

La movilidad avanza rápido. Para mantener el control tiene que estar preparado para el cambio.

¿Está preparado para el BYOD? He aquí siete cuestiones que debería responder cuando implementa nuevas funcionalidades móviles.



Contenidos

- 2 Introducción
- 2 El BYOD suscita cuestiones que posiblemente usted no se haya planteado.
 - 3 1. ¿Está su red preparada para soportar una complejidad mayor?
 - 4 2. ¿Su servicio de asistencia técnica podrá gestionar la avalancha que se le avecina?
 - 4 3. ¿Son seguros sus dispositivos móviles BYOD?
 - 5 4. ¿Tiene en funcionamiento su propia tienda de aplicaciones?
 - 5 5. ¿Están los nuevos servicios preparados para su implementación?
 - 6 6. ¿Se han establecido políticas y procedimientos de gestión?
 - 6 7. ¿Están al tanto todos sus empleados?
- 7 Conclusión
- 7 Para más información
- 7 Acerca del software Tivoli de IBM

Introducción

Cuando se habla de smartphones, tabletas y otros dispositivos móviles personales de los empleados en el puesto de trabajo, las cifras hablan por sí mismas. Según una encuesta reciente de Aberdeen Group, el 72% de las empresas participantes permitía la práctica conocida como 'trae tu propio dispositivo' (BYOD).¹ Y según otro estudio de Information Week, el 65% de las organizaciones prevé el aumento de la adopción del BYOD.²

El uso empresarial de dispositivos personales ha aumentado de forma espectacular. Entre los años 2008 y 2010 el número de empresas que permitían el uso de teléfonos basados en la plataforma Google Android pasó del 0% al 43%. Y el uso del iPhone de Apple subió del 28% al 66%.¹

¿Cuál es la razón? Los proveedores de smartphones han empezado a dirigirse de forma más activa a los mercados corporativos y a diseñar sus productos para que puedan satisfacer las necesidades de negocio.³ Es la consumerización de la TI (el deseo del usuario de disfrutar de la misma funcionalidad que tienen sus dispositivos personales en los del trabajo) la que por lo general se lleva el mérito. Para el 61% de los que respondieron a

la encuesta de Aberdeen Group, la razón principal para permitir la práctica del BYOD con smartphones y tabletas era la demanda de los empleados de disponer de más funcionalidad móvil que meramente el correo electrónico y la agenda.¹

Curiosamente, existe entusiasmo entre los empleados por el BYOD incluso cuando las empresas para las que trabajan no dan soporte a sus dispositivos. Mientras que el 43% de las organizaciones permitían y daban soporte corporativo formal al iPhone, otro 34% permitía su uso aunque no proporcionara soporte. En el caso de los teléfonos Android, el 30% proporcionaba soporte, pero otro 31% permitía su uso aunque no proporcionara soporte.¹

Está claro que los smartphones, las tabletas y otros dispositivos móviles han llegado a la empresa para quedarse. En la encuesta de *Information Week* de 2011, el 82% de los participantes dijeron, con la vista puesta en dos años más tarde, que esperaban que los smartphones tuvieran un 'papel esencial' en la productividad empresarial. Las tabletas no se quedaban lejos: el 79% de los participantes las consideraban esenciales para la productividad, lo que representa un aumento importante desde el 36% del año anterior. Por el contrario, sólo el 36% consideraba que los ordenadores portátiles fueran esenciales para la productividad, bajando desde el 53% del año anterior.²

Estas cifras constituyen un argumento convincente, pero para responder de forma más efectiva, la empresa tiene que hacer algo más que simplemente escuchar. Ha llegado el momento de actuar.

Este informe advierte que no basta, simplemente, con dar permiso a los usuarios para utilizar sus dispositivos personales para el trabajo. Para poner en práctica con éxito el BYOD, las organizaciones deben resolver cuestiones que es posible que no hayan considerado todavía pero que pueden tener consecuencias importantes para las operaciones de negocios y TI.

El BYOD suscita cuestiones que posiblemente usted no se haya planteado

Al tratar el tema del BYOD, es habitual manifestar al principio preocupación por la seguridad o centrarse en gestionar las grandes cantidades de datos que estos dispositivos adicionales generan. Pero el debate sobre el BYOD se extiende más allá de la seguridad y plantea un conjunto de problemas de gestión del

punto terminal. Y se extiende más allá de la carga de datos y abarca el impacto más amplio que los dispositivos tienen sobre la infraestructura y las operaciones. El debate sobre el BYOD es aún relativamente nuevo, pero está señalando el camino del cambio y está planteando cuestiones clave que las organizaciones tienen que estar preparadas para afrontar.

Desde el punto de vista de la organización, la rápida adopción de smartphones y tabletas ya está erosionando las políticas seguidas por TI para gestionar la tecnología y controlar el acceso a los recursos, ya que TI seleccionaba, compraba y desplegaba los dispositivos móviles de los empleados y les daba soporte. Estas prácticas y estos dispositivos (el más habitual es la plataforma BlackBerry, que se centra en la voz, el correo electrónico y la agenda) no han desaparecido. Pero el escenario BYOD y el enfoque más dirigido a las aplicaciones de los smartphones y las tabletas están tomando el mando.

En sólo un año, de 2010 a 2011, *Information Week* registró una caída del 73% al 58% en el número de organizaciones estandarizándose en una plataforma de dispositivos móviles.² Y en el período de dos años entre 2008 y 2010, según Aberdeen Group, el uso de la plataforma BlackBerry descendió del 81% de las organizaciones al 73%,¹ todavía una cifra importante pero que muestra que se aproxima una era de entornos heterogéneos más complejos para la TI y una funcionalidad más productiva para usuarios de negocio.

Tanto si recogen datos de posicionamiento global como si dan soporte a transacciones empresariales o interactúan con la red para garantizar el rendimiento óptimo de las funciones tecnológicas, los dispositivos móviles están en el centro de los servicios y operaciones actuales. En el planeta inteligente actual, la recopilación de datos, el intercambio de información y la toma de decisiones deben tener continuidad independientemente de la ubicación del usuario para dar apoyo a empresas altamente competitivas.

Como resultado de ello, la explosión en la cantidad y el tipo de dispositivos móviles suscita una serie de cuestiones que las organizaciones deben abordar si quieren sacar el máximo rendimiento posible de los empleados, de sus dispositivos y de las redes de negocio.



¿Está su red preparada para soportar una complejidad mayor?

Es cierto que un incremento del número de dispositivos no hace aumentar la cantidad de datos al mismo ritmo. Después de todo, cada empleado utiliza sólo un dispositivo a la vez. Pero más dispositivos significan más oportunidades de recopilar datos y más oportunidades de conectar con la red. Por eso, la red tiene que crecer y evolucionar para satisfacer esta mayor demanda.

En un escenario BYOD, la organización puede conseguir un ahorro de costes importante al no comprar dispositivos. Pero la necesidad resultante de gestionar múltiples sistemas operativos y plataformas de hardware puede ocasionar sus propios gastos, así como importantes problemas de TI. Porque aunque las aplicaciones de smartphones y tabletas llevan la conectividad empresarial móvil más allá de la voz y el correo electrónico, también incrementan la necesidad de disponer de más ancho de banda e infraestructuras más grandes. Y la organización se enfrenta a la necesidad creciente de realizar una gestión de redes más efectiva.

Una solución es la virtualización. La mejor utilización de los recursos y la gestión racionalizada hacen posible dar cabida a más usuarios y más dispositivos y a un mayor movimiento de datos. Pero cualquier entorno necesitará funciones tales como gestión de eventos y análisis de causas subyacentes para asegurar el buen funcionamiento de los dispositivos, así como descubrimiento y gestión centralizada para tener controlados los activos móviles remotos.



¿Su servicio de asistencia técnica podrá gestionar la avalancha que se le avecina?

Cuando los usuarios traen sus propios dispositivos, aportan un conjunto de capacidades personales, o una falta de capacidades, al uso del dispositivo. Incluso los empleados competentes con sus dispositivos o que confían en su proveedor para resolver problemas del dispositivo es probable que necesiten ayuda con procedimientos internos tales como la configuración del dispositivo o la conexión a redes. Y aún más: la demanda crece toda a la vez. Una empresa que inicia una política BYOD suele encontrarse con un gran número de empleados que quieren incorporarse al programa inmediatamente. La repentina necesidad de infraestructura y ancho de banda adicional puede provocar problemas de funcionamiento, y el servicio de asistencia técnica puede inundarse con llamadas de ayuda.

Es posible que sea necesario más personal en el servicio de asistencia técnica, al menos al principio. Pero existen otras medidas que la organización puede tomar. Al igual que gestionan la experiencia de los clientes, las organizaciones pueden gestionar la experiencia de los empleados-usuarios, y esto puede ayudar a mejorar la productividad y el estado de ánimo de los empleados, así como reducir el coste de soporte del servicio de asistencia técnica. Este proceso supone monitorizar datos como las horas o la frecuencia de conexión y garantizar que esté disponible un ancho de banda suficiente para satisfacer la demanda.



¿Son seguros sus dispositivos móviles BYOD?

Los smartphones son pequeños y pueden perderse o ser robados con facilidad. No es de extrañar, por tanto, que el 93% de las organizaciones sitúen la seguridad de los dispositivos móviles al menos a la misma altura que otras preocupaciones en materia de seguridad. Casi el 60% le conceden alta prioridad o la sitúan entre las principales prioridades, y ‘entre las principales prioridades’ es el nivel de preocupación que está creciendo más rápidamente.²

El escenario BYOD, sin embargo, eleva aún más el riesgo para la seguridad. Como los empleados utilizan también sus smartphones y tabletas para asuntos personales, suelen llevar consigo los dispositivos siempre, los smartphones están siempre conectados a la red y los usuarios se conectan a menudo a la empresa desde entornos informales y menos seguros, como cafeterías. También porque el equipo es personal, los empleados suelen oponer resistencia a las medidas de seguridad que instalan agentes o software de gestión en el dispositivo. En estos casos, TI debe encontrar otras formas de garantizar la seguridad tanto de los dispositivos móviles como del entorno de negocio.

Así pues, el reto es limitar de modo efectivo el acceso a redes a usuarios autorizados y verificados sin perjudicar la productividad del empleado. Debe gestionarse el cifrado para que los datos estén seguros durante su transmisión. El cambio, especialmente de las configuraciones del dispositivo, debe gestionarse para que sea compatible con el cumplimiento de los requisitos normativos. Y en caso de que un dispositivo quede comprometido, TI tiene que poder suprimir remotamente los datos empresariales confidenciales antes de que caigan en malas manos.



4 ¿Tiene en funcionamiento su propia tienda de aplicaciones?

Permitir el uso de dispositivos personales de los empleados que tienen más funciones que correo electrónico, agenda y voz puede ser un paso importante hacia una mayor eficiencia del negocio. Pero se trata sólo del primer paso. Como en la electrónica de consumo, con la que los usuarios pueden descargar aplicaciones de sitios de Internet conocidos como ‘tiendas de aplicaciones’, las organizaciones empresariales cada vez dan más soporte a la funcionalidad BYOD mediante el desarrollo y la distribución de sus propias aplicaciones.

Las organizaciones suelen desarrollar ahora aplicaciones ligeras y de poco peso que se centran en tareas específicas. Pero una organización que desarrolla sus propias aplicaciones y las distribuye a través de una tienda de aplicaciones interna puede conseguir grandes resultados. Las empresas que están dando este paso hablan de aumentos de la productividad de los empleados y de la eficiencia operativa de hasta el 45% y el 44%, respectivamente.¹

Los próximos pasos incluyen la ampliación de las aplicaciones empresariales existentes a dispositivos móviles y el despliegue de versiones para dispositivos móviles de software de terceros para funciones como la gestión de las relaciones con los clientes (CRM), lo que daría aún mayor funcionalidad, más amplia y fácilmente accesible que nunca.



5 ¿Están los nuevos servicios preparados para su implementación?

Por definición, los clientes, los socios comerciales y otros agentes implicados externos traen sus propios dispositivos cuando interactúan con la organización y su infraestructura. Por tanto, ampliar los servicios empresariales existentes y crear servicios nuevos para el mundo, fuera de la organización, puede encajar bien con una iniciativa interna de BYOD.

Los proveedores de servicios ya se están enfrentando a las cuestiones y oportunidades que llegan con una base grande y heterogénea de dispositivos del usuario. Necesitan ofrecer algo más que un canal de datos. Necesitan poner en marcha una infraestructura que aumente el ancho de banda y gestionarla con herramientas que mejoran la experiencia del cliente. Los proveedores de servicios necesitan controlar cuidadosamente las inversiones de capital y equilibrarlas con costes operativos para propiciar un flujo de ingresos sostenible.

Cada vez más, las organizaciones empresariales tienen que hacer lo mismo. A medida que el mundo se vuelve más instrumentado, interconectado e inteligente y se expande a nuevos mercados, las organizaciones necesitan proporcionar servicios cada vez más valiosos tanto interna como externamente, independientemente del dispositivo que el usuario final elija.



¿Se han establecido políticas y procedimientos de gestión?

Permitir la práctica BYOD con smartphones y tabletas significa algo más que decir que 'sí' a las preferencias de los empleados. Significa poner en marcha políticas que rijan cómo se utilizarán los dispositivos y cómo se gestionarán. Muchas de estas políticas regulan cuestiones que sólo afectan a los dispositivos portátiles, desde qué empresa de telecomunicaciones es mejor usar hasta quién paga por el servicio o cómo se pueden eliminar los datos del dispositivo si se pierde o es robado.

La mayoría de las organizaciones reconocen la importancia de tales políticas. El marco de cumplimiento normativo y las políticas, junto con la aplicación de éstas, son las medidas de control cuya importancia se cita más a menudo. Pero aún siendo tan importantes dichas políticas, sólo la mitad de las organizaciones tienen procedimientos y políticas por escrito que abordan directamente las cuestiones que rodean el uso de dispositivos móviles.²

Los procedimientos para gestionar dispositivos son igualmente importantes, y las organizaciones los sitúan casi al mismo nivel que las políticas entre sus prioridades.² En un entorno BYOD heterogéneo, la selección de herramientas de gestión puede ser crítica. Muchas soluciones de punto pueden crear un caos de gestión. De todas formas, las organizaciones pueden reducir la complejidad con soluciones de gestión de dispositivos móviles que se integren con su infraestructura de gestión existente, al igual que los smartphones y las tabletas utilizados en el BYOD se integran en los procesos de negocio.



¿Están al tanto todos sus empleados?

Utilizar un smartphone o una tableta en el trabajo no es lo mismo que utilizarlo en casa, aunque el usuario sea el propietario del dispositivo. Puede que los empleados hayan seleccionado sus propias plataformas y formatos. Puede que, en cierta medida, hayan seleccionado sus propias aplicaciones. Pero sigue siendo necesario un programa de formación de los empleados para garantizar que éstos entiendan las políticas que rigen el uso de sus dispositivos, ayudarles a sacar partido de los recursos disponibles y racionalizar la gestión de dispositivos para que tanto los usuarios como TI puedan continuar siendo los más productivos posible.

Tenga en cuenta, por ejemplo, que una afluencia grande y repentina de dispositivos móviles BYOD puede ralentizar el funcionamiento de la red Wi-Fi de la organización. Pero si los empleados son conscientes de las alternativas, por ejemplo la posibilidad de conectarse a una femtocelda (un dispositivo que transmite señal celular a distancias cortas y la encamina a la red de banda ancha), no sólo mejorarán su propia conectividad sino que aligerarán el tráfico intenso en la infraestructura inalámbrica de la organización.

Por lo tanto, es ventajoso para la organización desarrollar una plantilla espabilada en cuestiones de tecnología y no dar por sentado que el uso de dispositivos personales es exclusivamente responsabilidad individual. Los ajustes por defecto, las configuraciones, las cuestiones relacionadas... todo debe ser comunicado. La concienciación de los empleados se convierte en un componente básico clave que sirve de apoyo para el éxito del escenario BYOD.

Conclusión

Independientemente de si está ahora mismo implementando una política BYOD o de si ya la tiene totalmente en marcha, IBM puede ayudarle a superar los retos de TI asociados a los dispositivos móviles personales de los empleados, de múltiples proveedores y en múltiples plataformas.

Cuando amplía su red para dar cabida a nuevos requisitos tecnológicos y empresariales, IBM puede ayudarle a asegurarse de que dispone de la infraestructura y el ancho de banda necesarios y a establecer funciones para reducir costes, generar nuevos ingresos y lograr el éxito competitivo.

Cuando se enfrenta a los retos de gestión inherentes al uso empresarial de smartphones, tabletas y otros dispositivos móviles, IBM puede proporcionarle las herramientas que necesita para ir más allá del paradigma tradicional de gestión de punto terminal. El informe de IBM [‘Managing the growing pains in today’s expanding networks’](#) describe tecnologías de gestión efectivas para ampliar entornos y presenta productos de gestión que podrán satisfacer sus necesidades exclusivas.

IBM ofrece toda la cobertura que necesita para optimizar redes, asegurar y gestionar dispositivos móviles, desarrollar con eficacia y seguridad aplicaciones móviles, controlar de forma segura y gestionar el acceso a los recursos y dar soporte a servicios gestionados y opciones de externalización. El informe de IBM [‘Getting a better grip on mobile devices’](#) describe cómo puede gestionar la carga de trabajo de TI adicional derivada de la gestión de dispositivos móviles.

Para más información

Si desea obtener información adicional acerca de las soluciones de IBM para dar soporte a implementaciones móviles en la empresa, póngase en contacto con su representante de IBM o IBM Business Partner (BP) o entre en: ibm.com/tivoli.

Acerca del software Tivoli de IBM

El software Tivoli de IBM está diseñado para ayudar a las organizaciones a gestionar sus recursos, tareas y procesos de TI de forma eficiente y efectiva, con el objetivo de dar respuesta a las cambiantes necesidades de las empresas y proporcionar un modelo de gestión de servicios de TI flexible y adaptable, que contribuya también a reducir los costes. La cartera de Tivoli incluye soluciones de software en el campo de la seguridad, el cumplimiento normativo, el almacenamiento, el funcionamiento, la disponibilidad, la configuración, las operaciones y la gestión del ciclo de vida de la TI, avaladas por los servicios, la asistencia y la investigación de primera clase de IBM. Para obtener más información sobre el software Tivoli de IBM, entre en: ibm.com/tivoli.

Por otra parte, IBM Global Financing puede ayudarle a adquirir las soluciones de TI que su empresa necesita de la forma más estratégica y rentable posible. Nos asociaremos con clientes con crédito para personalizar una solución de financiación de TI que se adapte a sus objetivos empresariales, permitir una gestión eficaz del dinero y mejorar su coste total de propiedad. IBM Global Financing es su elección más inteligente para financiar inversiones fundamentales en TI y propulsar su empresa. Si desea más información, visite: ibm.com/financing/es.



IBM España

Santa Hortensia, 26-28
28002 Madrid
España

La página principal de IBM es ibm.com/es.

IBM, el logotipo de IBM, ibm.com, Smarter Planet y Tivoli son marcas comerciales o marcas comerciales registradas de International Business Machines Corporation en los Estados Unidos y/o en otros países. Si éstas o cualquier otra denominación de IBM protegida por una marca van acompañadas, la primera vez que aparecen en el documento, de un símbolo de marca (® o ™), estos símbolos indican que se trata de marcas registradas o marcas de hecho en los Estados Unidos propiedad de IBM en el momento de publicación de la información. Es posible que estas marcas también estén registradas o sean marcas de hecho en otros países.

Encontrará una lista actual de las marcas de IBM bajo el título 'Copyright and trademark information' en ibm.com/legal/copytrade.shtml.

Los demás nombres de empresas, productos y servicios pueden ser marcas comerciales o marcas de servicio de terceros.

Las referencias efectuadas en este documento a productos, programas o servicios de IBM no implican que IBM tenga intención de comercializarlos en todos los países en los que opera.

¹ Borg, Andrew. 'Mobility Becomes Core IT', Aberdeen Group, SAP Mobility Insights Webcast Series, Part I, 29 de marzo de 2011.

http://event.on24.com/event/29/75/81/rt/1/documents/slidespdf/mobile_latest_march_28.pdf.

² Moerschel, Grant. 'Mobile Device Management', InformationWeek Reports, noviembre de 2011.

<http://reports.informationweek.com/abstract/18/8484/Mobility-Wireless/research-mobile-device-management.html>.

³ Wingfield, Nick. 'Once Wary, Apple Warms Up to Business Market', The New York Times, 15 de noviembre de 2011.

http://www.nytimes.com/2011/11/16/technology/businesses-too-have-eyes-for-ipads-and-iphones.html?_r=1&hpw.

Las referencias a productos, programas o servicios de IBM no pretenden dar a entender que sólo pueden utilizarse productos, programas o servicios de IBM. Se puede utilizar en su lugar cualquier producto, programa o servicio equivalente desde el punto de vista funcional.

Esta publicación sirve únicamente como orientación general.

La información está sujeta a cambios sin previo aviso. Póngase en contacto con la oficina de ventas o distribuidor local de IBM para obtener la información más reciente acerca de los productos y servicios de IBM.

IBM no ofrece asesoramiento jurídico, contable ni de auditoría ni manifiesta o garantiza que sus productos o servicios aseguren el cumplimiento de las leyes. Los clientes son responsables del cumplimiento de las leyes y normativas relativas a valores aplicables, incluidas las leyes y normativas nacionales.

© Copyright IBM Corporation 2013



Reciclar por favor