



La guía sobre UEM para el CIO

Diez factores clave de decisión

Cómo usar esta guía

Esta guía está basada en estudios y aportaciones reales de empresas de la lista Fortune 500, así como en las reflexiones de analistas y expertos. Su objetivo es ayudar a los CIO a replantear su estrategia para una nueva era de la movilidad.

La movilidad está alcanzando un punto de inflexión en las empresas. Hasta hace poco, muchas organizaciones lo veían como una iniciativa aislada mediante la que el departamento de TI podía habilitar el correo electrónico en los dispositivos móviles. En la actualidad, la mayoría lo ve como una iniciativa estratégica para movilizar las aplicaciones empresariales que puede influir en diferentes resultados. Este cambio de perspectiva ha propiciado que las empresas inteligentes estén dejando atrás las soluciones puntuales para la gestión de dispositivos móviles y busquen una plataforma unificada, segura y con garantía de futuro para gestionar las aplicaciones móviles.

Las aplicaciones empresariales —muchas de ellas basadas en la nube— son ahora el foco de atención de la productividad móvil porque los trabajadores móviles necesitan acceso constante a la información, desde cualquier lugar y dispositivo. Los perímetros de seguridad tradicionales están cambiando a marchas forzadas dado que cada vez se comparten más documentos sensibles fuera de los límites de la empresa.

Ahora los datos pueden transferirse y residir en dispositivos móviles; en ordenadores portátiles y de sobremesa; o en nubes públicas, privadas, e incluso personales.

Estos cambios representan una oportunidad clara para impulsar la productividad y la satisfacción en el trabajo, mejorar la interacción con los clientes y aumentar la eficacia organizativa. Pero para poder aprovechar estas ventajas, las empresas tienen que estar preparadas para superar los retos asociados a la tecnología móvil.

Los acrónimos cambian con rapidez en el ámbito de la tecnología móvil: no hace mucho la atención se centraba en las soluciones MDM (gestión de dispositivos móviles); después llegaron las soluciones EMM (gestión de la movilidad empresarial); y actualmente las empresas buscan soluciones UEM (gestión unificada de terminales), que abarcan la gestión, la seguridad y la identidad en dispositivos móviles, así como en ordenadores portátiles, ordenadores de sobremesa y otros terminales. A medida que las organizaciones se preparan para afrontar un mayor número de requisitos de los usuarios finales y la tecnología IoT, es fundamental que puedan garantizar la visibilidad y el control de todos los terminales de su entorno desde una plataforma unificada.

Las empresas que desarrollen una estrategia de movilidad e implementen la solución adecuada pueden lograr importantes beneficios, al igual que aquellas que decidan cambiar de estrategia para adaptarse al nuevo panorama de la movilidad empresarial. Utilizar la solución adecuada mejora la productividad, la seguridad y la privacidad, al mismo tiempo que facilita a los administradores de TI la gestión de un número creciente de funciones, aplicaciones móviles, sistemas operativos y tipos de dispositivos.

Aunque este documento aborda muchos de los factores clave que deben tenerse en cuenta a la hora

de crear o cambiar su estrategia de movilidad, hay muchos otros que dependen de las características específicas de su organización. Si bien el proceso puede ser largo y, en ocasiones, una cuestión de estrategia, preparar las respuestas antes de elegir una solución nueva ahorra tiempo, reduce los costes y evita dolores de cabeza a lo largo del proceso.

La adopción de la movilidad es un recorrido y para empezar es útil saber en qué etapa de la curva de madurez de la movilidad está su organización. Esto permitirá garantizar que la solución que elija satisfaga sus necesidades ahora y en el futuro.

Por qué necesita una estrategia de movilidad

Una estrategia de movilidad es un plan que refleja y describe los principales requisitos y áreas funcionales de su empresa en relación con varios aspectos asociados a la movilidad. La finalidad es recopilar información de todas las partes interesadas para definir una estrategia que respalde los objetivos de la empresa sin comprometer la seguridad ni la privacidad. Sin una estrategia de movilidad, tomar la decisión adecuada sobre una solución de largo plazo puede ser casi imposible. A continuación, se incluyen algunas de las preguntas fundamentales que se hacen las empresas, en función de su etapa en la curva de madurez de la movilidad:

1. ¿Qué tipos de aplicaciones móviles necesitamos para aprovechar la movilidad y mejorar la productividad en nuestra organización?
2. ¿Podemos estar tranquilos en cuanto a la seguridad de nuestros datos corporativos, en un entorno cada vez más orientado a la nube y la movilidad?
3. ¿Podemos predecir con exactitud los gastos de TI asociados a la movilidad? ¿Disponemos de una solución que satisfaga nuestras necesidades ahora y en el futuro?

4. ¿Podemos estar tranquilos no solo en cuanto a la seguridad de nuestros datos corporativos, sino también de las credenciales de aplicaciones y las configuraciones de usuario que podrían estar almacenadas en dispositivos móviles?

5. ¿Cómo ayudamos a propietarios de aplicaciones, desarrolladores y personal de TI para que colaboren entre sí y adopten directrices de seguridad comunes?

6. ¿Cómo garantizamos que diferentes equipos de desarrollo puedan aplicar las mismas funciones de seguridad a todo tipo de aplicaciones?

7. ¿Cómo vamos a abordar el aumento constante de usuarios, dispositivos y datos a medida que la movilidad se extienda en la empresa?

8. ¿Podemos satisfacer fácilmente nuestros requisitos de seguridad o de conformidad?

9. ¿Qué ventajas podemos obtener si reducimos el número de proveedores y soluciones en nuestro entorno de movilidad?

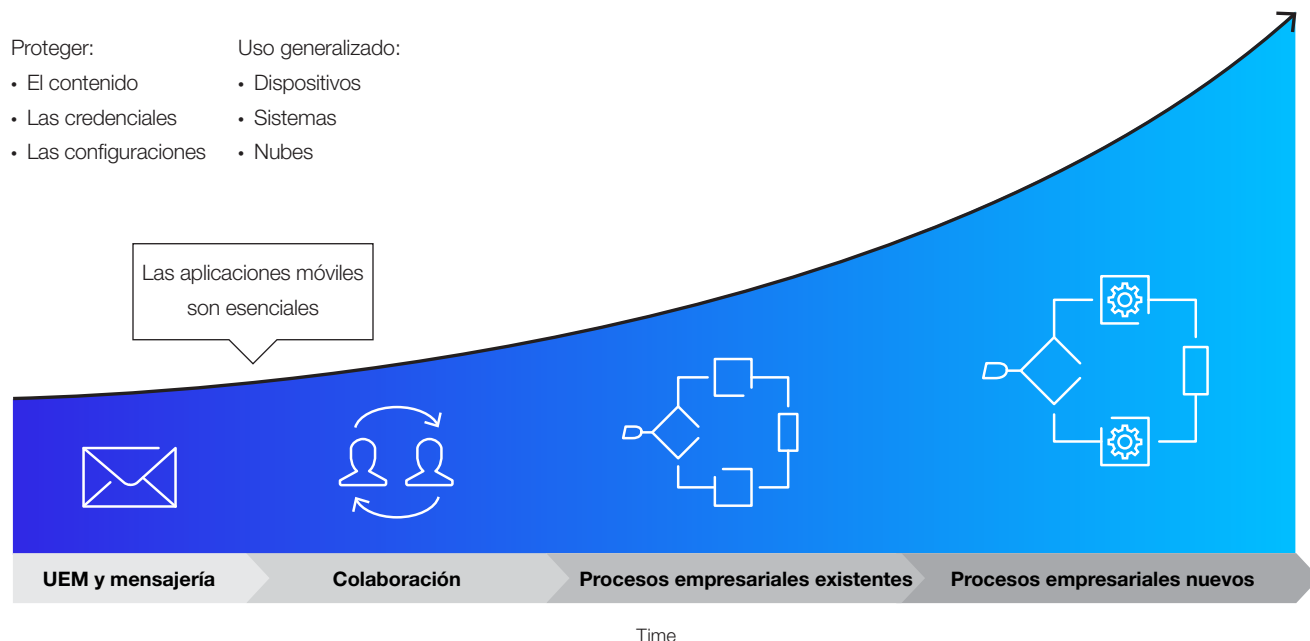
10. ¿Estamos abordando eficazmente los problemas asociados a la confianza y la privacidad de nuestros empleados?

La curva de madurez de la movilidad

La curva de madurez de la movilidad tiene cuatro etapas. A medida que su empresa avance por la curva, el enfoque de la movilidad será progresivamente más transformador al adoptar nuevas estrategias, incorporar nuevas herramientas, modificar los procesos empresariales existentes y, por último, crear modelos de negocio completamente nuevos.

Por otra parte, como cada vez se movilizarán más aplicaciones corporativas, aumentarán las exigencias de seguridad.

Vista de la curva de madurez de la movilidad



Movilidad básica

La gestión básica de dispositivos y el correo electrónico son las primeras inversiones que realizan las organizaciones en tecnología móvil. Esto puede aportar mejoras rápidas de la productividad con una inversión limitada, en especial si va asociado a una iniciativa de uso de dispositivos personales en el lugar de trabajo (BYOD). Sin embargo, gestionar una amplia flota de dispositivos móviles puede exponer su organización a nuevas amenazas.

Retos de esta etapa

- Empezar a proteger los datos corporativos básicos (el correo electrónico y los documentos adjuntos) en los dispositivos móviles.
- Saber qué uso se hace de los dispositivos.
- Desarrollar conocimiento técnicos en la empresa.

Señales de que su empresa se encuentra en esta etapa

- Hace relativamente poco que han implementado una solución de gestión de dispositivos. La inversión en movilidad ha sido mínima hasta el momento. Se trata de una proyecto local, más que de una iniciativa para toda la empresa.
- El desarrollo de aplicaciones móviles todavía no está entre sus planes.
- Saben que la movilidad es esencial de cara a sus objetivos empresariales, pero no tienen claro por dónde empezar.

Colaboración móvil

Una vez que los usuarios de una organización empiezan a recibir correos electrónicos y documentos adjuntos en sus dispositivos móviles, aspiran de forma natural a realizar más tareas y aprovechar todas las ventajas de la movilidad. Por tanto, si su empresa ya ha empezado a adoptar la movilidad, el paso siguiente es facilitar la colaboración de los empleados y optimizar el flujo de trabajo. La mayoría de las plataformas MDM carecen de las herramientas necesarias para proteger las aplicaciones móviles y los datos de la empresa.

Retos de esta etapa

- Movilizar las aplicaciones básicas de Microsoft® que los empleados utilizan: Exchange, Office 365, SharePoint™, OneDrive for Business, Skype for Business, Dynamics CRM, etc.
- Implementar flujos de trabajo de documentos con funciones de seguridad y control.

- Garantizar una experiencia óptima a los usuarios móviles.
- Proteger la privacidad de los empleados.

Señales de que su empresa se encuentra en esta etapa

- La inversión en movilidad continúa siendo de reducida a moderada.
- Han movilizado las aplicaciones empresariales horizontales asociadas a la colaboración, como SharePoint o la mensajería instantánea empresarial (EIM).
- A medida que han ido implementando nuevas aplicaciones móviles, le preocupa cada vez más la posibilidad de que puedan filtrarse datos.
- Las líneas de negocio empiezan a pedir aplicaciones más específicas basadas en funciones para mejorar los resultados empresariales.

Movilización de los procesos empresariales existentes

En este punto, los equipos están acostumbrados a trabajar en colaboración desde cualquier lugar a través de las herramientas básicas de colaboración y comunicación que la empresa ha movilizado, pero nuevamente los decisores de la empresa, en especial como los responsables de líneas de negocio, querrán que el departamento de TI haga mucho más. La siguiente etapa en la curva de la movilidad es la movilización a gran escala de los procesos existentes y las aplicaciones esenciales de su empresa. Normalmente, durante esta etapa las organizaciones detectan lagunas en su inventario de aplicaciones móviles y empiezan a plantearse desarrollar sus propias aplicaciones personalizadas.

Retos de esta etapa

- Adaptar las aplicaciones móviles y las iniciativas a los procesos empresariales existentes e identificar lagunas para cubrir por medio de proyectos personalizados.
- Abordar la aparición de nuevos tipos de datos, o bien nuevos usos de los datos existentes.
- Incorporar aplicaciones móviles o gestión de aplicaciones a la infraestructura.
- Continuar cumpliendo la política de seguridad corporativa y las normas del sector, en especial en lo referente a la información de los clientes y otros datos regulados.

Señales de que su empresa se encuentra en esta etapa

- La adopción de aplicaciones móviles de colaboración tiene buena acogida en toda la empresa, y los usuarios demandan más aplicaciones que les ayuden a realizar su trabajo.
- La empresa ha empezado a movilizar los procesos empresariales existentes o está planificando nuevas inversiones en movilidad.
- La inversión es moderada.
- Han empezado a implementar aplicaciones para dar apoyo a las principales áreas funcionales de su organización, como equipos de ventas, directivos, etc.
- Tienen previsto empezar a desarrollar aplicaciones internas en el futuro próximo.
- Han identificado lagunas que desean cubrir mediante aplicaciones personalizadas para todos los dispositivos, sistemas operativos y nubes.
- Han implementado una plataforma que les permite gestionar las tres «C» de la movilidad segura: el contenido de la empresa, las credenciales de usuarios y las configuraciones de aplicaciones.

Creación de nuevos procesos empresariales

Una vez que la empresa ha movilizado los procesos existentes, la etapa siguiente tiene que ver con transformar el negocio mediante la movilidad para lograr una ventaja competitiva, lo que incluye el ahorro de costes, mejoras en la experiencia del cliente y nuevas oportunidades de ingresos. En este punto el retorno de la inversión (ROI) se maximiza y el uso de la movilidad se generaliza en toda la organización. Las aplicaciones móviles se multiplican en la empresa. Los dispositivos móviles se extienden de tal manera que gestionar dispositivos y aplicaciones individuales resulta ineficaz. Con frecuencia, la gestión es desigual en lo referente a la seguridad. La empresa ha entrado en una etapa en la que el uso de la informática móvil se ha generalizado; y los datos corporativos ahora están en teléfonos, tabletas, ordenadores de sobremesa, dispositivos ponibles (*wearables*), sistemas *back-end*, servicios en la nube, e incluso nubes personales. Es preciso utilizar funciones de gestión de derechos digitales (DRM) para definir políticas de seguridad a nivel de archivo y proporcionar características de seguridad, detección y contención.

Retos de esta etapa

- Gestionar un gran volumen de aplicaciones empresariales para diferentes dispositivos, sistemas operativos y nubes.
- Desarrollar un sistema *back-end* para respaldar nuevas aplicaciones móviles, modelos de negocio y dispositivos.
- Aprovechar los sistemas de autenticación y los almacenes de identidades empresariales para utilizar un sistema de inicio de sesión único (SSO), incluso para los servicios en la nube.
- Asociar el desarrollo de aplicaciones móviles a las necesidades empresariales.

Señales de que su empresa se encuentra en esta etapa

- Su solución de gestión de dispositivos forma parte de un enfoque más amplio de gestión de la movilidad.
- Están buscando una forma de gestionar datos, documentos y funciones, además de aplicaciones y dispositivos.
- Han empezado a desplegar aplicaciones internas personalizadas.
- La inversión en movilidad es de moderada a alta.
- Nuevos modelos de negocio están irrumpiendo en su organización, que ahora maximiza el retorno de la inversión en movilidad.



Siete puntos débiles de la movilidad

1. La necesidad de aplicar seguridad real al contenido corporativo, las credenciales de las aplicaciones y los datos de configuración de los dispositivos, además de evitar una posible filtración de datos.
2. La necesidad de abordar las cambiantes exigencias del negocio ahora y en el futuro (p. ej., nuevas aplicaciones) e integrar una solución UEM con los sistemas y procesos empresariales.
3. La necesidad de una solución de seguridad que no obstaculice el trabajo de los empleados ni los impulse a buscar soluciones alternativas.
4. El auge de la tecnología en la nube, y las dificultades asociadas a la seguridad de los archivos tanto en las aplicaciones en la nube como en los dispositivos móviles.
5. La utilización de modelos de seguridad incompatibles entre aplicaciones debido al uso de diferentes tecnologías de desarrollo (aplicaciones nativas, HTML5, entornos híbridos, etc.).
6. La escalabilidad de la infraestructura de gestión móvil para responder a las necesidades cambiantes de la empresa.
7. Las dificultades de tener que prestar soporte técnico móvil en toda la empresa.

Factores fundamentales para elegir una plataforma UEM

Una vez que haya identificado el lugar donde se encuentra en la curva de madurez, es más fácil determinar el tipo de problemas que debe solucionar a corto plazo. Plántese también el largo plazo para asegurarse de que la solución que elija respalde sus objetivos de cara al futuro.

La lista que se incluye a continuación no es exhaustiva, pero le dará una idea de los principales factores para tener en cuenta. Si todos las partes interesadas de su empresa entienden y aceptan la importancia de estos aspectos, podrá elaborar una lista de soluciones seleccionadas.

- 1 Gestión multiplataforma de terminales
- 2 Gestión y seguridad de aplicaciones móviles
- 3 Acreditaciones y certificaciones de seguridad
- 4 Protección de la privacidad de los usuarios
- 5 Control de documentos
- 6 Modelo de implementación (local o en la nube)
- 7 Migración y adopción
- 8 Soporte técnico
- 9 Formación y funciones de usuario
- 10 Precios y TCO

1. Gestión multiplataforma de terminales

Tanto si en su empresa se utilizan dispositivos personales como corporativos —gestionados o no por el departamento de TI—, lo más probable es que en su entorno de trabajo se utilicen múltiples sistemas operativos y tipos de dispositivos. Debe asegurarse de que la solución UEM pueda gestionar esos dispositivos de acuerdo con sus necesidades, para cada caso de uso y función (p. ej., usuarios comerciales, trabajadores remotos, usuarios confidenciales, dispositivos de uso compartido, sistemas de sobremesa, quioscos, etc.). Tenga presente no solo las plataformas que utiliza en la actualidad, sino también las que podría utilizar en un futuro, como Android™ for Work, Samsung Knox Workspace o iOS Managed Apps.

Desde la perspectiva de la gestión diaria, la plataforma que elija debe permitir a los administradores de TI gestionarlo todo desde una consola unificada: grupos de usuarios, funciones administrativas, configuraciones de software, perfiles de correo electrónico, políticas de TI, etc. Y dado que el personal de TI ya tiene suficiente trabajo por delante, es fundamental que la interfaz sea intuitiva y no tenga que aprender a usar un modelo de gestión completamente nuevo.

Entre otros aspectos para valorar, debe saber si la solución UEM:

Simplifica el registro y la configuración de usuarios. Permite que los usuarios puedan registrarse de forma inalámbrica y rápida. Agilizar el proceso de registro aumenta la satisfacción del usuario y reduce los costes de soporte móvil.

Permite aplicar controles de políticas. Debe tener la posibilidad de definir y aplicar políticas adecuadas para su organización: contraseñas, cifrado de dispositivos, cámara, red wifi, VPN, etc.

En caso de pérdida, robo, retirada o sustitución de un dispositivo debe eliminar la información corporativa sin que afecte al contenido ni a las aplicaciones personales.

Respalda el cumplimiento normativo y un alto nivel de seguridad. Las organizaciones de sectores regulados, como el financiero, el sanitario, los servicios jurídicos o los servicios públicos, deben cumplir las disposiciones relativas a la seguridad de los datos de clientes, los datos financieros y otra información. Para muchas organizaciones satisfacer estas exigencias de seguridad, siempre en aumento, requiere un tiempo y una energía muy valiosos. La solución UEM que elija debe integrar funcionalidad de seguridad en el diseño. Compruebe las acreditaciones y certificaciones de seguridad para ver si las soluciones responden a sus necesidades específicas.

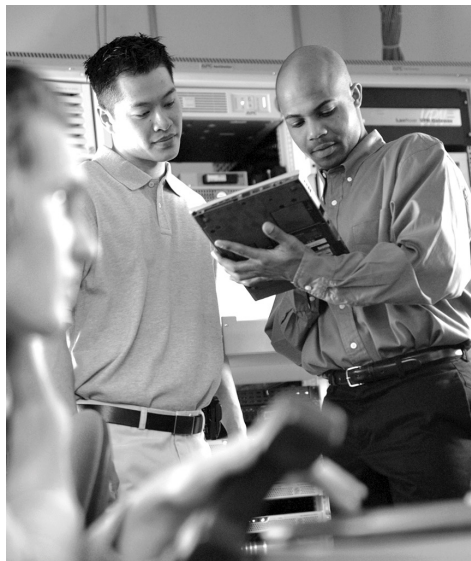
Detecta el desbloqueo de funciones. Para los usuarios finales, desbloquear la funcionalidad de un dispositivo (*rooting o jailbreaking*) puede resultar tentador, dado que proporciona más libertad para personalizar las funciones de sus *smartphones* o tabletas. Pero al mismo tiempo, plantea un riesgo de seguridad importante dado que el proceso implica desactivar las protecciones de seguridad integradas en el sistema operativo. Esto permite que el dispositivo se exponga a una amplia variedad de programas malignos y ataques dirigidos. Por lo tanto, es importante que su solución UEM incluya algún mecanismo para detectar los dispositivos cuya funcionalidad ha sido desbloqueada y combatir el software utilizado para camuflar el estado de desbloqueo (*jailbreak jammers*). Además, la tecnología de detección del desbloqueo de funciones no debe depender de los servicios de localización para realizar un análisis automático, ya que esto consume batería y afecta a la privacidad del usuario.

2. Gestión y seguridad de las aplicaciones móviles

Seguridad a través de la contenerización

Las aplicaciones contenerizadas permiten al departamento de TI aplicar un control minucioso al separar cada aplicación y sus datos en su propio almacén de archivos cifrado. Cada contenedor de aplicaciones puede tener sus propias políticas o normas de uso, y se puede proteger y borrar por separado. Las aplicaciones personales instaladas por el propietario del dispositivo pueden coexistir de forma segura con las aplicaciones aprobadas por la empresa, las aplicaciones ISV de terceros o las aplicaciones personalizadas que interactúan con los activos de propiedad intelectual de la empresa. Como las aplicaciones personales están aisladas de las corporativas, es posible restringirles el acceso a los datos de los contenedores de aplicaciones corporativas (por ejemplo, el uso de funciones nativas como copiar y pegar). Aún así, los usuarios pueden tener las aplicaciones corporativas junto a las personales, o bien organizarlas de otro modo.

Si el proveedor de su solución UEM ofrece kits de desarrollo de software (SDK) adecuados, puede integrar bibliotecas de seguridad directamente en el código de las aplicaciones antes de compilarlas. Aunque este sistema de contenerización requiere acceso al código fuente y que los desarrolladores escriban código, los SDK pueden aportar ventajas de productividad tanto a los desarrolladores como a la empresa. Además, los desarrolladores pueden incorporar a las aplicaciones otras funciones distintas a las de seguridad, como servicios de alta disponibilidad y recuperación ante desastres, o incluso preinstalar características, como la presencia de usuarios o la impresión.



Una solución de contenerización debe incluir al menos las siguientes funciones:

Autorización de aplicaciones. Permite la distribución de una aplicación solo al dispositivo de un usuario autorizado.

Cifrado a nivel de aplicación. Utilizar este cifrado, con independencia del cifrado a nivel de dispositivo, permite que aunque la clave de un dispositivo esté en peligro, los datos de las aplicaciones sigan estando protegidos.

Autenticación de aplicaciones. Facilita la autenticación de contraseñas a nivel de aplicación con opciones avanzadas adaptadas a sus necesidades, como el uso de la autenticación de dos factores.

Inicio de sesión único. Permite a los usuarios iniciar sesión en una aplicación contenerizada y acceder a todas las demás aplicaciones contenerizadas para simplificar y agilizar la experiencia de usuario.

Políticas de seguridad generalizadas. Por ejemplo, contraseñas robustas, prevención de pérdida de datos («Abrir en», cortar/copiar/pegar, gestión del contenido de archivos) y controles de conformidad (bloqueo/borrado remoto, detección de dispositivos con funciones desbloqueadas, versión de sistema operativo).

Acceso seguro. Facilita el acceso a los servidores y otros recursos protegidos por el cortafuegos que no necesitan los puertos de entrada abiertos ni la exposición innecesaria de la red corporativa.

Gestión de derechos digitales (DRM). Políticas de seguridad a nivel de archivo para proteger el contenido corporativo que se transfiere entre dispositivos, sistemas y nubes.

Despliegue y gestión de aplicaciones

Con una solución adecuada de gestión de aplicaciones móviles (MAM), el equipo de TI puede proporcionar a los empleados y colaboradores acceso a las aplicaciones y los datos que su función requiera, en los dispositivos personales de su elección, sin necesidad de aplicar un control restrictivo a esos dispositivos para satisfacer requisitos de seguridad y normativos.

Y lo que es más importante, las políticas y la tecnología de una solución MAM pueden ayudar a que la eliminación de datos se limite al borrado selectivo de aplicaciones corporativas específicas y su información, manteniendo intacto el contenido personal del dispositivo. De este modo, la movilidad puede utilizarse como un auténtico elemento facilitador, que no afecta a la experiencia del usuario y vela por la seguridad de los datos corporativos.

Una tienda de aplicaciones empresariales privada y personalizable puede funcionar como una «ventanilla única» para distribuir aplicaciones personalizadas o de contenido a empleados y miembros autorizados de la empresa (p. ej., contratistas, partners del ecosistema, etc.), incluso en el caso de que sus administradores de TI no gestionen el terminal. Esto permite ofrecer a los usuarios una experiencia óptima en diferentes plataformas, pero con los controles de la empresa.

Algunas soluciones también incluyen paneles gráficos que proporcionan una vista detallada de la adopción de aplicaciones en toda la empresa. Además, podrá obtener información sobre los usuarios registrados en la tienda de aplicaciones empresariales; el número de aplicaciones en uso; la distribución de estas según la plataforma/sistema operativo; las aplicaciones más populares; etc.

Valore todo el ciclo de vida de las aplicaciones

Su solución EMM debería proporcionarle un marco de seguridad y gestión a lo largo de todo el ciclo de vida de las aplicaciones móviles, que abarque lo siguiente:

- El desarrollo y la adquisición de aplicaciones (internas y de terceros).
- La distribución y la implementación de aplicaciones.
- La gestión de políticas y seguridad para las aplicaciones.
- La utilización de aplicaciones y la gestión de comentarios de los usuarios.
- La desactivación de aplicaciones y el borrado selectivo de datos.

Las siguientes características son signos de que su empresa ha tomado el camino correcto:

- La funcionalidad de inicio de sesión único, que permite a los usuarios autenticarse una sola vez para obtener acceso al contenido de diferentes aplicaciones.
- El cifrado de datos compartidos o en uso en las aplicaciones móviles, con independencia de si estas residen en el dispositivo, detrás del cortafuegos corporativo o en la nube.
- La contenerización de cualquier aplicación de forma sencilla.
- Un SDK que permita a los desarrolladores aprovechar funciones avanzadas, como el uso compartido de documentos entre aplicaciones, o bien un marco común de servicios para incorporar características habituales sin tener que escribir código nuevo.

3. Acreditaciones y certificaciones de seguridad

¿Qué tipo de certificaciones de seguridad tienen las plataformas UEM que ha seleccionado? ¿Y qué pasa con los proveedores? Dependiendo de su sector, es posible que la ley le obligue a elegir una plataforma que sea compatible con las normativas HIPAA, HITECH, GLBA, FISMA y otros requisitos de seguridad.

Preste también atención al tipo de organizaciones, analistas, clientes y sectores que hacen comentarios favorables acerca de cada plataforma. La mayoría de los clientes dicen disponer de una gran tecnología de seguridad y alardean de su lista de funciones, pero únicamente las organizaciones que han obtenido la validación de terceros pueden respaldar sus afirmaciones. ¿Han invertido esos clientes tiempo y recursos para comprobar que la seguridad es lo suficientemente robusta a fin de satisfacer sus necesidades?

Las aplicaciones móviles son una puerta abierta a la filtración de datos cuando los empleados envían información de la empresa a soluciones de almacenamiento en la nube o a cuentas de correo personales, e incluso realizan copias de seguridad de los dispositivos en sus ordenadores. Pero la seguridad móvil conlleva más que proteger los datos corporativos en tránsito o en reposo en los dispositivos. Las organizaciones también deben asegurarse de proteger la información de configuración y las credenciales de usuario que pueden almacenarse en los dispositivos móviles. Si esta información no está protegida, puede ser una puerta de acceso que ponga en peligro la red corporativa y las aplicaciones empresariales fundamentales. Proteger únicamente el dispositivo no evita la pérdida de datos corporativos. Es preciso salvaguardar las tres «C» de la seguridad móvil: el contenido, las credenciales y la configuración.

4. Protección de la privacidad de los usuarios

Con el auge de los dispositivos personales en el lugar de trabajo, las empresas cada vez son más conscientes de los celos y las posibles responsabilidades a la hora de gestionar la información y los dispositivos personales de los empleados. Los empleados desean privacidad por los mismos motivos que las organizaciones desean seguridad. Lo que es de los empleados les pertenece y debe permanecer en el ámbito privado.

Además, la legislación contra la discriminación de algunos países puede ver motivos de demanda si se accede al inventario de aplicaciones de un dispositivo, o a la información de geolocalización de este.

Uno de los ejemplos más serios de violación de la intimidad al que podría enfrentarse una empresa es

cuando hace un borrado completo del dispositivo personal de un empleado porque la información corporativa está en peligro (p. ej., debido a la pérdida o el robo del dispositivo o porque el empleado ha abandonado la empresa).

Además debe saber que exigir el uso de servicios de localización —algo que también gasta la batería— para garantizar la conformidad con las políticas, o bien guardar registros del teléfono o de localización son posibles infracciones de la vida privada del empleado.

Busque una solución que genere confianza al proteger no solo la información sensible de la empresa, sino también el contenido personal de sus trabajadores, en diferentes sistemas operativos, sin importar el modelo de propiedad del dispositivo.

5. Control de documentos

El intercambio de archivos, en especial a través de dispositivos móviles, se ha convertido en un elemento esencial de la colaboración en las empresas. A medida que las empresas movilizan sus procesos, aumenta la cantidad de datos sensibles que se transfieren a dispositivos móviles y residen en ellos.

Los archivos que contienen materiales sensibles, como activos de propiedad intelectual, datos financieros e información regulada pueden estar en riesgo si no se protegen. Esto es así con independencia de si se comparten dentro o fuera de los límites de la organización. Según un estudio reciente realizado por The Ponemon Institute¹, el 61% de los empleados admiten enviar correos electrónicos

sin cifrar, no eliminar documentos confidenciales, o bien reenviar por error datos sensibles a destinatarios no autorizados.

Para evitar que los datos regulados o la información sensible de la empresa terminen en manos equivocadas, tiene que proteger sus documentos directamente. Busque una plataforma UEM que proporcione una solución segura de sincronización e intercambio de archivos empresariales (EFSS) con gestión de los derechos digitales (DRM) para añadir políticas de seguridad a nivel de archivo, o bien una plataforma que se integre con dicha solución. Y en sectores regulados, necesitará llevar un control de los documentos con fines de autoría y conformidad.

6. Modelo de implementación (local o en la nube)

Muchas soluciones de gestión de terminales están disponibles como servicio en la nube (también llamado «software como servicio» o SaaS) o para instalar localmente en la empresa. Cada modelo tiene sus ventajas. Entre los factores que pueden influir en su decisión, se incluyen los siguientes:

Tiempo de implementación: las soluciones basadas en la nube normalmente pueden ponerse en funcionamiento muy rápido.

Mantenimiento: las soluciones basadas en la nube pueden aligerar la carga del personal de TI en lo que se refiere a actualizaciones y mejoras, algo especialmente útil cuando los recursos técnicos de la empresa son limitados.

Acceso y control: una solución local se instala en el lado del servidor en el centro de datos. Para algunas

organizaciones de TI, esto proporciona un mayor nivel de control sobre los datos y la funcionalidad de recuperación ante desastres, y una integración más estrecha con otros sistemas.

Conformidad: para algunas organizaciones reguladas o que requieren un alto nivel de seguridad (p. ej., ramas de la administración o del ejército), las exigencias normativas pueden inclinar la balanza a favor de una solución local, aunque a medida que han ido evolucionando las implementaciones en la nube (y la percepción del departamento de TI sobre ellas) esto también está cambiando.

Lo ideal es que su solución UEM le ofrezca ambas opciones de implementación, sin necesidad de renunciar a la seguridad ni a la funcionalidad, al margen de lo que usted desee hacer, incluso si necesita diferentes modelos en diferentes ubicaciones.

7. Migración y adopción

La migración a una nueva plataforma exige tiempo y recursos. Pero el proceso no tiene que ser estresante. Elegir el enfoque adecuado es esencial para que la empresa continúe su funcionamiento con las mínimas interrupciones para los empleados.

Su estrategia de UEM debe abordar este proceso. ¿Qué recursos necesita y de dónde los obtendrá? Normalmente, los clientes de grandes empresas

gestionan miles de terminales que operan en distintos continentes, desde múltiples oficinas en todo el mundo.

Necesita crear un plan de transición para la etapa de migración, un calendario de migraciones y un plan de formación para el equipo de TI y para los usuarios finales.

8. Soporte técnico

Usted confía en su plataforma móvil para agilizar la toma de decisiones; impulsar las ganancias y los resultados; facilitar el flujo de trabajo; y conectar usuarios, equipos, clientes y proveedores. Esto es fundamental para la empresa. Por tanto, cuando elija su solución UEM, cerciórese de que el proveedor proporciona los servicios y opciones de soporte

que su empresa necesita. Infórmese bien sobre los servicios disponibles (y los precios) para respaldar las necesidades de planificación, optimización y resolución de problemas de su empresa. De lo contrario, podría poner en peligro las mejoras que pretende lograr al invertir en una solución UEM.

9. Formación y funciones de usuario

¿Qué formación necesita? ¿Cómo puede acceder a ella y a qué precio? Cuanto más fácil sea su solución UEM para el equipo de TI y los usuarios finales (en lo referente a la implementación inicial y a la gestión

continua), menos tiempo de formación necesitará. Por tanto, averigüe lo que cada proveedor potencial ha hecho a fin de optimizar y simplificar los procesos para estos dos grupos de personas interesadas.

10. Precios y coste total de propiedad (TCO)

Migrar a una plataforma de gestión unificada de terminales ayudará a su organización a estandarizar la infraestructura, reducir la complejidad y aumentar el ROI.

Asegúrese de que la solución que elija ofrezca movilidad flexible y asequible, que se adapte a las necesidades de su empresa a lo largo del tiempo. Haga hincapié en el número de dispositivos que se pueden añadir por dominio. Infórmese sobre las condiciones de pago también; si la idea es evitar una

inversión elevada al principio, tal vez prefiera optar por un modelo de suscripción para prever mejor los gastos operativos anuales. Distribuir los costes de esta manera puede ser útil de cara al flujo de efectivo.

Por último, para obtener una visión completa del TCO, debe tener en cuenta los costes directos e indirectos. A medida que avance por la curva de madurez de la movilidad, la fiabilidad se convertirá en un factor fundamental.



La mejor solución de movilidad con BlackBerry Enterprise Mobility Suite



BlackBerry Enterprise Mobility Suite

Con BlackBerry Enterprise Mobility Suite®, las empresas pueden satisfacer las necesidades de sus usuarios y directivos a la hora de utilizar aplicaciones móviles seguras en cualquier momento y lugar para impulsar su productividad; y beneficiarse de controles y políticas coherentes en diferentes plataformas — como iOS®, Android™, Android™ for Work, Samsung Knox™, Windows®, macOS y BlackBerry®—, sin importar el modelo de propiedad del dispositivo o el grupo de usuarios.

BlackBerry® Enterprise Mobility Suite se caracteriza por:

- Ofrecer una solución «llave en mano» para distribuir aplicaciones de colaboración, de línea de negocio y personalizadas y, al mismo tiempo, proteger su negocio y la privacidad de sus empleados con políticas coherentes de contenerización y de seguridad para diferentes sistemas operativos, a fin de mantener separados el contenido personal y el de la empresa.
- Incorporar las herramientas, las API, la infraestructura y los kits de desarrollo de software (SDK) necesarios para desarrollar aplicaciones que garanticen una seguridad homogénea entre diferentes dispositivos y sistemas operativos.
- Haber superado rigurosas pruebas realizadas por terceros, como la certificación de seguridad Common Criteria para la gestión de aplicaciones y para la plataforma subyacente de seguridad de aplicaciones, lo que la convierte en la solución elegida por empresas de seguros, servicios financieros, bufetes de abogados, industria aeroespacial, sector de defensa y militar, y muchas otras organizaciones concienciadas con la seguridad.
- Proporcionar controles precisos del contenido al integrar tecnología de gestión de derechos digitales (DRM) en los archivos para protegerlos y permitir su rastreabilidad en todo momento, incluso después de que los archivos se hayan descargado y compartido con terceros.
- Ser lo suficientemente flexible para abordar sus necesidades sin perder de vista los costes, por lo que podrá añadir funciones fácilmente a lo largo del tiempo, sin interrupciones y sin sustituir componentes.
- Dar apoyo a organizaciones que deben cumplir los niveles más elevados de seguridad y garantizar la conformidad de su movilidad. Las soluciones empresariales de BlackBerry® son utilizadas por:
 - 16 gobiernos del G20;
 - las 10 mayores bufetes de abogados;
 - las cinco mayores compañías de petróleo y gas;
 - más de la mitad de las empresas de Fortune 100, incluyendo todos los bancos comerciales de la lista.

BlackBerry Enterprise Mobility Suite proporciona la funcionalidad que necesita para abordar sus requisitos de movilidad y productividad

Management Edition

Para aquellas organizaciones que necesitan funciones de gestión y control a nivel del dispositivo, esta edición incorpora BlackBerry® UEM, una completa solución de gestión unificada de terminales, multiplataforma y muy segura.

Enterprise Edition

Para organizaciones que necesitan funcionalidad de colaboración, aparte de una solución UEM, esta edición permite movilizar Microsoft® Exchange, con una experiencia de uso óptima, al tiempo que garantiza la seguridad de un extremo a otro y protege los datos corporativos.

Collaboration Edition

Con esta edición, las organizaciones que están preparadas para adoptar funciones más avanzadas de productividad móvil pueden movilizar aplicaciones de Microsoft —Exchange, Office 365, Office, SharePoint, Skype for Business, etc.— y otras aplicaciones importantes (como el CRM) a través de un ecosistema de aplicaciones líder.

Application Edition

Las organizaciones que ya utilizan funcionalidad avanzada de gestión de terminales, además de aplicaciones de colaboración y de terceros, pueden dar un paso más y desarrollar sus propias aplicaciones para habilitar nuevos procesos empresariales. Esta edición proporciona una plataforma completa para desarrollar, desplegar y proteger las aplicaciones móviles.

Content Edition

Para las organizaciones que desean añadir seguridad al contenido, además de la funcionalidad UEM y las aplicaciones personalizadas y de terceros, esta edición incluye BlackBerry Workspaces, la solución líder de sincronización e intercambio de archivos empresariales (EFSS). Workspaces integra protección DRM en los archivos para que el contenido esté seguro en cualquier lugar. Gestione los permisos de usuario para ver, editar, copiar, imprimir, descargar o reenviar archivos, incluso después de que los archivos hayan sido descargados o compartidos con terceros.

Descubra más sobre BlackBerry Enterprise Mobility en: www.blackberry.com/suite

* Actualizado en octubre de 2015

¹ 1 Disponible en: <https://www.complianceweek.com/sites/default/files/Ponemon-Intralinks%20File%20Sharing%20Report.pdf>

© 2017 BlackBerry Limited. Las marcas como BLACKBERRY, BLACKBERRY UEM, BBM y EMBLEM Design, entre otras, son marcas comerciales o marcas registradas de BlackBerry Limited. Todas las demás marcas comerciales pertenecen a sus respectivos propietarios.

iOS es una marca registrada de Cisco Systems, Inc. y/o sus empresas filiales en los Estados Unidos y otros países. iOS se usa bajo licencia de Apple Inc. Apple Inc no patrocina, autoriza ni avala este documento. Android es una marca comercial de Google Inc. que no patrocina, autoriza ni avala este documento.

Microsoft, SharePoint y Windows son marcas comerciales o marcas registradas del grupo de empresas de Microsoft.