

WHITEPAPER

**MDM: EL PILAR
ESTRATÉGICO PARA LA
GESTIÓN Y SEGURIDAD
DEL PARQUE MÓVIL
CORPORATIVO**

1. Introducción

La proliferación de dispositivos móviles en el entorno corporativo ha transformado la forma en que las organizaciones operan, acceden a la información y prestan servicios. Smartphones, tablets y otros dispositivos portátiles son hoy herramientas clave para la productividad y la agilidad del negocio, pero también introducen nuevos retos en términos de seguridad, control y cumplimiento normativo.

En este contexto, **la Gestión de Dispositivos Móviles (Mobile Device Management, MDM)** se consolida como un componente esencial dentro de la estrategia de gobierno de TI, permitiendo a las organizaciones mantener el control de su entorno móvil sin frenar la flexibilidad que demandan los modelos de trabajo actuales.

2. ¿Qué es MDM?

MDM es un conjunto de políticas, procesos y tecnologías que permiten a las organizaciones **administrar de forma centralizada los dispositivos móviles** que acceden a recursos corporativos. Su objetivo principal es proporcionar **visibilidad, control y seguridad** sobre el parque móvil, independientemente de si los dispositivos son corporativos, personales o compartidos.

Una solución MDM permite inventariar dispositivos, gestionar configuraciones, controlar aplicaciones y aplicar políticas de seguridad de forma remota y automatizada, reduciendo la dependencia de intervenciones manuales y mejorando la consistencia operativa.

La adopción de soluciones de Gestión de Dispositivos Móviles (MDM) sigue creciendo de forma acelerada. En 2025, cerca del 67 % de las organizaciones ya implementaron tecnologías MDM, impulsadas principalmente por la proliferación de políticas BYOD y la necesidad de reforzar la seguridad de los endpoints móviles. Adicionalmente, más del 80 % de las empresas permiten el uso de dispositivos personales en entornos corporativos, lo que enfatiza aún más la demanda de soluciones centralizadas de gestión y protección de dispositivos.

Fuente: LLCBuddy y Mordor Intelligence

3. El reto del parque móvil corporativo

La ausencia de una estrategia estructurada de gestión de dispositivos móviles suele derivar en una serie de problemas recurrentes, entre ellos:

- Dispositivos no inventariados o desconocidos por el área de TI.
- Configuraciones de seguridad inconsistentes entre usuarios y equipos.
- Riesgos de pérdida o fuga de información corporativa.
- Dificultades para cumplir normativas y superar auditorías.
- Incremento de la carga operativa y reactiva para los equipos de TI.

MDM responde a estos desafíos proporcionando una **visión unificada y estructurada del entorno móvil**, alineada con las políticas de seguridad y gobierno de la organización.

4. El coste de no gestionar los dispositivos móviles

No disponer de una solución de Gestión de Dispositivos Móviles (MDM) implica asumir una serie de **riesgos clave** para la organización:

- **Mayor exposición a brechas de seguridad**

Los dispositivos móviles corporativos concentran acceso a correo, aplicaciones internas, credenciales y datos sensibles. Sin gestión centralizada, un dispositivo perdido, robado o comprometido puede convertirse en un punto de entrada para atacantes.

- **Pérdida de control sobre la información corporativa**

La ausencia de cifrado, control de accesos o borrado remoto dificulta la protección de la información y aumenta el riesgo de fuga de datos.

- **Dificultad para cumplir normativas y auditorías**

La falta de visibilidad y trazabilidad sobre los dispositivos que acceden a datos corporativos o personales puede derivar en incumplimientos normativos y sanciones económicas.

- **Incremento del riesgo operativo**

Sin MDM, la gestión manual de dispositivos aumenta la carga del equipo de TI, reduce la capacidad de respuesta ante incidentes y limita la estandarización de políticas de seguridad.

5. Beneficios clave de implantar una solución MDM

- **Visibilidad y control centralizado**

MDM ofrece un inventario actualizado y en tiempo real de los dispositivos móviles, permitiendo conocer su estado, nivel de cumplimiento y relación con usuarios o servicios corporativos. Esta visibilidad es fundamental para la toma de decisiones y la gestión del riesgo.

- **Seguridad de la información**

Mediante la aplicación de políticas de seguridad, cifrado, control de accesos y capacidades como el borrado remoto, MDM reduce significativamente el riesgo de exposición de datos corporativos, incluso en escenarios de pérdida, robo o uso indebido del dispositivo.

- **Cumplimiento normativo**

La capacidad de auditar configuraciones, accesos y estados de cumplimiento facilita la alineación con normativas internas y externas, así como la preparación ante auditorías de seguridad, privacidad o gobierno de TI.

- **Eficiencia operativa**

La automatización de tareas como el enrolamiento de dispositivos, la configuración inicial o el despliegue de aplicaciones permite reducir errores manuales, acelerar la incorporación de nuevos equipos y liberar recursos del área de TI para actividades de mayor valor estratégico.

- **Soporte a modelos de trabajo flexibles**

MDM habilita escenarios como BYOD, COPE o trabajo híbrido, equilibrando la experiencia del usuario con las necesidades de control y seguridad de la organización, sin comprometer la privacidad ni la productividad.

El mercado global de Mobile Device Management alcanzará aproximadamente USD 26 mil millones para 2031, con una tasa de crecimiento anual compuesta de casi 19 %, lo que refleja la creciente importancia de la gestión de dispositivos móviles dentro de las estrategias corporativas de TI y seguridad.

Fuente: Mordor Intelligence

6. MDM como parte de la estrategia global de TI

La gestión de dispositivos móviles no debe abordarse como un elemento aislado. Integrar MDM dentro de una estrategia global de **gestión de activos, seguridad y gobierno de TI** permite que los dispositivos móviles formen parte del inventario corporativo, se relacionen con usuarios, servicios y riesgos, y contribuyan a una visión holística del entorno tecnológico.

Este enfoque integrado facilita una gestión más madura, coherente y alineada con los objetivos del negocio.

Integración con la gestión de activos (ITAM)

Los dispositivos móviles son activos tecnológicos con impacto directo en riesgo y costes. Integrarlos en la estrategia de IT Asset Management (ITAM) permite:

- Incorporarlos al inventario corporativo único
- Asociarlos a usuarios y centros de coste
- Gestionar su ciclo de vida completo
- Mejorar la trazabilidad y el control presupuestario

Sin esta integración, el parque móvil queda fragmentado y fuera del marco global de control.

Alineación con la ciberseguridad

Los dispositivos móviles amplían la superficie de ataque de la organización. Integrar MDM en la arquitectura de seguridad permite:

- Aplicar políticas homogéneas de acceso y configuración
- Reducir vulnerabilidades derivadas de configuraciones individuales
- Actuar con rapidez ante incidentes mediante acciones remotas

De este modo, MDM refuerza la postura de seguridad y contribuye a una gestión más coherente del riesgo.

Gobierno y visión unificada

Cuando los dispositivos móviles forman parte de la misma estructura de gestión que el resto de activos TI, la organización obtiene una visión consolidada del ecosistema tecnológico. Esto facilita la auditoría, la toma de decisiones basada en datos y la alineación entre tecnología y estrategia de negocio.

En este enfoque, MDM deja de ser una herramienta operativa y se convierte en un habilitador estratégico de control, seguridad y madurez digital.

7. Conclusión

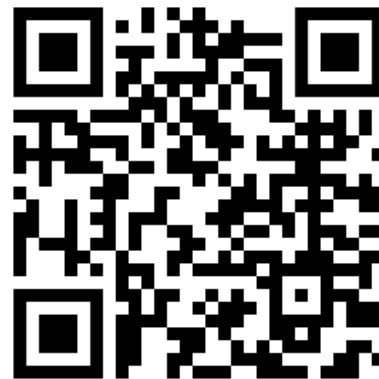
La **Gestión de Dispositivos Móviles (MDM)** es un componente esencial de la estrategia moderna de gestión de activos de TI y seguridad. Integrar MDM permite a las organizaciones:

- Aumentar la visibilidad de sus activos móviles.
- Automatizar procesos, reduciendo errores humanos.
- Fortalecer seguridad y cumplimiento regulatorio.
- Gestionar políticas y aplicaciones desde un único punto.

Como resultado, las organizaciones logran una administración proactiva, eficiente y segura de todos los dispositivos móviles dentro de su entorno TI.

Existen plataformas que integran la gestión de dispositivos móviles dentro de un enfoque más amplio de gestión de activos y seguridad, permitiendo consolidar la información del parque móvil junto con el resto del ecosistema TI. Soluciones como **Proactivanet** destacan por su capacidad de integración con ITAM, CMDB y gestión de riesgos, aportando una visión unificada y orientada a la toma de decisiones.

Toma el control
de tu entorno
móvil hoy mismo



proactivanet.com



PinkVERIFY es una marca
registrada por Pink Elephant.

