BYOD y la movilidad corporativa

Virgilio Ernesto Reyes Vásquez [1]

Resumen:
La Gestión de Dispositivos Móviles (MDM, Mobile Device Management) está provocando un cambio acelerado en la correcta y eficiente gestión de los departamentos de TI y sus entornos corporativos. Actualmente existe la necesidad de administrar un amplio conjunto de dispositivos móviles provenientes de los trabajadores, cuya actuación se denomina "consumerización de la tecnología", que consiste en la gestión de una tecnología accesible, sencilla y omnipresente, que permita a los usuarios emplear sus herramientas de trabajo en cualquier momento y lugar. Para ello se requiere que los departamentos de TI implementen políticas MDM, que conlleve a una gestión exitosa de este abanico amplio de dispositivos móviles, en pro de la movilidad corporativa de manera segura.

Palabras clave
Dispositivos móviles, BYOD, MDM, TI, movilidad corporativa, consumerización de la tecnología.

Abstract
The Mobile Device Management (MDM) is causing a rapid change in the proper and efficient management of IT departments and corporate environments. Currently there is a need to manage a wide range of mobile devices from workers, whose performance is called "consumerization of technology", which consiste of the management of a accessible technology, simple and ubiquitous, allowing users to use their working tools at any time and place. This requires that IT departments implement MDM policies that lead to successful management of this wide range of mobile devices, in favor of safe corporate mobility.

Keywords
Mobile devices, BYOD, MDM, IT, enterprise mobility, consumerization of technology.

1. Introducción

Bring Your Own Device (BYOD), que traducido al idioma español significa: trae tu propio dispositivo, es un nuevo fenómeno cultural y tecnológico que permite a los empleados de una organización utilizar sus propios dispositivos móviles personales en las actividades de la empresa donde trabaja conectado a la red corporativa.

El fenómeno del BYOD es una tendencia que se expande cada día en las empresas de todos los tamaños gracias a la reducción de precios de dispositivos móviles tales como: smartphones, tablets y laptops. Hoy en día es muy común que los empleados hagan uso de sus dispositivos móviles personales para realizar sus labores en la empresa donde brinden sus servicios y lo que era un dispositivo personal se convierte en parte de la red empresarial.

¿Qué hace que ocurra esto? La razón es que la tecnología que se usa en casa es tan buena como la que se usa en la empresa. Algo que ha contribuido a esta tendencia es la explosión de smartphones y tablets en los hogares. Otro punto igual de importante es que la tecnología usada en casa y en la oficina está interconectada.

Es tal este fenómeno que en Estados Unidos muchas compañías llegan a ofrecer a sus empleados cierta

1. El autor es Ingeniero en Ciencias de la Computación y Máster en Consultoría Empresarial, docente de la Escuela de Ingeniería Electrónica, de la Universidad Don Bosco.
(virgilio.reyes@udb.edu.sv)

Fecha de recepción: 15/11/2012; Fecha de aceptación: 22/11/2012.

cantidad de dinero para que ellos se compren la computadora o smartphone que más les atraiga, con la idea que quien trabaja a gusto, trabaja mejor.

Para los administradores de los departamentos de TI (Tecnologías de Información) esta tendencia les causa problemas en sus políticas de soporte, porque ahora hay dispositivos variados sobre los que no poseen control, pero que solicitan conectarse a las redes empresariales, lo que conlleva a una brecha potencial para la seguridad de la información.

Un punto en común que poseen los trabajadores y los responsables de TI de las empresas es que ya no adoptan la postura de "early adopters" (los primeros en adoptar). El 52% de los trabajadores y el 47% de los responsables de TI de las empresas[2], prefieren comprar la segunda o tercera versión de un producto, ya que está extendida la experiencia de que los "early adopters" deben afrontar más errores de los sistemas. Esto conlleva a una consecuencia positiva en la experiencia de uso y gestión de los departamentos de TI y el servicio que brindan a sus usuarios.

Innovación, inteligencia e inversión, son los tres pilares sobre los cuales las empresas necesitan apostar sus estrategias corporativas. Para lograr enlazar estos tres pilares, los departamentos de TI son fundamentales en la creación de plataformas que permitan interconectar a los actores involucrados en la consecución de dichas estrategias.

En un futuro, donde todo estará conectado, la ubicuidad de dispositivos acelerará un incremento en el desarrollo de servicios para un usuario móvil y que está permanentemente conectado. La implementación de una infraestructura inteligente, que permita gestionar la variedad de dispositivos móviles conectados a la red empresarial, implicará un uso racional de los recursos tecnológicos que posean las empresas.

Según varios estudios, para el año 2020, el concepto que tenemos hoy en día de oficina desaparecerá y el volumen de la información digital se multiplicará por 30 debido a los cambios tecnológicos que estamos experimentando en estos momentos. Que el volumen de información se multiplique en un factor de 30 para el 2020 implica la necesidad de llevar a los extremos las medidas de seguridad para evitar fugas de información que puedan darse a través de los múltiples dispositivos interconectados a la red empresarial.

Con la introducción de tecnologías móviles más seguras y capaces y con el inevitable crecimiento en la adopción de la nube (cloud computing) en la vida empresarial y personal el concepto actual de oficina desaparecerá. El patrón de trabajo que persistirá será el hibrido, porque la oficina se usará como un lugar para reuniones y networking, bajo la modalidad presencial, semipresencial o virtual. Y el trabajo desde el hogar tendrá una aceptación cultural mayor.

Ante el fenómeno del BYOD las compañías se han visto obligadas a actualizar sus plataformas de servicios, pero el envejecimiento de los sistemas heredados de back office tiene como consecuencia que el 79% de las empresas puedan racionalizar adecuadamente sus entornos tecnológicos y las plataformas que dependen de ellos.

Lo anterior está ocurriendo a pesar de que las empresas reconocen el gran poder de agente de cambio que las tecnologías involucran en un mercado en continuo cambio. En Europa las empresas líderes en diferentes áreas confiesan que se ven tentados a adquirir la última tecnología disponible, aunque todavía no se haya alcanzado la funcionalidad plena de la existente. Esto conlleva a denotar que existe una laguna entre las inversiones que han sido destinadas a las tecnologías de front y back office, porque se está destinando más inversión en nuevas tecnologías a nivel de front office mientras que las inversiones de back office decaen. Este enfoque dispar de la administración de las TICs implica que los procesos del negocio queden expuestos a cuellos de botella, riegos de seguridad o duplicación de esfuerzos.

2. Mejores prácticas para BYOD en las empresas

Cada día más empresas se suman al cambio generado por el BYOD, en el sentido de que ya cuentan con un programa formal que defina las políticas de seguridad, gestión y procesos de los dispositivos personales

2. Two Worlds, One Life. Investigación realizada por la empresa D-LInk.

de sus empleados. Por lo tanto, las siguientes recomendaciones son algunas de las mejores prácticas para tener en cuenta al momento de definir e implementar el programa BYOD.

2.1. Defina su directiva de BYOD

a) Establezca la disponibilidad del servicio. Es muy importante que tome a consideración los servicios y aplicaciones que desea proporcionar en los dispositivos de BYOD y si difieren por grupos de trabajo, tipos de usuario, tipos de dispositivos y redes utilizadas, a medida que defina su directiva.

b) Defina la elegibilidad. Es necesario que identifique quién puede usar dispositivos personales para trabajar y también las situaciones en las que sea inadecuado debido a la seguridad de los datos.

c) Determine los dispositivos permitidos. Las políticas de BYOD deben permitir que las personas utilicen el tipo de dispositivo que mejor se adapte a sus necesidades.

d) Aclare el reparto de los costos. Algunas organizaciones proporcionan una subvención para los dispositivos de BYOD y otros servicios, especialmente en los casos en que ya no se suministra un dispositivo corporativo. En el momento de considerar una inversión se deben tener en cuenta las consecuencias fiscales y el posible ahorro de costos de TI.

2.2. Implemente BYOD en su organización

a) Planifique su implementación. Proporcione asesoramiento para ayudar a decidir si se desea participar, elegir el dispositivo adecuado y conocer las responsabilidades que conlleva traer su propio dispositivo, incluso cómo se puede usar, almacenar y acceder a los datos.

b) Implemente seguridad. La información comercial confidencial debe residir en el dispositivo únicamente de forma aislada y cifrada, y solo cuando sea absolutamente necesario. La seguridad multicapa debe incluir la autenticación de usuario individualizada, basada en políticas con seguimiento y monitorización de conformidad, el control sobre las funciones para imprimir y el almacenamiento del lado del cliente, y el software antimalware/antivirus requerido. TI debe de tener en cuenta los mecanismos de borrado remoto en caso de que se habilite información comercial en el dispositivo.

c) Establezca niveles de soporte y mantenimiento. Detalle el tipo de incidentes que TI admitirá y el alcance de este soporte. La disponibilidad de un grupo de dispositivos en préstamo permite una productividad ininterrumpida durante el servicio, especialmente cuando se utiliza dispositivos de BYOD en lugar de un dispositivo corporativo. No olvide ofrecer a los miembros clave del personal soporte de asesoramiento adicional.

Una fuerza laboral tecnológicamente sofisticada exige mayor flexibilidad respecto de cómo, cuándo y dónde se puede acceder a las aplicaciones, los datos y la información necesarios para cumplir con el trabajo. Con la capacidad de usar su propio dispositivo, la gente puede ser más productiva en cualquier momento y lugar a través de su smartphone, tablet o portátil preferido. Esto, sin embargo, puede causar preocupaciones en el equipo de TI, debido a una serie de errores conceptuales acerca de la complejidad que conlleva permitir a los dispositivos de los usuarios conectarse a la red de trabajo corporativa.

3. El desafío de hacerlo posible: una política BYOD segura y sencilla es la más eficiente

Las organizaciones pueden aprovechar fácilmente la infraestructura de TI existente, además de implementar aplicaciones del tipo software como servicio (SaaS) para admitir el despliegue seguro y eficiente de una política BYOD. Si se hace correctamente esto seguirá protegiendo la privacidad de los datos y garantizará la seguridad de información comercial sensible a la vez que mantiene el cumplimiento de normas.

El equipo de TI tampoco necesita concentrarse en el aprovisionamiento y mantenimiento de dispositivos. Puede concentrarse, en cambio, en ofrecer servicios de seguridad, acceso seguro a escritorios y aplicaciones virtuales, y servicios basados en la nube. Naturalmente, la gente también puede cuidar mejor sus propios dispositivos y tener un mejor entendimiento de sus capacidades completas. Esto

no solo reduce la dependencia del soporte de TI, sino que además permite que las organizaciones establezcan y logren objetivos de ahorro de costos que incluyen reducciones en el costo de obtención y soporte de dispositivos.

En Citrix, más de la mitad de los empleados informan que su productividad se vio mejorada con la implementación del programa BYOD, mientras que la organización ha logrado ahorros de costos operacionales del 18-20 por ciento anual. El valor real generado gracias al programa BYOD es, entonces, bastante persuasivo.

Una vez que se establece una infraestructura de TI confiable y segura las organizaciones pueden garantizar que todas las prioridades comerciales tienen la capacidad de escalarse y acomodarse a las necesidades comerciales cambiantes. Por ejemplo, el workshifting permite a las organizaciones trasladar trabajo y reducir costos al permitir a la gente elegir el tiempo y lugar ideales para trabajar. Esto no solamente adopta la demanda del empleado para trabajar en cualquier parte, sino que asegura la continuidad comercial. La gente puede mantener la productividad total en cualquier momento y lugar.

4. Aspectos de Seguridad

En cuanto a seguridad el fenómeno de BYOD no está libre de riesgos. El utilizar dispositivos propios para acceder a redes corporativas, que a su vez podrían usar un software no recomendado por la empresa, representa un gran riesgo para la seguridad de los datos y a su vez un reto para el personal que labora en IT.

Asimismo, el comportamiento o los malos hábitos de seguridad de los usuarios pueden escaparse del control del departamento de IT en la medida que crezcan los BYOD en la red corporativa.

Sin embargo, aunque entendemos que las redes corporativas contienen información muy importante para las empresas y la seguridad de los datos debería ser una prioridad de protección, muchas compañías han abrazado el concepto de BYOD sin pensar en las consecuencias de seguridad.

Es necesario asegurar la solidez de los sistemas desde dentro, logrando que el entorno esté altamente protegido, independientemente de dónde provenga la petición de acceso y esa buena práctica debe venir acompañada de adiestramientos y educación al usuario a quien se le autoriza que traiga su dispositivo personal.

Por otra parte, el que los empleados utilicen sus propios dispositivos para el trabajo es algo que debe estar controlado. Por lo que se recomienda que la implantación del BYOD no se deje a la espontaneidad, sino que se planifique.

El personal de IT debe conocer y entender las necesidades de los empleados, pero valorando la conveniencia de poner en marcha un plan de BYOD, entendiendo a la vez que es trabajo de todos evaluar las ventajas y calcular los costos de planificación y de protección de datos.

En una encuesta desarrollada por la empresa Fortinet, y realizada en más de quince países, se encontró que cerca de 42% de los encuestados indicaron la pérdida de datos y la llegada de software malicioso a sus redes fue a consecuencia del BYOD.

Asimismo, Fortinet reportó que “más de uno de cada tres trabajadores, un 36%, admitió que ha infringido o infringiría la prohibición de usar sus dispositivos personales con fines laborales. A pesar de ello, cuando se autoriza el uso de éstos para uso corporativo dos de cada tres encuestados consideran que deben ser ellos mismos y no el departamento de sistemas de la empresa los responsables de la seguridad de los aparatos”.

De manera que queda establecido que este asunto de la seguridad es una responsabilidad de todos sus usuarios, no importa el aparato tecnológico que utilice para acceder a la información.

Para dar validez al artículo de investigación, se consultó una serie de encuestas realizadas por empresas especializadas en consultorías de TI y ventas de equipos de hardware y software. Entre tales empresas se tienen: IBM, CISCO, Citrix, iPass y Gartner Consulting.

5. Conclusiones

Las empresas pueden obtener una ventaja competitiva y beneficios económicos si logran implementar una estrategia corporativa en torno a la consumerización y el BYOD, que permita reducir la complejidad de la gestión, los agujeros de seguridad y la exposición financiera de la organización a terceros.

A partir de la complejidad inherente del ecosistema de dispositivos móviles existentes es necesario que se creen dentro de las compañías puestos de trabajo específicos, para la monitorización de los dispositivos conectados, y así entender mejor las necesidades de los usuarios.

Si las empresas no integran sus políticas de seguridad de la información con las estrategias del negocio se exponen al aumento de costos por las siguientes dos razones: reducción de la productividad de sus empleados y percepción de que los departamentos de TI han perdido relevancia en sus funciones.

6. Referencias bibliográficas

Best practices to make BYOD simple and secure. A guide to selecting technologies and developing policies for BYOD programs. Citado de internet del URL: www.citrix.com/byod, el 14 de noviembre de 2012.

Enterprises Must Develop Bring-Your-Own-Device (BYOD) Policies. Citado de internet del URL: http://www.cmswire.com/cms/information-management.com, el 14 de noviembre de 2012.

The new workplace: supporting “Bring your own”. IBM. Citado de internet del URL: http://www-935.ibm.com/services/uk/en/it-services/pdf/The_New_Workplace_Supporting_bring_your_own.pdf, el 14 de noviembre de 2012.

Cómo citar este artículo:
REYES VÁSQUEZ, Virgilio Ernesto. “BYOD y la movilidad corporativa”. Ing-novación. Revista semestral de ingeniería e innovación de la Facultad de Ingeniería, Universidad Don Bosco. Diciembre de 2012 – Mayo de 2013, Año 3, No. 5. pp. 117-121. ISSN 2221-1136.