Nuevo modelo BYOD:

Prácticas recomendadas para implementar un programa BYOD productivo

airwatch by vmware

Presentación

Introducción

A En los últimos años, BYOD, que hace referencia al uso de dispositivos personales en el trabajo, se ha convertido en uno de los términos más utilizados en la empresa, al generalizarse el uso de los dispositivos móviles en muchas organizaciones. Sin embargo, además de ser un término que está de moda, su significado no es el de unas simples siglas. BYOD forma parte de una tendencia más amplia y arraigada: la consumerización de las TI, que se remonta al principio de la década de 2000. Por aquel entonces, casi todos disponían de un ordenador personal, con lo que podían trabajar desde casa fuera del horario laboral, así como disfrutar de las ventajas de utilizar los dispositivos de su elección y con los que se sentían más cómodos en lugar de usar los dispositivos corporativos que les proporcionaban los departamentos de TI.

El modelo BYOD y la consumerización de las TI se siguieron generalizando a medida que los dispositivos se abarataban y estaban mejor conectados. Mientras que la única preocupación de los líderes de TI era el control del acceso a la red corporativa de dispositivos no aprobados, un informe de Intel y readwrite publicado recientemente muestra que el 49 % de los responsables de TI de Estados Unidos están totalmente de acuerdo en que el modelo BYOD aumenta la productividad de los empleados. La nueva era del modelo BYOD ha llegado, y los departamentos de TI lo consideran un valor añadido estratégico en lugar de una amenaza que debe controlarse.

Las empresas hacen un uso más inteligente del modelo BYOD», afirma Nick McQuire, director ejecutivo de la Alianza de Movilidad Corporativa Global (GEMA). «La idea original era trasladar los costes de los dispositivos y de conectividad a los empleados. Aunque esto es así en algunos casos, muchas empresas han descubierto una gran cantidad de matices relacionados con la situación empresarial», asegura McQuire. Uno de ellos es el elevado número de dispositivos que acceden a las empresas hoy en día. Según los datos de Pew Research Center, el número de propietarios de dispositivos móviles se ha disparado en los últimos años. Es más, el usuario medio ya posee varios dispositivos móviles.

Independientemente de que una empresa proporcione dispositivos, los empleados disponen de sus propios dispositivos personales y desean conectarlos a la red corporativa. Hoy en día, puesto que la mayoría de los usuarios tienen varios dispositivos, tanto los directivos de las empresas como los departamentos de TI deben elaborar una estrategia para gestionar y proteger unos dispositivos que, según el modelo BYOD, inevitablemente van a acceder al lugar de trabajo. Los programas BYOD ofrecen a los usuarios un método seguro y aprobado por el departamento de TI para acceder a los recursos corporativos desde sus dispositivos personales.

Además de proporcionar una seguridad básica, los líderes empresariales y de TI que han adoptado el modelo BYOD han descubierto su potencial para añadir valor a una serie de áreas empresariales. Según McQuire, estas empresas «comprenden mejor las ventajas y el motivo por el que se adopta el modelo BYOD. Tienen facilidad para aplicar el modelo BYOD a las iniciativas empresariales». Los departamentos de TI que son conscientes de la necesidad de proporcionar seguridad y entienden los factores que impulsan este cambio, conocen en gran medida la tecnología que utiliza un empleado en su día a día. Aunque los dispositivos móviles son uno de los tipos de dispositivos que utilizan los empleados, los departamentos de TI han ampliado las posibilidades para incluir los equipos de escritorio, ordenadores portátiles y dispositivos resistentes no solo como terminales que se pueden gestionar, sino como terminales que hay que proteger. Aunque es difícil cuantificar con exactitud el aumento de la productividad como resultado del modelo BYOD, son muchas las ventajas inmediatas que ofrece. En la mayoría de los casos, la implementación de programas BYOD para los empleados que no disponen de dispositivos corporativos aumenta significativamente el número de empleados

móviles y accesibles de una empresa. Según Gartner, el modelo BYOD podría ampliar el número total de usuarios móviles de una organización al menos en un 50 %. Si todos los dispositivos de un empleado están conectados a la empresa, la accesibilidad aumenta aún más.

Las empresas más ingeniosas de hoy en día utilizan el modelo BYOD como una herramienta para gestionar la accesibilidad móvil, aumentar la capacidad de supervisión del departamento de TI y permitir a los empleados realizar una tarea al momento con el dispositivo más cercano. En este documento técnico se describen las medidas básicas que los directivos de empresas y los profesionales de TI están adoptando para que los programas BYOD den lugar a un importante aumento de la productividad.

El modelo BYOD como facilitador

Los departamentos de TI necesitan que los usuarios del programa BYOD hagan uso de la gestión de la movilidad empresarial (EMM) para reducir al máximo los accesos no autorizados a las redes corporativas y proteger la organización frente a las vulneraciones de la seguridad. Para lograr la aceptación de los empleados, tanto los directivos de las empresas como el personal de TI deben informarles sobre las ventajas que les aportará su participación en el programa.

En primer lugar, presente el modelo BYOD como una ventaja. El modelo BYOD ofrece a los empleados la posibilidad de trabajar como deseen y con los dispositivos que elijan (o con aquellos que ya tienen). Como ventaja tanto para el empleado como para la empresa, los dispositivos de los empleados se pueden personalizar con las aplicaciones y herramientas de productividad que los usuarios consideren útiles. Al destacar la flexibilidad y las posibilidades que ofrece el modelo BYOD, se asegurará de que se perciba como un programa que permite a los empleados realizar su trabajo de una forma más productiva y eficiente.

Además de ofrecer a los empleados un gran número de posibilidades, los programas BYOD pueden ayudar al conjunto de los empleados y la empresa a lograr los objetivos empresariales generales. Piense en cómo el modelo BYOD puede impulsar los objetivos de la organización existentes. ¿Podría el personal de ventas utilizar el dispositivo móvil para interactuar con clientes potenciales y existentes? ¿Es esencial para sus empleados tener la posibilidad de recibir correos electrónicos en todo momento debido al alcance global de su organización? ¿Tienen interés sus empleados en el teletrabajo o en otros horarios de trabajo? Un programa BYOD puede ayudarle a optimizar los procesos empresariales, impulsar las ventas y mejorar el contacto con los clientes.

GA Communications Group, una empresa con sede en Chicago, ha implementado con éxito un programa BYOD que ofrece a los usuarios una serie de ventajas. Según Jason Dittmer, director de tecnología, el principal atractivo es la capacidad de acceder a los registros de horas diarios para registrar las horas facturables, un proceso que debe realizarse diariamente, a través de una conexión a una red privada virtual (VPN). El perfil de VPN se activa en los dispositivos de los usuarios mediante el uso de una aplicación web. En la aplicación, los empleados pueden rellenar y enviar sus propios registros de horas. «En el mundo empresarial, el registro de horas es el que manda», afirma Dittmer. «Juega un papel importante en el día a día de todos, por lo que si sale corriendo y en el tren se da cuenta de que se ha olvidado de rellenarlo, puede sacar el teléfono, conectarse a la red VPN e introducir el tiempo correspondiente».

En el futuro, Dittmer pretende utilizar la tecnología iBeacon y una aplicación de programación para simplificar la programación de las salas de reuniones. Si un empleado necesita utilizar una sala de reuniones, podrá conectarse a los iBeacons de la oficina para que la programación aparezca en su teléfono.

La identificación de las ventajas que el modelo BYOD ofrece a los empleados ayuda a facilitar su adopción y a crear una imagen positiva del programa. Sin embargo, para que los directivos de las empresas y los profesionales de TI puedan tomar esta postura, deben asegurarse de que los aspectos más importantes, como la supervisión por parte del departamento de TI y la seguridad de primer nivel, estén bien consolidados.

Implementación de las herramientas adecuadas

La llegada del iPhone® transformó el mercado de la movilidad empresarial y provocó un efecto dominó que aún se puede apreciar. Los empleados empezaron a llevarse sus iPhones personales al trabajo y a darles prioridad con respecto a los antiguos dispositivos de la empresa. Algunos encontraron la forma de acceder al correo electrónico y a otros recursos, mientras que el personal de TI se esforzaba por controlar los accesos no autorizados y detener la amenaza de la pérdida de datos. El personal de TI no pudo detener la afluencia de iPhones y otros dispositivos inteligentes, por lo que tuvo que buscar la forma de ofrecer un acceso seguro a los recursos corporativos para una variedad de dispositivos cada vez más amplia.

Antes de desarrollar una iniciativa BYOD, el personal de TI debe estar preparado para dicha afluencia en lo referente a la arquitectura de la red y la gestión. El personal de TI debe garantizar que la arquitectura de la red pueda gestionar el aumento del tráfico Wi-Fi. También debe asegurarse de que la plataforma de gestión de dispositivos existente puede escalarse para dar cabida a la gestión de los dispositivos de los empleados. En caso de que el departamento de TI ya haya invertido en un sistema EMM, lo ideal sería que pudiera aprovechar las políticas existentes desarrolladas para los dispositivos corporativos con la extensión de las políticas, las aplicaciones y el contenido necesario desde la misma consola.

En un entorno BYOD, los dispositivos que acceden a la empresa pueden ser muy diferentes. Una solución de EMM que admita únicamente un número limitado de tipos de dispositivos y sistemas operativos solo conseguirá, como mucho, aumentar la productividad de algunos empleados. En el peor de los casos, los usuarios cuyos dispositivos no sean compatibles buscarán soluciones alternativas y expondrán a las empresas a posibles vulneraciones de la seguridad. Una solución de gestión de dispositivos móviles (MDM) como AirWatch, que admite los principales tipos de dispositivos y plataformas, facilitará la participación de todos y se convertirá en la mejor protección ante la pérdida de datos.

También es importante buscar una solución que pueda mantener el ritmo de la innovación que marca el mercado. Las actualizaciones de los sistemas operativos móviles se publican cada dos semanas, y continuamente salen al mercado nuevos dispositivos. Con cada tipo de dispositivo nuevo o actualización del sistema operativo existe una posibilidad de que se produzca una vulnerabilidad de la seguridad. AirWatch es una solución independiente de los fabricantes de equipos originales y puede ofrecer compatibilidad inmediata con los principales tipos de dispositivos y sistemas operativos. AirWatch también ofrece a los administradores de TI una única consola que permite supervisar todos los dispositivos, independientemente de si pertenecen a la empresa, al programa BYOD o si se trata de dispositivos compartidos. La arquitectura multicliente de la plataforma AirWatch permite a los administradores establecer límites en la gestión de los dispositivos de los empleados, a la vez que mantienen la gestión integral de los dispositivos específicos de la empresa.

Sin embargo, puede que algunas organizaciones no deseen proporcionar acceso a todos los tipos de dispositivos y sistemas operativos y que, en su lugar, proporcionen a los empleados una lista de los dispositivos aprobados que la organización considera seguros. AirWatch ofrece la posibilidad de restringir el acceso al contenido en función del tipo de dispositivo, el sistema operativo o la versión de este último. Asimismo, AirWatch puede limitar el número de dispositivos con los que puede acceder un usuario concreto. Esto permite a las organizaciones establecer ciertas limitaciones y proteger sus redes ante un exceso de dispositivos hasta que se cree una arquitectura adecuada para gestionar el aumento del tráfico.

El planteamiento del uso de dispositivos personales en el trabajo es solo una de las piezas del gran puzzle que forma la movilidad empresarial y debe considerarse en contexto. La naturaleza de la tecnología es cíclica y, a la hora de abordar las necesidades del mercado, rápidamente surgen soluciones puntuales o proveedores para llenar el vacío. En lugar de implementar una solución provisional para detener una posible pérdida de datos y evitar que los dispositivos sin supervisión accedan a la red corporativa, la mayoría de las organizaciones móviles de hoy en día han encontrado soluciones completas que se pueden escalar conforme aumentan las iniciativas de movilidad.

Por ejemplo, su prioridad puede ser proporcionar acceso al correo electrónico en los dispositivos de los empleados. Sin embargo, es inevitable que los empleados tiendan a utilizar cada vez más sus dispositivos móviles, de forma que el personal de TI tenga que plantearse la aplicación del modelo BYOD más allá del correo electrónico. Anticípese y adquiera una solución que admita el uso de aplicaciones, el acceso al contenido, las conexiones seguras a los repositorios de la empresa y una exploración sin complicaciones de la intranet en los dispositivos de los empleados.

Una vez que cuente con la tecnología adecuada, viene la parte más difícil. Cuando el personal de TI haya seleccionado las herramientas correspondientes, este debe consultar con los directivos de la empresa y los grupos pertinentes la elaboración de políticas que aborden los aspectos legales y sobre privacidad del programa BYOD.

La importancia de la comunicación: establecimiento de políticas y condiciones de uso del programa BYOD claras

Un estudio realizado en abril de 2014 mostró que muchos empleados aún no se tomaban en serio el modelo BYOD. Las políticas sobre el uso de dispositivos personales pueden ayudar a garantizar la colaboración de los empleados al describir tanto el riesgo que implica el acceso no autorizado como las ventajas que ofrecen los programas BYOD. La política sobre el uso de dispositivos personales debe definir de forma clara las normas del programa de acuerdo con la normativa gubernamental y las políticas de seguridad de la empresa. También debe definir con claridad la capacidad de visualización y gestión del personal de TI con respecto a los dispositivos personales a fin de evitar que los datos personales se vean afectados o queden expuestos. Antes de aplicar el programa en toda la organización, los departamentos de TI deben recibir la aprobación del nivel ejecutivo y las aportaciones de distintos departamentos con el fin de garantizar que se atienden las diferentes inquietudes y se satisfacen todas las necesidades.

La privacidad es una de las principales preocupaciones de muchos empleados y puede ser un obstáculo a la hora de participar en los programas BYOD. AirWatch permite a las empresas separar los datos corporativos de los personales en los dispositivos mediante políticas de privacidad personalizables que pueden basarse en la propiedad del dispositivo. Los administradores pueden configurar políticas para evitar la recopilación de datos del correo electrónico, el contenido o las aplicaciones personales de un dispositivo propiedad de un empleado. La ubicación GPS, la información personal del usuario y los datos de telecomunicaciones también pueden seguir siendo privados, mientras que dispositivos propiedad de los empleados quedan protegidos ante un borrado completo o el control de forma remota. AirWatch también permite a las empresas reducir los riesgos que implica el acceso de los dispositivos de los usuarios a los recursos corporativos. Mediante acuerdos sobre las condiciones de uso personalizados y basados en la función de los usuarios, el grupo de la organización y la plataforma de los dispositivos, los usuarios pueden recibir información sobre los datos que se obtendrán y las acciones que podrán llevar a cabo con los dispositivos.

Mohegan Sun, un casino y complejo turístico situado en Connecticut, ha implementado recientemente un programa BYOD con éxito. Danny Lynn, director de tecnologías de la información, afirma que la actualización

de los dispositivos de empresa iPhone 4 y 4S de los usuarios no entraba en el presupuesto de este año, por lo que elaboró un programa BYOD que ofrecía a los empleados la posibilidad de hacerse cargo del contrato, actualizar sus dispositivos y participar en el programa BYOD.

Cuando Lynn empezó a trabajar en los detalles del programa, se percató de que necesitaría una política sobre el uso de dispositivos personales para comunicar las normas y las opciones de actualización, además de permitir el acceso de otros dispositivos personales. Según Lynn, eran muchos los empleados con teléfonos móviles propiedad de la empresa los que habían solicitado acceso al correo electrónico corporativo desde sus iPads personales. Asimismo, los empleados que no disponían de dispositivos corporativos también solicitaron la posibilidad de acceder desde sus dispositivos personales.

Lynn y el vicepresidente de TI de Mohegan Sun redactaron de cero la política y las condiciones de uso sobre el uso de dispositivos personales según las necesidades de los empleados y los distintos casos de uso. El equipo encargó la revisión al departamento jurídico y, una vez aprobadas, pusieron en marcha el programa. El contrato es breve y directo y, según Lynn, describe de forma clara los datos que pueden visualizar los administradores en los dispositivos propiedad de los empleados y autoriza al departamento de TI de Mohegan Sun para realizar el borrado de los dispositivos que supongan un riesgo. Aunque Lynn no observó ninguna respuesta desfavorable por parte de los empleados con inquietudes acerca de la privacidad, «la preocupación de algunos empleados estaba relacionada con la posibilidad de perder todos los datos, por lo que les recomendamos que realicen las copias de seguridad necesarias», asegura Lynn.

Para conectar los dispositivos del programa BYOD a la red, ahora los empleados pueden consultar el contrato, instalar AirWatch® Agent y aceptar las condiciones de uso que Lynn ha personalizado mediante la consola de AirWatch.

Nick McQuire, el director ejecutivo de GEMA, recomienda empezar con un marco de políticas básico sobre el uso de dispositivos personales en el trabajo y personalizarlo en función de las necesidades del sector, la geografía y la organización. «Existe una gran variedad de conjuntos de herramientas para políticas sobre el uso de dispositivos personales desarrolladas por especialistas en movilidad y miembros de GEMA disponibles en todo el mundo, como Vox Mobile», asegura McQuire, quien, a su vez, recomienda Gartner como una buena fuente de información. «Las empresas pueden empezar con una plantilla de referencia y, a partir de ahí, elaborar sus propios anexos y añadir sus aportaciones».

Jason Dittmer, director de tecnología de GA Communications Group, investigó en Internet y encontró una política sobre el uso de dispositivos personales adecuada. A continuación, la envió al equipo jurídico para que la revisara. Después, él y sus compañeros del departamento de TI propusieron un método personalizado para garantizar la aceptación por parte de los empleados.

Esta pequeña empresa ubicada en Chicago ha integrado el modelo BYOD en la cultura de la empresa desde el primer momento, con la presentación de la política y el programa de uso de dispositivos personales de la empresa durante el proceso de incorporación. «Todo aquel que desee formar parte de la red recibe las instrucciones para inscribirse en la solución MDM, o bien se remite al departamento de TI para la configuración», afirma Dittmer. En la actualidad, GA Communications Group ofrece acceso a una red Wi-Fi segura, al correo electrónico, a la red VPN y a un catálogo de aplicaciones de la empresa.

Una parte del proceso de configuración muestra a los empleados cómo acceder al portal de autoservicio, en el que pueden ver todos los aspectos gestionados del dispositivo. Dittmer asegura que, en el caso de los empleados a quienes preocupaba la recopilación de datos personales por parte del departamento de TI, el portal de autoservicio ha servido de ayuda para convencerlos para que se inscriban. Mediante el portal de autoservicio, los empleados pueden ver qué aspectos de sus dispositivos gestiona el departamento de TI.

A continuación se incluyen algunos enlaces a recursos online de plantillas de políticas sobre el uso de dispositivos personales en el trabajo, que pueden ser un buen punto de partida para elaborar una política personalizada que se adapte a las necesidades de su organización:

- TechRepublic BYOD Policy
- Política sobre el uso de dispositivos personales de TechRepublic
- Kit de herramientas para el uso de dispositivos personales de la Casa Blanca
- Plantilla de política sobre el uso de dispositivos personales de IT Manager Daily
- Plantilla de política sobre dispositivos móviles del modelo BYOD de Gartner
- Página de recursos relacionados con el modelo BYOD de Vox Mobile

Transición del uso de los dispositivos corporativos al programa BYOD: más opciones para los empleados

Si está realizando una transición gradual de los dispositivos corporativos a un modelo fundamentalmente BYOD, el hecho de ofrecer a los usuarios varias opciones puede simplificar este proceso. El casino y complejo turístico Mohegan Sun ha implementado un plan para realizar una transición gradual de los usuarios a un modelo BYOD.

Cuando salió el iPhone 5, los empleados quisieron actualizar el dispositivo», asegura el director de TI, Danny Lynn. Lynn ofreció a los empleados la opción de adquirir los contratos móviles de Mohegan Sun, actualizar los dispositivos y participar en el programa BYOD de la organización. Aunque los empleados pasen a ser los propietarios y responsables del nuevo hardware, Mohegan Sun se sigue haciendo cargo de la factura mensual. «Los empleados querían tener más posibilidades y eso fue lo que nos llevó a implementar nuestra política sobre el uso de dispositivos personales».

«Desde ese momento, las actualizaciones de hardware, las reparaciones, los problemas o todo lo que esté relacionado con el propio teléfono pasa a ser responsabilidad de los empleados», afirma Lynn. «Esto supone una ventaja para las empresas, ya que se reduce el desembolso de capital futuro relacionado con las actualizaciones de los teléfonos». Los empleados que no deseen asumir el coste de una actualización, simplemente mantienen los dispositivos existentes.

Aunque que el reembolso total o parcial de la factura puede facilitar la transición de los dispositivos corporativos al uso de dispositivos personales, la cobertura de los gastos de telefonía móvil de los empleados podría tener un impacto negativo en los resultados de la empresa. Un programa de gestión de gastos en telecomunicaciones garantiza que los planes de datos se adapten al presupuesto. AirWatch dispone de funciones de gestión de gastos en telecomunicaciones integradas, tales como la capacidad de restringir la descarga de documentos para que tenga lugar únicamente en redes Wi-Fi o la restricción del acceso a funciones nativas como las videollamadas, que pueden consumir una gran cantidad de datos. AirWatch también colabora con proveedores de gestión de gastos en telecomunicaciones como Wandera, que ofrece servicios de gestión y compresión de datos.

Antes de completar el proceso de implementación del programa BYOD, el personal de TI debe plantearse si va a ofrecer soporte a los dispositivos propiedad de los usuarios y cómo va a hacerlo.

Asistencia: la nueva función de consultoría del departamento de TI en el entorno BYOD

La afluencia de los dispositivos móviles personales en las redes corporativas, así como los datos alojados en la cloud a los que se accede, han cambiado la forma de trabajar de las personas y, por consiguiente, el funcionamiento de los departamentos de TI. Los dispositivos móviles ofrecen la posibilidad de trabajar con mayor eficiencia. La eficiencia aumenta cuando el usuario puede acceder al correo electrónico o realizar tareas relacionadas con el trabajo en todos sus dispositivos. Según Eric Klein, investigador de VDC, parece sencillo, pero proporcionar acceso a varios tipos de dispositivos y, a menudo, a varios dispositivos por usuario, plantea una serie de dificultades para los departamentos de TI.

Cuando una organización tiene que gestionar los dispositivos de una forma rentable y protegerlos ante los riesgos asociados a la apertura de los datos corporativos a estas plataformas, es necesario hacer frente a una gran cantidad de dificultades», afirma Klein. Los controles de MDM pueden hacerse cargo de los aspectos básicos, por ejemplo, mediante la capacidad de borrar los datos corporativos o bloquear un dispositivo que ha quedado olvidado en un taxi o un avión. «Sin embargo, son muchos los aspectos que debe tener en cuenta una organización.

El director de tecnología de GA Communications Group, Jason Dittmer, afirma que la transición a la cloud ha sido uno de los aspectos fundamentales de la implementación del programa BYOD en la empresa. «Hemos realizado un gran esfuerzo para mover muchos de nuestros sistemas internos a la cloud. En el entorno tradicional, todo lo necesario se protegía en la sala de servidores». Dittmer asegura que, hoy en día, los departamentos de TI se centran más en la gestión de distintos servicios, como los proveedores de almacenamiento en la cloud y MDM.

Los departamentos de TI que gestionan programas BYOD también suelen encargarse de solucionar los problemas de una amplia gama de dispositivos. Según Dittmer, la forma en la que el departamento de TI interactúa con los empleados ha cambiado en consecuencia. «El modelo BYOD supone un gran cambio en la forma de trabajar de los empleados y en su forma de interactuar. Puesto que son muchas las variables que entran en juego en un entorno BYOD, el departamento de TI empieza a convertirse en algo más parecido a un consultor.

Algunas organizaciones han establecido un servicio especializado de TI al que los empleados pueden acudir a determinadas horas para obtener ayuda con la conexión de los dispositivos, o bien para resolver problemas. Aunque la organización de Dittmer es lo suficientemente pequeña como para permitir a los usuarios acudir al departamento de TI cada vez que les surja alguna duda, asegura que el uso de una plataforma de gestión simplificada para los dispositivos tanto de uso personal como corporativos ha dotado a su departamento del tiempo necesario para adoptar la función de consultor cuando sea necesario. Según dice, el concepto también le ha ayudado a ampliar tanto sus conocimientos de TI como los de sus compañeros.

Creo que los integrantes de un departamento de TI tienen que poseer un conocimiento más amplio y profundo, ya que ahora se encargan de gestionar una gran variedad de sistemas», afirma Dittmer. «Ahora nadie [en nuestro departamento de TI] se encarga de hacer una sola tarea. Los cuatro tenemos que conocer todos los sistemas». En el caso de las organizaciones que no dispongan de recursos para ofrecer soporte de TI para los dispositivos propiedad de los empleados, el portal de autoservicio de AirWatch es una herramienta útil con la que los empleados pueden asegurarse de mantener la conformidad de los dispositivos, así como solucionar los problemas que surjan.

Ahora que los empleados tienen la capacidad de gestionar sus propios dispositivos y solucionar sus problemas, ¿cuál es el siguiente paso?

Preparación para el futuro del modelo BYOD: uso de todos los dispositivos personales

Nuestra forma de trabajar está cambiando», afirma Eric Klein, investigador de VDC. No se trata solo de la nueva generación de empleados, sino de todos nosotros.

La revolución móvil ha transformado los negocios. En la actualidad, resulta difícil no contar con al menos uno o dos dispositivos móviles como herramientas de trabajo básicas. Sin embargo, quedan más cambios por llegar. Prácticamente todos los días se introduce en el mercado un nuevo dispositivo conectado a la red. Pronto, muchos de estos dispositivos serán indispensables y se cogerán (o se llevarán puestos) a la hora de salir de camino a la oficina.

Mientras que el Internet de las cosas presenta un gran potencial para transformar los procesos empresariales, también introduce nuevos problemas y amenazas de seguridad. Ahora, el personal de TI debe tener en cuenta estas dificultades y amenazas. La implementación de una plataforma de gestión de la movilidad empresarial sólida para gestionar un programa BYOD junto con los dispositivos propiedad de la empresa y una serie de dispositivos empresariales es la mejor forma que tienen las organizaciones para prepararse para un futuro hiperconectado.

También representa una gran oportunidad para que los líderes de TI demuestren su valor. El personal de TI se encuentra en una encrucijada: con una afluencia de tecnología más elevada que nunca en el lugar de trabajo, los líderes de TI tienen una oportunidad única para actuar de forma proactiva y convertirse en elementos indispensables de la estrategia empresarial. Durante mucho tiempo, el departamento de TI ha quedado relegado a un segundo plano, asegura Klein. La movilidad cambia la situación por completo, lo que supone una gran oportunidad para que el personal de TI reafirme su papel en la empresa. Ahora que la posibilidad de integrar los dispositivos en la empresa es evidente, se ha abierto todo un abanico de posibilidades.

Recursos adicionales

Acceda a nuestros laboratorios prácticos :
http://vmware.com/go/try-airwatch-hol

Visite nuestro sitio web **www.vmware.com/enterprise-mobility-management**

Sede central global de AirWatch

1155 Perimeter Center West
Suite 100 Atlanta, GA 30338
Estados Unidos
T: +1 404 478 7500
E: sales@air-watch.com

Información sobre AirWatch

AirWatch® es líder en gestión de la movilidad empresarial con una plataforma que incluye las principales soluciones de gestión de dispositivos móviles, correo electrónico, aplicaciones, contenido y navegadores del sector. Adquirida por VMware en febrero de 2014, AirWatch tiene su sede en Atlanta y se puede visitar online en **www.air-watch.com**.