado: Miradore, Microsoft Intune y Kandji.

Descripción de Soluciones

- **Miradore:** Solución MDM basada en la nube, conocida por su facilidad de uso y una interfaz muy intuitiva. Ofrece un plan gratuito robusto y planes de suscripción escalables. Ideal para PYMEs (Pequeñas y Medianas Empresas) que buscan un control efectivo sin una alta complejidad.
- **Microsoft Intune:** Parte de la suite Microsoft Endpoint Manager (MEM). Ofrece una gestión avanzada y se integra nativamente con todo el ecosistema de Microsoft 365 y Azure Active Directory. Es más complejo de implementar y más costoso, orientado a empresas grandes (Enterprise).
- **Kandji:** Una solución MDM moderna y potente, pero **especializada exclusivamente en el ecosistema Apple** (macOS, iOS, iPadOS). Ofrece una automatización avanzada, pero no cumple el requisito multiplataforma de TechSolutions.

Tabla Comparativa

Característica	Miradore	Microsoft Intune	Kandji
Multiplataforma	✓	✓	✗
Facilidad de uso	Alta	Media	Alta
Costo	Bajo/Gratis	Alto	Alto
Funciones avanzadas	Media	Alta	Alta
Integración M365	Media	Nativa	Baja
Ideal para	PYMEs	Empresas grandes	Apple Business

3. Selección de la Solución y Argumentación

Basado en el análisis comparativo y los requerimientos de TechSolutions S.A., **se selecciona la solución Miradore**.

La argumentación de esta decisión se basa en los siguientes puntos clave:

- **Compatibilidad Multiplataforma:** Cumple con el requisito esencial de gestionar dispositivos Android, iOS y Windows desde una sola consola.
- **Facilidad de Implementación:** Al ser una solución 100% en la nube y con una interfaz intuitiva, no requiere una curva de aprendizaje pronunciada para el equipo de TI de TechSolutions.
- **Costo-Beneficio:** Ofrece un plan gratuito que cubre muchos de los requisitos básicos, y su plan Premium es accesible, permitiendo a la empresa escalar sin una inversión inicial masiva.
- **Cumplimiento de Requisitos:** Miradore permite forzar el cifrado, controlar aplicaciones, realizar borrado remoto y monitorear el estado de los dispositivos, cubriendo todas las necesidades identificadas.

Aunque Microsoft Intune es más potente, su complejidad y costo son excesivos para la situación actual de TechSolutions S.A. Kandji queda descartado por no ser multiplataforma.

4. Implementación de Miradore

4.1. Instalación

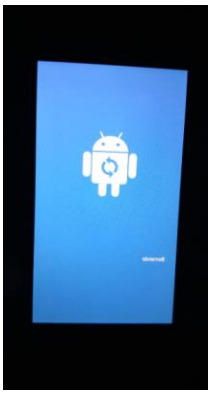
No se requiere instalación de servidores locales, ya que Miradore es una solución 100% en la nube (SaaS).

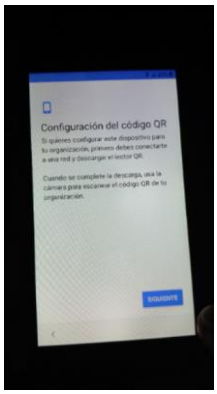
Los pasos para la puesta en marcha fueron:

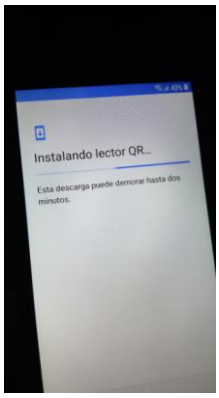
1. **Crear la cuenta:** Registrar la organización "TechSolutions S.A." en el portal de Miradore.
2. **Configurar Servicios:** Conectar los servicios de notificación (APNs para Apple y Android Enterprise) para permitir la comunicación con los dispositivos.

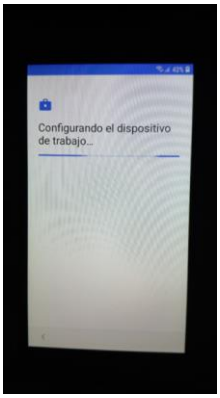
3. **Registrar Dispositivos (Enrollment):** Se simularon dos métodos de inscripción (BYOD):

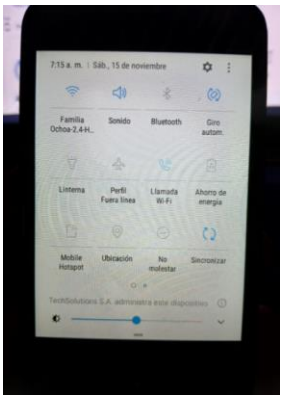
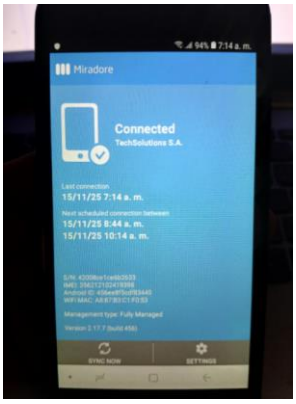
   - Inscripción mediante código QR para un registro rápido.

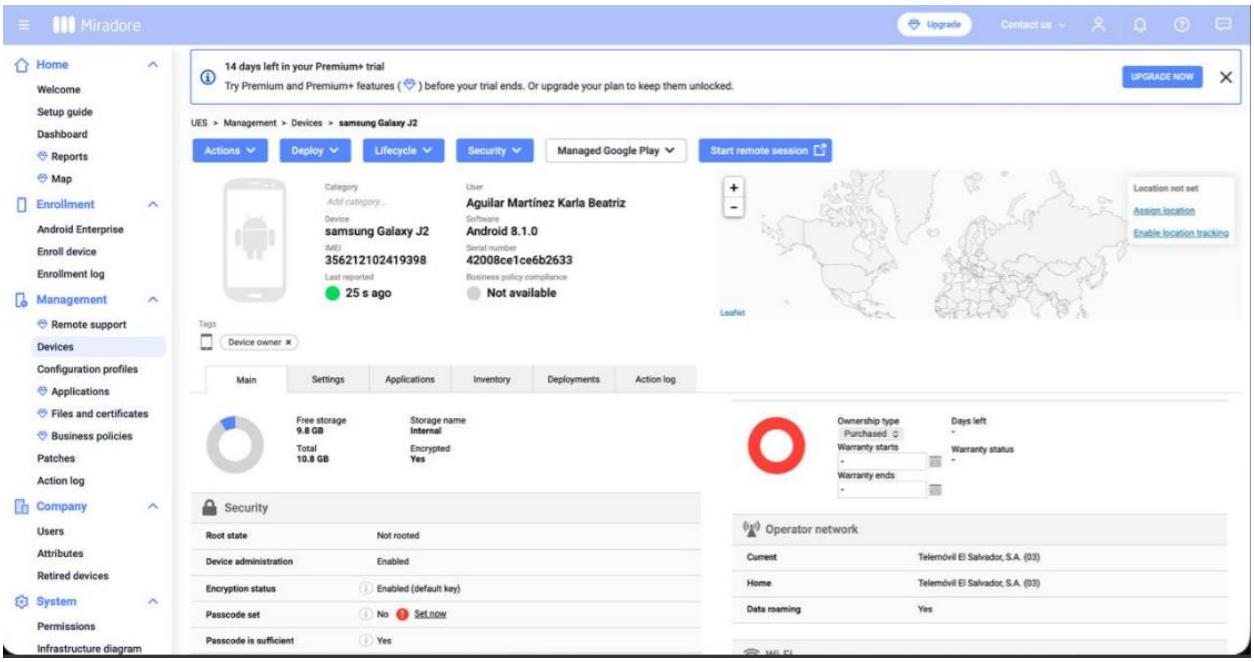








4.2. Configuración Inicial

Una vez inscritos los dispositivos, se realizaron las siguientes configuraciones en el dashboard:

- Creación de perfiles de seguridad (ej. "Perfil Básico Empleados").
- Creación de grupos de dispositivos (ej. "Ventas", "Desarrollo") para aplicar políticas diferenciadas.
- Activación del monitoreo de cumplimiento (compliance).

4.3. Políticas de Seguridad Aplicadas

Se implementó un perfil de seguridad base con las siguientes reglas:

- **Cifrado obligatorio:** Forzar el cifrado completo del disco en todos los dispositivos.
- **Política de contraseñas:** Requerir un PIN de 8 dígitos y el uso de biometría (huella o rostro).
- **Acciones remotas:** Habilitar el bloqueo, borrado selectivo (datos de empresa) y borrado total (en caso de robo).
- **Control de aplicaciones:** Creación de una lista negra con apps prohibidas (ej. redes sociales, juegos).
- **Actualizaciones:** Configurar la detección y notificación de actualizaciones de SO pendientes..

6. Mitigaciones y Contramedidas

Se definieron mitigaciones directas para los riesgos identificados, aplicando las políticas de Miradore:

Riesgo	Mitigación / Contramedida
Acceso No Autorizado	• Contraseñas robustas (PIN 6 dígitos). • Bloqueo automático tras 5 intentos fallidos. • Cierre de sesión automático por inactividad.
Robo o Pérdida	• **Borrado remoto total** (Wipe) como acción inmediata. • **Geolocalización** para rastrear el dispositivo. • **Cifrado obligatorio** (hace los datos ilegibles sin la clave).
Malware / Apps Inseguras	• **Lista negra** de aplicaciones (bloquea la instalación). • Restricción de instalación de apps de "fuentes desconocidas" (sideloading).
Redes Wi-Fi Inseguras	• **VPN obligatoria** para todo el tráfico corporativo. • Bloqueo de conexión a redes Wi-Fi abiertas no confiables.

7. Relación con ISO 27001 (Ampliado)

Nuestra implementación de MDM responde directamente a varios controles del Anexo A de la norma ISO 27001, lo cual era un requisito de TechSolutions.

Política / Función MDM	**Control ISO 27001 Relacionado**	**Descripción del Control**
Cifrado Obligatorio	**A.10.1** (Política de uso de controles criptográficos)	Asegura el uso de la criptografía para proteger la confidencialidad de la información.
Contraseñas, PIN, Biometría	**A.9** (Control de Acceso)	Asegura que el acceso a la información esté autorizado y restringido a usuarios legítimos.
Gestión Móvil (MDM)	**A.6.2** (Dispositivos móviles y teletrabajo)	Define políticas y medidas de seguridad para mitigar riesgos del uso de dispositivos móviles.
Actualizaciones Automáticas	**A.12.6** (Gestión de vulnerabilidades técnicas)	Asegura que las vulnerabilidades sean identificadas y parcheadas a tiempo.
Borrado Remoto	**A.11.2** (Seguridad de equipos fuera de las instalaciones)	Medidas para proteger equipos que operan fuera del perímetro de la organización.
Monitoreo y Reportes	**A.12.4** (Registro y monitorización de eventos)	Permite registrar y revisar eventos para detectar actividades no autorizadas.
Geolocalización	**A.11** (Seguridad física y del entorno)	Ayuda a la protección física de los activos de información.
Control de Aplicaciones	**A.16** (Gestión de incidentes de seguridad)	Previene incidentes (como malware) al controlar el software que se ejecuta.

8. Beneficios

- **Mayor seguridad:** Reducción drástica del riesgo de fuga de datos.
- **Disminución del riesgo:** Control proactivo sobre pérdida, robo y malware.
- **Mejor control y visibilidad:** Inventario centralizado de todo el hardware y software móvil.
- **Cumplimiento normativo:** Alineación directa con los controles de ISO 27001.
- **Eficiencia operativa:** Reducción del tiempo de soporte de TI para configurar dispositivos.

9. Limitaciones

- **Funciones Premium:** Algunas funciones avanzadas (como la automatización de flujos de trabajo o el filtro web) requieren el plan de pago de Miradore.
- **Dependencia de Internet:** Al ser una solución cloud, tanto el admin como los dispositivos requieren conexión para recibir políticas en tiempo real.
- **Complejidad de Intune:** Aunque no lo elegimos, reconocemos que Miradore no tiene el nivel de integración profunda con Azure AD que sí posee Intune, lo cual podría ser un factor a futuro.

16. Conclusiones

La implementación de una solución MDM es una necesidad crítica para TechSolutions S.A. dadas las vulnerabilidades identificadas en su operación actual.

La herramienta **Miradore** demostró ser la solución más adecuada para la empresa. Su balance entre **costo accesible, facilidad de implementación y un conjunto robusto de características técnicas** la convierten en la opción ideal para una PYME tecnológica.

El proyecto nos permitió validar que Miradore cumple con todos los objetivos de seguridad planteados: permite implementar políticas sólidas de cifrado y acceso, mitiga los riesgos de robo y pérdida, y centraliza la gestión de actualizaciones. Además, se integra de manera lógica con la cultura tecnológica de la empresa y proporciona una base sólida para el cumplimiento de la norma ISO 27001.

ANEXOS

Para Registrarlo

https://youtu.be/F4nvvJFC8cQ?si=ZAAX-8IEJapBc7BF

Implementaciones básicas

https://youtu.be/_6HVytKzogw?si=FDxQYoo04qef7c28

Para modificar los permisos de las aplicaciones

https://youtu.be/X5-7cBh9whs?si=3t4Ltbo_IAV8dTwn