BRING YOUR OWN DEVICE Oportunidades, retos y riesgos en las organizaciones

Moreno, David L.
dmorenor4@ucentral.edu.co

***Abstract*—The current availability of 3G services, 4G and growth having mobile technology in devices such as smartphones, tablets and laptops have given rise to a new phenomenon in organizations which integrates communication and the ability to conduct business from their own devices. BYOD (Bring Your Own Device), means that employees may use their personal devices to access resources within the organization and outside of it in order to do their jobs, this presents new opportunities but also involves mitigating and assume the risks are associated.**

This article discusses the opportunities, challenges and risks that can arise when organizations allow access to the corporate network of personal devices employees for their activities.

***Index Terms*— Mobile Device Management MDM Increased productivity, BYOD, Training, IT Consumerization, Security Policies, Challenges of organizations, Trends.**

***Resumen*— La actual disponibilidad de servicios 3G,4G y el crecimiento que presenta la tecnología móvil en dispositivos como Smartphone, tablets y equipos portátiles han dado origen a un nuevo fenómeno en las organizaciones el cual integra la comunicación y la capacidad de realizar negocios desde sus propios dispositivos. BYOD (Bring Your Own Device), significa que los empleados puedan utilizar sus dispositivos personales para acceder a los recursos de la organización dentro y fuera de ella con el fin de realizar su trabajo, esto representa nuevas oportunidades, pero también implica mitigar y asumir los riesgos que se encuentran asociados.**

Este artículo expone las oportunidades, los retos y los riesgos que pueden surgir en las organizaciones cuando permiten el acceso a la red corporativa de los dispositivos personales de los empleados para realizar sus actividades.

***Index Terms*— Administración de dispositivos móviles MDM, Aumento de productividad, BYOD, Capacitación, Consumerización de TI, Políticas de seguridad, Retos de las organizaciones, Tendencias.**

I. Introducción

BYOD es la nueva tendencia en la industria la cual facilita a los empleados en la organización el uso de sus dispositivos móviles personales para acceder a los recursos de la compañía para el desarrollo de sus funciones laborales, así como para su uso personal. Los accesos pueden ir desde los e-mails de trabajo, documentos, aplicaciones y recursos de red como impresoras entre otros. Es una tendencia que se ha producido debido a la potencia y flexibilidad de nuestros dispositivos portátiles inteligentes, que nos permite tener acceso a la información corporativa y personal [1].

Este fenómeno se inicia en el 2009 cuando los empleados de Intel empezaron a usar sus dispositivos móviles personales en su lugar de trabajo, esto fue bien recibido ya que los directivos de Intel visualizaron una forma de reducir costos y mejorar la productividad [2]. Fue sólo hasta el año 2011 cuando los proveedores de servicios de TI, como Unisys y proveedor de software como Citrix Systems compartieron sus puntos de vista y percepciones acerca de esta tendencia emergente y las organizaciones empezaron a considerar su implementación [3].

Existen muchos aspectos a considerar durante la implementación de esquema (BYOD) Traiga su propio dispositivo, dentro de los que se destacan los costos financieros, la seguridad y temas legales. Un gran número de organizaciones adoptan esta tendencia buscando un aumento de la productividad [4], Hoy en día los empleados parecen ser completamente dependientes del uso de sus dispositivos portátiles (laptops, Smartphones y tablets) para el desarrollo de su trabajo esto simplemente porque lo encuentran mucho más fácil que los recursos asignados por la compañía los cuales reposan en sus escritorios. Esto deja ver que para lograr ser más competitivos en el mercado las organizaciones deben estar a la vanguardia de los avances tecnológicos para los usuarios finales que realmente son sus empleados, todo esto sin comprometer la seguridad de la información y la privacidad del usuario final [5]. David A. Willis argumenta en su artículo Bring Your Own Device: The Facts and the Future que la implementación de una estrategia de BYOD, puede presentar un cambio radical en la economía y cultura a nivel de tecnologías de la información para las organizaciones en el mundo. Sin embargo, muchas de estas, especialmente las pequeñas y las medianas empresas (PYME) son culpables de subestimar el potencial ya sea ignorándolo o tomando medidas insuficientes para incorporar correctamente este tipo de tecnologías a su organización. Un error que se presenta de manera frecuente en las organizaciones que tratan de incursionar en la tendencia BYOD es que las políticas de seguridad existentes son bastante cerradas con la finalidad de proteger la red, causando inconvenientes cuando los empleados traen sus dispositivos móviles para desarrollar sus labores diarias, incluso el no contar con el conocimiento suficiente y pretender desplegar un sistema BYOD, sin tener en cuenta el antivirus, programas anti-malware que se encuentren instalados en los dispositivos móviles conduce a

una gran cantidad de vulnerabilidades ocasionando inconvenientes con las políticas de seguridad existentes en ocasiones hasta comprometiendo la confidencialidad de la información [6].

La aplicabilidad de esta tendencia BYOD podría funcionar dependiendo de la forma y el alcance con el que se realice su despliegue, aplicación y gestión, este es un esquema que cada vez más organizaciones sin importar su tamaño han venido adoptando, realizando asignación de presupuestos y recursos hacia esta nueva modalidad de trabajo [7]. Se habla que en promedio el 61% de las organizaciones a nivel internacional indican que sus empleados utilizan sus dispositivos personales para efectuar sus labores en su lugar de trabajo. Las organizaciones que adoptan una tendencia BYOD se ha incrementado en 73%, se prevé que para el 2015 el 90% de las organizaciones incentive a los empleados al uso de sus dispositivos móviles con aplicaciones y software empresarial [8].

La siguiente gráfica muestra el aumento del uso de dispositivos móviles en que se presenta en cada una de las regiones del mundo, el estudio realizado por Bussines Insider indica que para el 2016 los dispositivos más usados serán las tablets presentando un crecimiento del 20%, mientras que el uso de computadores de escritorio y portátiles decaerá en un 24%

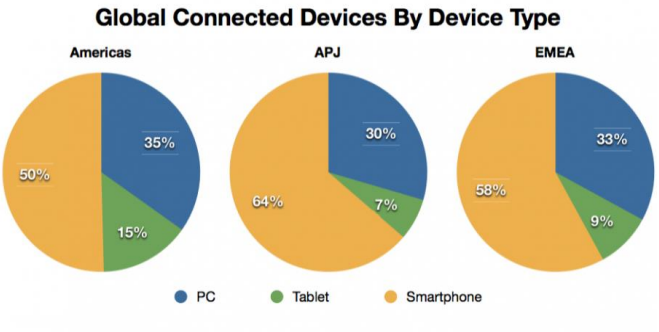

Fig. 1. Porcentaje de uso de dispositivos móviles a nivel América, Asia y pacífico, Europa, Oriente Medio y África [9].

II. OPORTUNIDADES

Contar con una buena política de BYOD representa nuevas oportunidades en las organizaciones, pero no se pueden dejar de lado los riesgos que se encuentran asociados, tales como:

- Confidencialidad de la Información; El contar con diversos dispositivos móviles en los que se encuentren configuradas aplicaciones de la organización, pueden verse expuestos a pérdida o robo de los mismos, dejando de manera explícita información sensible.

- Virus y Software malicioso, El no tener el software ni el hardware estandarizado y brindar acceso a la red corporativa a una gran cantidad de dispositivos si conocer su estado en actualizaciones o nivel de seguridad pueden ocasionar muchos inconvenientes.

- Control de acceso e integridad de la información, Se genera una mayor necesidad de controlar el acceso de red y la privacidad de la información, en caso de la salida de un empleado de la organización o la perdida de alguno de sus dispositivos, se debe actuar de manera inmediata para interrumpir el acceso a la red corporativa y restringir el acceso a los datos de la organización que se encuentran en el dispositivo. Adicional debe existir segmentación sobre los datos de la organización y los datos personales almacenados en el dispositivo.[10]

Las organizaciones pueden tener muchas razones por las que decidan implementar una política BYOD. Un aliciente importante es el ahorro en costos sobre los activos de TI al no tener que pagar por los dispositivos y planes de datos costosos. Al permitir que los empleados asuman estos costos, la organización puede orientar un nuevo presupuesto para el desarrollo de la política buscando la seguridad conjunta tanto de los datos como de los dispositivos de los empelados También hay beneficios en la productividad. Si el empleado puede hacer su trabajo en su propio dispositivo móvil, hay menos tiempo de inactividad durante la capacitación de un nuevo dispositivo desde el cual puede ponerse al día en sus labores, revisar mensajes de correo electrónico fuera del horario laboral, se reduce el soporte tecnológico en la mayoría de casos el empleado se encuentra en la capacidad de solucionar sus inconvenientes. Permitirle el uso de su propio dispositivo significa que tendría un mayor cuidado sobre el mismo, el contar con la información corporativa y personal de primera mano y en solo dispositivo mejoraría la forma de buscarla optimizando la comunicación e incrementando las oportunidades de negocio [11].

Según la encuesta realizada el 71% de las organizaciones permitiría el uso de dispositivos personales para el desarrollo de sus funciones, el 54% de los empleados usan tablets para temas laborales y personales, y un 72% de los empleados estarían dispuestos a usar sus datos personales sin necesidad de reembolso por parte de la organización.

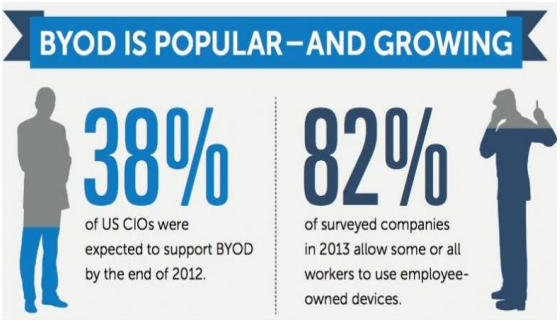

Fig. 2. Los Números detrás de BYOD [12].

Las políticas BYOD en las organizaciones pueden presentar una cierta resistencia por parte de TI y de los empleados, sin embargo, son una realidad en los negocios hoy en día. Con más del 82% de las empresas encuestadas indica que este año

van a permitir algún tipo de BYOD en su organización y el 50% de los gerentes de TI en Estados Unidos argumentan firmemente que BYOD mejora la productividad de los trabajadores, no es posible desconocer las estadísticas y el crecimiento que presenta esta tendencia, si el dispositivo es correctamente gestionado por el empleado y la seguridad alineada con las políticas de TI, existe menos riesgo para ambas partes. BYOD puede ser un gran beneficio tanto para sus empleados como para la organización [13].

III. RETOS

Uno de los mayores retos a los que se enfrentan las organizaciones al implementar una política BYOD, es la aceptación de que los datos entregados a los empleados y almacenados en sus dispositivos personales no son directamente administrados por el departamento de TI, esto evidencia que las organizaciones tienen menos control y menos alternativas de mitigación en un caso eventual. También se incremente la fuga de información y la pérdida de datos con el ingreso de dispositivos no administrados, Se debe tener en cuenta que el termino de dispositivo móvil abarca una gran parte de equipos tales como Laptops, tablets, smartphones, lo cual se convierte en algo muy complejo de controlar por su gran variedad de sistemas operativos como BlackBerry, Symbian, iOS, Android y Windows Mobile, los cuales a su vez cuentan con su propio modelo de seguridad.

Una clara identificación y clasificación de los dispositivos dentro de una política BYOD es fundamental para evitar las potenciales fugas de información en los dispositivos que se encuentren conectados. Con el actual crecimiento de la computación en la nube y la tecnología móvil, se pude llegar a considerar como dispositivos móviles aplicaciones web para el almacenamiento de la información como Dropbox, Drive, Skydrive [14].

El estudio realizado por ESET Latinoamérica, ver Fig. 3. el 83,3% de los empleados utiliza memorias USB de su propiedad para almacenar información del trabajo; un 82,2% portátiles y un 55% teléfonos inteligentes. Un dato que preocupa a las organizaciones es que sus empleados no cifran la información corporativa que tiene en sus dispositivos, en algunos casos indican no conocer el manejo que debe tener dicha información.

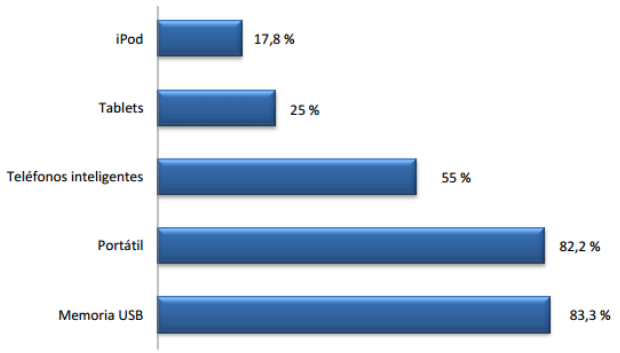

Fig. 3. Dispositivos móviles más usados por los empleados en las organizaciones para almacenar información corporativa [15].

En el estudio realizado por cisco BYOD and Virtualization Horizons Study, llego a la conclusión que para el 2014 los trabajadores en promedio llegaran a tener 3,3 dispositivos inteligentes compartiendo datos personales y corporativos, lo que significa que cada uno de ellos tendrá sus propios riesgos asociados [16]. Así mismo la investigación realizada por Deloitte afirma que en el 2016 se estima que los usuarios de dispositivos móviles lleguen a 350 Millones, de los cuales 200 millones harán uso de sus dispositivos personales para la realización de tareas relacionadas con su trabajo [17]. Es por esto que se hace esencial la existencia de una política clara que permita identificar los dispositivos para desarrollar las medidas y controles capaces de mitigar cada riesgo de manera individual y poder garantizar que los dispositivos no identificados no tengan acceso a la información.

A. Algunos inconvenientes al momento de pensar en BYOD

El creciente uso de dispositivos móviles personales dentro de las organizaciones está dando origen a nuevas amenazas de seguridad informática, incluyendo la fuga de información, problemas de incumplimiento, afectación de la imagen corporativa [18]. Informes de seguridad indican que solo el 5% de los dispositivos móviles de todo el mundo cuentan con algún software de seguridad instalado, esto sumado al descuido de los usuarios al navegar a través de internet en sitios no seguros y la instalación de Apps no confiables, empiezan a generar inconvenientes al tratar de implementar BYOD [18].

Estudios demuestran que el 89% de los dispositivos móviles de los empleados se encuentran conectados de alguna forma a la red de la organización y tan solo el 10% de las organizaciones son conscientes de las implicaciones de tener estos dispositivos con acceso a sus datos. Cifras que generan preocupación teniendo en cuenta que los datos allí almacenados son de carácter confidencial el estudio indica que el 34% de los empleados almacenan datos sensibles un sus dispositivos móviles, lo cual se convierte en toda una preocupación para las organizaciones ya que no pueden tener la certeza que estos datos se encuentren relacionados directamente con la organización [19].

La investigación realizada en un grupo de pequeñas y medianas empresas arrojo como resultado que el 46,5% de la organizaciones que decidió implementar BYOD presento fallas de seguridad originadas por algún dispositivo propiedad del empleado que se encontraba conectado a la red corporativa, La gestión del acceso a la red corporativa es uno de los mayores inconvenientes a los que se enfrentan las organizaciones que consideran realizar una implementación de BYOD, teniendo en cuenta que la mayoría de datos son confidenciales o sensibles y su perdida, divulgación o mala manipulación pueden ocasionar daños y pérdidas a la organización [20].

En el estudio realizado en el 2013 realizado por TrendMicro y la comisión Forrester Consulting luego de entrevistar a más de 200 líderes de TI en países como Estados Unidos, Francia, Alemania y Reino Unido, se encontraron resultados sobre cómo la consumerización de TI conduce a aumentos de los

costos en varias áreas importantes. Estos incluyen, Soporte Técnico, licencias de software de seguridad, la administración de los dispositivos móviles y el cumplimiento legal sobre estos.

Los administradores de TI esperaban que los costos bajaran teniendo en cuenta que los empleados están utilizando sus propios dispositivos, luego de la implementación encontraron que se aumentó el número de casos en sus mesas de ayuda en un 8%. En realidad las compañías prestadoras del servicio de telefonía y los operadores móviles no se encuentran en la capacidad de resolver incidentes con los dispositivos móviles que son de carácter corporativo.

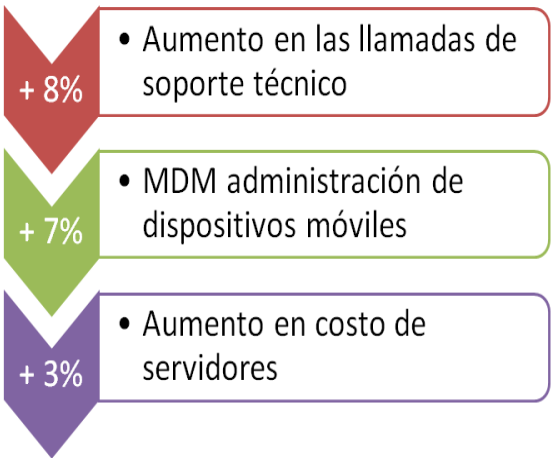

Fig. 4. Costos Ocultos de BYOD [21]

Así mismo se podría esperar que los costos en licenciamiento para los dispositivos disminuyeran teniendo en cuenta que los equipos son propiedad de los empleados, sin embargo, la investigación demostró que los costos se aumentaron en un 7%, esto se debe a que la organización no puede permitir el uso de aplicaciones de software sin la debida licencia para realizar tareas de tipo laboral, a lo que se suma el incremento en los gastos asociados con la seguridad y la gestión de los dispositivos móviles [22].

Otro punto que se debe tener en cuenta a la hora de optar por BYOD, es la idea de quien posee la información y quien es el responsable de dicha información, en el momento de establecer una política BYOD es importante para la organización demarcar que aunque el dispositivo sea propiedad del empleado y en él se encuentren datos personales, todos los datos relacionados con la organización almacenados allí siguen siendo propiedad de la organización por lo tanto el empleado es completamente responsable de la administración de esta información, en caso que algo le ocurriera al dispositivo y se perdiera la información, deberán existir consecuencias mediante acciones disciplinarias [23], lo cual puede no agradarle mucho a los empleados y pierdan motivación a la hora de usar sus dispositivos personales por temor a las consecuencias.

Por ultimo un tema que se relaciona con lo anterior es la perdida y/o robo de los dispositivos móviles personales, ya que en la gran mayoría de estos se encuentra información confidencial, la gran portabilidad y evolución que prestan estos dispositivos aumentan la probabilidad de su pérdida o robo especialmente por su tamaño y peso. La materialización de alguno de los eventos citado anteriormente puede tener consecuencias catastróficas para la organización como pérdida de la propiedad intelectual y la pérdida de información sensible tanto para los clientes como para los empleados desencadenando consecuencias legales [24].

IV. RIESGOS Y AMENZAS EN BYOD

El riesgo es un factor importante que se debe tener en cuenta a la hora de hablar de un ambiente BYOD, especialmente cuando se considera el depositar los datos de la organización en los dispositivos personales de los empleados. Bruce Schneier, analiza la percepción que tiene los empleados sobre los riesgos, y concluye que los mismos no se encuentran en la capacidad de realizar una adecuada evaluación de los riesgos a los que se encuentran expuestos, esto debido a la forma como los diferencian. También indica que los empleados y usuarios reaccionan a los riesgos a medida que se van presentando y no son proactivos en su reconocimiento [25], dando paso a que las amenazas puedan materializar estos riesgos.

A continuación se describen los principales riesgos y amenazas a los que se encuentran expuestas las organizaciones que desean implementar BYOD, los cuales deben ser tratados cuidadosamente en la descripción de la política para que al final sea un éxito y no se vean afectados por incidentes de seguridad ocasionando pérdidas financieras y de imagen corporativa.

TABLA I
PRINCIPALES RIESGOS ASOCIADOS A BYOD

RIESGO	DESCRIPCIÓN
Información de Usuario	Nombres de usuarios y contraseñas, información bancaria, certificados instalados, cuentas de correo, pueden verse comprometidas, en caso de pérdida o robo del dispositivo móvil
Información Corporativa confidencial	Datos de carácter confidencial perteneciente a la organización como correos electrónicos, archivos, informes, aplicativos se encuentran en riesgo en caso de un acceso no autorizado sobre el dispositivo sea por descuido, perdía o robo.
Teléfono y datos	Puede realizarse la interceptación de llamadas o el sniffing de paquetes, brindando acceso a los datos del dispositivo comprometiendo la información allí almacenada.
El mismo dispositivo móvil	La portabilidad que brinda los dispositivos hace que el riesgo de pérdida o robo aumente.

TABLA II
PRINCIPALES AMENAZAS ASOCIADOS A BYOD.

AMENAZAS	DESCRIPCIÓN
Malware	Un dispositivo infectado con algún software malicioso puede conducir a la fuga de información confidencial, el uso de servicios adicionales como llamadas y envió de mensajes de texto no programados, interrupción parcial o completa del correcto funcionamiento del dispositivo.
Spam	Mensajes de correo electrónico no deseados que se reciben de fuentes desconocidas los cuales generan consumo del dispositivo en recursos como ancho de banda y memoria.
Phishing	Esto puede llegar a presentar a través de un correo electrónico o un mensaje de texto para engañar al usuario e ingresar a un sitio web falso solicitándole información sensible de la organización.
Bluetooth y Wi-Fi	Al conectarse a diferentes redes o compartir archivos el dispositivo puede verse fácilmente infectado lo cual daría paso a la interceptación de datos que viajan desde o hacia los dispositivos móviles.

V. ESTRATEGIAS PARA ASEGURAR UN ESQUEMA BYOD

A. Una Política clara

Se debe contar con una política clara, coherente la cual debe minimizar los riesgos de seguridad, fortalecer el negocio y generar un retorno de inversión. La política que rige un esquema BYOD debe comprender toda la red corporativa, esta debe cubrir; Controles de acceso, la protección física, el cifrado de información, backups y software de antivirus. Debe generar los lineamientos para la conexión de dispositivos móviles personales de los empleados a la red corporativa junto con la forma que el dispositivo debe ser usado en redes públicas. [26]

Es importante diseñar y establecer una estrategia de cómo se gestionara la seguridad de los dispositivos que se encuentren fuera de la red de la organización, adicional se deben clasificar los equipos que se van a soportar, teniendo en cuenta que un celular, una Tablet y un portátil son completamente diferentes entre sí. Los administradores de TI deberán clasificar la información con el fin de definir a cual de esta se puede tener acceso desde los dispositivos.

Para una implementación exitosa se debe contar con una estricta planeación, en la que se fijaran metas y se cumplirá un cronograma, también se debe dedicar una parte de tiempo a la investigación con el fin de analizar cómo se puede integrar todo esto con la actual infraestructura de TI que tenga la organización [27].

B. Conocer quién y que está conectado a la red

Una red segura debe garantizar que conoce que dispositivos y su asignación con los correspondientes privilegios sobre esta, todo usuario debe registrar su dispositivo con el departamento de TI antes de poder acceder a la red interna.

Se debe realizar un completo registro teniendo en cuenta marca y modelo del dispositivo, identificador único y dirección MAC, de esta forma se podrá establecer una correcta gestión de los dispositivos y los recursos de red [28].

C. Conocer lo que tiene instalado el dispositivo.

Deberá existir un listado con aplicaciones autorizadas y no autorizadas que podrán tener instaladas los dispositivos, esto ayudara a mantener seguros los dispositivos que acceden a la red corporativa, El departamento de TI de la organización deberá implementar una herramienta para la gestión de dispositivos móviles MDM, con el fin de administrar el acceso de ciertas aplicaciones dependiendo de la red a la que se encuentre conectado el dispositivo, adicional permite conocer si un dispositivo ha sido manipulado "jail broken" o rooteado anulando su acceso a la red ya que podría llegar a tener software malicioso causando inconvenientes sobre la red corporativa [28].

D. Uso del dispositivo en redes públicas.

La política debe establecer reglas de comportamiento para los dispositivos cuando son conectados a redes públicas, para lo que se debe establecer comunicaciones cifradas mediante VPN o túneles de SSH, usando mecanismos de autenticación seguros que permitan la plena identificación mutua antes de realizar el intercambio de archivos [30].

E. Copia de Seguridad del dispositivo

Dentro de la política se debe establecer la periodicidad de backup que se le realizara a los datos sensibles que se encuentren almacenados en los dispositivos, las copias de seguridad deben ser cifradas y almacenadas. Esto asegura la protección de la información en caso de pérdida o robo de alguno de los dispositivos [30].

F. Plan de capacitación y entrenamiento para los empleados

Es importante difundir un documentó con la política de BYOD donde se expresen claramente las reglas aplicables, de esta forma los usuarios comprenderán los limitantes existentes y en caso de cometer una falta no se presenten excusas por desconocimiento

La capacitación y el entrenamiento deben ser de carácter obligatorio teniendo como objetivo principal el dar a conocer los riesgos existentes y los temas asociados al uso de los dispositivos móviles personales, no solo se debe hacer énfasis en las reglas de la política BYOD dentro de la organización, también deben explicarse las mejores prácticas para estar seguro al estar fuera del trabajo y conectado en redes públicas.

Dentro de la política deben existir normas de comportamiento referentes a quien tiene acceso al dispositivo móvil; Deben indicar que cualquier dispositivo móvil que almacene o cuente con acceso a información sensible de la organización no debe ser descuidado bajo ninguna circunstancia y de ser necesario guardado bajo llave. Los empleados deben conocer el procedimiento a seguir en caso de pérdida o robo de alguno de sus dispositivos móviles [31].

VI. CONLUSIONES

Actualmente son más las organizaciones que han decidió medirse a una implementación de BYOD, enfrentando los retos y riesgos que demanda el compartir la información de la organización en los dispositivos de los empleados, a su vez intentan sacar provecho de las oportunidades que pueden llegar a explotarse cuando se cuenta con una bien diseñada implementación de BYOD, dentro de las que destacamos el aumento de la productividad y eficiencia en cierre de negocios.

La preocupación en las organizaciones recae en la fuga de información que puede presentarse por la pérdida o robo de alguno de los dispositivos móviles que no se encuentre bajo una política clara de BYOD, Es importante la capacitación y el entrenamiento que se le debe impartir a los empleados con fin de disminuir este tipo de riesgos; Un estudio realizado por Dell SonicWALL indico que en el 68% de las empresas los empleados no lograron identificar posibles riesgos y amenazas existentes sobre la red de la organización [32], también es primordial concientizar a los empleados de las consecuencias laborales y legales que puede acarrear un fallo de seguridad.

Aparte de contar con unos claros lineamientos de seguridad sobre los dispositivos móviles, se debe garantizar que las aplicaciones corporativas estén disponibles y sean plenamente compatibles con los dispositivos móviles. Para poder plasmar la teoría en la práctica se debe desarrollar una clara y bien pensada estrategia de MDM diseñada por el departamento de TI, gestionando la autenticación al dispositivo, el comportamiento del mismo en redes no autorizadas y el aislamiento de los datos personales de los corporativos [32].

REFERENCIAS

[1] Sdad ICO, (2013), Bring your own device (BYOD). [Online].http://ico.org.uk/news/latest_news/2013/~/media/documents/library/Data_Protection/Practical_application/ico_bring_your_own_device_byod_guidance.pdf (Accedida el 2 de Julio 2014)

[2] Harkins, M., Mobile: Learn from Intel's CISO on Securing Employee-Owned Devices [Online]. Dsiponible en: http://www.govinfosecurity.com/webinars/mobile-learn-from-intels-ciso-on-securing-employee-owned-devices-w-264 (Accedida el 15 de Julio 2014)

[3] Lui, S., (2012) Citrix favours selective BYOD program [Online]. Dsiponible en: http://www.zdnet.com/au/citrix-favours-selective-byod-program-7000008790/ (Accedida el 15 de Julio 2014)

[4] Rege, O., (2011), Bring Your Own Device: Dealing With Trust and Liability Issues, CIO Network: Insights and Ideas for Technology Leaders, Forbes. [Online]. Disponible en: http://www.forbes.com/sites/ciocentral/2011/08/17/bring-your-own-device-dealing-with-trust-and-liability-issues/ (Accedido: 16/07/2014).

[5] Kevin Johnson, Barbara L. Filkins (March 2012), SANS Mobility/BYOD Security Survey, [Online]. Disponible en: http://www.sans.org/reading_room/analysts_program/mobility-sec-survey.pdf. (Accedido: 16/07/2014).

[6] Willis, D. A., (2013), Bring Your Own Device: The Facts and the Future, Research G00250384, Gartner. [Online]. Disponible en: https://l1.osdimg.com/remote-support/dam/pdf/en/bring-your-own-device-the-facts-and-the-future.pdf/jcr:content/renditions/original (Accedido: 18/07/2014).

[7] TechRepublic, (2013), The Executive's Guide to BYOD and the Consumerization of IT. [Online]. Disponible en: http://www.talkezy.com.au/uploads/whitepapers/The_Executives_Guide_to_BYOD_and_the_Consumerisation_of_IT.pdf (Accedido: 21/07/2014).

[8] Ponemon Institute, (2012), Global Study on Mobility Risks, [Online]. Disponible en: http://www.ponemon.org/local/upload/file/Websense_Mobility_US_Final.pdf (Accedido: 21/07/2014).

[9] Bort, .J (2012) Managing An Explosion Of Mobile Devices And Apps In The Enterprise. [Online] Disponible en: http://www.businessinsider.com/how-companies-are-managing-the-explosion-of-mobile-devices (Accedido: 21/07/2014).

[10] Belak, M. (2011): Allowing Personal Devices At Work: A Faustian Bargain?, InformationWeek, [Online]. Disponible en: http://www.informationweek.com/news/global-cio/interviews/231601782 (Accedido: 18/07/2014).

[11] SIFMA IT audit session, (2012) Bring your own device (BYOD) trends and audit considerations, [Online] Disponible en: http://www.sifma.org/uploadedfiles/societies/sifma_internal_auditors_society/bring%20your%20own%20device%20trends%20and%20audit%20considerations.pdf . (Accedido: 21/07/2014).

[12] Jen, C. (2013) What do Employees Really Think about BYOD? [Online]. Disponible en http://truewirelessinc.com/byod/what-do-employees-really-think-about-byod/ (Accedido: 21/07/2014).

[13] BYOD By The Numbers [Infographic] Disponible en: http://readwrite.com/2013/03/26/intel-byod-by-the-numbers (Accedido: 23/07/2014).

[14] Morrow, B. (2012). BYOD security challenges: control and protect your most sensitive data [Online] Disponible en http://www.businesscomputingworld.co.uk/byod-security-challenges-control-and-protect-your-most-sensitive-data/(Accedido: 23/07/2014).

[15] ESET (2012) Retos de la seguridad para las empresas a partir de BYOD. [Online] Disponible en: http://www.welivesecurity.com/wp-content/uploads/2014/01/seguridad_en_byod.pdf (Accedido: 23/07/2014).

[16] Cisco (2012) Disponible en: http://www.cisco.com/web/offer/grs/82089/3/IBSG_Research_Report-BYOD_and_Virtualization_Research_Report.pdf (Accedido: 21/07/2014).

[17] Deloitte, (2013) Tecnología, Medios de Comunicación y Telecomunicaciones Predicciones 2013 [Online] Disponible en: http://webserver2.deloitte.com.co/TMT/Deloitte%20Predicciones%20TMT%202013%20esp.pdf (Accedido: 23/07/2014).

[18] Ayrapetov, D., (2013), Cybersecurity challenges in 2013. [Online]. Disponible en: http://www.techrepublic.com/blog/security/cybersecurity-challenges-in-2013/9038. (Accedido: 23/07/2014).

[19] Goldman, J., (2012), 95 Percent of Smartphones and Tablets Are Unprotected. [Online]. Disponible en: http://www.esecurityplanet.com/mobile-security/95-percent-of-smartphones-and-tablets-are-unprotected.html. (Accedido: 23/07/2014).

[20] Fieldman, M., (2012), The Latest Infographics: Mobile Business Statistics For 2012. [Online]. Disponible en: http://www.forbes.com/sites/markfidelman/2012/05/02/the-latest-infographics-mobile-business-statistics-for-2012/. (Accedido: 23/07/2014).

[21] Harris, C., (2012), Mobile Consumerization Trends & Perceptions. [Online]. Disponible en:

http://www.trendmicro.com/cloud-content/us/pdfs/business/white-papers/wp_decisive-analytics-consumerization-surveys.pdf. (Accedido: 23/07/2014).
[22] Garlati, C., (2013)The Financial Impact of Consumerization – The Hidden Costs [Online]. Disponible en: http://bringyourownit.com/2013/02/04/the-financial-impact-of-consumerization-the-hidden-costs/#more-1127(Accedido: 24/07/2014).
[23] Bestmann, M (2012) The Evolution of IT: BYOD and Consumerization [Online] Disponible en: http://www.technewsworld.com/story/75723.html (Accedido: 24/07/2014)
[24] Juniper, (2011), Mobile Device Security – Emerging Threats, Essential Strategies. [Online]. Disponible en: http://www.juniper.net/us/en/local/pdf/whitepapers/2000372-en.pdf. (Accedido: 24/07/2014).
[25] Schneier, B., (2008), The Psychology of Security [Online]. Disponible en: http://www.schneier.com/essay-155.html (Accedido: 24/07/2014).
[26] Aranguren, M., Haciendo Inteligente mi movilidad (Oct 2011) Disponible en http://sasorigin.onstreammedia.com/origin/isaca/LatinCACS/cacs-lat/forSystemUse/papers/123.pdf. (Accedido: 24/07/2014).
[27] ISO/IEC 27002:2005. Information technology —Security techniques — Code of practice for information security management.
[28] Rhodes, A., (2013), 5 tips for secure, productive use of BYOD [Online]. Disponible en: http://www.usatoday.com/story/cybertruth/2013/07/17/5-tips-for-secure-productive-use-of-byod/2525663/ (Accedido: 28/07/2014).
[29] Bradford Networks, (2012), Ten Steps To Secure BYOD. [e-book] Cambridge: Bradford Networks. http://www.cadincweb.com/wp-content/uploads/2012/04/CAD_BRAD_Ten_Steps_to_Secure_BYOD.pdf. (Accedido: 28/07/2014).
[30] F-Secure, (2012), Mobile ThreaT reporT Q4 2012. [e-book] Finland: F-Secure Labs. http://www.f-secure.com/static/doc/labs_global/Research/Mobile%20Threat%20Report%20Q4%202012.pdf. (Accedido: 28/07/2014).
[31] Smith, C., (2014), Why you should always back up your smartphone before telling off your boss [Online]. Disponible en: http://bgr.com/2014/01/22/byod-remote-wipe/ (Accedido: 28/07/2014).
[32] Ayrapetov, D., (2013), Cybersecurity challenges in 2013, IT Security, Tech Republic. [Online]. Disponible en: http://www.techrepublic.com/blog/security/cybersecurity-challenges-in-2013/9038 (Accedido: 28/07/2014).

DAVID LEONARDO MORENO ROJAS

Ingeniero electrónico por la Universidad Manuela Beltrán; Bogotá-Colombia. Especialista en seguridad Informática (C) por la Universidad Piloto de Colombia.

Trabajo como CIO en la Universidad Central; Bogotá-Colombia, profesor de catedra para Fundación San Mateo; Bogotá-Colombia en materias de seguridad informática.

Cuento con un caso de éxito divulgado en medios masivos por Microsoft Latam - Implementación de Office 365 a nivel internacional para Blu Logistics Colombia S.A.S - http://www.microsoft.com/enterprise/es-xl/it-trends/platform-for-business-evolution/articles/blu-logistics-el-mejor-operador-de-logistica.aspx#fbid=TMmPR36XdLl