Retos de seguridad para las empresas a partir de BYOD

ESET Latinoamérica: Av. Del Libertador 6250, 6to. Piso - Buenos Aires, C1428ARS, Argentina. Tel. +54 (11) 4788 9213 - Fax. +54 (11) 4788 9629 - info@eset-la.com, www.eset-la.com

Autor:
H. Camilo Gutiérrez Amaya - Especialista de Awareness & Research

Fecha: Octubre 2012

Índice

Introducción

El fenómeno de que los empleados de una empresa utilicen sus propios dispositivos para cumplir con las tareas diarias del trabajo se ha consolidado en los últimos meses y hoy se conoce como la tendencia **BYOD** (por las palabras en inglés *Bring Your Own Device*). La gran dependencia que se ha desarrollado por la conectividad y el acceso a la información en cualquier lugar y momento, combinado con los cada vez más livianos y portables dispositivos personales, ha dado un gran impulso a este fenómeno.

Pero estas nuevas tendencias traen asociados riesgos para la seguridad de la información corporativa; lo cual lleva a que las áreas encargadas de estos temas planteen soluciones de acuerdo a la realidad de la empresa y procurando evitar conflictos con el desarrollo tecnológico.

El objetivo de este artículo es presentar cuáles son las principales características de la tendencia **BYOD**. Se tratará la realidad del fenómeno en la región y el reto que representa este fenómeno para la gestión de la seguridad en las empresas. Finalmente se enunciarán una serie de consejos que debería seguir una empresa que esté iniciando o revisando la implementación de políticas de BYOD en su compañía, garantizando siempre la seguridad de su información.

De lo que muchos hablan: BYOD

Una de las características principales que aprovechan los usuarios de sus dispositivos móviles, además de su portabilidad, es la facilidad que ofrecen para el trabajo colaborativo. Esto lo hacen, mayoritariamente, apoyados en el crecimiento y las innovaciones que brindan las redes sociales y las tecnologías de conectividad.

Precisamente la convergencia en el uso y aprovechamiento de todas estas características ha hecho que se consolide lo que se conoce como tendencia BYOD: la incorporación de dispositivos tecnológicos de los empleados en el ámbito laboral para cumplir con las tareas propias del quehacer profesional. Sin lugar a dudas, este fenómeno plantea una serie de riesgos y oportunidades para las empresas.

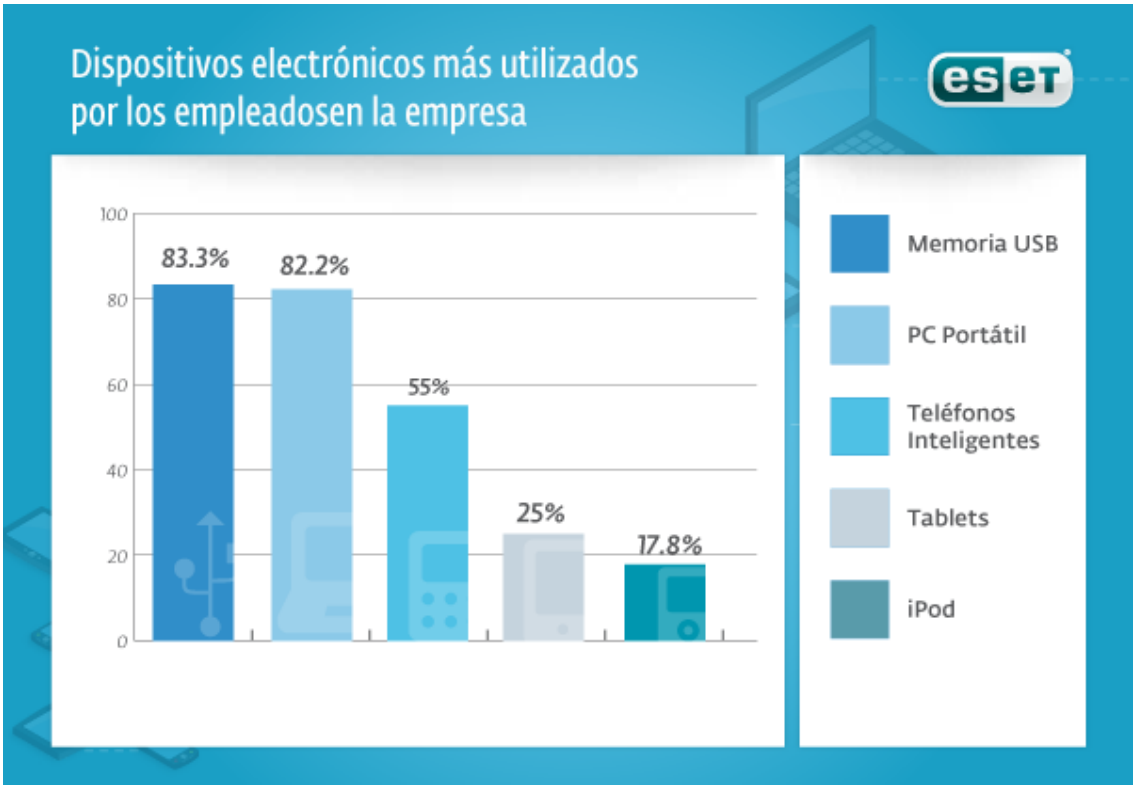
En este escenario, las compañías deberían aprovechar las ventajas que ofrece adoptar esta tendencia, y a su vez tomar todas las medidas preventivas para garantizar la protección de su información. Por ejemplo, las empresas mejorarían la productividad si consideraran que para los empleados puede ser mucho más cómodo trabajar en sus

propios dispositivos, pudiendo llevarlos consigo y de esta forma responder rápidamente a las novedades que se presenten. De igual manera, en ese contexto es esencial que las corporaciones cuiden la exposición de información sensible para evitar la pérdida o fuga de la misma. .

Algunas cifras sobre BYOD

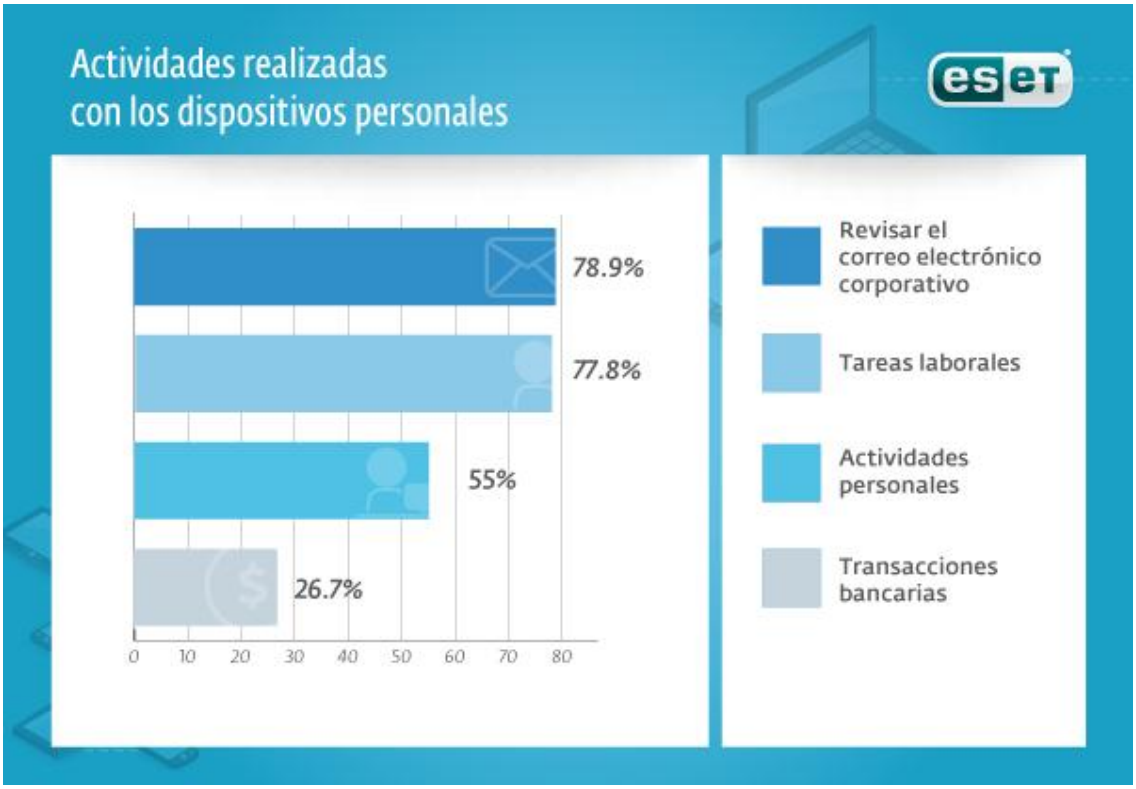
En agosto 2012, ESET Latinoamérica realizó una encuesta sobre esta temática. Participaron en ella personas, en su mayoría, entre los 21 y 30 años (43.9%) y entre los 31 y 50 años (32.8%). De los participantes, la mitad trabaja en pequeñas empresas, el 20% en organizaciones medianas y el 30% restante en compañías más grandes, con más de 100 empleados.

Algunos de los resultados dan cuenta los dispositivos personales que más se utilizan en el lugar de trabajo son las computadoras portátiles y los teléfonos inteligentes, además de las tabletas que tienen una participación alta dentro de estos dispositivos. A pesar que los dispositivos USB para almacenar datos no están incluidos estrictamente en la categorización de BYOD, en la encuesta han sido elegidos por el 83.3% de los consultados como dispositivos para manejar información corporativa.



En relación al acceso de información corporativa, cerca de la mitad de los encuestados afirmó utilizar redes WiFi, mientras que un poco más de la tercera parte accede a través de una red cableada provista por la organización. Como se mencionó los dispositivos personales se convierten en una herramienta para desarrollar las tareas laborales, al punto que el 58,3% de los encuestados indicó que su utilización facilita sus labores.

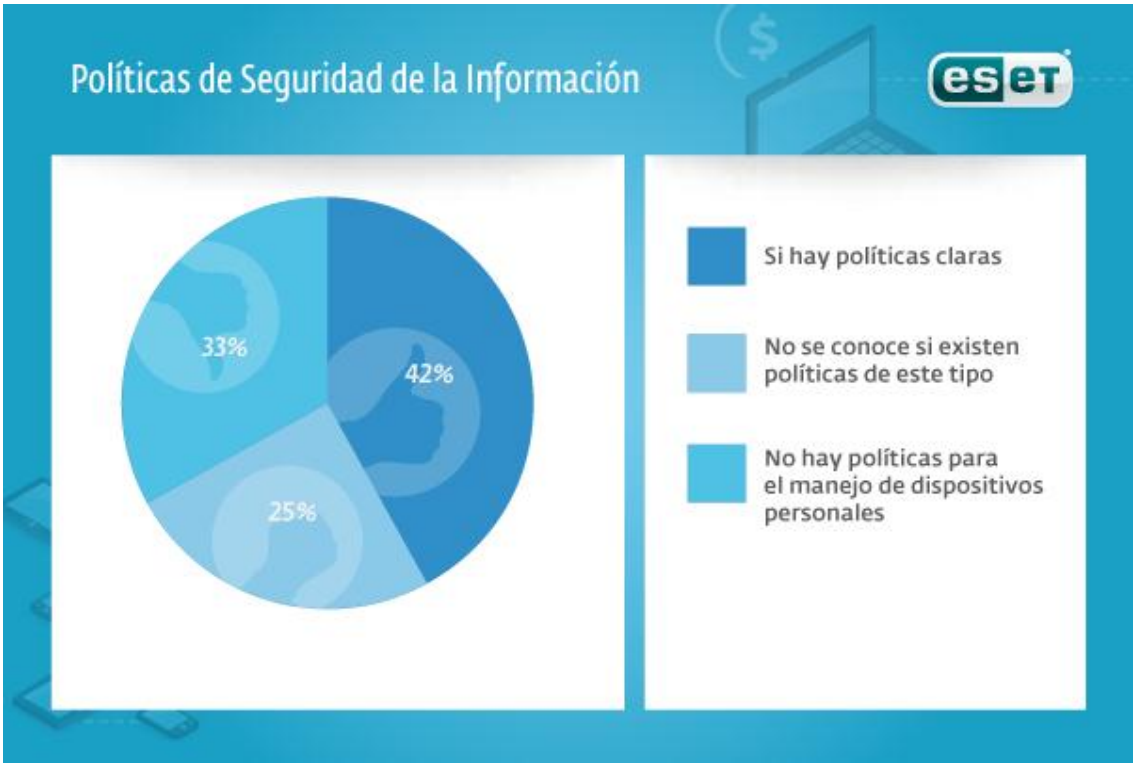
Como parte de las tareas más relevantes que se realizan con los dispositivos personales se encuentra la revisión del correo electrónico corporativo y el apoyo a las tareas del trabajo. De las personas que utilizan los dispositivos personales en la oficina, el 55% los usa únicamente para actividades personales que no están relacionadas con el trabajo. Queda claro que este tipo de usos también tiene como contrapartida la distracción por parte del empleado.



Respecto al uso de la información del trabajo, más de la mitad de los encuestados la almacena en su dispositivo personal y cerca de un 20% la revisa remotamente sin guardarla en su dispositivo; apenas una quinta parte dice eliminarla una vez terminado el trabajo. Estas cifras evidencian una tendencia que debería ser atendida por las empresas, y es que los usuarios utilizan sus dispositivos personales para guardar información corporativa.

Uno de los datos más interesantes tiene que ver con que cerca de la mitad de los encuestados no maneja la información de la empresa de forma cifrada en su dispositivo personal y el 15,6% dice no saber cómo se maneja la información. Solamente la tercera parte reconoce manejar la información cifrada. Tanto la decisión de utilizar la información cifrada como el conocimiento por parte de los usuarios dentro de la red corporativa, son cuestiones de importancia a tener en cuenta por parte de quienes se encargan de gestionar la seguridad de la información de una compañía.

Finalmente, en menos de la mitad de las empresas los encuestados reconocieron que existen políticas claras para el manejo de la información, mientras que una tercera parte de los encuestados reconoció lo contrario. La cuarta parte restante no conoce si existen políticas de este tipo.



Cambio de paradigma en la infraestructura

Al revisar los resultados mencionados anteriormente se puede inferir que se están dando cambios en la forma en que se maneja la información corporativa. Estas nuevas tendencias en las organizaciones llevan a que los departamentos de TI deban cambiar la concepción del manejo de sus recursos para garantizar la seguridad de los datos de la empresa.

Estas nuevas formas de manejar la información hacen que las organizaciones presten mucha más atención a la forma en que los usuarios se conectan a las redes de la empresa para manipular la información. Es decir, buscan garantizar la seguridad, los altos niveles de rendimiento y el control adecuado para los diferentes tipos de dispositivos que se podrían conectar para compartir información.

Esta nueva concepción alrededor del cómo se accede a la información hace que las áreas de TI se preocupen cada vez menos por la infraestructura física a la vez que se reducen los costos relacionados a la adquisición de dispositivos como teléfonos celulares y portátiles. Sin embargo, también plantea nuevas preocupaciones ya que se generan nuevos riesgos

que deben ser gestionados adecuadamente para garantizar la seguridad de la información.

Debido a que en este momento la tendencia se está consolidando y para muchas organizaciones aún puede ser un tema que consideren ajeno, se encuentra poca claridad en las empresas para el manejo de la información. De esta manera, se dan casos en los que no hay ninguna posición respecto de la utilización de dispositivos personales en el lugar de trabajo, y en muchos casos optan por cerrar cualquier forma de interacción o simplemente lo dejan abierto.

Todo este cambio de concepción implica que las políticas de seguridad de las compañías se empiecen a enfocar en mayor medida en la efectividad de la seguridad de las redes, con controles o seguimientos sobre los empleados y las aplicaciones que se utilizan y no exclusivamente sobre los dispositivos.

Retos para la empresa

Como se ha mencionado, la adopción de BYOD implica para las organizaciones un cambio en la forma de gestionar la seguridad de la información en una amplia variedad de dispositivos, aplicaciones y sistemas operativos. A continuación se mencionan algunos de estos retos.

Gestión de riesgos

Lo primero para garantizar la seguridad de la información es una adecuada gestión de riesgos la cual parte del conocimiento de los activos de información con los que cuenta la empresa. Los análisis de riesgos deben partir de la clasificación de la información con el objetivo de establecer, por ejemplo, cuáles son los datos más sensibles que requieren mayores niveles de protección, qué información se puede acceder desde dispositivos personales, qué información puede accederse por fuera de la red de la empresa y a qué información se debe restringir el acceso.

A partir de este análisis se llega a establecer cuáles son las medidas de control más adecuadas para garantizar la seguridad de información, que van desde dispositivos o medidas de carácter tecnológico (soluciones antivirus, DLP, VPN, Firewall, IDS, IPS, etc.) hasta el establecimiento de políticas para la gestión de dispositivos, donde se determina qué tipo de dispositivos y aplicaciones es posible utilizar. Además, medidas como los

controles de acceso a la red (NAC) pueden ser de gran ayuda para tener un monitoreo de cómo se utilizan los recursos de red compartidos por los empleados.

Toda esta gestión de riesgos, debe estar complementada con un adecuado plan de educación y concientización que involucre a todos los niveles de la organización para que conozcan las implicaciones del uso de sus dispositivos personales, los riesgos a los que están expuestos y las medidas de seguridad que deben tener en cuenta.

Homeworking

Al ser posible el manejo de información laboral en dispositivos personales, otras tendencias como la posibilidad de trabajar desde la casa (*homeworking)* tienen un impulso importante. Este tipo de tendencias promueven que las empresas incluyan en sus análisis otro tipo de riesgos y que consideren algunas implicaciones legales que pueden llegar a tener. Por ejemplo, a partir de la manipulación de información laboral en dispositivos con sistemas operativos o aplicaciones *no licenciadas.* Es necesario entonces que las empresas asignen licencias en los dispositivos de los empleados o consideren alternativas, como por ejemplo el uso de software libre en estos casos.

Disposición de la información

Si el empleado manipula información de la empresa en su dispositivo, debe estar claro cuál será la disposición de la misma una vez terminada la relación contractual. Ya que es muy complicado tener la seguridad que está información será eliminada. Una vez más es necesario tener claro qué tipo de información se puede descargar y manipular desde dispositivos personales. Además, aspectos contractuales como la firma de acuerdos de confidencialidad pueden ser complementos que brinden a la empresa herramientas adicionales para actuar en caso de que la información sea expuesta.

Gestión de aplicaciones

Ya se mencionó que uno de los principales retos para las empresas es la gestión de la gran diversidad de aplicaciones que un empleado puede tener instalado en su dispositivo. El reto para las organizaciones se vuelca entonces en garantizar que los dispositivos, a través de los cuales se accede a la información, cuenten con aplicaciones seguras que no pongan en peligro la integridad de la información.

En esta misma línea es necesario que la empresa diferencie el uso que los empleados puedan tener de los recursos de la misma a través de sus dispositivos personales. Es así como seguramente muchos de los empleados solamente utilizarán sus dispositivos para manipular información personal. En estos casos la gestión de los recursos de red se vuelve sensible para impedir la intrusión ilegal a los sistemas de la compañía.

¿Permitir o prohibir?

Hasta este punto se han mencionado los retos y las ventajas que esta tendencia tiene para las empresas. De esta forma, la pregunta que surge es: ¿Se debe permitir o prohibir el uso de dispositivos personales en el lugar de trabajo para manipular la información de la empresa?

La respuesta en este caso tiene que estar precedida de un juicioso análisis de riesgo. El resultado de este análisis le da a las organizaciones el panorama completo de qué información maneja y cuáles son las características más adecuadas para garantizar su seguridad.

Más allá de si finalmente se adopte o no el BYOD en la organización, lo más coherente es que las organizaciones se preocupen por tomar una postura ya que este tema es una realidad y lo más peligroso para la información es adoptar una posición indiferente.

Lineamientos de seguridad

Independientemente de la posición que adopte la empresa alrededor del BYOD, es necesario que se tomen algunos recaudos para garantizar la seguridad de su información:

- Analizar la capacidad y la cobertura que tienen las redes corporativas para permitir el acceso de dispositivos diferentes a los de la empresa. El acceso a estos recursos debería estar protegido con credenciales que permitan individualizar quién accede y qué tipo de información manipula.
- La gestión debe estar basada en roles. El acceso a la información debe ser restringido de forma que se garantice que solamente podrán acceder a la información aquellas personas que realmente lo necesiten. Esta gestión debe ser precedida de una adecuada clasificación de la información que le permita a la empresa conocer todos sus activos de información.

- Teniendo en cuenta que son muchos los dispositivos en el mercado, es prudente hacer un análisis de qué tipo de dispositivos son los más adecuados para manejar la información de la empresa.
- Según la diversidad de dispositivos y aplicaciones que se pueden manejar, se debe redactar la política que aclaré qué dispositivos pueden acceder a la información corporativa. Además, para garantizar que códigos maliciosos no afecten los datos, todos los dispositivos deben contar con soluciones de seguridad que detecten proactivamente este tipo de amenazas.
- El acceso a través de conexiones WiFi debe ser correctamente configurado, utilizando protocolos de cifrado, para garantizar la seguridad de la información. El tráfico de dispositivos BYOD debería ser claramente identificable, además de tener un control más estricto.
- Para permitir el acceso remoto, el uso de tecnologías como VPN garantizan la protección de la información que se manipula. Además, debe llevarse un control de quién accede y los cambios que se realiza.
- La educación debe ser un pilar importante para que todos los usuarios sean conscientes de los riesgos a los cuales pueden verse expuestos y cuáles son los cuidados que deben tener en cuenta al manejar la información de la empresa.
- Realizar con mayor periodicidad los análisis de riesgos y vulnerabilidades para determinar el estado de la empresa ante esta tendencia, ya que la aparición de nuevos dispositivos o aplicaciones pueden beneficiar o afectar a las organizaciones.

Conclusión

Cuando se habla de BYOD se hace referencia a una tendencia consolidada y ante la cual las empresas deben hacer un análisis de riesgos para tomar una posición al respecto. La adopción de esta tendencia por parte de las compañías puede traer grandes beneficios relacionados con la disminución de gastos en infraestructura, la comodidad de los empleados para el manejo de la información y por tanto el incremento de la productividad. Pero a su vez, enfrenta a la empresa a nuevas amenazas que deben ser gestionadas, las principales y quizás las más preocupantes son la fuga y el acceso no autorizado a la información.

Es así como las empresas para enfrentar estos retos deben establecer una mezcla entre políticas claras para el manejo de la información y el uso de herramientas adecuadas que permitan la gestión de la seguridad de la misma. Todo esto debería estar alineado con los objetivos del negocio, pues cualquier decisión que se tome debe estar enfocada en

aumentar la productividad y hacer más ágiles y seguros los procesos internos. Estas dos medidas se deben complementar con un adecuado plan de divulgación y educación para que a todos los niveles de la organización conozcan las restricciones alrededor del manejo de la información.