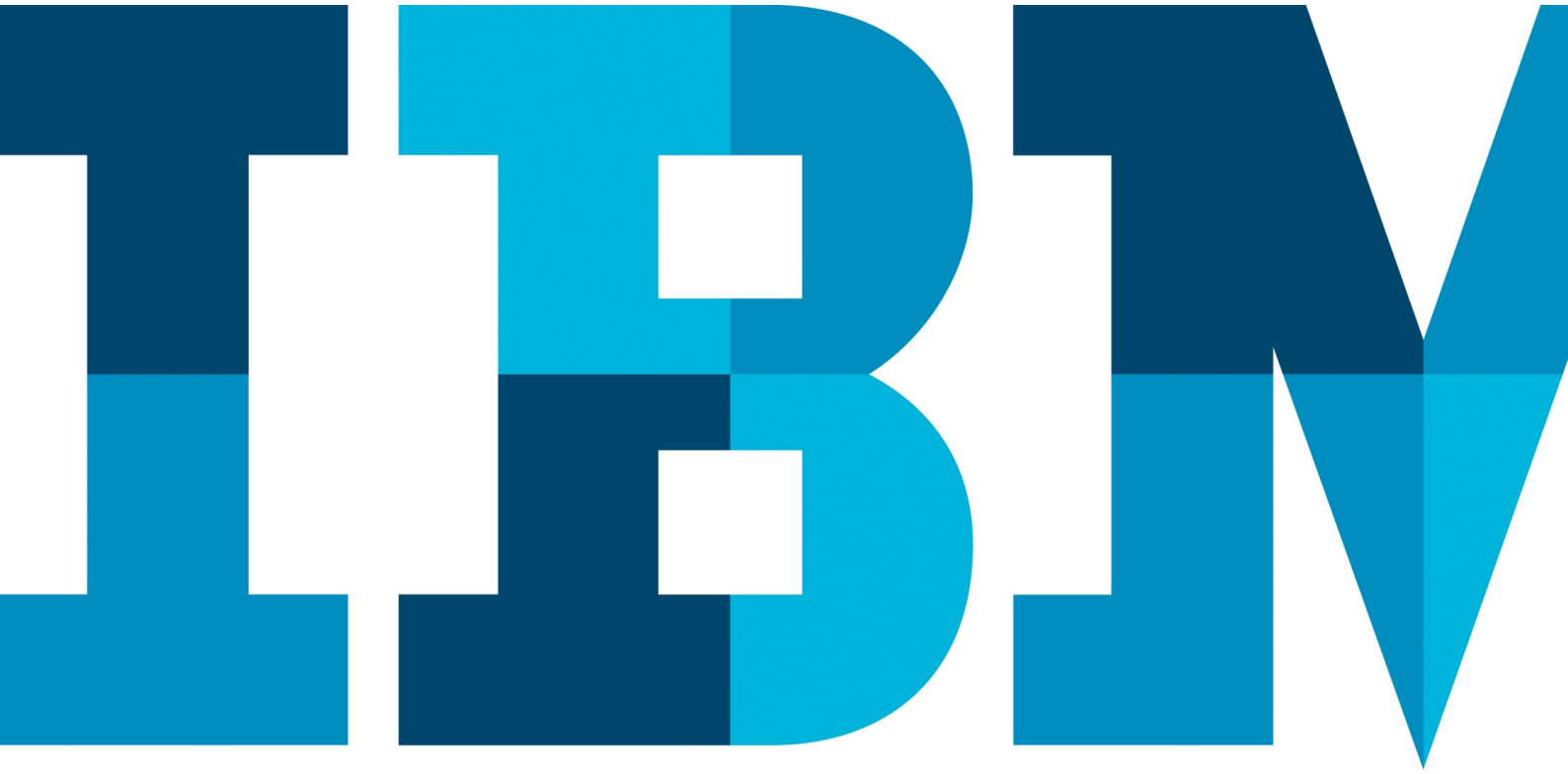
IBM Global Technology Services
Informe de liderazgo de pensamiento

Noviembre de 2012

# El lugar de trabajo flexible: Liberar el valor de la era ‘bring your own device’



IBM

## Contenidos

**2** Resumen ejecutivo

**2** Detrás del impulso de 'bring your own device' (BYOD)

**3** Adoptar BYOD en toda la organización

**4** Soporte de usuario final para BYOD

**4** Soluciones que se adaptan a su estrategia

**4** Viaje a la movilidad: Lecciones aprendidas

**6** Conclusión

**6** Para más información

## Resumen ejecutivo

Las ventas de smartphones y tabletas de medios como Apple iPad están aumentando y los analistas estiman que actualmente existen más de mil millones de smartphones en uso[1]. Aunque los avances en tecnología de consumo no sean ninguna novedad, lo que sí ha cambiado es el impulso para aprovechar los smartphones y tabletas con fines comerciales. Con la inauguración de la era BOYD en la consumerización de las TI, los empleados esperan tener un lugar de trabajo flexible, con acceso rápido a las aplicaciones y la información prácticamente desde cualquier lugar y en cualquier dispositivo.

Esta nueva mentalidad del cualquier momento y cualquier lugar ocasiona un impacto significativo y consecuencias en la organización TI, la cual debe intentar encontrar un equilibrio entre la promesa de una mayor productividad y satisfacción del usuario y las incertidumbres de seguridad que crea. Mientras que algunas empresas entregan smartphones y tabletas a sus empleados, una creciente mayoría de empleados traen dispositivos de propiedad personal al lugar de trabajo con fines comerciales, muchas veces sin la aprobación explícita de la empresa. En este artículo se explora la forma en que las organizaciones pueden generar valor de negocio en la era BOYD y seguir proporcionando una infraestructura TI segura y niveles de seguridad coherentes.

## Detrás del impulso de BYOD

Un reciente informe de Gartner llegaba a la conclusión de que 'el aumento de los programas BOYD es el cambio más radical experimentado en la economía de la informática de cliente en las empresas desde que el PC invadió el lugar de trabajo'[2]. Existen numerosos motivos subyacentes a la gran velocidad y amplitud con la que esta tendencia ha arraigado. Por ejemplo:

- Muchos de estos smartphones y tabletas, junto con el creciente número de aplicaciones móviles para la empresa, disponen de potentes capacidades y aplicaciones. En la actualidad superan en exceso las del dispositivo 'estándar' del departamento de TI, lo cual lo hace mucho más deseable.
- Los dispositivos móviles de consumo se han generalizado tanto en la vida diaria como consecuencia de los avances tecnológicos (por ejemplo, tamaño pequeño, activación instantánea, conectividad Internet inalámbrica, etc.) y por lo tanto se produce un nivel de confort que no existe con los dispositivos 'corporativos'. En realidad, esto refleja seguramente un cambio cultural tanto como uno tecnológico.
- Las empresas exigen a sus empleados hacer más con menos. El empleado actual es un trabajador del conocimiento cada vez más exigente y con más dominio tecnológico. Los empleados acude a todo aquello que les ayude a alcanzar dicho objetivo – y en muchos casos, no es el PC encadenado a un escritorio de oficina.
- Muchas empresas facilitan dispositivos de responsabilidad corporativa a un reducido subconjunto de la empresa, como pueden ser ventas. Aunque los requisitos de movilidad estén aumentando, la mayoría de empresas no amplían sus programas corporativos debido a presiones de coste. En su lugar, exploran el modelo con responsabilidad del empleado (BOYD) para prestar servicios móviles a una mayor población de usuarios con un menor coste.

## Adoptar BYOD en toda la organización

Puede ser tentador prohibir el uso de dispositivos de propiedad personal en la empresa como consecuencia del soporte añadido y la complejidad de la seguridad, pero las políticas corporativas que adoptan un enfoque restrictivo simplemente no se pueden aplicar. Los usuarios corporativos de smartphones y tabletas pueden omitir la política corporativa y poner en grave riesgo a la empresa. Por ejemplo, los usuarios pueden reenviar correo corporativo, documentos y presentaciones a servicios de consumo como Google Mail o Dropbox para que sean accesibles desde sus smartphones y tabletas, creando una especie de 'infraestructura a la sombra' en la cual las empresas tienen poco control y hace aumentar el riesgo de fugas de datos. Además, la no adopción de BOYD también puede conducir a una satisfacción más baja del empleado y a la dificultad de atraer y retener el mejor talento.

*'Los directores TI y directores del departamento de información (CIOs) deben darse cuenta de que aunque no permitan utilizar sus propios dispositivos, encontrarán métodos alternativos y BOYD seguirá existiendo en la empresa. Los departamentos de TI deberán encontrar el equilibrio correcto entre ofrecer a los empleados la flexibilidad para utilizar dispositivos propios y los riesgos de seguridad y costes potenciales que supone la adopción de BYOD'. IDC, 'Addressing security issues and concerns of BYOD Initiatives,' Junio de 2012.*[3]

¿Cómo puede decirse 'sí' a los dispositivos personales sin tener que desordenar el gobierno, la seguridad, la integración y el soporte? Adoptando un enfoque metódico en lugar de uno reactivo. Algunos de los temas claves a considerar son los siguientes:

- Soporte de dispositivo móvil – ¿Qué dispositivos móviles admitirá? ¿Qué trabajo debe realizarse y dónde? Mientras que el soporte de una gran variedad de dispositivos móviles probablemente aumentará la satisfacción del usuario final, este soporte también puede incrementar los costes, la complejidad y los plazos de despliegue. Por ejemplo, el desarrollo, el despliegue y la protección de aplicaciones móviles para varias plataformas (por ejemplo, Apple iOS, Google Android, RIM BlackBerry, Windows® Phone, etc.).
- Cultura corporativa y política corporativa – ¿Define su empresa una política para el uso de dispositivos de propiedad personal? ¿Es voluntaria dicha política? ¿A qué datos corporativos puede accederse? ¿Cuál es la política de seguridad? ¿Tendrá una política de reembolso de los gastos de móviles? (por ejemplo dispositivo, voz, datos) ¿Cuál es la cultura corporativa para los trabajadores móviles y está alineada con la estrategia de la organización? ¿Necesita separar los datos personales y del trabajo en los dispositivos móviles? ¿Dispone de una estrategia para gestionar los dispositivos perdidos o robados y la separación del empleado?
- Tecnologías de la información (TI) – ¿Qué soluciones TI necesita para implementar su estrategia? ¿Cómo gestiona y protege los dispositivos móviles? ¿Cuál es su estrategia para las aplicaciones móviles? ¿Cómo dará soporte a una amplia gama de dispositivos móviles? ¿Cómo supervisará el cumplimiento normativo de la política corporativa?

## Soporte de usuario final para BYOD

Ante la necesidad de dar soporte a una amplia gama de smartphones y plataformas, el centro de atención al cliente puede verse rápidamente saturado. El autoservicio de soporte y la automatización pueden ayudar a resolver estos problemas. Las capacidades concretas pueden ser las siguientes:

- Documentación online actualizada con los dispositivos, plataformas y servicios proporcionados y las responsabilidades de los empleados
- La capacidad para activar online un nuevo dispositivo sin interacción administrativa
- Uso intensivo de las redes sociales dentro de la empresa para utilizar el 'sentido común'. Esto es crítico, ya que cada semana se publican nuevas versiones de dispositivos y sistemas operativos
- La capacidad para llevar a cabo tareas comunes online, incluyendo el restablecimiento y borrado de dispositivos.

## Soluciones que se adaptan a su estrategia

Una vez haya considerado detenidamente su estrategia BOYD, querrá explorar las soluciones TI que pueden desarrollarla con éxito. A continuación encontrará algunos de los temas clave a considerar:

- **Seguridad:** ¿Cómo gestionará y protegerá los dispositivos móviles y los datos? ¿Necesita segregar los datos personales y los del trabajo? ¿Cómo elimina los datos corporativos si el empleado deja la empresa o cambia de cargo en el trabajo? ¿Cómo comprueba la postura de seguridad del dispositivo antes de permitirle que se conecte a la red corporativa? (por ejemplo, ¿se ha desbloqueado o 'pirateado' el dispositivo?)
- **Aplicaciones:** ¿Qué aplicaciones utilizarán los usuarios? ¿Su disponibilidad es directa? ¿Son web, nativas, híbridas o virtuales? ¿Cumplen mis requisitos de seguridad? ¿Necesito crear aplicaciones personalizadas? ¿Necesita explorar plataformas de aplicación de empresa móvil? (MEAP). ¿Cómo desplegará y gestionará la aplicación? ¿Necesita una tienda de aplicación de empresa para gestionar y distribuir aplicaciones? ¿Debe prohibir las aplicaciones a las que los usuarios pueden acceder en sus dispositivos móviles? ¿Existen aplicaciones necesarias que deben ejecutarse en el dispositivo? ¿Existen aplicaciones que no se pueden ejecutar en el dispositivo? ¿Cómo actualizará las aplicaciones?
- **Red:** ¿Cómo conectarán los usuarios sus dispositivos a la red corporativa a través de Wi-Fi y teléfono móvil? Si los empleados se conectan a la red Wi-Fi corporativa, ¿existe una cobertura y una capacidad Wi-Fi adecuada? Si los empleados se conectan desde el exterior, ¿necesito una o varias soluciones de red privada virtual (VPN)? ¿Cómo gestionará la complejidad añadida y el mayor tráfico de red que pueden causar estos dispositivos?
- **Soporte:** ¿Cómo proporcionará soporte para varios dispositivos? ¿Automatizará tareas comunes tales como el registro de dispositivos para reducir la sobrecarga administrativa? ¿Cómo formará a los empleados en la forma de utilizar eficazmente los dispositivos móviles?

## Viaje a la movilidad: Lecciones aprendidas

Más de la mitad de la población mundial de empleados de IBM® es móvil. La compañía necesitaba ampliar su programa de movilidad corporativa – lanzado en el 2004 con un único dispositivo facilitado por la empresa – para acoger una mayor variedad de nuevas plataformas móviles que se introducen en el lugar de trabajo. En el 2009, IBM llevó a cabo una campaña agresiva para dar soporte a la movilidad de empresa y a los smartphones y tabletas en concreto.

En el transcurso de tres años, IBM creó un programa piloto de acceso móvil con diferentes dispositivos y sistemas operativos, incorporando nuevos elementos tales como tabletas a medida que el mercado los producía. El software de colaboración de IBM se convirtió en una parte integral de la solución. En el 2011 se puso en marcha el despliegue de producción a gran escala, en el que se contemplaba la movilidad como un servicio de infraestructura central y con más de 100.000 usuarios de smartphones y tabletas con acceso a la red corporativa de IBM. En la actualidad, el programa cubre 120.000 usuarios móviles, incluyendo 80.000 dispositivos personales, y sigue ampliándose.

Algunas de las lecciones más importantes aprendidas son las siguientes:

- Los empleados se encargan de los smartphones y tabletas de propiedad (y financiación) personal.
- Los empleados quieren utilizar un único smartphone para uso personal y de trabajo. La mayoría de usuarios no quieren utilizar dos smartphones – uno para el trabajo y otro para uso personal.
- La mayoría de empleados cuidan los dispositivos y plataformas que IBM ha optado por soportar (por ejemplo Android 2.2+, iPhone 3GS+, BlackBerry, etc.). Sin embargo, existen dispositivos y plataformas adicionales que piden los empleados y que no pueden admitirse por motivos de seguridad.
- En general, los empleados aprecian la necesidad de imponer políticas de seguridad en el dispositivo. No obstante, esto ha supuesto un impedimento para algunos usuarios. El mayor motivo de insatisfacción del cliente es la contraseña alfanumérica de ocho caracteres para desbloquear el dispositivo. Los empleados desean tener mejores técnicas de autenticación y la posibilidad de que se les pida una contraseña cuando accedan a datos del 'trabajo'.
- Por motivos de seguridad, deben existir mejores soluciones de contenediración para separar los datos personales de los del trabajo y la capacidad para gestionar todos los datos del trabajo como un único contenedor. Este disminuye la necesidad de proteger individualmente cada una de las aplicaciones.
- La limpieza remota de todo un dispositivo no es popular entre los empleados. Los empleados aplauden las mejoras realizadas en Lotus Traveler que permiten la limpieza remota de datos solamente corporativos (por ejemplo, el correo).
- Soluciones cloud basadas en navegador, como la modalidad ultraligera de IBM Lotus iNotes, proporciona flexibilidad, reduce las dependencias de dispositivo y resuelve las dudas sobre la seguridad de los datos en reposo.
- Con varias opciones de smartphones y tabletas, necesitábamos dar instrucciones a los empleados para que puedan tomar decisiones informadas sobre cuál era el mejor dispositivo para sus necesidades concretas.
- El uso del proxy de capa de sockets seguros (SSL) sin cliente de Lotus Mobile Connect proporcionó la mejor experiencia de usuario final en Apple iOS y Google Android. No obstante, esto exigió el uso de una solución separada de cliente VPN para el acceso general a la red corporativa.
- Los empleados eran receptivos a las opciones de autoservicio de soporte, incluyendo la incorporación automatizada y los diagnósticos.

### Cronología de IBM Mobile

**2004 - 2007: El smartphone BlackBerry es la única opción, con acceso limitado de los empleados.**

**2008: Prueba limitada de concepto para Windows Mobile que utiliza IBM Lotus Traveler.**

**2009: Lanzamiento de la prueba piloto y su ampliación para incluir Nokia y Apple iOS, así como adopción de modelos de propiedad personal con acceso ampliado a través de Lotus Traveler.**

**2010: Finalización de la prueba piloto e inicio del despliegue de producción. Ampliación del soporte de plataforma para incluir Apple iPad y Google Android.**

**2011: Se ofrecen despliegues de producción a gran escala para dar soporte a un mayor uso del móvil como dispositivo informático principal (sustituyendo al portátil), con clientes móviles nativos para Sametime Instant Messaging, IBM Connections y Symphony Viewers en Apple iOS y Android además de una aplicación móvil personalizada, desarrollada internamente y desplegada a través de una tienda de aplicaciones interna.**

**2012: Lanzamiento de la iniciativa IBM Mobile Enterprise. Lanzamiento cruzado de software, hardware y servicios de IBM para ayudar a los clientes a transformar sus empresas con soluciones de movilidad para aplicaciones "front-office" y "back-office".**

## Conclusión

Lejos de disminuir, el impulso de BOYD sigue ampliándose y cada vez son más los empleados que exigen un lugar de trabajo flexible que les permita acceder a las herramientas que necesitan en cualquier lugar y desde cualquier dispositivo. Las organizaciones avanzadas buscan los medios para implementar satisfactoriamente un entorno móvil flexible que soporte las opciones de los empleados, permite el acceso seguro a los datos y las aplicaciones de empresa y permite la coexistencia de dispositivos de propiedad personal en la infraestructura con dispositivos inalámbricos corporativos y de propósito especial. Dicha transformación ya se produce en IBM.

Además de nuestra propia transformación bien documentada en una empresa móvil, IBM ha estado proporcionando soluciones de movilidad para cientos de clientes durante más de 15 años. Los profesionales de IBM han desarrollado sólidas soluciones para dar soporte a las necesidades de seguridad, soporte y aplicaciones globales, permitiendo la expansión de nuestros servicios a otras importantes plataformas y dispositivos móviles. Respaldado por un amplio ecosistema de Business Partners (BP), IBM puede ayudarle a conocer los requisitos de los móviles, empezar a evaluar su entorno actual y diseñar una estrategia para la gestión de dispositivos móviles.

## Para más información

Si desea obtener más información sobre IBM Enterprise Services – managed mobility services, póngase en contacto con su representante comercial de IBM, BP de IBM o visite la siguiente página web: **ibm.com**/services/mobility

**IBM España, S.A.**
Tel.: 901 100 400
C/Sta. Hortensia, 26-28
28002 Madrid
España

La página de IBM se puede encontrar en **ibm.com**



[1] Strategy Analytics, 'Global Smartphone Installed Base Forecast by Operating System for 88 Countries: 2007 to 2017.' Octubre de 2012.

[2] Gartner, 'BYOD: New Opportunities, New Challenges', agosto de 2012. Doc # G00238131

[3] IDC, 'Addressing Security Issues and Concerns of BYOD Initiatives.' Junio de 2012. Doc # AE53U



ENW03010-ESES-02