Seguridad Para Byod
(Trae Tu Propio Dispositivo)

Rincón Quevedo Javier Antonio, Salgado Vivas Fabián Guillermo
f.salgado.vivas@gmail.com javier.rincon@gmail.com
Especialización en Seguridad Informática, Universidad Piloto de Colombia
Bogotá, Colombia

Abstract- The communication needs at enterprising level in the world today, have made personal mobile devices to become essential tools for productive development of any company. Deciding on the use of this technology requires companies to take security measures to protect their most valuable asset "information" this to ensure that the fundamental pillars of security are maintained: Confidentiality, Integrity and Availability and giving additional value to the core business.

Keywords: BYOD, mobile devices, computer security policies.

Resumen- Las necesidades de comunicación a nivel empresarial del mundo de hoy, han hecho que los dispositivos móviles personales se conviertan en herramientas esenciales para el desarrollo productivo de cualquier compañía. El decidirse por el uso de esta tecnología obliga a las empresas a adoptar medidas de seguridad con el fin de proteger su activo más preciado "la información" garantizando que se conserven los pilares fundamentales de la seguridad: Confidencialidad, Integridad y Disponibilidad y dando valor agregado al core del negocio.

Palabras clave: BYOD, dispositivos móviles, seguridad informática, políticas.

I. INTRODUCCIÓN

Hoy en día las compañías vienen adoptando nuevas políticas empresariales, que permitan que dentro de su infraestructura tecnológica se dé uso de dispositivos móviles propios de sus empleados, tecnología conocida comúnmente como "trae tu propio dispositivo o BYOD".

La adopción de uso de este tipo de políticas empresariales trae para las compañías varios beneficios, pero también plantean la implementación de controles de seguridad y cumplimento de ciertas normativas que apoyen el objetivo comercial de la organización y no la pongan en peligro.

A partir de este escenario las compañías o las empresas deben tomar decisiones ligadas al uso de BYOD, como que medidas de seguridad se deben implementar con el fin de no poner en riesgo sus activos principales. Esta situación se ha venido convirtiendo en un verdadero desafío en la aplicación de las prácticas esenciales de gestión de la seguridad y del riesgo.

A través de este documento se busca dar a conocer una guía de beneficios y riesgos asociados al uso de BYOD, al igual que un una serie de consideraciones muy importantes relacionadas con la seguridad que se debe diseñar e implementar cuando se opta por el uso de esta tecnología, estas determinaciones deben abarcar todos los aspectos propios de estos sistemas y deben buscar proteger los datos de la compañía con el apoyo de los empleados.

II. BYOD (TRAE TU PROPIO DISPOSITIVO)

Los dispositivos móviles vienen invadiendo las empresas, lo que ha hecho que nazca una política empresarial que permite a los empleados utilizar sus dispositivos móviles propios en el desarrollo de sus actividades; esto sin duda y de acuerdo a estudios realizados hace que se aumente el nivel de productividad de la personas pero igualmente puede poner en riesgo la seguridad de los datos de la organización.

Es por esto que cuando una compañía opta por la implementación de este modelo, debe establecer un nivel de seguridad que permita gestionar los dispositivos personales y los accesos de estos a la red corporativa.

Adicionalmente y como es de conocimiento mundial el uso de los dispositivos móviles está superando cualquier expectativa, lo que hace que las empresas deben trabajar de manera más fuerte en el establecimiento de políticas y controles de seguridad que les permita mantener el control de acceso y la pérdida posible de información.

III. TENDENCIA BYOD

La firma Microsoft en su Newsletter de Seguridad para Latinoamérica de mayo 2014, indica que a través de investigaciones recientes se ha encontrado que el 78% de las organizaciones están optando por que sus empleados lleven sus propios dispositivos móviles a su oficina para realizar actividades de trabajo. [1]

Microsoft también indica que el 67% de los trabajadores de pequeñas y medianas empresas utilizan dispositivos móviles propios en sus oficinas, a pesar de que las compañías donde laboran no tengan establecida esta política empresarial, convirtiéndose en un desafío mucho mayor.

A. Encuesta

Teniendo en cuenta las cifras indicadas por la multinacional Microsoft y con el fin de tener mayor claridad de esta situación en el ambiente laboral colombiano, se decide efectuar una encuesta a un total de 40 personas con conocimientos altos en tecnología, para lo cual se obtienen los siguientes resultados:

La primera pregunta que se formula está relacionada con el conocimiento sobre esta política empresarial, como se observa en la gráfica de resultado el 87% de los encuestados conocen lo que es BYOD, situación que facilita la comprensión y nivel de conciencia empresarial, que permite adicionalmente tener un muestreo claro de la situación para BYOD en Colombia. Figura 1.

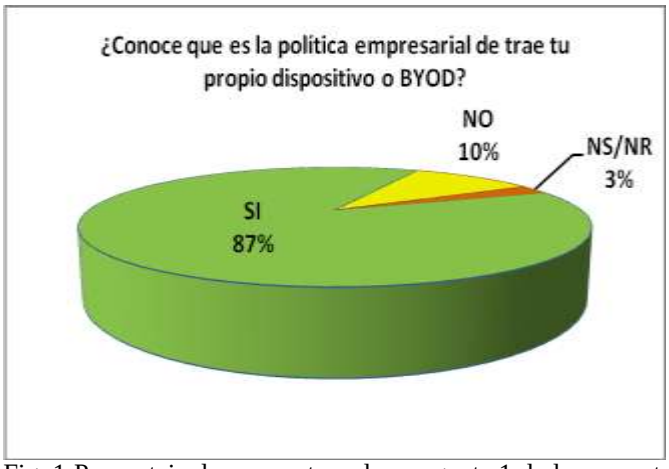

Fig. 1 Porcentaje de respuestas a la pregunta 1 de la encuesta – Autores: Fabián Salgado, Javier Rincón.

Para la segunda pregunta se busca conocer si los encuestados de acuerdo a la definición de la política empresarial BYOD, estarían o no de acuerdo con la implementación de la misma en su compañía. Los resultados obtenidos muestran que más de la mitad de las personas estarían de acuerdo con la implementación de BYOD en su compañía, situación que compromete mucho más a las áreas de seguridad de la información. Figura 2.

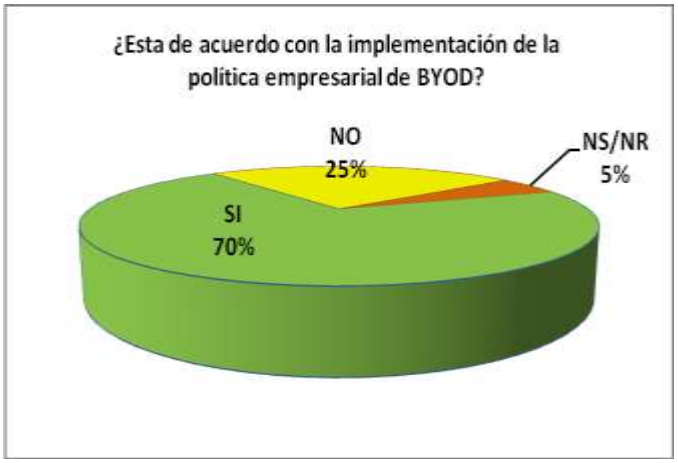

Fig. 2 Porcentaje de respuestas a la pregunta 2 de la encuesta – Autores: Fabián Salgado, Javier Rincón.

A través de la tercera pregunta lo que se busca es conocer, sí los encuestados creen que el implementar BYOD trae beneficios o riesgos, este es un resultado fundamental a la hora en que una compañía decida si implementa o no este sistema. Como se observa los resultados la mayor parte de los funcionarios cree que su implementación traerá beneficios; aunque se debe tener en cuenta que las

[1] http://technet.microsoft.com/library/dn656905.aspx

personas pertenecen al área de tecnología que muy seguramente se verán beneficiadas en caso de implementar el uso de sus propios dispositivos. Igualmente se pudo percibir que aquellos funcionarios que optaron por indicar que el uso de BYOD acarrea más riesgos, son aquellos que tienen un mayor conocimiento en aspectos de seguridad y para quienes significa el uso de dispositivos móviles propios de los empleados en el desarrollo de actividades laborales todo un reto. Figura 3.

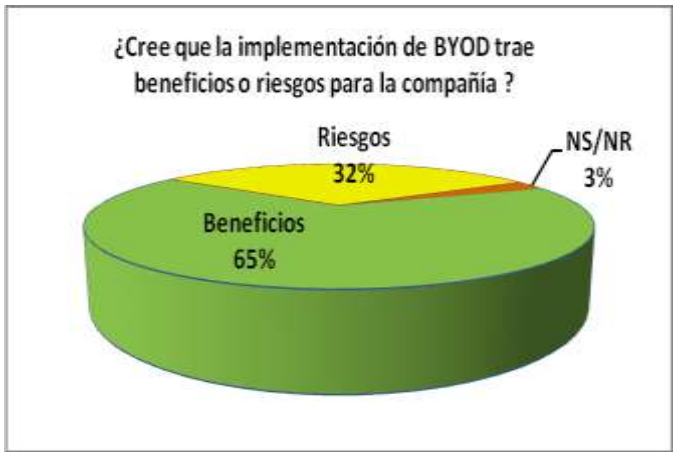

Fig. 3 Porcentaje de respuestas a la pregunta 3 de la encuesta – Autores: Fabián Salgado, Javier Rincón.

La última pregunta de nuestra encuesta, busca conocer si el nivel de conciencia de seguridad con la implementación de BYOD debe aumentar o disminuir y si los funcionarios estarían dispuestos a aceptar las nuevas medidas de seguridad en caso de que se deban aumentar. Los resultados de esta pregunta cómo se observan en la gráfica, son altamente beneficiosos desde el punto de vista de nosotros como Especialistas de Seguridad, ya que si se cuenta con un alto nivel de conciencia de los funcionarios de la compañía respecto del uso seguro de los dispositivos móviles, se facilitará de gran manera su implementación y por consiguiente la aplicación de las nuevas políticas destinadas para el aseguramiento de los datos allí utilizados, acarreando consigo no solamente beneficios para la compañía sino también para sus empleados que se sentirán favorecidos con el aseguramiento de sus dispositivos móviles (tabletas, smartphone, portátiles, relojes inteligentes, cámaras, etc.).

Fig. 4 Porcentaje de respuestas a la pregunta 4 de la encuesta – Autores: Fabián Salgado, Javier Rincón.

IV. VENTAJAS Y RIESGOS DEL USO DE BYOD

Debido a que una parte fundamental de la encuesta que realizamos buscaba conocer, sí la implementación de BYOD traía ventajas o riesgos, creemos importante que se den a conocer los dos puntos de vista a fin de que este artículo sirva igualmente como base en la definición de uso o no de los dispositivos móviles propios de los empleados para el desarrollo de tareas laborales.

A. Ventajas

No cabe duda que la mayor ventaja que da el uso de dispositivos móviles propios, en el desarrollo de actividades laborales está relacionado con el aumento del rendimiento y comodidad que proporciona a los empleados, ya que estos podrían trabajar en cualquier momento y desde cualquier lugar en el que puedan establecer una conexión con su compañía.

Otra ventaja se da para la economía de la compañía que disminuye su inversión en dispositivos tecnológicos.

Otros estudios como los señalados por Inteco indican que se dan ventajas adicionales como: mejorar la relación y disponibilidad de comunicaciones con clientes, proveedores, administradores y entre departamentos de la misma compañía. También reduce costos de desplazamiento.[2]

[2] http://www.inteco.es/blogs/post/Seguridad/BlogSeguridad/Articulo_y_comentarios/moviles_personales_wearalbes_empresa_riesgos_byod

B. Riesgos

Como los habíamos observado a través de la encuesta, los Especialistas de Seguridad consideran que la implementación de la política BYOD trae consigo una diversidad de riesgos; que deben ser controlados porque de lo contrario dejarían expuesta la organización.

En nuestro caso se considera que el principal riesgo está asociado a las personas, pues ellos al ser los dueños de sus dispositivos, ¿estarían dispuestos a limitar en la mayoría de casos varias de sus funcionalidades, para satisfacer las necesidades de protección de la información de la compañía? Esto es un aspecto fundamental a tener en cuenta en el análisis de riesgo previo que se debe realizar para la implementación del uso de dispositivos móviles propios de los empleados.

Otros de los riesgos detectados en el uso de dispositivos móviles propios son los siguientes: Exposiciones de la información de la compañía en redes móviles que no poseen seguridad, instalación de cualquier tipo de aplicación por el usuario, ausencia de seguridad en el cifrado de la información almacenada en el equipo, ausencia de controles de acceso a los dispositivos, robo o pérdida de los dispositivos, infecciones o propagaciones por malware en la red de la compañía. En definitiva se da una pérdida de gestión de administración sobre los dispositivos por parte del área de TI de la compañía.

V. IMPLEMENTACIÓN DE BYOD DE FORMA SEGURA

Cuando se piensa en implementar la política empresarial de BYOD, se deben tener en cuenta grandes aspectos de seguridad y por tanto la implementación de controles que ayuden a conservar la confidencialidad, integridad, disponibilidad, no repudio y autenticidad de la información.

Igualmente es importante y para cumplir con la no violación de los principios de seguridad, tener en cuenta algunas reglas básicas en las que se deben fundamentar las recomendaciones de seguridad para la implementación de BYOD, que garanticen el uso de dispositivos móviles de forma segura dentro de una empresa, como los establecidos por Symantec[3] en una de sus publicaciones:

Los Cinco Pilares de Seguridad en los dispositivos móviles en la Empresa
1. Acceso de usuarios y aplicaciones
2. Protección de aplicaciones y datos
3. Administración de dispositivos
4. Protección contra amenazas
5. Uso compartido seguro de archivos

Fig. 5 Pilares de seguridad en los dispositivos móviles en la empresa Fuente: www.symantec.com

VI. RECOMENDACIONES DE SEGURIDAD PARA LA IMPLEMENTACIÓN DE BYOD

Si bien es cierto que el uso de dispositivos personales en las compañías a nivel laboral genera un valor agregado en el desarrollo de las actividades de los empleados, también se abre una brecha a nuevos riesgos que exponen la información de la organización y por esta razón se debe ser consiente que se deben tomar medidas necesarias para hacer más segura la implementación de esta tecnología y que a continuación damos a conocer:

A. Definir una política de servicio abierto bajo el criterio byod.

El objetivo principal de tener una política para la implementación BYOD en la organización es dar a entender a los empleados los límites que hay entre el mundo personal y el mundo laboral al momento de presentarse un conflicto entre los dos que pueda interferir en el desarrollo normal de las actividades del empleado y afectado el objetivo de negocio de la organización, por tal motivo la política que se defina debe tener como objetivo el poder minimizar los riesgos de seguridad que puedan afectar la organización.

La política debe contener lineamientos que aseguren los dispositivos que se encuentren fuera del perímetro de la empresa que es donde más se

[3] http://www.symantec.com/es/mx/products-solutions/solutions/detail.jsp?parent=mobile&child=5_pillars_mobile

pueden correr riesgos con la información contenida en los dispositivos, así como identificar cuáles van a ser los equipos que van a ser utilizados para la implementación de esta tecnología. Igualmente la política debe contemplar las recomendaciones de los dueños de la información sobre qué datos se pueden acceder a través de estos dispositivos móviles. Vale aclarar que la política no debe dejar a un lado el objetivo de negocio de la compañía.

B. Establecer una política de seguridad estricta para todos los dispositivos.

El establecer esta política permite que los empleados, estén obligados a cumplir esta directriz si quieren utilizar sus dispositivos personales con contraseñas robustas y pantallas de bloqueo automático, de lo contrario deberán utilizar los dispositivos proporcionados por las organizaciones y que cumplen con todos los lineamientos de seguridad que protegen la información contenida en los dispositivos.

C. Especificar que dispositivos están permitidos.

Se recomienda que la organización contemple el tipo de dispositivos que se van a admitir, ya que como es conocido existen en el mercado una gran variedad de estos que tienen diferentes características que van acorde a la necesidad de cada usuario, sin embargo lo ideal sería que se utilizaran dispositivos que cuenten con la supervisión y el soporte técnico por el área de TI.

D. Dejar claro quién es dueño de las aplicaciones y de los datos.

La información que está contenida en los dispositivos corporativos utilizados, por obvias razones es de propiedad de la organización, sin embargo cuando esta información es accedida o almacenada desde un dispositivo personal corre el riesgo de que sea robada, dañada o eliminada perdiendo de alguna forma u otra datos personales como fotos, música o aplicaciones que han generado un costo para el empleado, pero que no han sido cubiertos por la organización. Dado lo anterior la política BYOD implementada debe contemplar como sus empleados podrían recuperar la información perdida del dispositivo.

E. Decidir las aplicaciones permitidas y las bloqueadas.

La decisión sobre que aplicaciones deben ser instaladas o bloqueadas sobre los dispositivos, se debe aplicar tanto a los equipos personales como corporativos ya que muchas de estas tienen acceso a redes sociales, aplicaciones de correo electrónico o a software que permite el acceso remoto a la información corporativa de la organización.[4] Por esta razón se debe tener mucha precaución en la instalación de estas aplicaciones ya que podrían estar poniendo en riesgo la seguridad de la información que está siendo accedida desde estos dispositivos.

F. Capacitación de los empleados.

Se recomienda mantener un programa de capacitación para los empleados donde se les dé a conocer los riesgos a los que están expuestos tanto los equipos como la información con la implementación de BYOD en la organización.

VII. CONCLUSIONES

Cuando oímos hablar sobre BYOD, sabemos que es una nueva tendencia que están adoptando las organizaciones y que mediante un análisis de riesgos saben si es viable o no, ya que como todos sabemos puede traer grandes beneficios para la organización disminuyendo sus gastos en infraestructura, el manejo de información corporativa por sus empleados de una forma más cómoda y generando un incremento de mayor productividad para su organización.

El estar incursionando en esta nueva tendencia obliga a las organizaciones a implementar políticas y a educar a sus empleados para evitar que usen las herramientas equivocadas y que pongan en peligro la seguridad de la información de la organización ante las nuevas amenazas que se presentan al incursionar en este nuevo rol de manejo de información.

[4] http://www.pcworld.com.mx/Articulos/24049.htm

REFERENCIAS

[1] Newsletter de Seguridad–Latinoamerica. Mayo 2014. BYOD y el incremento de dispositivos personales en el ámbito laboral. http://technet.microsoft.com/library/dn656905.aspx

[2] Móviles personales y otros « wearables » en la empresa: los riesgos del BYOD. 04/02/2014, por Juan D. Peláez (INTECO). http://www.inteco.es/blogs/post/SeguridadBlogSeguridad/Articulo_y_comentarios/moviles_personales_wearalbes_empresa_riesgos_byod

[3] www.symantec.com, Los cinco pilares de los dispositivos móviles en la empresa. http://www.symantec.com/es/mx/products-solutions/solutions/detail.jsp?parent=mobile&child=5_pillars_mobile

[4] http://www.pcworld.com.mx/Articulos/24049.htm

[5] http://www.inteco.es/blogs/post/Empresas/BlogSeguridad/Articulo_y_comentarios/Trabajando_dispositivos_personales_BYOD_ciberseguridad_empresas

[6] http://www.enter.co/especiales/enterprise/consejos-para-una-politica-byod-coherente/

[7] http://www.inteco.es/blogs/post/Empresas/BlogSeguridad/Articulo_y_comentarios/Trabajando_dispositivos_personales_BYOD_ciberseguridad_empresas