BYOD: COLABORACIÓN VS RIESGO

Pinilla Alarcón, Juan Fernando.
jpinillaalarcon@gmail.com.
Universidad Piloto de Colombia

Resumen - Con la llegada de los dispositivos inteligentes como Smartphone's y tabletas se ha generado la tendencia del BYOD, las personas conectan sus dispositivos personales en la empresas, accediendo desde el mismo a aplicativos empresariales, lo cual supone un riesgo para la información de la compañía y la seguridad perimetral de la misma, en este artículo se busca sensibilizar y exponer diferentes puntos de vista sobre este fenómeno.

Abstract - With the advent of smart devices like Smartphone's and tablets has led the trend of BYOD, people connect their personal devices in the companies, accessed from the same to enterprise applications, which poses a risk to company information and perimeter security of it, this article seeks to sensitize and expose different views on this phenomenon.

Índice De Términos: Dispositivo inteligente, BYOD, Selfie, Rooteo.

I. INTRODUCCIÓN

A PARTIR DE LA LLEGADA DE LOS DISPOSITIVOS INTELIGENTES A LA VIDA COTIDIANA DE LAS PERSONAS SE GENERÓ UN BOOM PARA EL ACCESO A REDES SOCIALES, todos queremos estar conectados a todo momento y en todo lugar, generamos información, tomamos fotos a situaciones divertidas o compartimos nuestros "selfies", por ello no es sorpresa cuando llegamos a la compañía, con nuestros teléfonos celulares o tabletas, e iniciar la jornada laboral y tener algunos espacios de tiempo para mirar las últimas publicaciones de Facebook o generar algún comentario en WhatsApp, el proceso ha sido tan transparente que las empresas en un primer momento no vieron esta situación como un riesgo para su información, sin embargo, con el transcurrir del tiempo, ya no solo utilizamos nuestros dispositivos para temas personales, resulta más "cómodo" ver el correo de la empresa en nuestro teléfono celular, durante una reunión o inclusive estar aguardando un correo importante durante la hora del almuerzo. Esta situación es tan común y ha sido producto de los nuevos desarrollos pensados para la movilidad.

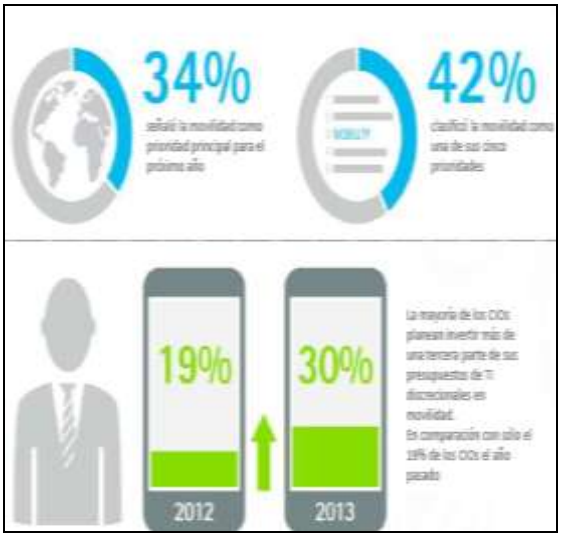

Fig1. La movilidad como generador de ingresos clave y canal primario para el compromiso al cliente [1]

Los correos empresariales y aplicativos son ahora fácilmente accesibles desde Internet, lo que lleva a cuestionarnos si aún es válido el concepto de seguridad perimetral de la compañía.

Fig2. La Gran división [2]

Recordemos que la pérdida de datos en una empresa puede terminar en multas, procesos penales, afectación de la reputación, etc.
El reto es más complejo cuando se tiene un escenario de miles de aplicaciones en las tiendas de descarga para dispositivos y se desconoce si lo que se está instalado es una aplicación original o por el contrario el paquete descargado tiene embebido código malicioso.
Actualmente muchas personas sacrifican la seguridad del dispositivo para instalar ciertos programas, realizar actualizaciones sobre el dispositivo inteligente, aplicando lo que se conoce como rooteo haciendo que se eleven las posibilidades de que el equipo sea más vulnerable.

El tema de hurto o pérdida de dispositivos, es bastante alto en Colombia, sobre éste aspecto debemos recordar que en la mayoría de los casos toda la información que se descarga sobre el dispositivo se almacena en la memoria extraíble del mismo, a pesar que es posible activar opciones de cifrado sobre la misma, no activamos esta funcionalidad, ya que se está sacrificando velocidad de acceso a los datos almacenados y el temor a la pérdida de los mismos en caso de olvido de contraseñas.

A continuación comparto una infografía generada por ISACA, sobre las múltiples formas de fuga de información y el costo de su pérdida, como se aprecia el panorama para el segmento BYOD es alarmante:

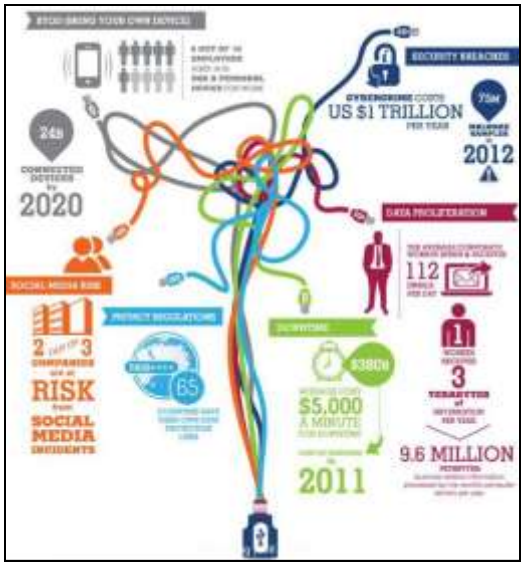

Fig3. Extrayendo valor de la información del caos [3]

Un factor importante que no es visible desde un aspecto técnico es el tema generacional, de acuerdo a la información recopilada por una importante empresa de gestión de dispositivos móviles (http://www.soti.net/es) se obtuvieron los siguientes datos acerca de las personas pertenecientes a la generación Y (personas nacidas entre los años 1982 hasta 2004):

• 75% utilizan activamente dispositivos móviles personales en el lugar de trabajo.

• 35% no puede resistir un día sin revisar las redes sociales.

• 47% no logran 24 horas sin la necesidad de enviar un texto.

• 66% cree que los departamentos de TI no tienen el derecho de controlar o restringir el comportamiento de sus dispositivos.

• 52% de los profesionales de TI afirman que los empleados siguen las políticas de TI, pero 71% de la fuerza de trabajo de la generación Y no obedecen las reglas de la compañía.

Ahora que tenemos el escenario con algunos riesgos conocidos, debemos apreciar la proyección de esta tendencia hacia el futuro:

Fig4. Hoy vs Mañana [4]

Basados en las cifras se incrementa la necesidad de tomar acciones, sabemos que el BYOD será una tendencia que apalancará los procesos en las compañías y generará un grado de confort para los dueños de los dispositivos donde se tendrá una situación gana-gana, por ello ahora debemos enfocarnos en hacer una revisión de cómo aplicar seguridad sin transgredir las barreras de la confidencialidad del dueño del dispositivo y la información confidencial de la empresa.

II. POSIBLES PASOS PARA PROTEGER LA INFORMACIÓN ANTE EL BYOD

1. Concientización: En mi concepto, es el aspecto con mayor relevancia cuando se está hablando de seguridad y así está demostrado por la teoría donde aplica la frase "el eslabón más débil es el usuario", entonces, debemos generar una estrategia donde se invite al usuario a aplicar normas básicas para proteger su equipo y su propia información personal, evitar descargar aplicaciones no conocidas, desconfiar de aplicaciones gratuitas que requieren demasiados permisos sobre el teléfono (por ejemplo, acceso a mensajes SMS o la libreta de contactos) o activar un bloqueo de pantalla e instalar software antivirus de una empresa reconocida en el mercado.

2. Capacitación: La empresa debe generar una estrategia de capacitación para los dueños de los dispositivos con el fin de orientarlos en los procedimientos a seguir para acceder a los recursos de la empresa, por ejemplo: "No olvides apagar los datos de tu teléfono y conectarte a la red inalámbrica para acceder al correo corporativo" ó "instala un antivirus reconocido sobre tu dispositivo y no olvides analizar tu Smartphone con periodicidad en busca de amenazas.

3. Documentación: La compañía no solo debe generar políticas para garantizar la confidencialidad, integridad y disponibilidad de los datos que estén en tránsito sobre el dispositivo, también debe generar guías que le permitan a los colaboradores conocer el nivel de seguridad en el que se encuentra su dispositivo, para ello una simple lista de verificación de requisitos puede apoyar esta labor y evita sobrecostos al disminuir el soporte del área de tecnología.

4. Soporte: La compañía debe establecer lineamientos bien definidos especificando en que situaciones aplica el soporte por parte del área de tecnología y en cuales casos no.

5. Auto Soporte: La compañía debe generar procedimientos que permitan al usuario brindarse auto soporte en situaciones específicas.

6. Aspectos Jurídicos: El tema del BYOD tomó a todos por sorpresa, sin embargo, es necesario aplicar dentro del reglamento de la compañía estatutos donde se comprometa al colaborador a seguir los lineamientos de la misma respecto al manejo de sus dispositivos inteligentes personales dentro de la empresa.

7. Documentarse sobre procesos de implementación y casos de éxito aplicables al BYOD: Esto permite que la compañía agilice las técnicas para implementar los esquemas de seguridad a aplicar tanto a nivel de dispositivos como de personas.

8. Implementar herramientas de software: Siempre debemos procurar implementar controles adicionales, es por esto que se debe contemplar la adquisición de software que permita el monitoreo de los equipos, esto con el fin de tener controles que automaticen procesos y cubrir las brechas restantes de seguridad.

9. Hardening de dispositivos: Por último la empresa debe ingresar la tendencia de BYOD dentro de su estrategia de gobierno, ya que los dispositivos inteligentes generarán un riesgo alto importante dentro de la organización, adicionalmente contemplar esta tendencia fortalecerá en ultimas los objetivos del negocio "más rendimiento y colaboración", por ello se sugiere visitar el sitio web de ISACA y apreciar la documentación relacionada al hardening para estos dispositivos. [5]

III. CONCLUSIONES

1. Las empresas deben asumir que los colaboradores no abandonarán los dispositivos móviles, por ende, debe generar estrategias para proteger la información corporativa.

2. La mejor manera para generar el proceso de adopción al cambio es generar la cultura de seguridad por medio de la concientización al usuario.

3. Ninguna herramienta es tan efectiva para proteger la información, como el usuario en sí mismo.

4. El proceso de adopción y apoyo para la implementación del BYOD debe surgir de la alta gerencia, ya que igual que cualquier proyecto requiere recursos, presupuestos y ajustes de procesos dentro de la organización

5. La implementación del BYOD generará ahorro sobre las empresas, ya que se evitan inversiones en renovación de equipos, planes de datos para los dispositivos y apalancará la colaboración dentro de la compañía y por ende eficiencia y rapidez en los procesos, lo que se traduce en ganancia.

6. No solo se deben tener en cuenta los aspectos técnicos, como lo vimos en el artículo, inclusive un brecha generacional puede ser factor de riesgo para fuga de información, como resultado del rechazo hacia el cambio y la correcta adopción de las políticas de seguridad.

7. No es suficiente con desarrollar planes para concientizar, políticas a seguir, siempre existirá una brecha que pone en riesgo la información de la compañía, por ello se debe pensar en planes de inversión para implementar herramientas que apoyen de manera automática el control de la información.

8. No se puede proteger lo que no se conoce, por ello se sugiere realizar actividades con los usuarios para conocer los dispositivos y los aplicativos que utilizan.

9. Se deben evitar métodos de ensayo y error para realizar el Hardening sobre los dispositivos inteligentes, por ello se sugiere antes de cualquier configuración documentarse accediendo a artículos publicados por entidades reconocidas, estos generan una guía, evitando reprocesos generando ahorros de tiempo y dinero.

IV. REFERENCIAS

[1]http://www.mercadoit.com/blog/productos-hardware-it/accenture-movilidad-2013/
[2] Presentación: Los Retos de Seguridad en la Administración de la Movilidad Empresarial (Empresa SOTI)
[3]http://www.isaca.org/Knowledge-Center/Research/ResearchDeliverables/Pages/BYOD-Audit-Assurance-Program.aspx
[4] Presentación: Los Retos de Seguridad en la Administración de la Movilidad Empresarial (Empresa SOTI)
[5]Securing-Mobile-Devices [online], Disponible en: http://www.isaca.org/Knowledge-Center/Research/Documents/Securing-Mobile-Devices-Using-COBIT-5-for-Information-Security_res_English_1112.pdf