# La guía definitiva sobre BYOD (uso de dispositivos móviles personales en la empresa)

MobileIron®

www.mobileiron.com

# CONTENIDO

# BYOD o el uso de dispositivos móviles personales en la empresa: fomentar la transformación corporativa móvil

La velocidad a la que las empresas están adoptando la tecnología móvil es mucho más que una evolución; es una transformación global. De hecho, considerando la rapidez con la que usuarios y empresas de todo el mundo están abandonando su dependencia del PC a favor de los dispositivos móviles, IDC predijo que las ventas de PC caerían hasta cifras récord en 2013.

La enorme popularidad de los dispositivos móviles y de las aplicaciones rerpesentauna gran oportunidad para que cualquier compañía se convierta en una organización de tipo «Mobile First», es decir, que asuma la movilidad como la tecnología con mayor proyección para las empresas en la actualidad. Las organizaciones *Mobile First* comprenden que la tendencia *Bring Your Own Device* («Trae tu propio dispositivo») o BYOD ha llegado para quedarse, y que está impulsada por los usuarios que esperan una flexibilidad total a la hora de administrar sus asuntos profesionales y personales estén donde estén, en el dispositivo que ellos elijan. Sin embargo, la capacidad de habilitar de forma segura y rentable el sistema BYOD presenta un reto considerable, incluso para las empresas más vanguardistas.

Proteger los datos corporativos y los recursos de la red a la vez que se aprovechan las ventajas de la movilidad es un acto de equilibro constante, que requiere que el departamento informático deje de centrarse en el bloqueo de la seguridad y pase a centrarse en la preparación de las empresas. Aunque algunas empresas (sobre todo en el sector de la tecnología) están «haciendo» bien el proceso de BYOD, la mayoría siguen intentando trazar una estrategia integral de prácticas recomendadas para asegurar y habilitar los dispositivos personales en el entorno laboral. Muchas organizaciones están sencillamente descubriendo sobre la marcha cómo funciona, dejando tanto al departamento informático como a los empleados con muchas dudas sobre las políticas y expectativas exactas sobre el uso y la administración de dispositivos personales.

Por ejemplo:

- ¿Cuánto control debe ejercer la empresa sobre el dispositivo y el contenido del empleado?
- ¿Quién debe costear el dispositivo y el servicio mensual?
- ¿Qué se considera un acuerdo de usuario final razonable?
- ¿Qué dispositivos debe admitir la empresa?
- ¿Qué ocurre con los datos corporativos en un dispositivo personal cuando el empleado se va de la empresa?

Este eBook está diseñado para ayudarle a su organización a anticipar, comprender y gestionar estas y otras preguntas sobre el sistema BYOD en la empresa. En esta guía formada por cuatro partes, analizaremos las prácticas recomendadas para preparar, crear, lanzar y mantener un exitoso programa de BYOD a largo plazo.

# Determinar su tolerancia a los riesgos del programa BYOD

La movilidad está abriendo los datos y las aplicaciones a una cantidad inimaginable de usuarios, en cualquier dispositivo y prácticamente en cualquier parte del mundo. Pero, ¿cómo pueden las organizaciones sacar el máximo partido al potencial corporativo de la transformación móvil sin que ello afecte a la seguridad y a la productividad?

Identificar la tolerancia de su empresa a los riesgos es el primer paso para comprender cómo puede funcionar el sistema BYOD en su organización. El sector al que pertenece su empresa puede ser un indicador relevante para determinar la tolerancia a los riesgos. Por ejemplo, las organizaciones que están en los sectores de la atención médica, los servicios financieros, el gobierno o los servicios de seguridad, es probable que adopten una postura más defensiva hacia el sistema BYOD que las empresas tecnológicas basadas en Internet.

Completar una evaluación de tolerancia a los riesgos del sistema BYOD le ayudará a identificar áreas de particular interés o preocupantes para su organización. Además, le permitirá hacerse una buena idea de la tolerancia de su empresa a la flexibilidad de los empleados, la gama de dispositivos permitidos, la participación del departamento informático y las políticas de seguridad. Es pocas palabras, identificar su tolerancia a los riesgos es un buen punto de partida para garantizar que su programa de BYOD se adapta a la cultura de su empresa y a sus objetivos corporativos sin afectar a la seguridad ni a la satisfacción de los empleados.

# Involucrar pronto a las partes interesadas para definir los objetivos del programa

Uno de los pasos más importantes para desarrollar un programa BYOD es conseguir la aprobación inicial de las personas clave en la empresa. Aunque puede resultar difícil conciliar los intereses de los diferentes líderes de la empresa: dirección ejecutiva, RRHH, departamento legal, financiero e informático, su apoyo es fundamental para garantizar una financiación y un impulso adecuados al programa.

Si bien la aprobación de las partes interesadas a nivel ejecutivo es esencial, también habrá que asegurarse de que el programa cumpla con las necesidades y expectativas de los usuarios finales. En general, los usuarios móviles esperan tener acceso a los datos que necesitan tanto para trabajar como para sus asuntos personales, en el dispositivo que elijan y estén donde estén. Cualquier programa de BYOD que no cumpla con estos requisitos será probablemente rechazado por la mayoría de los usuarios móviles. Para evitar que esto ocurra, puede incorporar a uno o dos representantes de los empleados al equipo para que le ayuden a hacerle llegar las valiosas opiniones y comentarios sobre las preferencias de los usuarios finales, requisitos de los dispositivos, asistencia técnica, necesidades de comunicación, etc.

La anticipación de las objeciones más comunes al sistema BYOD también le ayudará a facilitar la fase de planificación. Estas son las respuestas a algunas de las típicas preocupaciones que suelen plantearse durante esta fase:

| PATROCINIO EJECUTIVO | RECURSOS HUMANOS | FINANZAS | DEPT. INFORMÁTICO |
|---|---|---|---|
| **No podemos conseguir la aprobación de la dirección ejecutiva, pero avancemos de todos modos con el plan BYOD.** | **No se puede hacer responsable a la empresa de los datos personales en riesgo en los dispositivos propiedad de los empleados.** | **No podemos financiar un programa que no ofrezca un ahorro de costes demostrado.** | **No podemos admitir la gran variedad de aplicaciones que la empresa quiere en los dispositivos personales.** |
| Es sencillo y claro: un proyecto BYOD puede fracasar fácilmente si no cuenta con el apoyo de la alta dirección. Como los proyectos BYOD requieren la participación de diferentes partes interesadas, normalmente es necesario un liderazgo ejecutivo para garantizar que se cumplan los plazos y las responsabilidades. | El departamento de RRHH y el informático deben trabajar conjuntamente para definir los límites claros entre los datos corporativos y personales. Además, su acuerdo de usuario final debe especificar que la empresa podrá acceder a los datos personales si el dispositivo está sujeto a un análisis forense. Asimismo, tras dejar la empresa, se hará todo lo posible por conservar los datos personales en el dispositivo del empleado, pero también se podrá realizar un borrado total de los datos si fuera necesario. | En realidad, se puede ahorrar reduciendo la asistencia técnica y los costes operativos mediante un modelo de usuario final y autoservicio que aproveche las herramientas de autoayuda, las comunidades de asistencia técnica para usuarios, las redes sociales y los foros de usuarios. | Para implementaciones de iOS: los nuevos controles disponibles con AppConnect permiten mover, añadir y cambiar las configuraciones y políticas de las aplicaciones sin tener que implementar nuevas versiones de las aplicaciones. Si se tiene la posibilidad de modificar o actualizar dinámicamente las políticas de seguridad, el acceso de los usuarios y las configuraciones del servidor en las aplicaciones móviles ya implementadas, se reducirán los gastos generales operativos de la gestión de aplicaciones móviles. |

Para ayudarle a solucionar estas y otras preocupaciones desde el principio, deberá crear un comité de dirección BYOD formado por representantes de todos los departamentos involucrados. Este comité de dirección podrá ayudar a que los grupos con distintas prioridades creen consenso y definan objetivos del programa con los que estén de acuerdo todas las partes interesadas. La documentación de estos objetivos servirá como recurso de utilidad para ayudar a que todas las partes implicadas mantengan el foco en los objetivos generales a medida que el programa BYOD va evolucionando.

# Dialogar y comunicarse con los empleados

Créelo y ya vendrán, ¿no? Bueno, no necesariamente. Un programa de BYOD que sea demasiado restrictivo o que carezca de compatibilidad para los dispositivos adecuados terminará en falta de participación y en tiempo y en dinero perdidos. Para evitar estos inconvenientes, debe recopilar las opiniones de los empleados al principio de la fase de preparación.

Una vez que haya determinado la tolerancia a los riesgos del sistema BYOD de su empresa y los objetivos de las partes interesadas, el siguiente paso es realizar una breve pero específica encuesta para los empleados de toda la empresa. Cuanto mayor sea su tolerancia a los riesgos, más importante será adaptar el cuestionario para que refleje las preferencias de los usuarios sobre dispositivos, aplicaciones, herramientas de comunicación y asistencia técnica. Para garantizar que recopila la información necesaria para diseñar un programa BYOD de éxito, su encuesta debe incluir preguntas que identifiquen:

- Qué SO/dispositivos tienen actualmente los empleados y cuáles tienen previsto comprar en el futuro
- Qué factores motivarían su participación en el programa BYOD
- Qué factores desmotivarían su participación en el programa BYOD
- Qué aplicaciones corporativas valoran más
- Hasta qué punto se siente cómodos con la asistencia técnica de autoservicio
- Los efectos del programa BYOD en la percepción, la productividad y el equilibrio personal/profesional de la empresa

# Identificar su capacitación en tecnología móvil

Una vez que conoce su tolerancia a los riesgos del programa BYOD, los objetivos del programa y las preferencias de los usuarios, ¿sabe si cuentan con las personas y recursos adecuados para desarrollar el programa que su empresa necesita y los usuarios desean? una evaluación de su capacitación le ayudará a determinar si dispone de las personas, procesos y tecnología adecuados para permitir a los empleados que utilicen sus dispositivos y aplicaciones preferidos y accedan de forma segura a los datos corporativos en cualquier red.

En realidad, una evaluación de capacidades es sencillamente una lista de verificación de requisitos, el estado actual o la disponibilidad y la identificación de dónde se encuentra dicha capacidad o tarea en el proceso de obtención. Por ejemplo, una lista de verificación para el personal del departamento informático deberá reflejar todos los recursos necesarios para implementar el programa, estén ya disponibles o no así como indicar quién es el responsable de incorporar todas esas personas al equipo.

A continuación se muestra un resumen de algunos de los requisitos de personal que deberán estar incluidos en la evaluación de capacidades de BYOD:

| **Suficiente personal** | *Ponga una 'X' en la columna adecuada* | | | | |
|---|---|---|---|---|---|
| | **Listo** | **Planificado** | **Inexistente** | **N/A** | **Comentarios** |
| **Recursos informáticos** | | | | | |
| **Exportaciones de dispositivos** | | | | | |
| **Blackberry: <enumerar los nombres>** | | | | | |
| **iOS: <enumerar los nombres>** | | | | | |
| **Android: <enumerar los nombres>** | | | | | |
| **Windows Phone: <enumerar los nombres>** | | | | | |
| **Pruebas en dispositivos** | | | | | |
| **Proceso de diseño: <enumerar los nombres>** | | | | | |

# Actualizar su infraestructura para que admita el programa BYOD (continuación)

Las habilidades tecnológicas necesarias para administrar una infraestructura informática móvil son drásticamente diferentes de las que se precisan para dirigir una empresa tradicional con equipos de sobremesa. Adquirirlos conocimientos adecuados resulta crítico para llevar a cabo un programa BYOD con éxito. Estas son las funciones recomendadas que necesitará para crear y mantener un programa BYOD (tenga en cuenta que una sola persona puede realizar muchas tareas; no es necesario dedicar una persona para cada tarea).

## INGENIERO DE SISTEMAS MÓVILES

El ingeniero de sistemas móviles es un experto en todo lo relacionado con la tecnología móvil. Esta función abarca todo el hardware, software y tecnologías de red necesarias para implementar un programa BYOD. El ingeniero de sistemas móviles tiene además conocimientos específicos sobre cómo integrar las tecnologías móviles con componentes corporativos como la identidad, mensajería, seguridad, redes y servicios de base de datos. Sus conocimientos incluyen las siguientes áreas:

- Sistemas operativos móviles, como iOS, Android y Windows Phone 8
- Tecnologías de red de operadores, como GSM/CDMA/LTE y otros protocolos subyacentes
- Hardware móvil, software, aplicaciones, interfaces de programación de aplicaciones (API) y kits de herramientas de desarrollo

## EXPERTO EN DISPOSITIVOS MÓVILES

El experto en dispositivos móviles es un «fanático de los gadgets» que siempre está al día de los dispositivos actuales y futuros, así como de los lanzamientos de software, que pueden influir en la infraestructura móvil. Como siempre está al día en tendencias y tecnología móvil, el experto en dispositivos puede preparar el entorno para que admita o restrinja el uso de nuevos dispositivos. Además, el experto en dispositivos conoce a la perfección las plataformas y fabricantes más populares, como por ejemplo:

- Android: Samsung, Motorola, HTC, LG, Sony Ericsson, Huawei, Dell, Lenovo, Acer, Asus
- Windows Phone 8: Nokia, HTC, Samsung
- iOS: todos los dispositivos Apple
- Blackberry: todos los dispositivos Blackberry

## EXPERTO EN SEGURIDAD MÓVIL

El experto en seguridad móvil es responsable de establecer las políticas y controles de seguridad móvil, así como de determinar su efectividad y revisarlas cuando sea necesario. El experto en seguridad móvil se dedica además a informar a los usuarios sobre los riesgos de seguridad social y conductual, a establecer políticas de uso adecuadas y a ayudar a desarrollar estrategias para:

- Seguridad móvil y mitigación de riesgos
- Protección de datos móviles
- Revisión y posicionamiento de plataformas de SO móviles
- Administración de amenazas de aplicaciones móviles

## DESARROLLADOR DE APLICACIONES MÓVILES

Independientemente de si su empresa desarrolla sus propias aplicaciones o subcontrata el desarrollo de aplicaciones móviles a terceros, es posible que necesite desarrolladores de aplicaciones internos con las siguientes habilidades:

- Experiencia en ciclos de vida y metodologías de desarrollo de aplicaciones
- Capacidad de diseñar y desarrollar aplicaciones para Android y Windows Phone 8
- Experiencia práctica con Objective-C, Cocoa Touch, iOS SDK, XCode, programas Developer, Java, Android Market, Android SDK y API de fabricantes de dispositivos, .NET, Web Services, XML y HTML5
- Habilidades de programación y diseño muy orientadas a objetos

## SERVICIOS MÓVILES Y RECURSOS DE ASISTENCIA TÉCNICA

El rápido ciclo de vida de los dispositivos y servicios móviles precisa de una infraestructura que pueda adaptarse rápidamente a las condiciones en constante evolución. Para responder de forma eficiente, su empresa debe personalizar el modo en que hace llegar los servicios y la asistencia técnica a los usuarios móviles, ya que sus necesidades y expectativas son muy diferentes a los de los usuarios de PC. Para ser eficientes, los servicios móviles y recursos de asistencia técnica deben ser capaces de:

- Proporcionar herramientas de autoservicio para ayudar a mejorar la satisfacción del usuario y reducir costes
- Establecer un grupo de asistencia técnica móvil básica que administre todas las ampliaciones móviles
- Desarrollar y distribuir artículos de la base de conocimientos, guiones de asistencia técnica y procedimientos a todos los usuarios
- Compartir conocimientos a través de las redes sociales y comunidades móviles
- Establecer una comunicación clara y frecuente por múltiples canales para mantener a los usuarios actualizados sobre el estado y los cambios del servicio

# Los ocho componentes de una buena estrategia BYOD

El reto máximo para cualquier programa BYOD no consiste solo en administrar la seguridad de los datos y optimizar la productividad del usuario final, sino que se trata de mantener un equilibrio constante entre seguridad, cumplimiento, responsabilidad legal, preocupación por los costes y una experiencia de usuario positiva. Los ocho componentes de una buena estrategia BYOD están diseñados para ayudarle a crear un programa sostenible que cumpla las necesidades de su empresa y sus empleados a largo plazo.

## LOS OCHO COMPONENTES DE UNA BUENA ESTRATEGIA BYOD (CONTINUACIÓN)


Estos componentes son los ingredientes esenciales que garantizan que su estrategia BYOD pueda cumplir los requisitos de seguridad, control de costes, responsabilidad, productividad y satisfacción de los usuarios.

*Los ocho componentes de una buena estrategia BYOD (continuación)*

## 1 SOSTENIBILIDAD:

### Mantener una experiencia de usuario positiva

El BYOD es una tendencia relativamente nueva que todavía está en proceso de establecer sus prácticas recomendadas. Como resultado, muchas empresas se apresuran a crear políticas y procesos que terminan no siendo sostenibles a largo plazo. Como es lógico, las empresas están preocupadas principalmente por los costes de implementación y la seguridad, por lo que tienden a centrarse en esos problemas al principio. Pero si no se respeta la experiencia del usuario, puede que el programa BYOD nunca llegue a despegar.

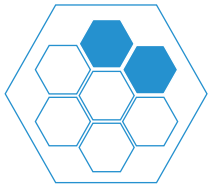
El motivo es el siguiente: si las políticas BYOD son demasiado restrictivas, carecen de la compatibilidad adecuada para los dispositivos preferidos de los empleados o sencillamente resultan demasiado complejas y confusas, los empleados encontrarán cualquier excusa para evitar dichas políticas o dejar de participar en ellas. En ambos casos las necesidades de la empresa no se cumplen, ya que la seguridad se ve afectada o el valor de negocio se pierde. Por tanto, si bien las preocupaciones por los costes y la seguridad son temas importantes a tratar, la sostenibilidad del programa BYOD dependerá totalmente de si se ofrece una experiencia de usuario que resulte siempre positiva a largo plazo.

## 2 MODELO DE CONFIANZA:

### Mitigar los riesgos de seguridad

Hace mucho tiempo, los equipos de sobremesa propiedad de la empresa eran los pocos dispositivos de los empleados que las empresas tenían que administrar. Actualmente, la empresa media utiliza diferentes dispositivos para trabajar, como equipos de sobremesa, ordenadores portátiles, tabletas y *smartphones*. La administración de la gran cantidad y variedad de dispositivos –ya sean propiedad del empleado o de la empresa– ha introducido problemas de seguridad sumamente dinámicos y complejos. Por lo tanto, es absolutamente esencial crear un modelo de confianza que identifique cómo y cuándo un dispositivo está infringiendo el cumplimiento, los pasos para remediarlo y el alcance hasta que estas medidas sean aceptables para los usuarios. El modelo de confianza debe:

- Evaluar el riesgo de los problemas de seguridad más comunes en los dispositivos personales.
- Indicar las medidas para remediarlo (como las notificaciones, control de acceso, cuarentena o borrado selectivo) que se activarán dependiendo de las preocupaciones de seguridad y de si el dispositivo es propiedad de la empresa o del empleado.
- Establecer políticas por niveles para la seguridad, privacidad y distribución de aplicaciones basándose en la propiedad del dispositivo.
- Establecer claramente la identidad del usuario y del dispositivo mediante certificados u otros medios.
- Garantizar que las políticas de seguridad sean suficientemente sostenibles y flexibles como para respaldar una experiencia de usuario positiva sin comprometer la seguridad de los datos.





## 3 SELECCIÓN DE DISPOSITIVOS:

### Un concurso de popularidad

A partir de las opiniones obtenidas en la encuesta inicial a los empleados, ya debería haberse hecho una buena idea de qué dispositivos y plataformas utilizan actualmente los empleados y tienen pensado comprar. Cuando se lance el programa, debe incluir tantos de estos dispositivos como sea posible para maximizar la participación de los empleados. Además, su proceso de selección de dispositivos debería:

- Incluir todas las plataformas móviles deseadas en el programa, siempre que cumplan con sus requisitos de seguridad y asistencia técnica, como la administración de activos, cifrado, política de contraseñas, bloqueo/borrado remoto y configuración de correo electrónico/Wi-Fi/VPN. Sin estos elementos básicos, la plataforma móvil no será viable para la empresa.
- Desarrollar un plan de certificación para garantizar que los futuros dispositivos se puedan evaluar de forma rápida y eficiente para una posible inclusión en su programa.
- Identificar claramente qué dispositivos están (o no) permitidos y por qué; de lo contrario, los empleados podrían comprar dispositivos que su programa no admita.
- Asegurarse de que su equipo informático mantiene los conocimientos y experiencia sobre los dispositivos móviles y sistemas operativos en constante evolución; de lo contrario, su programa de BYOD puede quedar obsoleto rápidamente.

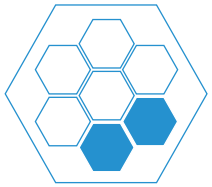
## 4 RESPONSABILIDAD:

### Proteger a su empresa de acciones legales

La implantación de un programa BYOD puede suponer además nuevos retos relativos a la responsabilidad en la que se verá implicada su empresa. Como parte de su programa de BYOD, necesitará políticas y procedimientos claros que protejan a su empresa de las diferentes amenazas, como la pérdida de propiedad intelectual y de datos confidenciales de los clientes, hasta acciones legales, multas y daños a la reputación resultantes del filtrado de datos.

Si bien todas las empresas deben buscar asesoramiento legal específico sobre responsabilidad en BYOD, su política de dispositivos móviles o acuerdo de usuario final debería incluir, como mínimo:

- Políticas de seguridad para datos corporativos en los dispositivos personales (sobre todo, porque pueden ser necesarios diferentes tipos de seguridad en diferentes dispositivos. Por ejemplo, puede requerir una mayor protección contra aplicaciones de consumidores con demasiados privilegios en Android en comparación con iOS).
- Políticas para webs personales y uso de aplicaciones (durante y después del horario laboral, tanto en las instalaciones de la empresa como fuera de ellas).
- Limitaciones claras sobre la responsabilidad de la empresa, debido a la pérdida de datos personales del propietario del dispositivo.
- Comprender cómo el reembolso de BYOD (remuneración parcial comparado con el pago total de los costes del servicio) afecta a la responsabilidad de la empresa.
- El alcance de la responsabilidad de la empresa por pérdida de datos personales (por ejemplo, si el departamento informático realiza accidentalmente un borrado total de los datos en un dispositivo personal).





## 5 EXPERIENCIA Y PRIVACIDAD DEL USUARIO:

### Establecer la confianza de los empleados

Optimizar la experiencia del usuario debe ser una de las principales prioridades de su programa BYOD. Una comunicación clara sobre temas sensibles como la privacidad, resulta fundamental para establecer la confianza de los empleados. Por tanto, se debe establecer un contrato social que defina claramente la relación del programa BYOD entre la empresa y los empleados. El contrato es un acuerdo bien definido que ayuda a:

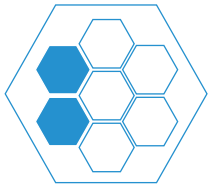
- Identificar las actividades e información que el departamento informático supervisará en el dispositivo, como el inventario de aplicaciones, para protegerlo frente a aplicaciones no autorizadas que podrían afectar a los datos corporativos.
- Aclarar qué medidas de seguridad llevará a cabo el departamento informático para responder a ciertas circunstancias.
- Definir los controles pormenorizados, como la supervisión de actividades, el seguimiento de localizaciones y la visibilidad de aplicaciones.
- Evaluar de forma crítica las políticas de seguridad y restricciones para garantizar que no sean demasiado restrictivas.
- Identificar los servicios básicos, como el correo electrónico y las aplicaciones críticas, que la empresa puede implementar en el dispositivo del empleado.
- Conservar la experiencia nativa para que los empleados puedan seguir utilizando sus aplicaciones preferidas para las tareas rutinarias.
- Cuándo los dispositivos de los empleados estén infringiendo políticas, informar de las posibles consecuencias y emitir notificaciones proactivas para ayudar a los usuarios a que solucionen los problemas rápidamente.

## 6 FACTOR ECONÓMICO:

### El coste de implantar un programa BYOD

Los programas BYOD son relativamente nuevos, por lo que los estudios definitivos sobre sus beneficios y consecuencias económicas son todavía lejanos. No obstante, eso no significa que sea demasiado pronto para determinar cómo estructurar los aspectos financieros de su programa BYOD. Los aspectos fundamentales a considerar incluyen aspectos cómo:

- Financiar los dispositivos y el servicio: determinar si el empleado será 100 % responsable del dispositivo y los costes de servicio o si la empresa reembolsará parte o la totalidad.
- Sacar partido a los acuerdos con operadores móviles para proporcionar opciones corporativas, de asistencia y autoservicio a los usuarios.
- Estudiar los servicios y procesos de telecomunicaciones existentes; cuando sea posible, ofrecer descuentos corporativos a los usuarios, que incluyan exenciones de tasas de rescisión y concesiones para actualizaciones tempranas.
- Investigar nuevos servicios y planes de operadores que puedan mejorar y enriquecer el programa BYOD.
- Ahorrar dinero en recursos de soporte técnico implementando servicios de autoayuda.





## 7 DISEÑO Y GOBERNANZA DE APLICACIONES:

### Exigir seguridad sin necesidad de convertirse en un "Gran Hermano"

En un entorno de BYOD, las aplicaciones abarcan datos corporativos confidenciales que pueden ponerse en riesgo fácilmente si el dispositivo se pierde o si, accidentalmente, resulta infectado por malware. Por tanto, su organización necesitará cierto nivel de control para evitar que los datos caigan en las manos equivocadas. A pesar de todo, los empleados no querrán tener la sensación de que la empresa está supervisando todos sus movimientos, publicaciones y tuits, sobre todo en sus propios dispositivos. Para ganarse la confianza de los empleados y proteger los datos críticos, su programa de BYOD deberá implementar procedimientos de diseño de aplicaciones y gobernanza que:

- Modifiquen la disponibilidad de las aplicaciones basándose en los requisitos de seguridad.
- Comuniquen y justifiquen el alcance hasta el que el departamento informático admita o restringa las aplicaciones personales.
- Definan la disponibilidad de aplicaciones de acuerdo con la propiedad del dispositivo, ya que ciertas aplicaciones internas podrían no ser adecuadas en dispositivos personales por motivos de seguridad.
- Definan los niveles de implementación o remedio para infracciones en uso de aplicaciones (como las notificaciones, el control de acceso, la cuarentena o el borrado selectivo).

## 8 COMERCIALIZACIÓN INTERNA:

### Crear su «marca» informática

El proceso de implementación de un programa BYOD ofrece una estupenda oportunidad para mejorar las relaciones entre los empleados y la empresa. Puede publicitar su programa como una iniciativa corporativa para mejorar el equilibrio personal/profesional a través de una mayor movilidad y flexibilidad. Asimismo, la empresa puede fomentar la percepción interna del departamento informático como defensor de los usuarios finales y partidario de las tecnologías que los empleados quieran utilizar. Además, el programa BYOD puede servir como efectiva herramienta de captación para demostrar que la empresa valora la tecnología de vanguardia y una mayor autonomía para sus empleados.

Aunque la comunicación interna puede parecer una actividad de menor importancia, puede resultar una forma sumamente efectiva de mejorar la satisfacción de los empleados, la productividad y la longevidad, además de permitir que el departamento informático se posicione como aliado de los empleados móviles.

# «Lanzamiento selectivo» de su programa BYOD

Una vez que se han establecido los objetivos, políticas, procesos e infraestructura técnica del programa, podrá comenzar el lanzamiento por fases o «lanzamiento selectivo». Al dividir el lanzamiento en fases, permitirá que un pequeño subgrupo de usuarios pruebe el programa y le dé su opinión sobre cómo mejorar el rendimiento, la compatibilidad y otros problemas que quizá no haya descubierto durante las fases iniciales de la creación de la infraestructura. El lanzamiento del programa BYOD suele seguir tres fases: pruebas piloto, implementación y mantenimiento. En algunos casos, estas fases se pueden combinar o pasar por alto conjuntamente, como detallaremos más adelante en esta guía.

## INICIAR LAS PRUEBAS PILOTO

Las pruebas piloto le ayudan a solucionar problemas antes de lanzar el programa BYOD en toda la empresa. Le dan la oportunidad de probar con seguridad las funciones de un extremo a otro, además de recopilar las opiniones de los usuarios para identificar que está funcionando bien y qué hay que arreglar.

### PASO 1:

### Seleccione el grupo de usuarios de muestra para las pruebas piloto

Elija un grupo de usuarios de muestra para que completen el registro del dispositivo y el proceso de configuración. El grupo de muestra debe ser un conjunto representativo de toda la empresa e incluir una amplia gama de funciones, unidades corporativas y perfiles profesionales, para que pueda poner a prueba el proceso de cualificar a los usuarios según su función y la aprobación del superior. También, deberá distribuir las políticas de dispositivos móviles o el acuerdo del usuario final del BYOD que tenga en ese momento para asegurarse de que los usuarios comprenden los términos del programa.

Si incluye un gran porcentaje de usuarios corporativos y no técnicos en su grupo de muestra, podrá comprender mejor la experiencia del usuario media del BYOD. No obstante, el personal de operaciones informáticas también deberá participar en la prueba piloto, para garantizar que podrán identificar cualquier problema técnico durante la fase piloto.

*«Lanzamiento selectivo» de su programa de BYOD*

# Implementar el programa BYOD y los servicios de formación

## PASO 2:

### Consultar a los empleados para seguir mejorando la experiencia del usuario

No podemos insistir más en ello: es necesario que consulte a los usuarios durante cada fase de la implementación del programa BYOD para asegurarse de que el programa está cumpliendo las necesidades y expectativas de los empleados. Hay tres tipos de encuesta:

- **Encuesta previa a la implementación,** que recopilará las preferencias de los empleados por diferentes dispositivos, sistemas operativos, aplicaciones, planes de datos y modelos de asistencia técnica.

- **Encuesta sobre el registro,** que abarcará la primera experiencia de usuario con el programa BYOD y podrá identificar cualquier carencia en el proceso de registro del dispositivo. Como el registro es un paso esencial en la participación del empleado en el programa BYOD, le recomendamos que se asegure de que el proceso sea lo más rápido, eficiente y fácil de comprender posible.

- **Encuesta de seguimiento o final,** que incluirá preguntas tanto cerradas como abiertas para recoger las opiniones sobre la experiencia general del usuario durante la prueba piloto. Esta encuesta puede abarcar métricas sobre el rendimiento y determinar si el proceso ha cumplido las expectativas del empleado y los objetivos del programa.

Una vez que se ha asegurado de que todos los procesos de registro y configuración funcionan correctamente, el siguiente paso es implementar totalmente el programa. Sin embargo, en lugar de lanzar el programa en toda la empresa, le recomendamos que divida la implementación en fases para minimizar los posibles impactos en el rendimiento y la disponibilidad. Si divide el lanzamiento de acuerdo con la geografía, el departamento, el puesto de trabajo u otros criterios, se asegurará de tener disponibles los recursos adecuados para mitigar cualquier problema.

También, deberá configurar funciones efectivas de formación y autoservicio cuando implemente el programa. Tener instrucciones completas y fáciles de usar sobre el registro y la solución de problemas en los dispositivos podrá ayudarle a simplificar el proceso de ir sumando empleados. Puede considerar la posibilidad de llevar a cabo su programa de formación en diferentes formatos —en línea, presencial y mediante documentación por escrito— para adaptarse las diferentes formas en que los usuarios acceden a la información.

En última instancia, el objetivo de la formación de usuarios es minimizar las llamadas a soporte técnico y mantener el tiempo de actividad, anticipando y resolviendo problemas, evitando que puedan llegar a afectar a la productividad, riesgo de pérdida de datos o incidencias más graves. Además, al proporcionar formación integral mediante guías de autoservicio, herramientas en línea y una amplia comunidad de usuarios, podrá aumentar la satisfacción de los empleados al otorgarles más autonomía sobre su forma de trabajar.

PARTE IV: MANTENIMIENTO DE LA SEGURIDAD Y EL RENDIMIENTO DEL SISTEMA BYOD

# Ya ha alcanzado una cómoda altitud de crucero. Y ahora, ¿qué?

Una vez que su programa BYOD esté totalmente implementado en toda la empresa, comenzará la tarea de mantenerlo. El primer paso es la transición de los servicios de BYOD desde el equipo de desarrollo hasta el equipo de mantenimiento, es decir, de los ingenieros al personal de operaciones. Esta transición incluye la transferencia de conocimientos, la revisión de documentación, los servicios de soporte técnico, la asistencia técnica y el diseño de procesos de remisión a instancias superiores. Es cierto que el proceso de aprobación puede ser trabajoso y complicado, sobre todo si la transición se realiza a centros de asistencia técnica externos o de terceros. Para garantizar que la transición no afecte a los niveles de servicios móviles ni a la seguridad, deberá establecer procesos claros para la gestión de la remisión a instancias superiores, incidentes, problemas, configuración y disponibilidad.

# Permita la autoconfianza, el autoservicio y la autoresolución.

En un programa BYOD, el antiguo modelo de llamadas y tickets para el soporte técnico da paso a una nueva era de autoservicio basado en el usuario. Aunque la necesidad de soporte técnico informático nunca va a desaparecer, uno de los componentes esenciales del sistema BYOD es disponer de un servicio de asistencia técnica integral que permita a los usuarios resolver la mayoría de los incidentes sin que tenga que intervenir el soporte técnico. Este modelo de autoservicio debería permitir a los usuarios que:

- Ellos mismos registren los nuevos dispositivos, supervisen y gestionen los dispositivos actuales y borren o retiren sus dispositivos, según sea necesario.
- Pongan en práctica ellos mismos soluciones a problemas de hardware, software, aplicaciones y cumplimiento mediante notificaciones claras e instrucciones de resolución.
- Sigan siendo productivos y eficientes a la vez que mantienen la seguridad y el cumplimiento.

# Incorpore cada vez más dispositivos, sistemas y aplicaciones

Tal y como mencionamos anteriormente, el lanzamiento inicial del programa debe incluir tantos dispositivos populares como sea posible para fomentar la participación de los empleados. Sin embargo, el mercado introduce dispositivos nuevos cada 3-6 meses, de modo que su empresa necesitará un plan de certificación rápido, eficiente y sencillo para evaluar todos los futuros dispositivos móviles. El proceso de certificación debe ser constante y siempre en evolución. Si el proceso es demasiado complicado, terminará siendo caro y al final quedará detrás de la curva de la tecnología, así que la velocidad y la eficiencia son factores esenciales.

# Garantice una retirada de dispositivos segura y eficiente

El ciclo de vida de los dispositivos móviles es considerablemente más breve que el de los equipos de sobremesa y portátiles; a veces, menos de un año. Como los usuarios actualizan sus dispositivos con más frecuencia, usted necesitará tener implementado un proceso seguro de retirada de dispositivos para garantizar que los datos corporativos no se vean afectados una vez que el dispositivo deje de estar bajo su control:

- Actualice o compre un nuevo dispositivo
- Se vaya de la empresa

## ACTUALIZACIÓN O COMPRA DE UN DISPOSITIVO

Cuando haya que comprar o actualizar un dispositivo, el usuario deberá notificar al soporte técnico la recepción del nuevo dispositivo. Hay que recordar al usuario que haga una copia de seguridad de los datos y aplicaciones del dispositivo antiguo y mueva este contenido al nuevo dispositivo. Después, el departamento de soporte técnico podrá completar el proceso de seguridad eliminando todos los accesos de red, configuraciones, aplicaciones y datos que se habían otorgado al dispositivo antiguo.

Para respaldar los esfuerzos de comercialización internos de la empresa, deberá poder ofrecere antemano con algunas recomendaciones de centros de reciclaje o donación donde el empleado pueda enviar su antiguo dispositivo (siempre que no se lo vaya a dar a un amigo o familiar). Fomentar el reciclaje o donación de los dispositivos supone una excelente oportunidad para mejorar la imagen de la empresa, a la vez que ayuda a evitar que los dispositivos reutilizables, con componentes peligrosos, terminen en vertederos.

*(continuación)*

## CAMBIO DE EMPRESA

El proceso de retirada de dispositivos para usuarios que se van de la empresa, es ligeramente diferente del proceso de actualización de dispositivos. En lugar de iniciarlo el usuario, el proceso de separación deberá notificar al usuario cuándo se va a revocar el acceso a los recursos corporativos y cuándo se retirará el dispositivo. Los plazos temporales y el tipo de notificación pueden ser diferentes dependiendo de si la marcha de la empresa se debe a una dimisión, una reducción de personal o a una rescisión del contrato, y se deberá integrar con los procesos de separación existentes de acuerdo con el departamento de recursos humanos.

# Mida y demuestre el valor del sistema BYOD

Para medir el retorno de la inversión de su programa BYOD, resulta esencial garantizar el respaldo ejecutivo a largo plazo. Como los sistemas BYOD son un desarrollo relativamente nuevo, la mayoría de las organizaciones todavía están determinando cuál es el mejor modo de medir el retorno de la inversión. Normalmente, incluirá una combinación de las siguientes variables:

- Ahorros de hardware en dispositivos propiedad de los empleados, a menos que la empresa los subsidie.
- Mayores recargos debido al exceso de personal o uso corporativo.
- El coste de los planes de servicio, que dependerá de la capacidad de su empresa para aprovechar las ventajas de la consolidación con el operador.
- Ganancias de productividad, que si bien son difíciles de cuantificar, se pueden lograr aumentando la satisfacción de los empleados y la flexibilidad con las herramientas que utilizan para trabajar.
- Costes del soporte técnico: aunque la complejidad y variedad de los dispositivos puede llegar a aumentar los costes de soporte técnico, los empleados móviles suelen estar dispuestos a invertir tiempo en solucionar sus problemas antes de llamar al departamento informático. Con las herramientas de autoservicio adecuadas, el soporte técnico podría convertirse en un último recurso para solucionar problemas de los usuarios finales, lo cual contribuiría a controlar los costes del departamento informático.
- Los costes de responsabilidad, que pueden variar dependiendo de quién sea propietario del dispositivo: el empleado o la empresa.
- Implicaciones fiscales, que pueden variar dependiendo de si es la empresa o el empleado el propietario / a del dispositivo o de qué porcentaje del reembolso se debe notificar para auditorías.

CONCLUSIÓN

# Conseguir la transformación «Mobile First»

Si está leyendo esto, probablemente sepa que los sistemas BYOD son más bien una cuestión de «cómo», no de «cuándo» o de «si». A finales de 2014, los sistemas BYOD podrían alcanzar hasta el 80 % de su equipo de trabajo y transformar su empresa de una forma que nunca habría llegado imaginar. Prepararse para esta transformación es mucho más que una cuestión de seguridad. Es una cuestión de sacar partido a las personas, a los procesos y herramientas necesarios para transformarse en una organización «Mobile First» que esté lista para explorar un nuevo entorno de oportunidades totalmente nuevas.

Esta guía sobre BYOD es un magnífico primer paso para culminar con éxito su transformación móvil. Si sigue las recomendaciones de esta guía, podrá lograr un programa que cumpla las necesidades y preferencias de sus empleados móviles, a la vez que se adapte a la seguridad corporativa y a los requisitos presupuestarios. Sin embargo, el verdadero éxito de cualquier programa BYOD depende de su sostenibilidad a largo plazo. Esto quiere decir que deberá garantizar la seguridad de sus datos corporativos, fomentar la adopción de los usuarios respetando las preferencias sobre dispositivos de los empleados y mantener una cartera tecnológica flexible que dé cabida a la innovación empresarial.

La sostenibilidad de los programas BYOD también dependerá de la puesta en marcha de una comunicación constante y efectiva con las partes interesadas y los usuarios. Las partes interesadas tienen que ver que el programa respalda sus objetivos y los usuarios deben recibir actualizaciones constantes sobre la seguridad y las políticas de los dispositivos para fomentar su participación continua.

En resumen, su programa BYOD precisa atención y aportes constantes para lograr el éxito. Es necesario que invierta en recursos capacitados para perfeccionar la asistencia técnica y el mantenimiento, y seguir mejorando constantemente las pautas y procesos de autoservicio y de soporte técnico. Además, debe estar dispuesto y ser capaz de ajustar las políticas y procesos para adaptarlos a las necesidades de los usuarios, el crecimiento de la empresa y las tecnologías cambiantes.

Algo en lo que todos están de acuerdo es que los sistemas BYOD están aquí para quedarse. Si utiliza las prácticas recomendadas y las recomendaciones que se detallan en esta guía, podrá cumplir incluso con los requisitos más exigentes de seguridad y gestión informática, a la vez que proporciona a los usuarios finales una experiencia móvil siempre excelente y productiva.

## MÁS INFORMACIÓN

Descubra cómo MobileIron proporciona la base que las organizaciones necesitan para lograr la transformación «Mobile First» fomentando la innovación, la productividad y el ahorro de costes en toda la empresa. Visítenos en **www.mobileiron.com**.

## ACERCA DE MOBILEIRON

Como líder en seguridad y administración de aplicaciones móviles, contenido y dispositivos, la misión de MobileIron es permitir que organizaciones de todo el mundo adopten la movilidad como su principal plataforma informática, con el fin de transformar sus negocios y aumentar su competitividad. Las principales compañías multinacionales confían en la arquitectura escalable de MobileIron, en su rápida innovación y en sus mejores prácticas como base para sus iniciativas *Mobile First*, entre las que se encuentran 8 de los 10 principales fabricantes de automóviles, 7 de las 10 principales empresas farmacéuticas, 5 de los 10 principales bancos, 5 de los 10 principales bufetes de abogados y 4 de las 10 principales empresas de venta al por menor. Para más información, visite

**www.mobileiron.com.**

415 East Middlefield Road
Mountain View, CA 94043 EE. UU.
Tel. +1.650.919.8100
Fax +1.650.919.8006
info@mobileiron.com

MobileIron®