SOPHOS

# Guía para la adquisición de soluciones de gestión de dispositivos móviles

Los departamentos informáticos son como el aceite del motor que hace funcionar una empresa. El uso de dispositivos personales en el trabajo (también conocido como BYOD, por sus siglas es inglés) puede aportar grandes facilidades a los usuarios. Pero las comodidades siempre van en detrimento de la seguridad. ¿Cómo se puede conseguir un equilibrio entre la seguridad y la productividad? En esta guía le explicamos los factores a tener en cuenta para encontrar la solución de gestión de dispositivos móviles que mejor se ajuste a sus necesidades.

## ¿Se atreve a dar permiso a los usuarios?

Las soluciones de gestión de dispositivos móviles permiten a los departamentos informáticos administrarlos y vigilarlos de forma centralizada, así como ofrecer la asistencia necesaria. Este tipo de dispositivos pueden incluir teléfonos inteligentes y tabletas de diferentes fabricantes y desarrolladores de sistemas operativos. Al utilizar una solución de gestión para controlar y proteger los datos y las opciones configuradas en los dispositivos móviles de los usuarios, es posible reducir los costes de soporte y los riesgos empresariales del uso de dispositivos personales en el trabajo (BYOD).

Con la solución adecuada, podrá permitir que los usuarios utilicen sus propios dispositivos sin aumentar los riesgos de que se produzcan fugas de datos ni la carga de trabajo del departamento informático.

## Riesgos y ventajas del uso de dispositivos personales en entornos laborales

Tanto las empresas como los usuarios están empezando a darse cuenta de las ventajas de utilizar dispositivos personales en el trabajo.
Cuando los empleados pueden trabajar con sus propios dispositivos, la productividad aumenta. La comodidad que se deriva de trabajar con un dispositivo que el empleado conoce y prefiere, mejora la productividad tanto dentro como fuera de la oficina.

Las políticas para el uso de dispositivos personales en el trabajo también pueden resultar beneficiosas para la contratación de personal. Los empleados quieren utilizar sus propios teléfonos inteligentes y tabletas, y no verse limitados a los proporcionados por la empresa ni tener que aprender a utilizar o cargar con otro dispositivo. Como consecuencia, las empresas que fomentan el uso de dispositivos personales en el trabajo atraen a candidatos que dominan las tecnologías.

Pero como con cualquier otra tendencia tecnológica, existen ciertos problemas que pueden anteponerse a las ventajas. El uso de dispositivos personales en el trabajo presenta dos retos fundamentales: la protección de los datos y la gestión.

**Protección de los datos:** cuando los datos se transfieren entre dispositivos que pueden perderse o extraviarse fácilmente y a través de redes públicas, la protección de los datos se convierte en una preocupación primordial. Es difícil saber a qué datos acceden los usuarios, quiénes los utilizan y a través de qué canales.

**Gestión:** el personal informático necesita métodos para controlar los dispositivos que se utilizan para acceder a los datos de la empresa, independientemente de a quién pertenezcan. Y si los empleados utilizan dispositivos personales, es necesario gestionar varios sistemas operativos y plataformas diferentes, lo que puede consumir recursos informáticos de forma significativa. Gestionarlos de forma individual no es una posibilidad viable.

# Qué deben ofrecer los proveedores de soluciones de gestión de dispositivos móviles

Está claro que es necesario controlar y proteger los dispositivos móviles. Lo difícil es elegir el proveedor adecuado. Las funciones de control y seguridad incluidas en las soluciones de gestión vienen determinadas por los permisos establecidos por los proveedores de los sistemas operativos móviles. De hecho, no es aconsejable fiarse de los proveedores de soluciones de gestión de dispositivos móviles que afirman poder superar las limitaciones de determinados sistemas operativos. Probablemente no sea cierto o solo sea posible en el caso de dispositivos liberados (iOS) o con derechos de administración de la raíz (Android). Entonces ¿qué requisitos deben cumplir los proveedores de soluciones de gestión de dispositivos móviles? Es aconsejable tener en cuenta los factores siguientes.

## Modelo flexible de distribución

El proveedor debería ofrecer diferentes modelos de distribución, incluidas implementaciones en las instalaciones en el caso de infraestructuras de gran tamaño. A pesar de exigir inversiones iniciales de capital y gastos operativos, las implementaciones en las instalaciones se integran totalmente en las infraestructuras informáticas de las empresas, lo que permite conseguir un control más preciso. Los despliegues en las instalaciones utilizan servidores proxy EAS, Active Directory y conexiones LDAP, y ofrecen opciones para la creación de copias de seguridad.

Aunque es el modelo más habitual, no es la única opción. Algunos proveedores ofrecen el software como servicio, una solución ideal para aquellas empresas que necesitan poner el sistema en marcha rápidamente. No es necesario realizar instalaciones in situ ni tareas de mantenimiento, por lo que ahorran tiempo y gastos operativos. Además, al no modificar el entorno informático local ni tener que invertir en hardware nuevo, no acarrean gastos de capital.

El software como servicio (SaaS) suele considerarse como una opción solo en empresas grandes, pero también puede resultar adecuado en empresas más pequeñas y grupos específicos de usuarios. De hecho, las soluciones de gestión de dispositivos móviles en la nube ponen este tipo de funciones al alcance de empresas más pequeñas y grupos de usuarios que requieren un control central pero no cuentan con los recursos necesarios para implementar y gestionar distribuciones en las instalaciones. Las empresas deben buscar soluciones que ofrezcan la escalabilidad necesaria pero sin un tamaño excesivo que aumente la complejidad.

## Compatibilidad con dispositivos iPhone, iPad, Android, BlackBerry y Windows Mobile

No todas las soluciones de gestión de dispositivos móviles son compatibles con todas las plataformas y sistemas operativos. Por eso, es importante tener en cuenta los dispositivos que se necesitan gestionar ahora y en el futuro. Si elige la solución equivocada, podría terminar gestionando grupos de usuarios de forma independiente. Los administradores tendrán que controlar y proteger de forma manual los datos y la configuración de los dispositivos móviles que no sean compatibles con la solución, reduciendo la rentabilidad de la inversión y generando riesgos.

## Soluciones ligeras frente a soluciones de contenedores pesados

Hoy en día, existen dos métodos para proteger los dispositivos móviles y los datos. Las soluciones ligeras protegen los dispositivos móviles mediante la combinación de las funciones de seguridad disponibles en el sistema operativo y las herramientas proporcionadas por el proveedor de la solución. Las soluciones pesadas utilizan una aplicación contenedor que almacena todos los datos y ofrece a los usuarios funciones de correo electrónico, calendario y edición de documentos.

Ambos métodos presentan sus propias ventajas y desventajas. Las soluciones pesadas ofrecen un control total de las funciones de la aplicación (por ejemplo, el cifrado) y permiten separar los datos personales de los corporativos. Pero dicho control tiene un precio. Las restricciones en la facilidad de uso de los dispositivos y el impacto en el rendimiento y la batería de los mismos pueden no ser del agrado de los empleados, que además deben aprender a utilizar la nueva interfaz. Aunque este método permite realizar fácilmente borrados selectivos, los datos del resto de las aplicaciones no están protegidos y no es posible controlar las demás opciones de configuración de los dispositivos.

Las soluciones ligeras permiten seguir utilizando los dispositivos de la forma habitual, por lo que no exigen formación adicional y resultan más cómodas para los usuarios. Aunque los administradores pueden controlar y configurar una mayor cantidad de funciones de los dispositivos (como la cámara, la tienda de aplicaciones, la configuración de la VPN, etc.), dichas funciones vienen determinadas por los permisos establecidos en el sistema operativo móvil. Sin embargo, con las soluciones ligeras, los administradores pueden gestionar también el inventario de dispositivos, comprobar el cumplimiento de las normativas y distribuir software, tareas fundamentales en las políticas de uso de dispositivos personales en el trabajo.

## Soporte global 24 horas, todos los días de la semana

El soporte técnico puede ser necesario a cualquier hora del día. Los usuarios de dispositivos móviles trabajan las 24 horas del día y el soporte técnico del proveedor de la solución elegida debería estar disponible en igual medida. Busque una solución con asistencia ininterrumpida en el idioma local, proporcionada por técnicos cualificados y tiempos de espera reducidos (cuando no nulos). Elija una solución cuyo servicio haya sido auditado de forma independiente y que cuente con la aprobación SCP. Los estándares SCP evalúan la efectividad de la atención al cliente y el soporte técnico según un conjunto de normas de rendimiento muy estrictas, y se consideran prácticas recomendadas en el sector.

## Seguridad completa para los trabajadores que se desplazan

Las soluciones de gestión de dispositivos móviles permiten protegerlos y administrarlos de forma centralizada, pero las estrategias de protección de este tipo de dispositivos están formadas por muchos otros componentes. Los teléfonos inteligentes y las tabletas no son los únicos dispositivos móviles. Preste atención a cualquier otro método utilizado por los usuarios para sacar datos de la oficina como, por ejemplo, ordenadores portátiles, memorias USB o incluso soluciones de colaboración como sistemas de almacenamiento en la nube.

Para evitar fugas de datos, es necesario asegurarse de que la información delicada no se almacena como texto sin formato y de que no existen aplicaciones instaladas que abran las puertas a vulnerabilidades en el dispositivo. Además, es necesario cifrar los datos en todos los lugares y proteger los dispositivos contra programas maliciosos. Hoy en día, las empresas son conscientes de que las soluciones para dispositivos móviles deben integrarse con el resto.

Lo ideal es encontrar un proveedor que ofrezca una suite integrada de soluciones que satisfagan todas estas necesidades para simplificar las tareas de administración y reducir el coste total. Por ejemplo, puede utilizar el almacén empresarial de aplicaciones de la solución de gestión de dispositivos móviles para administrar las aplicaciones y para obligar a los usuarios a instalar software antivirus.

# Funciones de las soluciones de gestión de dispositivos móviles

La mayoría de soluciones de gestión de dispositivos móviles comparten una serie de funciones comunes. Sin embargo, la metodología y la facilidad de uso de cada proveedor suelen ser diferentes. Al evaluar las distintas soluciones, tenga en cuenta las funciones y capacidades siguientes.

## Protección de los datos corporativos

El principal objetivo de las soluciones de gestión de dispositivos móviles es proteger los datos de la empresa. Para ello, obligan a cumplir las normativas mediante políticas de seguridad.

Para poder acceder a los datos, los dispositivos móviles deben estar registrados en la solución. Cuando un dispositivo registrado se conecta, la solución lo compara con un conjunto de reglas empresariales (por ejemplo, de detección de dispositivos desbloqueados, configuración de contraseñas o aplicaciones prohibidas). Los dispositivos que cumplen las políticas de seguridad obtienen permiso para acceder a los datos corporativos.

Las técnicas de atenuación de riesgos limitan o deniegan el acceso a los dispositivos que no las cumplen. Por ejemplo, los usuarios de dispositivos que no cumplen las normativas pueden dejar de tener acceso a todos los recursos de red, recibir una notificación por correo electrónico o tener un acceso limitado a los datos. Algunos proveedores ofrecen también portales de autoservicio en los que los usuarios pueden iniciar sesión para comprobar el estado del cumplimiento o si los dispositivos cumplen las normativas (en el caso de los sistemas operativos que ofrecen esta función como, por ejemplo, iOS y Android).

Muchos dispositivos móviles cuentan con funciones de seguridad incorporadas como, por ejemplo, restricciones de las funciones (cámaras) y cifrado (en el caso de iOS y Android 4). Algunas soluciones ligeras permiten activar dichas funciones para proteger mejor los datos.

La posibilidad de borrar de forma remota los dispositivos extraviados es fundamental y está incluida en cualquier solución de gestión de dispositivos móviles. Gracias a ella, los administradores pueden eliminar datos corporativos almacenados en dispositivos que pudieran haber caído en manos de usuarios no autorizados. Busque soluciones que ofrezcan también la posibilidad de localizar y bloquear los dispositivos desde la consola de administración web para poder encontrarlos e impedir su uso hasta que vuelvan a estar en posesión de sus dueños. Lo ideal es que los usuarios puedan localizar, bloquear y borrar sus propios dispositivos a través de un portal de autoservicio.

## Gestión de aplicaciones

Las soluciones de gestión de dispositivos móviles también pueden ayudar a las empresas a gestionar las aplicaciones presentes en dichos dispositivos de manera que los usuarios dispongan de las herramientas necesarias para trabajar de forma eficaz y sin poner en peligro los datos de la empresa.

La gestión de aplicaciones móviles se consigue principalmente a través de un almacén empresarial de aplicaciones que permite definir los programas que los usuarios pueden instalar o deberían tener instalados en sus dispositivos. El almacén puede incluir tanto aplicaciones a disposición del público general como desarrolladas de forma interna.

Lo ideal es que las soluciones de gestión de dispositivos móviles sean compatibles con las aplicaciones administradas de iOS disponibles desde el lanzamiento de iOS 5. De esta forma, las empresas pueden distribuir aplicaciones a los usuarios, e instalarlas o eliminarlas de forma sencilla junto con todos los datos relacionados y de forma remota desde la consola web.

Además, el almacén de aplicaciones debe permitir crear una lista de aplicaciones prohibidas que no deban instalarse en los dispositivos de los usuarios, por ejemplo, aplicaciones que puedan poner en peligro los datos corporativos o la productividad.

## Simplificación de la administración informática

Los departamentos informáticos ya están sobrecargados con tareas de aprovisionamiento, mantenimiento y soporte. El uso de dispositivos personales en el entorno laboral no debe aumentar la productividad de los usuarios a costa de la del departamento informático. La simplificación de la administración informática es fundamental y una de las principales diferencias a tener en cuenta a la hora de elegir una solución de gestión de dispositivos móviles.

Este tipo de soluciones pueden simplificar las tareas de administración de varias formas. Gracias a la administración y gestión remotas, los departamentos informáticos pueden ocuparse del mantenimiento de los dispositivos móviles en cualquier momento y en cualquier lugar para que los usuarios no tengan que acudir al servicio de asistencia. La configuración inicial también puede llevarse a cabo de forma remota. Además, debe ser posible asignar dispositivos de forma automática a los grupos existentes en el directorio de usuarios y aplicar las políticas correspondientes cuando se registran a través del portal de autoservicio.

La vigilancia y el control centralizados de todos los dispositivos registrados es uno de los distintivos de las soluciones de gestión de dispositivos móviles, pero la facilidad de uso y la precisión de las funciones varían de una solución a otra. Busque una solución que permita administrar todos los teléfonos inteligentes y tabletas compatibles desde una misma consola, independientemente del sistema operativo, el proveedor de servicios, la red o la ubicación del dispositivo.

Si también utiliza dispositivos BlackBerry, es aconsejable añadirlos a la solución para disponer de un inventario completo en un mismo lugar. También debe ser posible hacer un seguimiento y crear informes acerca de todos los dispositivos registrados, así como ver información detallada sobre la configuración, el número de serie o modelo, el hardware o las aplicaciones instaladas en cada uno de ellos. Desde el panel de control se pueden ver rápidamente los dispositivos registrados y si cumplen las políticas. Las funciones de auditoría muestran los cambios realizados en los dispositivos y el estado del cumplimiento.

Los informes gráficos deben ofrecer un resumen de los datos más importantes. Por ejemplo, deben mostrar el porcentaje de dispositivos que cumplen las políticas frente a los que no, el número de dispositivos administrados y no administrados, los dispositivos propiedad de la empresa o de los empleados, etc., en lugar de tener que utilizar menús diferentes para encontrar dicha información.

Por último, la interfaz administrativa debe ser práctica y fácil de usar. Tenga en cuenta cuántas veces necesita hacer clic para realizar funciones básicas como suprimir un dispositivo, ver la distribución de sistemas operativos o definir las versiones compatibles con una aplicación. Para completar dichas tareas, no deberían ser necesarios más de uno o dos clics.

## Portal de autoservicio para usuarios

Los portales de autoservicio para usuarios reducen la carga de trabajo de los departamentos informáticos y otorgan poderes a los propietarios de los dispositivos. Los usuarios pueden ocuparse personalmente de tareas rutinarias como el registro de sus propios dispositivos o la aceptación de las políticas de uso definidas. Una vez registrados, las soluciones de gestión de dispositivos móviles pueden asignar de forma automática perfiles y políticas a los usuarios y grupos según el grupo del directorio al que pertenezcan, por ejemplo, Active Directory. De esta forma, se elimina la necesidad de que el departamento informático tenga que participar en el proceso de configuración del dispositivo.

Como mencionamos anteriormente, los portales de autoservicio amplían las funciones de protección de los datos a los usuarios, que pueden localizar o bloquear sus dispositivos de forma remota, eliminar la información que contienen o restablecer la contraseña sin necesidad de ponerse en contacto con el centro de asistencia técnica, lo que ahorra tiempo al departamento y mejora la seguridad general de la empresa.

Los propietarios suelen ser los primeros en percatarse del robo o el extravío de sus dispositivos. En el tiempo que tarda un usuario en darse cuenta de que ha extraviado un dispositivo y llamar al servicio de asistencia para que borre de forma remota los datos almacenados, la información delicada puede haber caído ya en las manos equivocadas. Al ofrecer a los usuarios la posibilidad de localizar, bloquear o borrar sus propios dispositivos, se ahorra un tiempo muy valioso.

Por último, los portales de autoservicio ofrecen información a los usuarios sobre el estado de los dispositivos, por ejemplo, en relación con el cumplimiento o por qué han dejado de recibir mensajes de correo electrónico, lo que reduce el número de llamadas al servicio de asistencia por problemas de normativas o bloqueos del acceso al correo.

# Resumen

Las soluciones de gestión de dispositivos móviles deben permitir administrar todos los dispositivos presentes en la red. Además, deben ser fáciles de usar. Siga estas pautas para encontrar la solución más adecuada. Pruebe soluciones diferentes y decida cuál le resulta más fácil de usar. El gráfico siguiente puede ayudarle a comparar las diferentes funciones para encontrar el proveedor que mejor se ajuste a las necesidades de su empresa.

**Qué deben ofrecer los proveedores de soluciones de gestión de dispositivos móviles**

| Factor | Opciones que debe proporcionar |
|---|---|
| Opciones de distribución | ☐ Implementación en las instalaciones<br>☐ Software como servicio |
| Plataformas | ☐ iPhone y iPad<br>☐ Android<br>☐ BlackBerry<br>☐ Windows Mobile |
| Enfoque | ☐ Ligero<br>☐ Pesado |
| Soporte técnico | ☐ Soporte global ininterrumpido<br>☐ Técnicos que hablan el idioma local<br>☐ Auditorías de calidad superadas |
| Integridad del catálogo de seguridad móvil | ☐ Solución de cifrado de datos<br>☐ Solución contra programas maliciosos para móviles<br>☐ Protección de portátiles<br>☐ Protección de medios extraíbles<br>☐ Cifrado de archivos para sistemas de almacenamiento en la nube<br>☐ Prevención de fugas de datos<br>☐ Planteamiento integrado de la seguridad |

## Funciones de las soluciones de gestión de dispositivos móviles

| Función | Funciones que debe proporcionar |
|---|---|
| Protección de datos | ☐ Comprueba que los dispositivos cumplen las políticas de seguridad corporativas<br>☐ Ofrece diferentes técnicas de atenuación de riesgos para los dispositivos móviles que no cumplen las políticas, por ejemplo, bloqueo de redes VPN, bloqueo del correo electrónico, notificaciones a los usuarios, etc.<br>☐ El portal de autoservicio ofrece información sobre el cumplimiento de las normativas a los usuarios<br>☐ El estado del cumplimiento se indica en el propio dispositivo<br>☐ Los administradores pueden activar funciones de seguridad propias de la plataforma<br>☐ Los dispositivos extraviados se pueden localizar, bloquear o borrar desde la consola de administración o a través del portal de autoservicio para usuarios |
| Administración de aplicaciones | ☐ Almacén empresarial de aplicaciones para aplicaciones tanto de consumo como internas<br>☐ Lista de aplicaciones prohibidas<br>☐ Implementación y eliminación remotas de aplicaciones |
| Simplificación de la administración informática | ☐ Administración y gestión remotas<br>☐ Administración centralizada de todos los dispositivos<br>☐ Estado del cumplimiento a través del panel de control<br>☐ Informes gráficos detallados<br>☐ Interfaz administrativa fácil de usar |
| Portal de autoservicio para usuarios | ☐ Los usuarios registran sus propios dispositivos<br>☐ Los usuarios pueden localizar, bloquear y borrar sus propios dispositivos<br>☐ Los usuarios pueden restablecer sus contraseñas<br>☐ Los usuarios pueden ver el estado del cumplimiento |




Ventas en el Reino Unido:
Teléfono: +44 8447 671131
Correo electrónico: sales@sophos.com

Ventas en Norteamérica:
Línea gratuita: +1 866 866 2802
Correo electrónico: nasales@sophos.com

Ventas en España:
Teléfono: (+34) 913 756 756
Correo electrónico: comercialES@sophos.com

Boston (EE. UU.) | Oxford (Reino Unido)




Guías de compra de Sophos 09.12v1.dNA