Universidad Internacional de La Rioja
Máster universitario en Seguridad Informática

RIESGOS DE SEGURIDAD ASOCIADOS AL USO DE DISPOSITIVOS MÓVILES PERSONALES (SMARTPHONE - ANDROID) EN ENTORNOS BYOD - Bring Your Own Device

Trabajo Fin de Máster

Presentado por: Cadena Herrera, Andrés Giovanny

Director/a: Muñoz Muñoz, Alfonso

Ciudad: Bogotá, Colombia
Fecha: Julio de 2017

Resumen

En la actual era digital cuya tendencia de conexión a internet de forma permanente a través de dispositivos móviles personales para atender asuntos laborales, personales, familiares, de ocio, etc., las empresas se han visto involucradas por parte de sus empleados para que permitan el uso de sus dispositivos móviles en sus ambientes corporativos para la realización tanto de actividades laborales como personales.

Por esta razón surge la necesidad a nivel mundial en las empresas de adaptar sus políticas, procesos y plataformas tecnológicas para permitir el uso de BYOD como tendencia de trabajo a sus empleados. Por lo anterior se propone a título personal del autor de este documento una metodología para realizar de la mejor manera y desde el enfoque de un profesional de la seguridad, la transición e implementación de BYOD en cualquier organización.

Basado en una metodología investigativa acerca de BYOD – “trae tu propio dispositivo”, se obtiene como resultado de ésta, una recopilación de información acerca de ventajas, desventajas, principales riesgos, posibles herramientas para administración de dispositivos móviles en BYOD, y posteriormente aplicando la metodología deductiva y los conocimientos adquiridos en la maestría frente a la seguridad de la información, se identifican y plasman los riesgos que genera la inclusión de este ambiente en una organización, se propone una política de seguridad de la información para ambientes BYOD, se plantea una serie de controles de seguridad que se deben implantar basados en la norma ISO/IEC 27001:2013, se propone un modelo básico de evaluación de riesgos de la información a nivel de dispositivos móviles en general y se plantea como característica fundamental de apoyo a las propuestas y sugerencias anteriores del autor del presente TFM, la concientización de los usuarios, referente a los riesgos a los que se ven expuestos a diario, con la finalidad de que apoyen los esfuerzos organizacionales, técnicos y demás, en pro de la defensa y resguardo de la información corporativa y la privacidad de los usuarios.

Palabras Clave: Teléfono, Inteligente, Dispositivo, Móvil, BYOD

Abstract

In the current digital era, the trend of permanently connecting to the internet through personal mobile devices to attend to work, personal, family, leisure, etc., companies have been involved by their employees to allow the Use of their mobile devices in their corporate environments for the accomplishment of both work and personal activities.

For this reason, there is a worldwide need for companies to adapt their policies, processes and technology platforms to allow the use of BYOD as a working trend for their employees. For the above, it is proposed in the personal capacity of the author of this document a methodology to carry out the transition and implementation of BYOD in any organization in the best way and from the perspective of a security professional.

Based on a research methodology about BYOD - "bring your own device", you get as a result of this, a collection of information about advantages, disadvantages, main risks, possible tools for managing mobile devices in BYOD, and then applying the Deductive methodology and the knowledge acquired in the mastery of information security, identify and capture the risks generated by the inclusion of this environment in an organization, proposes an information security policy for BYOD environments, a question arises Series of security controls to be implemented based on ISO / IEC 27001: 2013, a basic model for assessing the risks of information at the level of mobile devices in general is proposed as a fundamental characteristic to support the proposals And previous suggestions of the author of the present TFM, the users' awareness With respect to the risks to which they are exposed on a daily basis, in order to support the organizational, technical and other efforts, in defense of the protection of corporate information and the privacy of users.

Keywords: Phone, Smart, Device, Mobile, BYOD

Índice de contenidos

Índice de tablas

Índice de figuras

1. Introducción

Históricamente la tendencia de incorporación de los dispositivos móviles a los entornos corporativos estaba orientada a que se permitía exclusivamente para algunos ejecutivos de las compañías, lo anterior obedecía a sus posibilidades económicas para adquirir este tipo de tecnología, a la forma en la cual manejaban su información crítica y por ultimo a su poder jerárquico dentro de las organizaciones.

Desde otra perspectiva diferente, también se contempla a los demás usuarios o trabajadores de las compañías, los cuales se veían obligados y enfrentados a trabajar con las herramientas tecnológicas provistas por las empresas para las cuales laboraban, que en su mayoría presentaba altos niveles de obsolescencia, debido a costos elevados en la renovación de los parques tecnológicos, costos de licenciamiento, costos de migración y reingeniería de sus aplicativos, malas asesorías por parte de los CIO o jefes de los departamentos de tecnología y finalizando el tema, con la falta de apoyo por parte de la Alta Dirección (CEO) a nivel de crecimiento y mejora de los sistemas informáticos, sumado a los bajos recursos financieros asignados a los procesos de reestructuración tecnológica.

En la actualidad informática a nivel empresarial desde hace varios años se ha venido incorporando una nueva tendencia mundial que se identifica bajo el acrónimo **BYOD,** en inglés (Bring Your Own Device), cuyo significado en nuestro idioma español es “Trae tu Propio Dispositivo”. Esto hace referencia a la nueva tendencia tecnológica que se está viviendo en las empresas sin importar su tamaño o sector de negocio, en las cuales los empleados de las diferentes organizaciones han solicitado que en los ambientes empresariales se permita la incorporación y uso de sus dispositivos móviles (teléfonos inteligentes y/o tabletas), en especial los de sistema operativo ANDROID, en los cuales se enfocará este documento, dado que en los últimos años se ha masificado su adquisición y uso debido al fácil acceso adquisitivo y a la gran variedad de herramientas y servicios que estos ofrecen a sus usuarios.

Esta necesidad de los usuarios o trabajadores obedece en gran parte a la facilidad en la portabilidad y acceso a los dispositivos móviles, a la centralización, administración, modificación y uso de información tanto personal como laboral, razón por la cual los

departamentos de tecnología de las compañías han tenido que asumir el reto y permitir la incorporación y uso de los dispositivos móviles personales de los usuarios en las redes empresariales y a su vez aprobar y gestionar el acceso a la información corporativa desde éstos dispositivos.

La inclusión de BYOD como una nueva tendencia de trabajo y de producción empresarial se ha presentado con ***mayor fortaleza desde comienzos del año 2012 a nivel mundial***, desde este momento se ha masificado la tendencia de los CIO y Departamentos de Tecnología a la aceptación y puesta en producción de BYOD, aunque aún se encuentran muchos opositores a esta tendencia, por temor al cambio, por los peligros que conlleva, por falta de recursos humanos y financieros, por los cambios a nivel empresarial que se deben asumir, entre otros factores que se pueden sumar a esta lista.

1.1 Justificación

El presente documento tiene como finalidad contribuir en identificar y dar a conocer las principales vulnerabilidades o riesgos que deben ser tenidos en cuenta por un departamento de tecnología de cualquier organización, de cualquier sector de negocio y tamaño que pretenda incorporar dispositivos móviles corporativos o de propiedad de los usuarios en su plataforma informática es decir BYOD.

Lo anterior obedece a que las empresas se han visto avocadas a implementar soluciones informáticas de acuerdo a su nivel de madurez en el área de TI, a sus recursos tecnológicos, recursos económicos, al segmento de negocio y tamaño de la empresa, teniendo en cuenta lo anterior y sumado a la tendencia de aparente “libertad” de BYOD, la conclusión general de cualquier departamento de sistemas es que la implementación de BYOD pone en riesgo absoluto la seguridad de la información (Confidencialidad, Disponibilidad e Integridad), de los servicios y sistemas de información propios de cada organización tales como (aplicativos misionales, servicios de autenticación, ofimática, antivirus, correo, ftp, intranet, extranet, almacenamiento, bases de datos, servicios en la nube, otros), razón por la cual deben identificarse las vulnerabilidades y riesgos a los que se expondrá cualquier organización,

asimismo deben ser identificados los riesgos específicos de cada servicio que se permita al usuario.

No hay que dejar de lado que la implementación de BYOD en cada compañía depende obviamente del alcance que se pretenda y de las necesidades de cada una en específico, es decir que BYOD no es simplemente implementar y otorgar acceso y uso de la plataforma y servicios de tecnología corporativos a los usuarios con cualquier dispositivo móvil, sino que BYOD debe estar alineado con la parte estratégica de la organización y orientado según las directrices corporativas definidas por la alta dirección, con el apoyo y lineamientos del gobierno de TI, así como con el apoyo, las observaciones y recomendaciones del equipo de TI (CIO, CISO, REDES, COMUNICACIONES, INFRAESTRUCTURA, DESARROLLO, SOPORTE, OTROS), con lo cual se garantizará la alineación de los servicios y sistemas de información propios de cada empresa, orientados al cumplimiento de los objetivos misionales y estratégicos de la organización, los cuales están directamente relacionados con el sector de negocio, los servicios que se ofrecerán y de la contribución que la empresa espera que la implementación y uso de BYOD genere al negocio.

1.2 Planteamiento del trabajo

Con el presente desarrollo de Trabajo Fin de Máster, se pretende obtener como producto final, la consolidación y recopilación de los principales riesgos que deben ser contemplados, previo a cualquier implementación de un proyecto de tipo BYOD en una organización, cuyo insumo pueda ser utilizado como una “metodología” de punto de partida general para un Departamento de TI o de sus responsables (CIO, CISO, Otros) al momento de realizar un despliegue o implementación de BYOD en alguna organización, y que basados en este documento puedan complementar y definir los riesgos propios de cada organización, analizar, actualizar y hacer seguimiento a la(s) política(s) de seguridad de la información, acuerdos firmados de aceptación y uso razonable de BYOD, causas de revocatoria del acceso a BYOD, planes de tratamiento, evaluación y mitigación de riesgos, verificación de cumplimiento y eficacia de los controles basados en la ISO/IEC 27001:2013.

El presente documento aportará como contribución la identificación de riesgos, la formulación de una política de seguridad de la información y la sugerencia de implementación de controles de seguridad que deben ser implementados y aplicados en ambientes BYOD. La consideración e implementación de este aporte será el complemento primordial del plan acción que debe plantear, realizar y poner en marcha el departamento de TI de cualquier organización para el tratamiento y mitigación de las vulnerabilidades detectadas.

1.3 Estructura de la memoria

El presente documento de TFM se encuentra compuesto por 10 capítulos.

CAPÍTULOS

1. En este capítulo se realiza la introducción a BYOD, se da a conocer al lector aspectos generales sobre el tema, se realiza la justificación del por qué este trabajo de TFM es importante y se realiza la justificación.

2. En este capítulo se presenta al lector el estado del arte de BYOD a nivel mundial, la penetración y uso de dispositivos móviles, sus sistemas operativos y se presenta como aporte un análisis de riesgos generales de BYOD para cualquier organización.

3. En este capítulo se presenta al lector el planteamiento general del presente Trabajo de Fin de Máster acerca de BYOD.

4. En este capítulo se presenta al lector la contribución que se realiza con la investigación y elaboración del presente TFM.

5. En este capítulo se presenta al lector una breve reseña acerca de las herramientas y/o dispositivos de Gestión de Móviles, se muestran datos actuales de los mejores fabricantes de estos en el 2017 y sus principales características.

6. En este capítulo se presenta al lector de forma sintetizada el compendio de riesgos de seguridad de la información a los que se exponen los dispositivos móviles como

tal, y a su vez los riesgos que asumen los usuarios de los dispositivos móviles por las acciones que realizan y por ser blanco económico de los ciberdelincuentes.

7. En este capítulo se presenta al lector de forma clara y expresa las ventajas y desventajas que conlleva la aceptación, implementación y uso de BYOD a nivel corporativo.

8. En este capítulo se presenta al lector las conclusiones del trabajo realizado y las aportaciones futuras que podrían realizarse.

9. Bibliografía

10. Otros Recursos Electrónicos

2. Contexto y Estado del Arte

El mundo de la tecnología siempre se ha caracterizado por ser cambiante, se encuentra en continuo desarrollo e innovación, con el pasar de las décadas y de los años se ha evidenciado como día a día la informática, la electrónica, la computación, los desarrollos de Hardware, Software y demás relacionados con la Tecnología y las Comunicaciones, han avanzado a tal punto que han logrado evolucionar y dejar atrás los enormes dispositivos electrónicos, computadores, pantallas de tubos de rayos catódicos – "CRT", y demás elementos de gran tamaño, para darle fortaleza a la tendencia tecnológica de las ultimas décadas de reducir el tamaño de los dispositivos finales y de los componentes electrónicos con los que son diseñados y fabricados, no sin antes ofrecer mayores beneficios, versatilidad y capacidades a los consumidores y usuarios finales.

Dada esta tendencia a la reducción del tamaño y versatilidad de los dispositivos, me remonto a Junio del año 2007, cuando Apple con Steve Jobs como director ejecutivo, realiza la presentación e introducción al mercado Estadounidense del primer IPhone, el cual superaba tecnológicamente a los dispositivos móviles y Smartphone que se encontraban vigentes en el mercado hace 10 años, puesto que incorporaba novedades como: sólo teclado táctil, reproductor de música, cámara fotográfica de 2 megapíxeles, conectividad a internet por Wi-Fi.

En mi opinión, este evento se convirtió en un hito a nivel mundial, pues todos los usuarios de dispositivos móviles, vimos el nacimiento y aparición de la nueva tendencia tecnológica en cuanto a las telecomunicaciones y sus nuevos alcances orientados a la reducción en el tamaño de los dispositivos móviles, mayor funcionalidad, conectividad, acceso a redes sociales, multitarea y multipropósito, versatilidad y otros avances. En este punto hago especial hincapié en "Dispositivos Móviles" cuya definición es: "*Aparatos Electrónicos pequeños, fáciles de transportar y versátiles*" los cuales tienen unas características muy puntuales, según artículo en .PDF tomado de, https://www.exabyteinformatica.com/uoc/Informatica/Tecnologia_y_desarrollo_en_dispositivos_moviles/Tecnologia_y_desarrollo_en_dispositivos_moviles_(Modulo_2).pdf

1. **Movilidad**, tal vez es una de las características primordiales es decir que son dispositivos fáciles de transportar y de utilizar.
2. **Tamaño**, es decir que son dispositivos pequeños.
3. **Capacidad de conexión** y sincronización con computadores.
4. **Capacidad de almacenamiento** y memoria limitada.
5. **Capacidad de conexión a redes** (Telefónicas, Wi-Fi, otras) de forma permanente o intermitente
6. Son **diseñados para cumplir con funciones específicas**, pero son dispositivos de gran versatilidad, permiten realizar diversas tareas.

Dadas estas características, se diferencian claramente los dispositivos móviles, de los computadores portátiles. Estos dispositivos móviles en su constante evolución, masificación de uso y penetración en el mercado de consumo, se han convertido en pequeños computadores de bolsillo, cuya versatilidad permite que cada usuario los personalice y adapte a sus necesidades personales y laborales.

2.1 Marco Conceptual

2.1.1 Definiciones:

Dispositivo móvil: También conocido como computadora de bolsillo o computadora de mano (*palmtop* o *handheld*), es un tipo de computadora de tamaño pequeño, con capacidades de procesamiento, con conexión a Internet, dotado de memoria RAM, diseñado específicamente para una función, pero que pueden llevar a cabo otras funciones más generales.

Estrictamente hablando, muchos de los llamados dispositivos móviles no tienen la capacidad de moverse. Más bien son dispositivos que pueden ser fácilmente transportados por sus usuarios.

Smartphone: Es un término para denominar a un teléfono móvil o dispositivo móvil, que tiene mayores prestaciones que un teléfono móvil común, este tipo de teléfonos inteligentes se destacan por su capacidad de instalación de aplicaciones lo cual incrementa su potencial. Son considerados como computadores de bolsillo.

Tablet: Es un dispositivo electrónico que tiene un tamaño intermedio entre el ordenador y el móvil. Sus principales características son las siguientes: ligereza, manejo intuitivo utilizando las manos, elevada autonomía de uso y no dependencia de otros accesorios complementarios.

Amenaza: Causa potencial de un incidente no deseado, que puede provocar daños a cualquier sistema o a una organización.

Vulnerabilidad: Debilidad de un activo o control que puede ser explotada por una o más amenazas.

Alcance: Cualquier ámbito de una organización, que queda sometido a lo que defina puntualmente una empresa o compañía en su SGSI o proyecto.

SGSI: Es la abreviatura de Sistema de Gestión de la Seguridad de la Información, lo que en otras palabras es la aplicación de una serie de políticas para el manejo de la seguridad de la información en una organización.

Servicios Web: Aplicaciones a las cuales se accede por medio de un navegador web, las cuales se encuentran y establecen conexión con servidores web.

Riesgo: Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad, para causar una pérdida o daño en un activo de información. Suele considerarse como una combinación de la probabilidad de que un evento ocurra y sus posibles consecuencias.

Salvaguarda / Control: Son las políticas, los procedimientos, las prácticas y las estructuras organizativas concebidas para mantener los riesgos de seguridad de la información por debajo del nivel de riesgo asumido. Control es también utilizado como sinónimo de salvaguarda o contramedida. *En una definición más simple, es una medida que modifica el riesgo*.

Análisis de riesgos: Proceso para comprender la naturaleza del riesgo y determinar el nivel de riesgo.

Autenticación: Provisión de una garantía de que una característica afirmada por una entidad o persona es correcta y da la garantía de que es quien dice ser.

Confidencialidad: Propiedad de la información de no ponerse a disposición o ser revelada a individuos, entidades o procesos no autorizados. Determina que la información no ha sido revelada a quien no esté autorizado.

Integridad: Propiedad de la información relativa a su exactitud. Determina que la información no ha sido modificada y que es integra en su totalidad.

Disponibilidad: Propiedad de la información de estar accesible y utilizable cuando se requiera.

CheckList: Lista de apoyo para un auditor con los puntos a auditar, ayuda a mantener claros los objetivos de una auditoría, sirve de evidencia del plan de auditoría, asegura su continuidad y profundidad, y reduce los prejuicios del auditor y su carga de trabajo. Este tipo de listas también se pueden utilizar durante la implantación del SGSI para facilitar su desarrollo.

Directriz: Es una descripción que clarifica, qué debería hacerse y cómo, con el propósito de alcanzar los objetivos establecidos en una política.

Evaluación de Riesgos: Proceso global de identificación, análisis y medición de riesgos. Se verifica puntualmente el impacto que podría tener la materialización de un riesgo y la probabilidad de que ocurra, y con esto planificar controles para (Aceptar, Disminuir, Trasladar, o Evitar) el riesgo.

Identificación de Riesgos: Proceso de análisis que permite identificar los activos, reconocer sus vulnerabilidades, amenazas y describir los riesgos a los cuales está sujeto.

ISO: Organización Internacional de Normalización, con sede en Ginebra (Suiza). Es una agrupación de entidades nacionales de normalización cuyo objetivo es establecer, promocionar y **gestionar estándares** (normas).

ISO/IEC 27001:2013: Norma o estándar que establece los requisitos para un Sistema de Gestión de Seguridad de la Información (SGSI). Primera publicación en 2005; segunda edición en 2013. Es la norma en base a la cual se certifican los SGSI a nivel mundial.

ISO/IEC 27002:2013: Código de buenas prácticas en Gestión de Seguridad de la Información. Primera publicación en 2005; segunda edición en 2013. No es certificable.

Parte interesada: Persona, organización u otro, que puede afectar a, ser afectada por, o percibirse a sí misma como afectada por una decisión, normatividad, ley o actividad.

Política: Planes, medidas y acciones que indique puntos principales en el ámbito de sistemas (informática) para el tratamiento de la información, la protección y la seguridad de los datos y medios informáticos.

Hardware: Es un término en inglés, que significa partes duras. En sí son las partes físicas de un sistema, necesarias para que un equipo funcione.

Software: Hace referencia a un programa(s), que permiten realizar diferentes tareas.

Adware: Software malicioso que llena de anuncios y publicidad un dispositivo.

Spyware: Software de tipo malware que se encarga de recopilar y enviar información.

Malware: Es otra forma de llamar a los virus, o programas maliciosos que son perjudiciales para un equipo, o un sistema.

Spoofing: En términos de seguridad es hacerse pasar por otro, lo cual es una técnica usada por delincuentes para conseguir cualquier tipo de información que le interese de los usuarios, por ejemplo, suplantar la página de un proveedor de correo electrónico.

Phishing: Es una técnica basada en la suplantación de identidad y se combina con estrategias de ingeniería social, para que los delincuentes puedan obtener información confidencial de sus víctimas, como puede ser información de tarjetas de crédito, contraseñas y demás.

Sniffing: Es una técnica que se encarga de “escuchar” todo el tráfico de datos, que es transmitido por una red, cuyo resultado final es el robo e interceptación de información, para la realización de esta técnica se requiere de software especializado conocido como “sniffer”.

TI/IT: Tecnologías de la Información y las comunicaciones / Information Technology.

Agente: Programa o aplicación que se instala en un computador o dispositivo móvil y se comunica con una herramienta, para informar de la actividad del equipo que la tiene instalada, y a su vez permitir la gestión y administración de los mismos dispositivos.

MDM/EMM: Por su sigla en inglés Mobile Device Management /Enterprise Mobility Management, es una herramienta que permite la gestión y administración de dispositivos móviles, computadores portátiles y tabletas.

SaaS: Software como Servicio.

PaaS: Plataforma como Servicio.

IaaS: Infraestructura como Servicio.

2.2 Dispositivos Móviles, Nuevo Blanco de la Ciberdelincuencia

Los dispositivos móviles, se han convertido en el nuevo objetivo de la delincuencia en todos los ámbitos, los criminales se aprovechan de la ingenuidad de los usuarios, se ha incrementado el robo físico de los dispositivos, el ransomware, el phishing, entre otra cantidad de ciberdelitos que no sólo están afectando a los usuarios, sino a su vez a las empresas para las cuales prestan sus servicios los usuarios.

Según James Lyne, responsable de la seguridad global en Sophos, entrevistado en 2015 en el *Mobile World Congress* en Barcelona, Lyne, responsabiliza a los fabricantes de los dispositivos móviles, de la insuficiente sensibilización de los riesgos de seguridad y privacidad a los que se encuentran expuestos los consumidores, de los que solo un 40% utiliza un código PIN para proteger sus dispositivos móviles. Ahora también se ha evidenciado que en las tiendas de descarga de aplicaciones, en el caso del presente TFM enfocado a ANDROID, la tienda *Google Play Store*, lugar en el que se supone los usuarios pueden conseguir aplicaciones seguras y libres de código malicioso (adware, spyware, malware, otros) pues ya no lo es!, los delincuentes están incorporando virus en algunas aplicaciones, las cuales al instalarse hacen que el usuario les dé permisos de acceso completo a los dispositivos móviles, sin percatarse de esta anomalía de seguridad, con lo cual los ciberdelincuentes tienen acceso completo a todo el dispositivo y se camuflan y van robando la información que el propio usuario les entrega.

En el anterior párrafo se comprueba perfectamente que el usuario es el eslabón más débil en la cadena de la seguridad, por más que se tengan programas antivirus y dispositivos de seguridad sofisticados, políticas de seguridad, controles, y demás actividades de aseguramiento de la información, no existe suficiente sensibilización para que el propio usuario no ponga en riesgo su propia seguridad y la de los sistemas informáticos en los cuales interactúa, puesto que es él mismo, el que le otorga en determinadas ocasiones, acceso completo a los delincuentes a sus dispositivos móviles y por medio de estos a la infraestructura y plataformas tecnológicas de cualquier organización, asimismo les entrega a los delincuentes cuentas de acceso, password, e-mail, geolocalización, datos de la red, información de sistemas operativos, servidores de bases de datos, etc., con lo cual los delincuentes pueden lograr sabotear, robar, dañar, modificar los sistemas informáticos de las organizaciones.

Basado en consultas realizadas a la base de datos del CVE – Common Vulnerabilities and Exposures, sobre vulnerabilidades del Sistema Operativo Android, información consultada en http://www.cvedetails.com/product/19997/Google-Android.html?vendor_id=1224, se puede concluir que en los últimos años se ha vuelto un sistema operativo muy inseguro, cabe recalcar en este punto, que a los delincuentes les interesa atacar los sistemas más usados y ANDROID a nivel mundial en dispositivos móviles es uno de ellos, por esto es un sistema demasiado expuesto, en el cual los delincuentes están a la búsqueda diaria de vulnerabilidades que puedan permitir sus actividades delictivas, a continuación, se presenta la información de las vulnerabilidades detectadas y recopiladas por CVE, de ANDROID desde el año 2009 hasta lo corrido de Junio de 2017.

Vulnerability Trends Over Time

Year	# of Vulnerabilities	DoS	Code Execution	Overflow	Memory Corruption	Sql Injection	XSS	Directory Traversal	Http Response Splitting	Bypass something	Gain Information	Gain Privileges	CSRF	File Inclusion	# of exploits
2009	5	3								1					
2010	1	1	1												
2011	9	1	1		1					3	2	3			
2012	8	5	4	2							1				1
2013	7	1	2	2	2					1	1	3			
2014	13	2	4	1		1				1	2	2			1
2015	125	56	70	63	46					20	19	17			
2016	523	104	73	92	38					48	99	250			
2017	255	38	134	36	25					24	42	34			
Total	946	211	289	196	112	1				98	166	309			2
% Of All		22.3	30.5	20.7	11.8	0.1	0.0	0.0	0.0	10.4	17.5	32.7	0.0	0.0	

Ilustración 1. Vulnerabilidades detectadas del Sistema Operativo Android en los últimos 9 años

Fuente: http://www.cvedetails.com/product/19997/Google-Android.html?vendor_id=1224

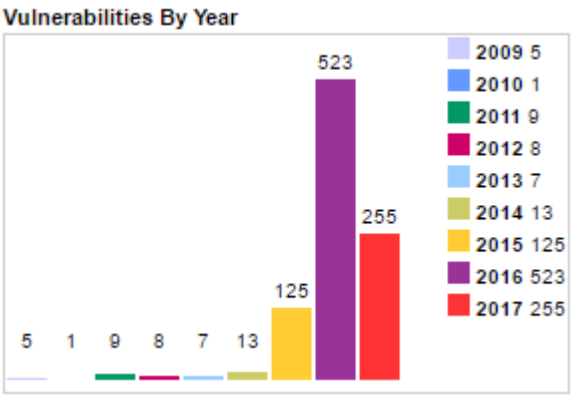

Ilustración 2. Top de Vulnerabilidades de Android por Año

Fuente: http://www.cvedetails.com/product/19997/Google-Android.html?vendor_id=1224

Para complementar la información de la versión de Android, con relación al año de detección de las vulnerabilidades, se consultó el histórico de versiones de Android de la página oficial del proveedor (https://www.android.com/intl/es_es/history/#/marshmallow), con la finalidad de ubicar cronológicamente al lector del documento en cuanto al año, nombre, número de la versión y cantidad de vulnerabilidades detectadas por año, pues están directamente relacionadas con cada nueva versión de este sistema operativo, las cuales han salido al mercado para corregir fallas y agregar nuevas funcionalidades.

Nombre de la Versión	Número de la Versión	Año de Lanzamiento
Donut	Android 1.6	Septiembre de 2009
Eclair	Android 2.1	Octubre de 2009
Froyo	Android 2.2	Mayo de 2010
Gingerbread	Android 2.3	Diciembre de 2010
Honeycomb	Android 3.0	Febrero de 2011
Ice Cream Sandwich	Android 4.0	Octubre de 2011
Jelly Bean	Android 4.1	Julio de 2012
KitKat	Android 4.4	Octubre de 2013
Lollipop	Android 5.0	Noviembre de 2014
Marsmallow	Android 6.0	Octubre de 2015
Nougat	Android 7.0	Agosto de 2016

Tabla 1 Versiones de Android

Fuente: Elaboración Propia

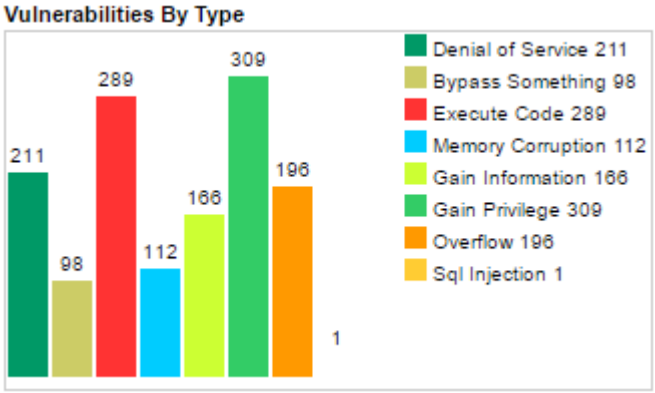

Ilustración 3. Top de Vulnerabilidades de Android por Tipo

Fuente: http://www.cvedetails.com/product/19997/Google-Android.html?vendor_id=1224

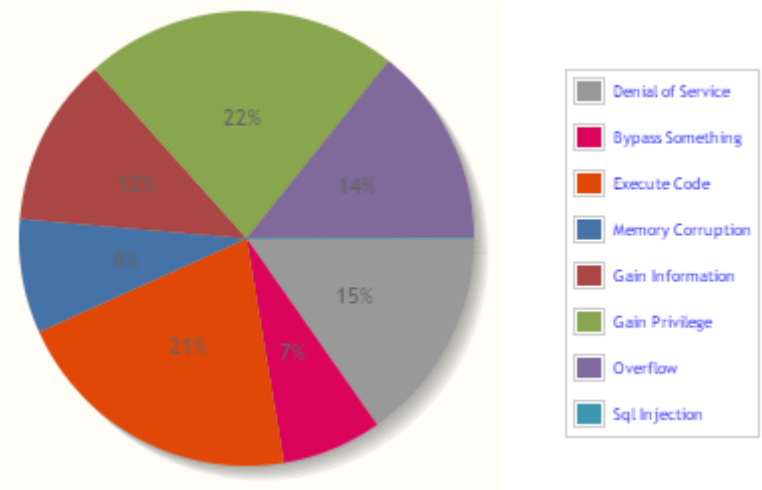

Ilustración 4. Porcentaje de Vulnerabilidades por tipo

Fuente: http://www.cvedetails.com/product/19997/Google-Android.html?vendor_id=1224

Según los informes de distribución de versiones de Android proporcionados por Google, a fecha **02 de Mayo de 2017**, presenta el porcentaje de uso a nivel mundial, de las versiones de Android más utilizadas por los usuarios. En este informe Google destaca el importante crecimiento que ha tenido Android Nougat en los dispositivos, a menos de un año de su lanzamiento (Agosto 22 de 2016), Google informa que ya se encuentra presente en el 7.1% de los dispositivos. La información ha sido tomada de https://www.xatakandroid.com/mercado/android-nougat-ya-esta-presente-en-mas-del-7-de-los-dispositivos-gingerbread-sorprende-con-un-ligero-repunte.

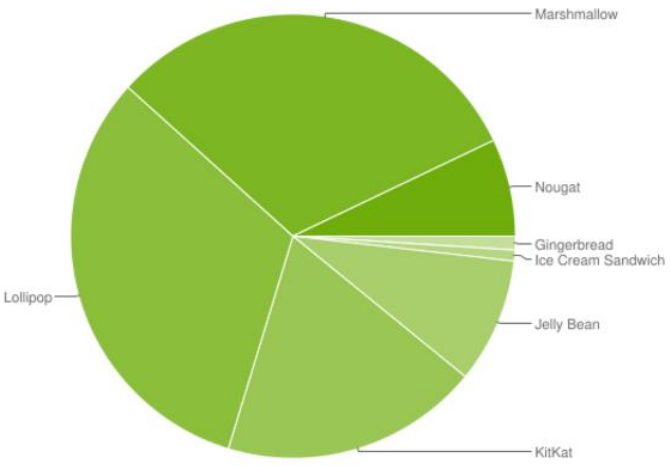

Ilustración 5. Gráfica de distribución de versiones de Android – Mayo de 2017

Fuente: https://www.xatakandroid.com/mercado/android-nougat-ya-esta-presente-en-mas-del-7-de-los-dispositivos-gingerbread-sorprende-con-un-ligero-repunte

Version	Codename	API	Distribution
2.3.3 - 2.3.7	Gingerbread	10	1.0%
4.0.3 - 4.0.4	Ice Cream Sandwich	15	0.8%
4.1.x	Jelly Bean	16	3.2%
4.2.x		17	4.6%
4.3		18	1.3%
4.4	KitKat	19	18.8%
5.0	Lollipop	21	8.7%
5.1		22	23.3%
6.0	Marshmallow	23	31.2%
7.0	Nougat	24	6.6%
7.1		25	0.5%

Tabla 2 Porcentaje de uso de las Distribuciones de Android - Mayo de 2017

Fuente: https://www.xatakandroid.com/mercado/android-nougat-ya-esta-presente-en-mas-del-7-de-los-dispositivos-gingerbread-sorprende-con-un-ligero-repunte

https://developer.android.com/guide/topics/manifest/uses-sdk-element.html#ApiLevels

Según Kaspersky Labs, Mayores Riesgos con BYOD (https://blog.kaspersky.com.mx/tag/byod/). “Si añadimos la creciente adopción de las iniciativas BYOD (traiga su propio dispositivo), los riesgos de seguridad se multiplican. Puesto que los dispositivos móviles propios de los empleados, incorporan una mezcla de sus datos y aplicaciones personales, además de los datos de la empresa, cuentas de usuario y contraseñas de acceso, lo que finalmente ha aumentado significativamente las brechas de seguridad de la información. Además, debido a que los dispositivos móviles son tan pequeños, estos pueden ser robados, o perdidos fácilmente por los usuarios, lo anterior pone en total riesgo la información, dando acceso directo a usuarios no autorizados, a información personal, correos electrónicos, redes sociales, sistemas y aplicativos de las empresas, etc.

Ilustración 6 Evolución de amenazas de TI en el segundo trimestre de 2015

Fuente: Kaspersky Lab

2.2.1 Penetración de Dispositivos Móviles en América Latina

Según Juan Manuel Gómez, Gerente Regional de Ventas para la Región Sur de Latinoamérica de Citrix, “se rompió esa barrera en que las empresas compraban el dispositivo para el empleado y controlaban todo, ahora es el empleado quien trae un dispositivo con alta capacidad de trabajo y eso representa el punto de acceso inicial de la productividad”.

Según Ángel García Zaballos, especialista en Telecomunicaciones del Banco Interamericano de Desarrollo, en América Latina entre 2010 y 2016, ha habido un crecimiento vertiginoso del mercado de la industria de los móviles, en este lapso de tiempo pasó de 27 millones a 372. "Ha habido un impresionante crecimiento en la penetración de teléfonos inteligentes", señaló el director para Latinoamérica de GSMA, Sebastián Cabello, en una rueda de prensa en el *Congreso Mundial del Móvil* (MWC 2016) en Barcelona. Información tomada de http://www.elnuevodiario.com.ni/especiales/420676-venta-smartphones-alza-latinoamerica/.

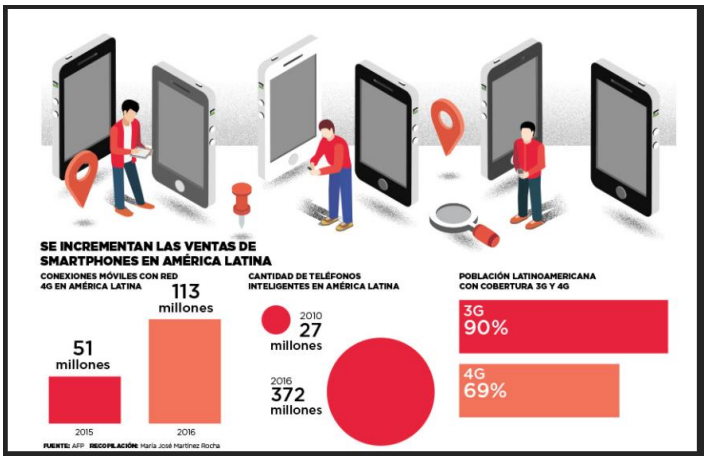

Ilustración 7. Crecimiento de Ventas de Smartphone en Latinoamérica 2010 – 2016

Fuente: http://www.elnuevodiario.com.ni/infografia/4417/

En Latinoamérica se tiene esta tendencia de crecimiento en el uso de los dispositivos móviles inteligentes, dado que se está logrando una mejora significativa de la infraestructura de comunicaciones en la región en lo corrido del (2017); aún hoy en día todos los usuarios de telefonía móvil y de datos, no pueden tener acceso a redes 4G, es más amplio el porcentaje de cobertura en redes 3G y esto sin mencionar que ya está ad portas, la entrada de las redes de comunicaciones 5G. En las zonas rurales de la región, hoy en día no hay suficiente masificación de los servicios de telecomunicaciones, ni el acceso a buenas bandas, se tienen problemas para el uso del espectro y frecuencias electromagnéticas, la oferta del servicio de datos de los dispositivos móviles es demasiado costosa y medida con planes limitados de datos que van por lo general entre 1 GB y 10 GB mensuales.

Para clarificar el caso de la cobertura 4G en las zonas rurales de los países de Latinoamérica, se propone como ejemplo el caso de cobertura en las zonas rurales de Colombia, que tiene 1122 municipios y el operador más grande de telecomunicaciones del país “Claro”, ofrece cobertura 4G en 405 municipios, es decir que no alcanza a cubrir el 50% del país.

Ilustración 8. Cobertura 4G en Colombia Junio de 2017 - Operador de Telecomunicaciones Claro

Fuente: http://www.claro.com.co/personas/servicios/servicios-moviles/postpago/beneficios/#

Según un estudio realizado en Enero de 2015 por comScore, empresa que se dedica al marketing en internet; en Latinoamérica se ha observado un elevado nivel de penetración, uso y acceso por parte de los consumidores a los dispositivos móviles, a continuación, se presenta una figura que ilustra el contexto de uso de determinados dispositivos móviles en 6 países de Latinoamérica.

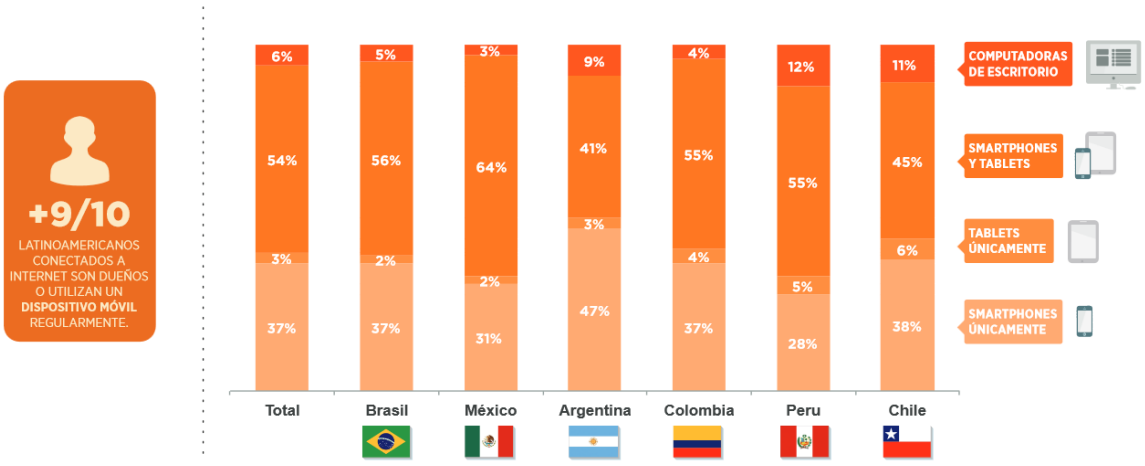

Ilustración 9: Uso de Dispositivos

Fuente: http://www.imscorporate.com/news/Estudios-comScore/IMS-Mobile-Study-Enero2015.pdf

Complementando la información anterior, se presentará la estadística que recopiló comScore, con relación a las preferencias de sistema operativo, tipo de conexión a la red de datos y promedio de aplicaciones instaladas en los dispositivos móviles, lo cual aporta un panorama

amplio de la masificación de uso de este tipo de dispositivos móviles, por parte de los consumidores en la región de Latinoamérica.

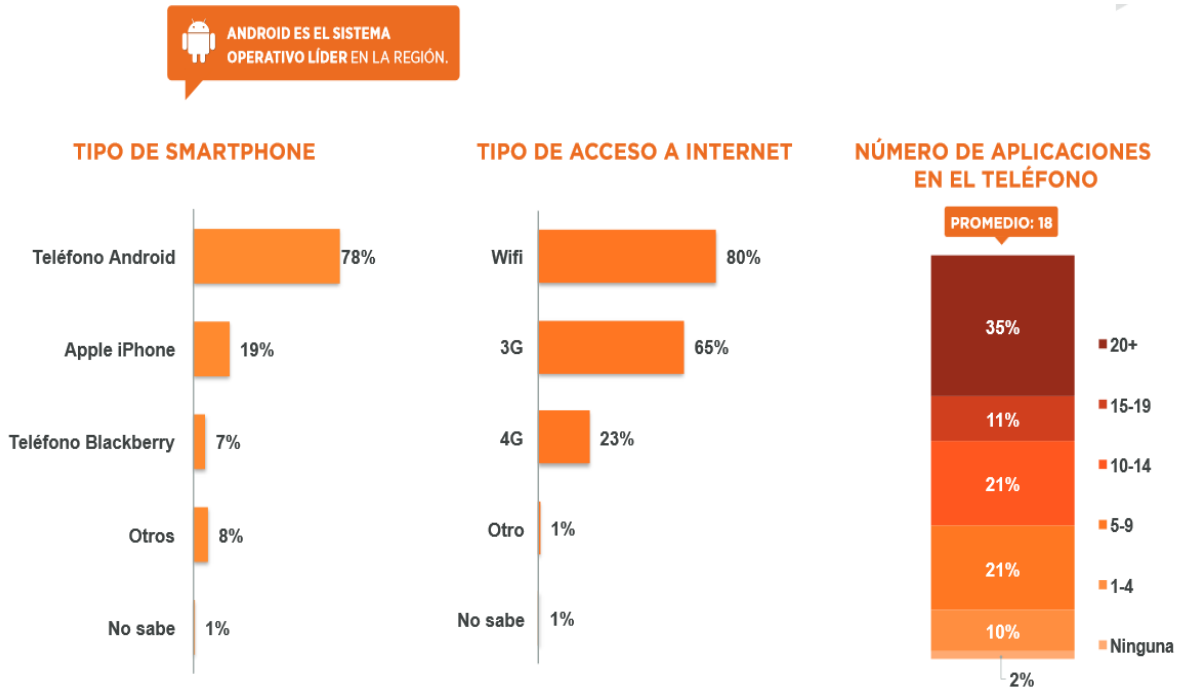

Ilustración 10 Posesión y Utilización de Smartphone en la Región Latinoamericana

Fuente: http://www.imscorporate.com/news/Estudios-comScore/IMS-Mobile-Study-Enero2015.pdf

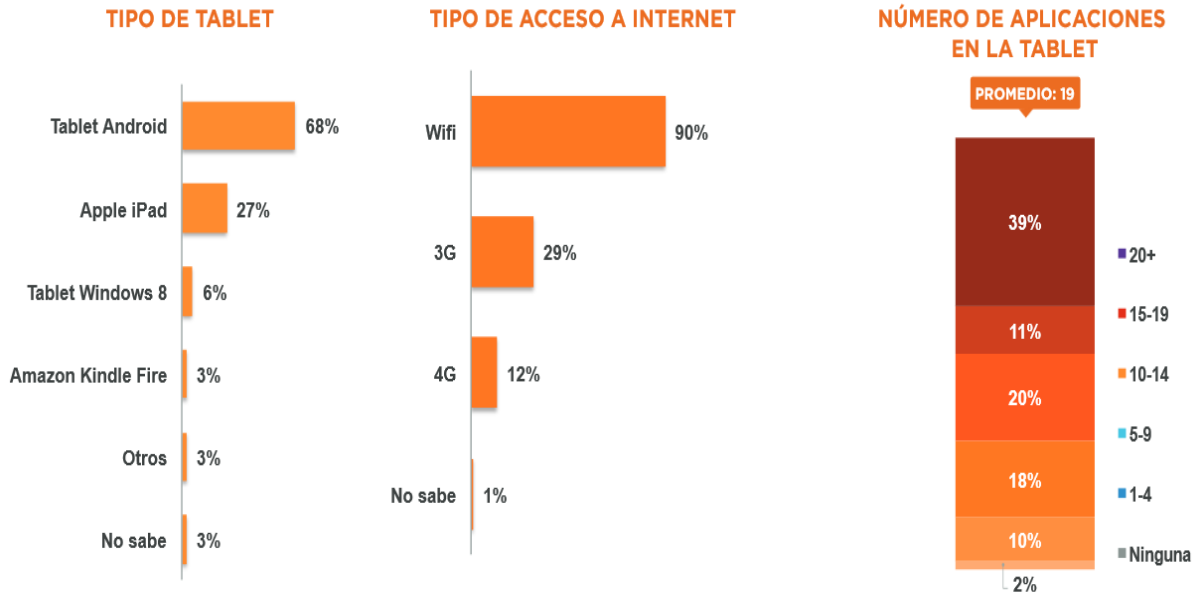

Ilustración 11 Posesión y Utilización de Tabletas en la Región Latinoamericana

Fuente: http://www.imscorporate.com/news/Estudios-comScore/IMS-Mobile-Study-Enero2015.pdf

2.2.2 Penetración de Dispositivos Móviles en España y en el Mundo

Según un estudio realizado en 2016 por Ditrendia, empresa española, que se dedica al marketing digital en internet, a finales del año 2015 la penetración de teléfonos móviles en el mundo es de un 97%, con una cifra aproximada de 7.9 mil millones de dispositivos móviles, cuya cifra supera a la cantidad de personas que habitamos el planeta. Según el informe se evidencia que se aumentó la venta de dispositivos móviles, en 341 millones de unidades entre 2014 y 2015.

España se sitúa en la primera ubicación de mayor penetración de dispositivos móviles en Europa, representados con un 87% de penetración, cuya cifra supera la de penetración y uso de computadores personales que se encuentra en un 80%, otro factor muy importante es que el 98% de los niños y jóvenes de entre 10 y 14 años se han sumado a la tendencia cotidiana de uso de dispositivos móviles con conexión a internet. La anterior información tiene su soporte en los siguientes gráficos y fuente de referencia.

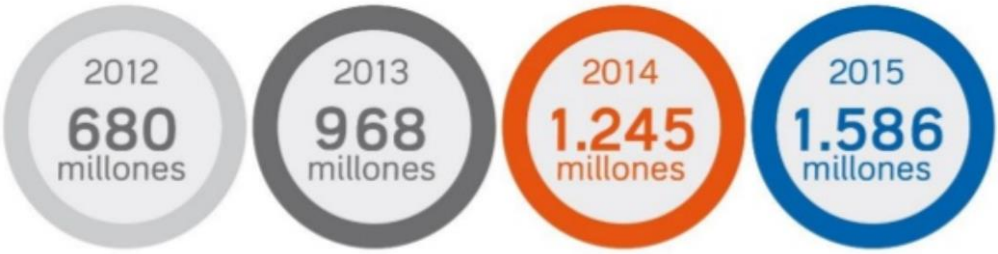

Ilustración 12 Evolución de la cantidad de Smartphone vendidos en el mundo

Fuente: http://es.slideshare.net/ditrendia/informe-ditrendia-mobile-en-espaa-y-en-el-mundo-2016

http://es.slideshare.net/ditrendia/informe-ditrendia-mobile-en-espaa-y-en-el-mundo-2016

Según las cifras del informe se tiene que a la fecha de elaboración del presente documento en (2017), existían más de 4.600 millones de usuarios de móviles en el mundo, de los cuales 2 mil millones son usuarios de teléfonos inteligentes, la presente información se puede observar de forma clara en la siguiente ilustración cuyos datos están expresados en miles de millones.

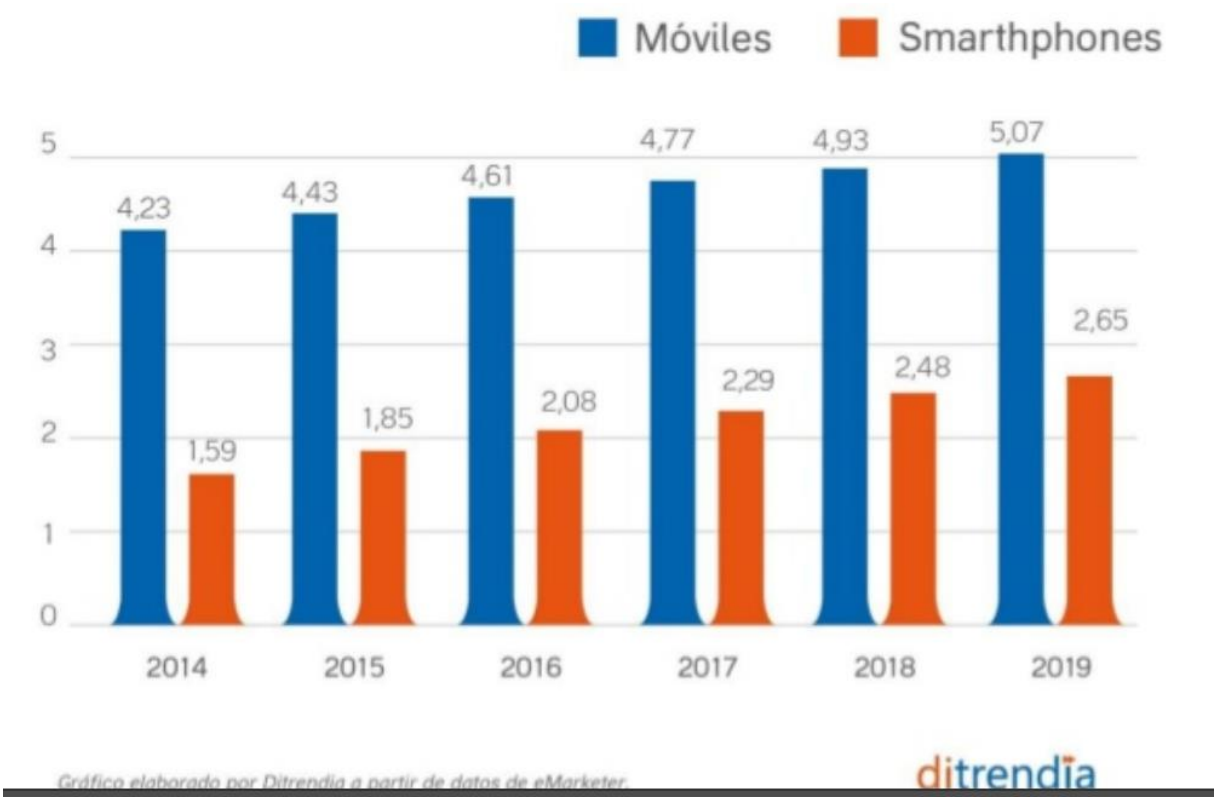

Ilustración 13 Evolución del número de Móviles VS Smartphone en el Mundo

Fuente: http://es.slideshare.net/ditrendia/informe-ditrendia-mobile-en-espaa-y-en-el-mundo-2016

En la siguiente ilustración, se presentan los porcentajes de penetración de los móviles a nivel mundial, representados por regiones para el año (2016).

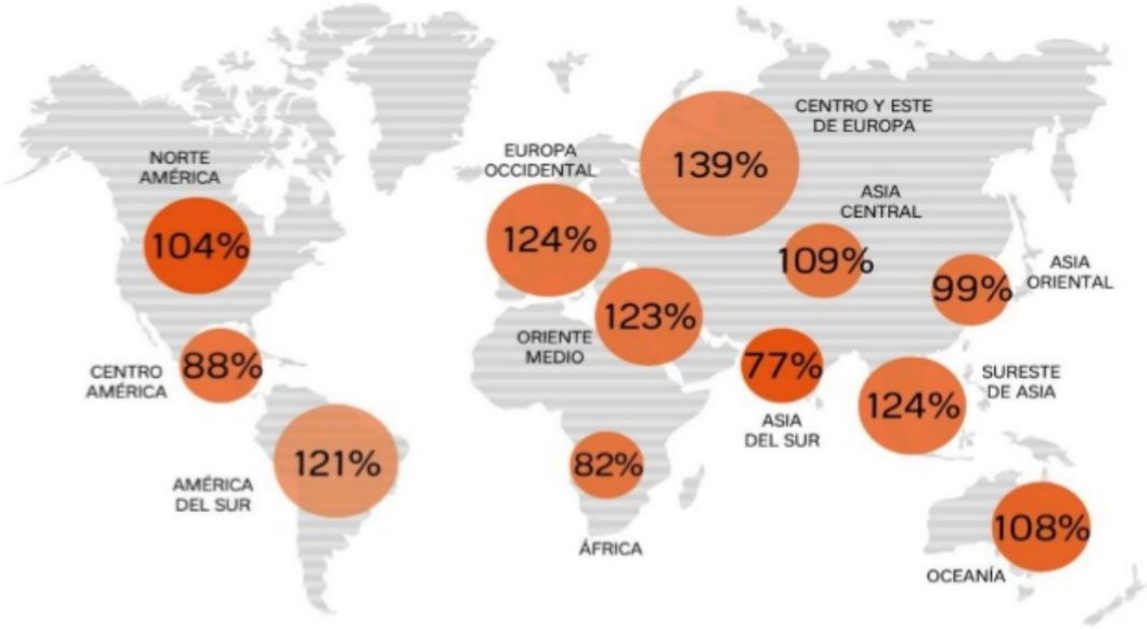

Ilustración 14 Penetración del móvil en el mundo

Fuente: http://es.slideshare.net/ditrendia/informe-ditrendia-mobile-en-espaa-y-en-el-mundo-2016

En España, el número de líneas móviles para el año 2015, alcanzó la cantidad de 50.8 millones de líneas móviles, cuya cifra supera la cantidad de población española. A la fecha, Junio de 2017, la población de España es de 45.959.958. Información tomada de: http://countrymeters.info/es/Spain

Ilustración 15. Datos de Población de España a 01 de Junio de 2017

Fuente: http://countrymeters.info/es/Spain

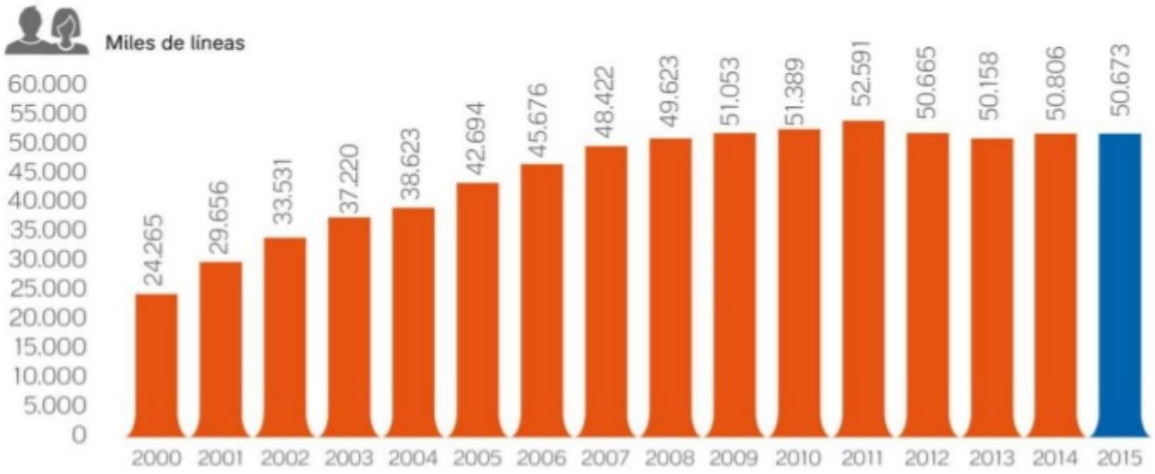

Ilustración 16 Número de clientes de telefonía móvil en España

Fuente: http://es.slideshare.net/ditrendia/informe-ditrendia-mobile-en-espaa-y-en-el-mundo-2016

2.2.3 Retos de BYOD

BYOD, en inglés (Bring Your Own Device) cuyo significado es, “Trae tu Propio Dispositivo”, es una tendencia que está redefiniendo la visión y la gestión de las áreas de TI a nivel mundial,

en pocas palabras BYOD, es planteado y usado como un mecanismo de mayor productividad tanto para el empleado como para las empresas, dado que se lleva a cabo por medio del uso e incorporación a los sistemas corporativos, de dispositivos móviles en su mayoría de propiedad de los usuarios, para la realización de actividades de índole laboral, esto aporta directamente a la organización, debido a que sus empleados pueden ser más productivos y competitivos en cualquier momento y desde cualquier lugar en el que se encuentren, y tendrán acceso a servicios e información como correo electrónico, bases de datos, web services, intranet, extranet, información corporativa, documentos, estaciones de trabajo, etc.

Vale la pena destacar que la inclusión de BYOD, aportará a las organizaciones, dispositivos móviles en su gran mayoría de última generación, los cuales ofrecen grandes beneficios a las partes interesadas en cuanto a Hardware, Aplicaciones y Capacidad. Según Gartner, la tendencia a futuro de BYOD en (2020), será que los empleados realicen sus funciones y actividades laborales completamente desde sus dispositivos móviles, reduciendo de esta manera para las organizaciones los altos costos relacionados con la adquisición y gestión de estaciones de trabajo para los empleados, con lo cual las áreas de TI, centrarán su atención a robustecer sus plataformas de seguridad, comunicaciones, aplicaciones y de integración de nuevos dispositivos.

La incorporación de BYOD, ha traído consigo la necesidad de afrontar y gestionar al interior de cada organización, fundamentalmente 3 retos:

1. **Gobierno y cumplimiento**: Es un ítem de especial atención con relación al cumplimiento y acato de la normatividad interna y externa a la organización, (Contexto Interno y Contexto Externo), en la cual se debe garantizar que se han contemplado los aspectos legales, de índole nacional e internacional, según aplique a la organización, y asimismo garantizar el cumplimiento de las directrices de Gobierno (interno), evitando infringir o violar las políticas establecidas, reglas, regulaciones, leyes, decretos y demás factores críticos de seguridad de la información, para la organización, relacionados con la prestación del servicio BYOD.

   Este apartado es de gran importancia especialmente en el establecimiento, revisión y cumplimiento estricto de las políticas internas de gobierno establecidas por la organización, y que adicionalmente establezca, afine y divulgue una **política** de uso de los dispositivos móviles amplia y suficiente, en la cual se defina claramente el **alcance, condiciones de uso,**

restricciones y revocatoria del uso de los dispositivos móviles, que proteja la información y sistemas tanto de los usuarios como de la organización.

2. **Gestión de los dispositivos móviles**: Es otro de los grandes retos a cubrir, puesto que se encuentra directamente relacionado con la propiedad de los dispositivos móviles por parte de los usuarios, con la protección de la privacidad de su información y con el alcance propuesto por cada organización para BYOD, lo cual requiere que la empresa adquiera, implemente y administre dispositivos de tipo *Mobile Device Managment*, en adelante (MDM), para la gestión de los dispositivos móviles, no dejando de lado velar por el cumplimiento de los derechos de propiedad intelectual y legalización del software utilizado en los dispositivos móviles, dado que la instalación de aplicaciones por parte del usuario, no estará dentro de un ambiente de TI totalmente restringido en cuanto a instalaciones, puesto que los dispositivos móviles en la mayoría de los casos no serán de propiedad de la empresa, lo cual se presta con mucha facilidad para que los usuarios instalen y utilicen aplicaciones de forma indiscriminada, sin percatarse, o tener los conocimientos suficientes para verificar la legalidad y la seguridad en cuanto a virus que puedan tener las aplicaciones.

3. **Seguridad:** BYOD, no es sinónimo de sin "control", por lo cual es un reto de gestión de las áreas de TI que la incorporación de BYOD opere en un ambiente controlado, que garantice la disponibilidad de la información, el acceso a los servicios, mitigue el riesgo de pérdida de información y se pueda realizar la trazabilidad completa de las acciones que realizan los usuarios sobre los servicios ofertados, esto se logra con la estrecha correlación de los dos puntos anteriores, en los cuales la empresa determina el alcance y las políticas y adicionalmente se incorporan a la infraestructura los dispositivos MDM, en los cuales se configura de acuerdo al alcance, los niveles de permisividad o restricciones, que garanticen la seguridad y por ultimo pese a las medidas anteriores, se debe realizar el trabajo más fuerte, SENSIBILIZAR A LOS USUARIOS, pues en últimos, son ellos el talón de Aquiles, en cuanto a la seguridad; por más medidas y controles que se establezcan, si el usuario comete algún error, abre la puerta a los delincuentes.

2.2.4 Análisis de Riesgos Generales de BYOD

En la actualidad existe diversidad de vulnerabilidades y amenazas enfocados a los dispositivos móviles, para el caso del presente TFM, se enfoca directamente al sistema operativo ANDROID, que es el más difundido y utilizado a nivel mundial, como se logró clarificar en los apartados anteriores. Desde hace por lo menos 5 años, los dispositivos móviles se han vuelto una herramienta imprescindible para cualquier persona, puesto a que en ellos tiene a la mano toda la información relevante que necesita de forma cotidiana, debido

a esto se han posicionado como un blanco más atractivo para los ciberdelincuentes, dado que este tipo de dispositivos móviles contiene suficiente información crítica de los usuarios que puede ser utilizada por la delincuencia para obtener dinero.

En estos dispositivos los usuarios manejan todo tipo de información, que parte desde información personal, agenda, ubicación y desplazamientos diarios (GPS), información de lugar de trabajo y vivienda, redes sociales, lugares en los que fueron tomadas fotografías y videos, números telefónicos personales y laborales, datos de cuentas bancarias, contraseñas de acceso a los servicios de redes sociales, financieros, correo electrónico y demás datos con los cuales a nivel personal los usuarios son el blanco perfecto de la delincuencia, como objetivo lucrativo.

De otra parte, también se tiene la información laboral, entre la cual se puede encontrar bases de datos de clientes, teléfonos de contacto, contraseñas de acceso a los servicios corporativos, credenciales de acceso a las redes empresariales, cuentas y contraseñas de acceso a información crítica de la organización, datos de correo electrónico, entre otra gran cantidad de información que también puede ser convertida en dinero por los delincuentes informáticos, o la cual puede conllevar a la localización e identificación de nuevas víctimas.

Los ciberdelitos se han masificado, debido a que los usuarios de los dispositivos móviles han cambiado de habito y ahora hacen uso de forma cotidiana con conexión a internet las 24 horas del día de las capacidades que tienen los dispositivos móviles, los cuales ya se comparan con las bondades de un computador, la diferencia en este punto radica en que los usuarios de computadores de alguna manera se preocupan hoy en día por proteger este tipo de dispositivos con la implementación de software de seguridad, pues ya son un poco más conscientes de los peligros a los que se enfrentan, lo mínimo que establecen son contraseñas de acceso a los perfiles de usuario, y lo complementan con algunos cuidados básicos de comportamiento y actividades en internet, pero dejan de lado la seguridad de los dispositivos móviles, que en la actualidad con los servicios en la nube, tienen prácticamente la misma información que tienen almacenada en sus estaciones de computo, olvidan o pasan por alto aplicar medidas de protección tales como la realización de un BACKUP de la información relevante de sus dispositivos móviles, NO hacen uso de las herramientas de cifrado de los medios de almacenamiento de sus dispositivos móviles, NO adquieren, ni implementan aplicaciones de seguridad, como mínimo un antivirus, guardan contraseñas de acceso a los servicios a los cuales accede por medio dichos dispositivos (correo, redes, bancos, estaciones

de trabajo, etc.) entre otra gran cantidad de malas prácticas de seguridad que se deberían tener en cuenta, olvidan por completo que están expuestos 24 horas al día todos los días, pues este tipo de dispositivos por lo general mantiene conectado a internet y no se apaga con frecuencia, lo cual facilita que este tipo de dispositivos pueda caer en manos criminales con mayor probabilidad y sigilo, adicionalmente no se tienen las suficientes medidas de seguridad por parte de los usuarios para detectar este tipo de eventos, evitarlos y/o contrarrestarlos.

Según un informe publicado por la CCN-CERT (CCN-CERT IA-09/13 Ciberamenazas 2012 y Tendencias 2013) https://www.ccn-cert.cni.es/informes/informes-ccn-cert...ccn-cert-ia-21.../file.html, el cual argumenta que las vulnerabilidades en los dispositivos móviles ha aumentado de forma vertiginosa y silenciosa, dado que este tipo de ataques se realizan de forma silenciosa y duraderos en el tiempo, cuando se detectan las vulnerabilidades o ataques a estos dispositivos ya es muy tarde, los delincuentes han tenido tiempo suficiente para hacerse a la información personal, bancaria, corporativa y demás que les pueda interesar de los dispositivos móviles; en estos casos lo único que queda por hacer, es poner en marcha un plan de acción reactivo el cual también toma un tiempo en estudiar de qué forma se comprometió el dispositivo y aplicar las salvaguardas pertinentes para evitar nuevos ataques de este tipo.

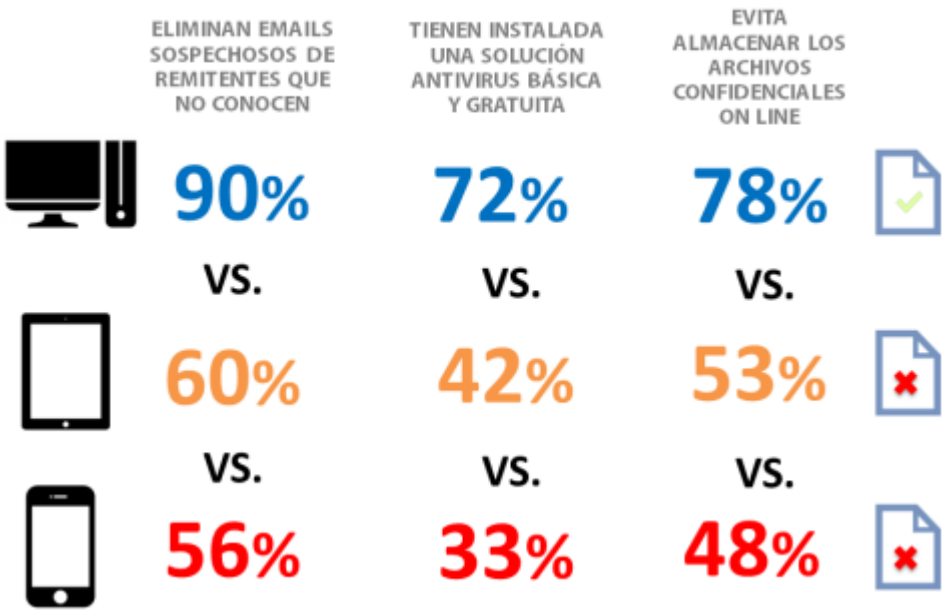

Ilustración 17. Comparativa de medidas de seguridad adoptadas según los distintos dispositivos

Fuente: https://www.ccn-cert.cni.es/informes/informes-ccn-cert-publicos/677-ccn-cert-ia-21-13-riesgos-y-amenazas-del-byod-1/file.html

Según FortiGuard (FortiGuard Midyear Threat Report, http://www.fortinet.com/resource_center/whitepapers/quarterly-threatlandscape-report-q213.html) en la primera mitad del año 2013 se analizaron más de 1300 muestras de móviles diarias que arrojaron 250.000 muestras enfocadas a sistemas Android.

Una encuesta desarrollada y realizada por la firma Fortinet en más de quince países (Fortinet® Global Survey Reveals 'First Generation' BYOD Workers Pose Serious Security Challenges to Corporate IT Systems (2012). http://www.fortinet.com/press_releases/120619.html) arrojó como resultado que el 42% de los consultados habrían sufrido perdida de datos y explotación de software malicioso a causa de BYOD.

Según Fortinet, en su reporte de amenazas del **primer trimestre de 2017** https://www.fortinet.com/demand/gated/Threat-Report-Q1-2017.html las cosas aún no mejoran en cuanto a malware para los dispositivos móviles, ni para Android, las cifras de propagación de malware en dispositivos móviles van en aumento en lo corrido del 2017. Las políticas de BYOD han sido desafiadas por el incremento del malware del cuarto trimestre de 2016 al primer trimestre de 2017.

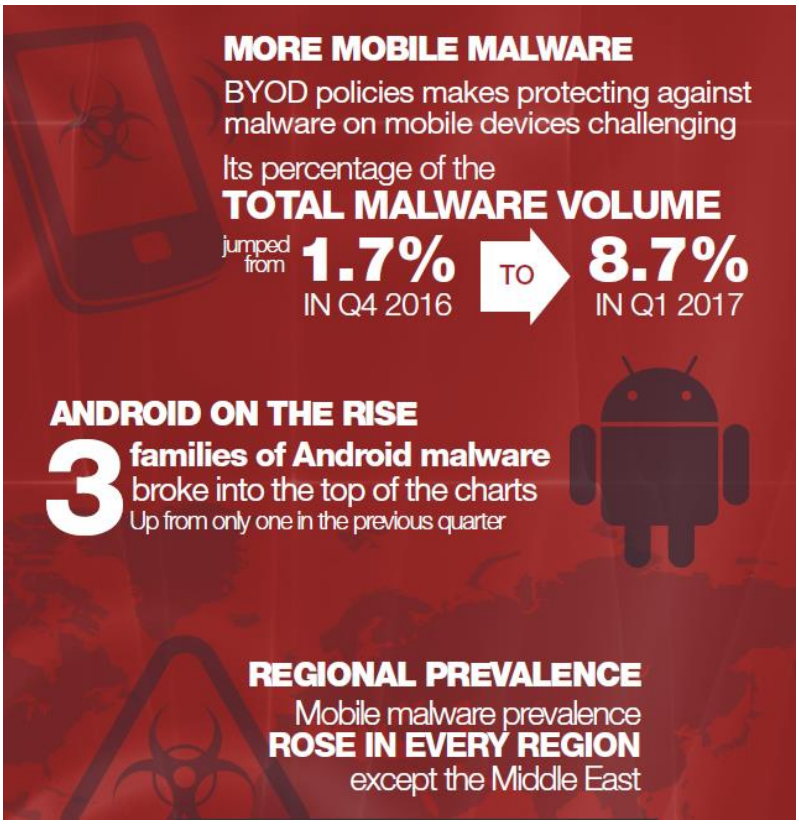

Ilustración 18. Amenazas Primer Trimestre de 2017 – Fortinet

Fuente: https://www.fortinet.com/content/dam/fortinet/assets/infographics/fortinet-infographic-threat-report-q12017.pdf

Asimismo se pudo constatar que el 36% de los empleados aceptó haber infringido las prohibiciones corporativas de usar sus dispositivos móviles con fines laborales, con lo cual generaron riesgos en la seguridad de la información a sus organizaciones, este es uno de los aspectos más difíciles de atacar para cualquier organización o área de TI, la delincuencia siempre ataca al eslabón más débil, el “usuario”; las organizaciones pueden implementar todas las medidas y dispositivos de seguridad, pero existirá siempre la amenaza persistente de ser expuestos por parte de sus propios empleados, que de forma voluntaria o involuntaria dan paso a la intrusión de los delincuentes.

Cada organización debe realizar un estudio juicioso de las vulnerabilidades y amenazas a las que podría estar expuesta, teniendo en cuenta las características de su negocio, el alcance de los servicios que va a publicar, los controles necesarios, la verificación y actualización de sus políticas y la probabilidad de materialización de las posibles amenazas antes de poner en marcha la implantación de un proyecto de tipo BYOD.

En cuanto a los riesgos relacionados con la movilidad de los dispositivos es uno de los grandes retos de seguridad para cualquier área de TI, puesto que pueden ser utilizados desde cualquier ubicación interna o externa a la organización, en especial cuando los dispositivos móviles son utilizados en lugares públicos (WI-FI), representan un alto nivel de exposición por la facilidad de acceso a los dispositivos móviles, por medio de conexión a redes inseguras o no confiables, lo cual puede venir acompañado de ataques de *hombre en medio* (MitM), por manipulación física de los dispositivos por parte de terceros, pérdida o robo de los dispositivos, ataques de redireccionamiento de URL por medio de códigos QR falsos, o mediante el simple acceso a otras redes como 2G, 3G, 4G, Bluetooth, NFC, entre otros factores de riesgo externo que resultan bastante complejos de controlar.

Este riesgo de movilidad, es de gran magnitud para cualquier organización dada la criticidad de la información, que según las políticas de BYOD pueda ser almacenada en los dispositivos móviles (cuentas y credenciales de acceso, correo electrónico, documentos confidenciales, registro de llamadas, contactos, galería multimedia, redes sociales, aplicaciones bancarias etc.)

Las técnicas de Jailbreaking en (IOS) o Rooting en (ANDROID), introducen otro riesgo muy habitual y peligroso tanto para las organizaciones, como para los usuarios, debido a que estas acciones que ejecutan los usuarios en sus dispositivos móviles favorecen la pérdida de control y seguridad establecida por el sistema operativo de sus dispositivos móviles y permiten que pueda ser utilizado software no oficial (manipulado, modificado, malicioso, pirata, etc.), que puede venir con malware inyectado, el cual podría conseguir y transmitir información al atacante, otorgarle el control remoto de los dispositivos móviles por medio de backdoor y finalmente, lograr la infección y acceso a estaciones de trabajo, servidores y/o redes corporativas.

Otro aspecto no menos riesgoso es la interconexión de los dispositivos móviles con otros sistemas, como es el caso de la sincronización de éstos con un computador de escritorio, o la conexión a dispositivos no confiables de carga de batería, los cuales pueden servir de plataforma para el robo y almacenamiento de información en ubicaciones inseguras. Este mecanismo de interconexión con otros sistemas, no solo conduce a la perdida de información, sino que abre la puerta a la transmisión de la misma en sentido bidireccional, lo cual puede

permitir que se introduzca software malicioso a los dispositivos sin que el usuario se percate y a su vez permitir que el usuario y el dispositivo propaguen el software malicioso a los demás sistemas o dispositivos con los que se interconecte.

El uso de los sistemas de posicionamiento global o GPS, es otra vulnerabilidad que debe ser tenida en cuenta, dado que dicha opción aporta a los atacantes ubicaciones físicas de los usuarios, por medio del uso de redes sociales, o la conexión a los diferentes servicios de las cuentas de Gmail en los dispositivos móviles, así como interferencia en las señales, ciberataques y demás riesgos asociados al GPS.

Ilustración 19. Vulnerabilidades Típicas GNSS – Sistema Global de Navegación por Satélite

Fuente: https://www.spirent.com/Assets/WP/WP-Fundamentals-of-GPS-Threats

El costo en cuanto a seguridad y privacidad al mantener operativo este servicio, es alto dado que los ciberdelincuentes pueden construir patrones de comportamiento y actividades cotidianas de los usuarios, facilitando a los delincuentes el acceso a mapas, desplazamientos, tiempo de desplazamiento, lugares visitados y con esto realizar cruce de información entre contactos y lugares, lo que supone un alto riesgo de pérdida de privacidad, tanto para la organización como para el usuario.

Es importante que cualquier organización tenga siempre presente como una posible vulnerabilidad latente, los aspectos legales y regulatorios a los que se deben adaptar tanto a nivel de leyes nacionales o internacionales que aplique según el sector de negocio de la organización, como también incluir la normatividad y políticas internas de la organización, que para el caso de BYOD, como mínimo debe contemplar la aceptación y firma de un consentimiento informado en el cual el usuario acepta y conoce las directrices bajo las cuales la organización permitirá, o revocará el uso de los dispositivos móviles personales, así como

también acepta que conoce las limitaciones y acciones que no están permitidas en virtud de que tengan impacto directo hacia la seguridad de la información tanto de la organización como personal.

Según el grado de madurez tecnológica de las organizaciones, puede contemplarse el seguimiento a los dispositivos móviles por medio de sistemas de monitoreo y gestión MDM, que se encarguen de validar la presencia de aplicaciones permitidas y rechazadas, habilitar el borrado seguro de información, denegación de medios adicionales de almacenamiento de información, denegación de descarga de archivos, denegación de envío de correos con archivos adjuntos, ubicación geográfica de un dispositivo, responsabilidad de las partes en caso de pérdida o deterioro de la vida útil de los dispositivos móviles, directrices de renovación y actualización del sistema operativo ANDROID y parches de seguridad en los dispositivos móviles, que en estos momentos Google, está publicando mensualmente para corregir los problemas detectados.

Aceptación de acuerdos de confidencialidad de la información que se maneje a través de los dispositivos móviles, así como también sobre la información sensible de la organización, que puede ser almacenada o no, en los dispositivos, gestión remota (eliminación) de la información almacenada en los dispositivos móviles en caso de pérdida, robo y cese de actividades del empleado, o en caso de que la organización detecte que el usuario desacata las medidas y políticas de seguridad de la información, la revocación del permiso de uso de los dispositivos.

Aceptación firmada por parte de los usuarios, del uso de agentes y sistemas de monitoreo presentes en sus dispositivos, y la obligatoriedad de acceso a plataformas de autoservicio de aplicaciones, que se encarguen de instalar, desinstalar y verificar las aplicaciones que se encuentran instaladas en los dispositivos, acorde a la(s) política(s) de seguridad establecidas por la organización, con la finalidad de proteger la seguridad de la información y garantizar que no se violarán las leyes de derechos de autor en cuanto a aplicaciones y demás, así como también garantizar que los dispositivos contarán con aplicaciones previamente testeadas por sistemas de seguridad, que garanticen que se encuentran libres de virus.

3. Objetivos y Metodología de Trabajo

En la actualidad las personas a nivel mundial se encuentran viviendo en una nueva sociedad de la información, en la cual la mayoría de personas que poseen un dispositivo inteligente, llámese Tablet o Smartphone, se encuentran conectados a la red por lo general 24 horas al día, por medio de las conexiones de datos de los planes de telefonía móvil y de los puntos de acceso Wi-Fi en los diferentes lugares en los que se tenga acceso, pero la tendencia de los usuarios es mantener una conexión permanente a internet, tanto para aspectos personales como laborales.

Esta nueva forma de vida dependiente de la tecnología, el internet, los dispositivos móviles y las aplicaciones, se ha vuelto indispensable para los usuarios en la vida cotidiana a nivel mundial, como por ejemplo ver el tráfico para regresar del trabajo a la casa, buscar un determinado restaurante, consultar un menú, verificar precios, hacer compras y reservas en un hotel, realizar teleconferencias de trabajo mientras conduce hacia la oficina, responder un correo electrónico desde un autobús, en fin, múltiples actividades tanto laborales como personales que se realizan hoy en día de forma inmediata, por medio de los dispositivos móviles y de una conexión a internet, lo cual mejora la oportunidad de reacción y respuesta de las personas y sus actividades.

Ilustración 20. Usos de los dispositivos móviles

Fuente: https://www.marketingdirecto.com/digital-general/digital/como-nos-relacionamos-con-los-dispositivos-moviles-los-datos-de-esta-encuesta-conseguiran-llamar-su-atencion

La actual tendencia de vida en la era digital, en la cual se marca una delgada línea en la que es muy difícil diferenciar de las 24 horas del día, de los 7 días de la semana, y de los 365 días del año, cuándo es tiempo personal, familiar, de esparcimiento o cuándo es tiempo laboral, puesto que por medio del uso de la tecnología y de la permanente conexión a internet y uso de las aplicaciones apropiadas, se pueden realizar múltiples actividades y cumplir con todos los compromisos tanto personales como laborales, surge BYOD, como una solución en la cual las personas en general, ya no necesitan utilizar y transportar a diario varios dispositivos tanto personales como empresariales (Agenda, Computador Portátil, Tablet, Smartphone, Ipad, etc.) para poder realizar sus actividades cotidianas, ni desperdiciar tiempo en la personalización de estos diferentes tipos de dispositivos, y sincronizarlos con otros sistemas, para mantenerlos actualizados, ni gastar tiempo en desplazamientos innecesarios para realizar actividades bancarias, compras, o simplemente realizar pagos de tarjetas, servicios públicos y otras actividades que se realizan diariamente.

Por lo expresado, y adicional a otras razones como poder emplear dispositivos de última generación, los cuales no siempre pueden ser puestos a disposición de los usuarios por parte de sus empleadores, por los altos costos que conlleva la renovación de un parque tecnológico, entre otras, la incapacidad de las empresas de poder satisfacer las expectativas tecnológicas de cada empleado, estos factores y la constante solicitud por parte de los empleados de que puedan usar sus dispositivos móviles en sus actividades laborales, han puesto a una cantidad importante de empresas a nivel mundial a cambiar los modelos tradicionales de demanda y oferta de servicios de TI, para adaptarse a la nueva era, en la cual deben cambiar sus infraestructuras y sistemas, para que los usuarios puedan utilizar sus propios dispositivos móviles para prestar sus servicios profesionales a las empresas.

Cabe resaltar que el ahorro económico es un beneficio directo para las empresas al momento de implementar BYOD, dado que no tendrían que adquirir grandes parques tecnológicos y dispositivos para sus empleados, ni costear los servicios de administración, mantenimiento y soporte, pero este ahorro económico no es del todo cierto, puesto que las empresas y los encargados de las áreas de sistemas para implementar BYOD, deben hacer inversión económica en dispositivos de conectividad, seguridad, almacenamiento, alta disponibilidad, servidores de aplicaciones, servidores de autenticación, soportar alta concurrencia de dispositivos, gestión de dispositivos móviles específicos para los dispositivos permitidos (ANDROID, IOS, otros) etc., para adaptar las infraestructuras a BYOD.

Las inversiones no sólo son de tipo económico, también requieren el apoyo y el impulso por parte de la alta dirección, de los líderes de los procesos, de los dolientes de los mismos, de los jefes de cada área y demás involucrados tanto de forma interna como externa en las organizaciones, para lograr la alineación estratégica de los sistemas y servicios BYOD, con Gobierno y la misión de cada organización, pudiendo de esta manera establecer y divulgar políticas, directrices, condiciones de uso, entre otros cambios que se deben definir y aplicar.

Es aquí en donde el presente trabajo de fin de máster, a grosso modo ha empezado a dar aportes claros y concisos en este apartado de “Estado del Arte, y esbozado un análisis de riesgos generales” a los que se enfrenta cualquier organización y los usuarios que pretendan formar parte de la implementación de un proyecto de BYOD.

El presente documento también incluirá como aporte una guía básica de implementación de BYOD, acompañado de una serie de salvaguardas que el autor del presente TFM recomienda a título personal, para que sean analizadas y aplicadas en cualquier tipo de organización, las cuales serán tomadas de la norma ISO/IEC 27001:2013 que servirán como plataforma de controles, adaptable a cualquier organización que se encuentre en proceso de implementación de BYOD, con lo cual logrará la estandarización de este proceso que es una de las ventajas de aplicar este tipo de norma; cabe aclarar que esto también depende del grado de madurez de los procesos, procedimientos, responsables y de la tecnología implementada en cada organización, así como del apoyo que logre conseguir el área de TI por parte de la alta dirección, esto podrá ser utilizado como punto de partida, para certificar el proceso de BYOD bajo la norma ISO/IEC 27001 y se dará por terminada la aportación del presente TFM con la elaboración de una política de seguridad mínima para el ambiente BYOD.

3.1. Objetivo General

Proponer un modelo de implementación de BYOD para organizaciones de cualquier tamaño y sector de negocio, basado en un análisis general de riesgos de seguridad de la información en dispositivos móviles de tipo ANDROID, en el cual se identificarán los puntos clave a tener en cuenta, que permitirán tener una claridad de los riesgos que este tipo de dispositivos móviles aporta a una organización, y con este insumo inducir a los lectores del documento, a

planear la mitigación de forma preventiva, de los posibles incidentes de seguridad, vulnerabilidades, malware, pérdida, secuestro y robo de información de los dispositivos móviles, que podría materializarse en una organización que implemente BYOD, como ambiente de trabajo para dispositivos móviles con sistema operativo ANDROID.

3.2. Objetivos Específicos

- Investigar sobre el estado del arte de BYOD a nivel general.
- Identificar los principales riesgos de seguridad a los que se enfrentan los dispositivos móviles ANDROID, las organizaciones y sus usuarios.
- Proponer controles o salvaguardas de seguridad para la implementación de ambientes BYOD los cuales serán basados en la norma ISO/IEC 27001:2013.
- Proponer una política de seguridad de la información para BYOD, con la finalidad de incorporación de dispositivos móviles con sistema operativo ANDROID, en las redes empresariales.
- Identificar de forma general Ventajas y desventajas del uso de BYOD en una organización.
- Identificar los principales fabricantes de herramientas para gestión de Dispositivos móviles (MDM) del año 2017, y un comparativo de sus características.

3.3. Metodología del Trabajo de TFM

La metodología aplicada en el presente Trabajo de Fin de Máster, es de tipo ***investigativo y deductivo,*** cuya finalidad es la obtención e identificación de aspectos específicos acerca de los riesgos de seguridad, asociados al uso de dispositivos móviles ANDROID y los problemas de seguridad que se pueden generar en ambientes BYOD para la gestión de los dispositivos, el resultado de la investigación se encuentra plasmado en el presente documento por medio de la aplicación de la metodología deductiva. Se producirá como aporte una propuesta metodológica de análisis, para la implementación de ambientes BYOD de forma "segura", aclarando en este punto que ningún sistema es 100% seguro e invulnerable. *El presente TFM está basado en la investigación del tema y la aportación intelectual y profesional del autor,* incluyendo en la contribución, sugerencias de controles o salvaguardas, basados en la norma ISO/IEC 27001:2013, que pueden ser aplicadas, modificadas, ampliadas o certificadas por cualquier organización, dependiendo del alcance esperado de su implementación de BYOD, se incluye una propuesta de política de seguridad que sirva de punto de partida según el nivel de proyección, de crecimiento y madurez que se pretenda de los proyectos BYOD.

Ilustración 21 Diagrama de desarrollo de la metodología propuesta
Fuente: Elaboración Propia

4. Implementación de BYOD

Permitir en una organización el uso de dispositivos móviles para la realización de cualquier tipo de actividad laboral, (BYOD), supone un riesgo inminente para la seguridad de la información de la organización, así como también para los sistemas de información, para la red corporativa, estaciones de trabajo, servicios que sean publicados y puestos al servicio de los empleados, etc.

Teniendo claro lo anterior y siendo conscientes de la importancia de la seguridad, se evidencia la necesidad de realizar el proceso de implementación de BYOD, siguiendo unos procedimientos adecuados que parten de un análisis de riesgos generales, para cualquier organización, asociados al uso de dispositivos móviles en sus ambientes corporativos, los cuales deben contemplar por lo menos estos 3 aspectos fundamentales:

1. Gobierno
2. Gestión de dispositivos
3. Seguridad (Física - Lógica)

Luego de que los responsables de identificar y gestionar los riesgos propios de la organización, y de tener clara la misión de la empresa, se deben alinear estos factores y dar inicio a la planeación de BYOD, que parte de identificar y definir al interior de la empresa quiénes tendrán acceso a BYOD, qué dispositivos se van a permitir (definición de especificaciones), qué espera la empresa cómo beneficio, qué información será accesible, qué información será sólo de consulta, definir si permite, o deniega la descarga de información, qué servicios se brindarán (correo, chat, video conferencia, acceso a bases de datos, acceso a aplicativos, descarga de archivos, servicios en la nube, otros), se deben definir los roles y niveles de acceso de los usuarios, con estos y otros insumos como base, se define qué se requiere tecnológicamente, para poder cumplir con los objetivos de negocio y de BYOD, se deben definir quién(es) serán los responsables por cada área, definir muy claramente las directrices y políticas que se deben aplicar y realizar seguimiento periódico, definir salvaguardas o controles que respalden la viabilidad y la seguridad de la información en BYOD, entre otras actividades que irán apareciendo según el alcance, la experiencia y nivel de madurez de cada organización.

Como parte integral del presente documento de TFM y dada la metodología deductiva empleada, se incluye la realización y presentación de un Análisis de Riesgos General y no en profundidad, puesto que esto es labor propia de cada organización. De acuerdo a esto se plasma la recopilación y presentación de los **Riesgos,** a los que se enfrentan no sólo los dispositivos móviles de tipo ANDROID, sino los usuarios, las organizaciones, sus sistemas y redes corporativas, luego, se plasmará la propuesta de los controles aplicables a proyectos de implementación de BYOD, los cuales estarán basados en la norma ISO/IEC 27001:2013, para lo cual se realizará la revisión general de la norma, los objetivos y dominios, para definir los controles pertinentes, aplicables y oportunos para implementaciones de BYOD de forma segura en una organización.

4.1 Propuesta Plan de Trabajo para la Implementación de BYOD

La presente propuesta de plan de trabajo, deberá ser desarrollada y gestionada por el área de Tecnología de la organización, cuyo resultado se presentará a las partes interesadas y a la Alta Dirección, para que validen el plan de trabajo y pueda ser comunicado y socializado con las partes interesadas dentro y fuera de la organización, para sus respectivas observaciones, aportes, modificaciones, aceptación y/o aprobación.

Plan de Trabajo

A) Identificación del estado actual de la infraestructura (Dispositivos de comunicaciones, Servidores, Dispositivos de seguridad, Antivirus, Servicios en la Nube, etc.).
B) Verificación de las especificaciones y configuración de los dispositivos de seguridad y comunicaciones, validar factibilidad de crecimiento.
C) Verificar la documentación de Incidentes y Evaluación de seguridad física y lógica.
D) Verificar la documentación de Seguridad, Acuerdos de Nivel de Servicio, Acuerdos de confidencialidad, e Incidentes en los procesos de desarrollo de software y aplicativos internos y/o externos de la organización.

E) Identificación y definición de los aplicativos y servicios que se van a ofertar a los usuarios en BYOD. Identificar y definir los responsables de aprobar el acceso de los usuarios.
F) Verificación del Análisis de vulnerabilidades actuales de los aplicativos y servicios de la organización, retroalimentación con los nuevos riesgos que pueden surgir por BYOD.
G) Revisión y ajustes del plan de contingencia o continuidad de negocio (BCP).
H) Revisión y ajustes del plan de recuperación de desastres y operación en centro de datos alterno.
I) Verificación, Análisis y Observaciones o actualización de los manuales de procesos y procedimientos con la incorporación de BYOD.
J) Elaboración de informe de hallazgos, plan de mitigación y formulación de propuesta de transición de la actual Infraestructura, a BYOD, el cual incluirá los cambios que se requieren realizar, el impacto, observaciones y recomendaciones, así como las adquisiciones e implementaciones tecnológicas, que soporten BYOD, bajo las directrices definidas, que como mínimo incluirán la adquisición de herramientas de Administración de Dispositivos Móviles – MDM/EMM.
K) Definición de la política de seguridad que se va aplicar a BYOD y la integración de la misma a las demás políticas de seguridad vigentes de la organización.
L) Retroalimentación del informe con las partes interesadas, para definir modificación, eliminación o adición de directrices y políticas, o demás fines inherentes.
M) Presentación del informe final a la Alta Dirección de la organización, el cual incluye previa retroalimentación de todos los actores involucrados, para que la Alta Dirección pueda tomar las decisiones respectivas.
N) Retroalimentación con el equipo de Gestión Tecnológica, en el cual se definirán roles y responsabilidades, cronograma de actividades, tiempos de ejecución y posiblemente la necesidad de incorporación de personal adicional, así como las demás tareas que se estimen convenientes para el cumplimiento de los objetivos de la organización.
O) Inicio del plan de trabajo de implementación de BYOD, aprobado por la alta dirección, acorde a los lineamientos y objetivos de negocio de la organización.

4.2 Propuesta Evaluación de Riesgos

ÍTEM	Riesgo	Objetivos de Control	Controles	Prueba de Cumplimiento	Prueba Sustantiva
R1 Gobierno	Identificación del contexto Interno y Externo de la Organización respecto a BYOD.	Proteger a la organización contra la materialización de incumplimientos de tipo legal, jurídico y normativo. Proteger a la organización contra la materialización de ataques de código malicioso desde los dispositivos móviles.	Procedimiento de verificación de leyes nacionales, internacionales e internas de la organización, que debe aplicar. Procedimiento de estudio de amenazas, asociadas a los dispositivos móviles.	Existe procedimiento? Verificar la documentación existente, de la normatividad vigente aplicada a BYOD. Verificar la documentación de las amenazas asociadas a los dispositivos móviles y al sistema operativo ANDROID.	Validar la gama de versiones de ANDROID que se conectan a la red, para identificar vulnerabilidades.

R2 Gobierno	Divulgación de las directrices de la organización.	Proteger a la organización de la materialización de riesgos de seguridad por desconocimiento de las medidas de seguridad, por parte de los empleados y usuarios.	Procedimiento de verificación de campañas de sensibilización y de divulgación oportuna de directrices, campañas de sensibilización e información relevante.	Existe procedimiento? Verificar la documentación que la organización ha elaborado, actualizado y divulgado respecto al uso de los dispositivos móviles y de BYOD.	Verificar la existencia de documentación, versiones, actualización y disponibilidad de la información de uso de los dispositivos móviles y de BYOD.
R3 Gobierno	Definir el alcance, restricciones y revocatoria respecto al uso de BYOD.	Proteger los sistemas de información y en general la infraestructura de la organización del robo, modificación, pérdida y/o secuestro de información.	Procedimiento de verificación de documentación de usuarios con acceso por BYOD, dispositivos, permisos y procesos de autorización y denegación de acceso a servicios.	Existe procedimiento? Verificar la documentación que la organización ha elaborado, divulgado y publicado respecto al alcance, restricciones y revocatoria de acceso a BYOD.	Verificar la documentación de usuarios con permiso de acceso, dispositivos móviles activos, usuarios dados de baja y motivo de la baja. Verificación aleatoria de acuerdos de uso firmados.

R4 Gestión de Dispositivos	Consentimiento informado de la Privacidad de la Información de los Dispositivos Móviles, firmado por los empleados y usuarios.	Proteger la seguridad y privacidad de la información empresarial y personal de los dispositivos móviles.	Procedimiento de verificación de existencia, aceptación y firma de los consentimientos informados, en los cuales se permita el monitoreo de los dispositivos móviles y acciones de respaldo y/o eliminación de información.	Existe procedimiento? Verificar la existencia y funcionalidad de procesos y procedimientos de monitoreo, respaldo y/o eliminación de información de los dispositivos móviles.	Ampliar toma de muestra y revisar de forma aleatoria algunos consentimientos informados y verificar aceptación y firma. Verificar la existencia de los procesos y procedimientos de monitoreo.
R5 Gestión de Dispositivos	Verificación de listas blancas de dispositivos permitidos que acceden a la red. Verificación de listas negras de dispositivos rechazados que	Garantizar la disponibilidad de acceso de los dispositivos permitidos. Proteger la red empresarial de	Procedimiento de verificación de control de acceso de dispositivos y usuarios. Procedimiento de monitoreo de actividades de los dispositivos y verificación de listas	Existe procedimiento? Verificar la existencia de herramientas de monitoreo de acceso de dispositivos a la red. Verificar la existencia de herramientas de monitoreo de registro de	Verificación de la documentación de los procesos de autorización y aprobación de acceso de usuarios y dispositivos a BYOD

	no deberían acceder a la red	accesos no autorizados.	blancas y negras de dispositivos.	actividad de los dispositivos.	
R6 Gestión de Dispositivos	Políticas de seguridad y de uso de BYOD	Proteger la información, los sistemas de información de la organización y los dispositivos móviles e información de los usuarios de BYOD.	Procedimiento de verificación de existencia, aplicabilidad, actualización concientización y divulgación de las políticas de BYOD.	Existe procedimiento? Verificar la existencia y aplicación de políticas para el acceso de usuarios y dispositivos al proyecto de BYOD.	Ampliar la muestra, seguir y aplicar la(s) política(s) en una muestra aleatoria de dispositivos móviles de prueba y validar el cumplimiento de las políticas, desde ambientes tanto interno como externo.
R7 Gestión de Dispositivos	Software ilegal, riesgo de seguridad de la información.	Proteger la organización del uso de software o aplicaciones ilegales, posibles violaciones de seguridad y violación de derechos de autor, así como	Validar la gestión del software por medio de herramientas automatizadas de gestión, instalación y desinstalación de software, en los dispositivos permitidos.	Existe procedimiento? Verificar la existencia de los procedimientos de administración y gestión de dichas plataformas para el monitoreo y reporte de aplicaciones	Ampliar la muestra, solicitar reporte de dispositivos que han reportado instalación de software no autorizado en los últimos 60 días, verificación de

		también de la instalación y uso de aplicaciones de terceros que no han sido comprobadas y autorizadas por la organización. Proteger los dispositivos de instalación de código malicioso.	Validar la existencia de lineamientos de prohibición de instalación y uso de aplicaciones no avaladas por la organización.	permitidas y no permitidas. Verificar reportes de aplicaciones detectadas en los dispositivos.	acciones tomadas y/o revocatoria de uso.
R8 Red	Fallo en las comunicaciones.	Mantener la conectividad de los dispositivos entre ellos y hacia los aplicativos y servicios.	Procedimiento de implementación de dispositivos de conectividad redundantes.	Existe procedimiento? Verificar que se cuenta con un plan de contingencia de conectividad LAN – WAN, ISP, otros.	Ampliar muestra y comprobar el porcentaje de disponibilidad de las plataformas de comunicaciones.

				Verificar la documentación y pruebas del procedimiento de alta disponibilidad de comunicaciones.	
R9 Red Antivirus.	Propagación de Virus por la Red. Instalación de código malicioso que tenga privilegios de robo de información.	Proteger la plataforma tecnológica de la organización de propagaciones de virus por medio de la red.	Procedimiento de gestión y administración de herramientas Antivirus y políticas.	Verificar las estadísticas o reportes de los últimos 60 días en cuanto a infección y desinfección. Verificar que las actualizaciones de la consola Antivirus no sean superiores a 30 días.	Ampliar la muestra, verificar que se estén aplicando las actualizaciones de seguridad en los equipos cliente como mínimo.
R10 Seguridad	Acceso de usuarios no autorizados a BYOD.	Prevenir el ingreso de usuarios no autorizados a la plataforma BYOD.	Procedimiento de monitoreo, revisión de control de acceso y actividades.	Existe procedimiento? Verificar que existe una política de control y denegación de acceso.	Ampliar muestra y comprobar que se tiene documentación física, digital o en

	Cambios no autorizados o sin adecuado seguimiento.	Validar las actividades que realizan los usuarios y dispositivos móviles en BYOD.	Procedimiento de verificación de cambios realizados. Procedimiento de aprobación o denegación de acceso a BYOD.	Comprobar que se lleva un registro detallado de control de cambios. Comprobar que se lleva un registro de accesos y actividades sobre los servicios BYOD.	sistemas de información de los seguimientos realizados los últimos 6 meses. Verificar si existen informes de incidentes y acciones tomadas.
R11 Contingencia	Desastre Natural, asonada, terrorismo.	Plan de contingencia en caso de desastres naturales, asonadas, terrorismo.	Procedimiento de recuperación en caso de desastres naturales, asonadas, terrorismo.	Existe procedimiento? Verificar que exista un proceso y procedimientos de recuperación.	
R12 Seguridad Lógica	Obsolescencia de actualizaciones y parches de seguridad del sistema	Actualización y parches de seguridad del sistema operativo ANDROID y	Procedimiento de verificación de actualización y parches de seguridad del sistema operativo ANDROID y	Existe procedimiento? Verificar las evidencias de actualizaciones y parchado de seguridad.	Ampliar muestra, revisar el listado de fabricantes de dispositivos admitidos en la organización, que cumplen con el

	operativo ANDROID y aplicaciones de los dispositivos móviles.	aplicaciones de los dispositivos móviles.	aplicaciones de los dispositivos móviles.	Verificar que los modelos de dispositivos que se admiten puedan contar con actualizaciones por parte del fabricante (Samsung, Sony, Huawei, HTC, LG, Motorola, otros)	envío de actualizaciones para los dispositivos.
R13 Seguridad Lógica	Fallas de los controles de autenticación.	Evitar la suplantación de usuarios y accesos no autorizados.	Procedimiento de autenticación de usuarios, control de acceso a los sistemas de información y conectividad, autenticación en 2 vías.	Existe procedimiento? Verificar la documentación de cuentas de usuario, permisos de acceso y métodos de autenticación.	Ampliar muestra, revisar el proceso de creación de usuarios y permisos, verificar responsables de aprobación de uso de BYOD.
R14 Seguridad Lógica	Vulnerabilidades asociadas a cada versión de ANDROID.	Mantener la confidencialidad disponibilidad e integridad de la	Procedimiento de verificación y pruebas de seguridad en los dispositivos móviles.	Existe procedimiento? Verificar la documentación relacionada con	Ampliar muestra, Verificar si existen incidentes de seguridad

		información en los dispositivos móviles.		incidentes de seguridad de los dispositivos móviles.	documentados y de las acciones ejecutadas.
R15 Seguridad Lógica	Conexión de los dispositivos móviles a redes inseguras (redes públicas). Ataques de Man in the Middle.	Proporcionar adecuados niveles de seguridad mediante el cifrado de comunicaciones y certificados que garanticen la autenticación.	Procedimiento de control de acceso de los dispositivos móviles por medio de (VPN, Certificados, Cifrado, etc.) a BYOD. Campañas de sensibilización de los peligros de la conexión a redes públicas.	Existe procedimiento? Verificar la documentación de las herramientas de seguridad de los dispositivos móviles. Verificar la documentación, temas y periodicidad de las campañas de sensibilización de seguridad informática.	
R16 Seguridad Física	Préstamo de los dispositivos móviles.	Proporcionar a los usuarios adecuada información sobre los peligros de facilitar sus	Procedimiento de publicación y divulgación de	Existe procedimiento? Verificar la documentación, temas y periodicidad de las campañas de	

		dispositivos móviles a otras personas.	campañas de sensibilización. Procedimiento de Cifrado de la información en los dispositivos móviles.	sensibilización de seguridad informática. Verificar las directrices de la organización acerca del cifrado de la información en los dispositivos móviles.	

Tabla 1. PROPUESTA EVALUACIÓN DE RIESGOS – Fuente: Elaboración Propia

4.3. Propuesta de Controles ISO/IEC 27001:2013

ISO/IEC 27001:2013, es un estándar internacional aceptado para la gestión de la seguridad de la información, el cual puede ser aplicado a todo tipo de empresas, sin importar el tamaño o el sector de negocio.

La aplicación de esta norma en una organización, aporta sustancialmente en la forma como se Establece, Implementa, Opera, Monitorea, Revisa, Mantiene y Mejora la seguridad de la información.

La forma de trabajo que se emplea para aplicar adecuadamente la norma y sacar las mejores ventajas en el desarrollo y mantenimiento de la seguridad de la información, está basada en la metodología PDCA (Plan, Do, Check, Act) o la misma PHVA (Planear, Hacer, Verificar y Actuar), o también conocido como el "Ciclo de Deming".

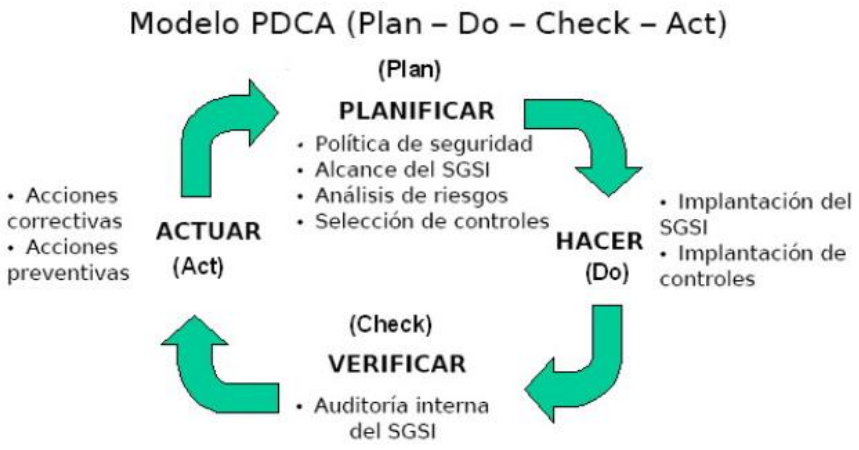

Ilustración 22 Modelo PDCA/PHVA

Fuente: www.s21sec.com – La seguridad digital del futuro, hoy

4.3.1 Contexto de la Organización

Antes de dar inicio a la implementación de la norma como tal es muy importante que la organización defina 2 puntos cruciales de su contexto:

1. Partes Interesadas en la seguridad de la información, las cuales pueden ser tanto internas como externas a la organización.

2. Los requerimientos de las partes interesadas, con respecto a la seguridad de la información.

4.3.2 Visión General de la Norma ISO/IEC 27001:2013

Ilustración 23 Visión General de la ISO/IEC 27001:2013

Fuente: Elaboración Propia

Anexo A – Dominios ISO/IEC 27001:2013

Ilustración 24 Anexo A – Dominios ISO/IEC 27001:2013

Fuente: Elaboración Propia

4.3.3 Dominios, Objetivos de Control y Controles

Dominio A.5 POLÍTICA DE LA SEGURIDAD DE LA INFORMACIÓN

5.1 Orientación de la Dirección para la Gestión de la Seguridad de la Información

Objetivo: Brindar orientación y soporte, por parte de la dirección, de acuerdo con los requisitos del negocio y con las leyes y reglamentos pertinentes.

Actividades de control del riesgo

5.1.1 Políticas para la seguridad de la información: Se debería definir un conjunto de políticas para la seguridad de la información, aprobado por la dirección, publicado y comunicado a los empleados, así como a todas las partes externas relevantes.

5.1.2 Revisión de las políticas para la seguridad de la información: Las políticas para la seguridad de la información se deberían planificar y revisar con regularidad o si ocurren cambios significativos para garantizar su idoneidad, adecuación y efectividad

Dominio A.6 ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

6.1 Organización interna

Objetivo: Establecer un marco de referencia de gestión para iniciar y controlar la implementación y operación del SGSI.

Actividades de control del riesgo

6.1.1 Asignación de responsabilidades para la Seguridad de la Información: Se deberían definir y asignar claramente todas las responsabilidades para la seguridad de la información.

6.1.2 Segregación de tareas: Se deberían segregar tareas y las áreas de responsabilidad ante posibles conflictos de interés con el fin de reducir las oportunidades de una modificación no autorizada o no intencionada, o el de un mal uso de los activos de la organización.

6.1.3 Contacto con las autoridades: Se deberían mantener los contactos apropiados con las autoridades pertinentes.

6.1.4 Contacto con grupos de interés especial: Se debería mantener el contacto con grupos o foros de seguridad especializados y asociaciones profesionales.

6.1.5 Seguridad de la información en la gestión de proyectos: Se debería contemplar la seguridad de la información en la gestión de proyectos e independientemente del tipo de proyecto a desarrollar por la organización.

6.2 Dispositivos móviles y teletrabajo

Objetivo: Garantizar la seguridad del teletrabajo y el uso de dispositivos móviles.

Actividades de control del riesgo

6.2.1 Política de uso de dispositivos para movilidad: Se debería establecer una política formal y se deberían adoptar las medidas de seguridad adecuadas para la protección contra los riesgos derivados del uso de los recursos de informática móvil y las telecomunicaciones.

6.2.2 Teletrabajo: Se debería desarrollar e implantar una política y medidas de seguridad de apoyo, para proteger a la información accedida, procesada o almacenada en ubicaciones destinadas al teletrabajo.

Dominio A.7 SEGURIDAD DE LOS RECURSOS HUMANOS

7.1 Antes de asumir el empleo.

Objetivo: Asegurar que los empleados y contratistas comprenden sus responsabilidades y son idóneos en los roles para los que se consideran.

Actividades de control del riesgo

7.1.1 Investigación de antecedentes: Se deberían realizar revisiones de verificación de antecedentes de los candidatos al empleo, en concordancia con las regulaciones, ética y leyes relevantes y deben ser proporcionales a los requerimientos del negocio, la clasificación de la información a la cual se va a tener acceso y los riesgos percibidos.

7.1.2 Términos y condiciones de contratación: Como parte de su obligación contractual, empleados, contratistas y terceros deberían aceptar y firmar los términos y condiciones del contrato de empleo, el cual establecerá sus obligaciones y las obligaciones de la organización para la seguridad de información.

7.2 Durante la ejecución del empleo

Objetivo: El objetivo es el de asegurarse de que los empleados y contratistas están en conocimiento y cumplen con sus responsabilidades en seguridad de la información.

Actividades de control del riego

7.2.1 Responsabilidades de la Dirección: La Dirección debería requerir a empleados, contratistas y usuarios de terceras partes aplicar la seguridad en concordancia con las políticas y los procedimientos.

7.2.2 Toma de conciencia, educación y formación de la Seguridad de la Información: Todos los empleados de la organización y donde sea relevante, contratistas y usuarios de terceros deberían recibir entrenamiento apropiado del conocimiento y actualizaciones regulares en políticas y procedimientos organizacionales como sean relevantes para la función de su trabajo.

7.2.3 Proceso disciplinario: Debería existir un proceso formal disciplinario comunicado a empleados que produzcan brechas en la seguridad

7.3 Terminación y cambio de empleo

Objetivo: Proteger los intereses de la organización como parte del proceso de cambio o terminación del empleo.

Actividades de control del riesgo

7.3.1 Terminación o cambio de responsabilidades de empleo: Las responsabilidades para ejecutar la finalización de un empleo o el cambio de éste deberían estar claramente definidas, comunicadas a empleado o contratista y asignadas efectivamente.

Dominio A.8 GESTIÓN DE ACTIVOS

8.1 Responsabilidad por los activos

Objetivo: Identificar los activos organizacionales y definir las responsabilidades de protección apropiada.

Actividades de control del riesgo

8.1.1 Inventario de activos: Todos los activos deberían estar claramente identificados, confeccionando y manteniendo un inventario con los más importantes.

8.1.2 Propiedad de los activos: Toda la información y activos del inventario asociados a los recursos para el tratamiento de la información deberían pertenecer a una parte designada de la Organización.

8.1.3 Uso aceptable de los activos: Se deberían identificar, documentar e implantar regulaciones para el uso adecuado de la información y los activos asociados a recursos de tratamiento de la información.

8.1.4 Devolución de activos: Todos los empleados y usuarios de terceras partes deberían devolver todos los activos de la organización que estén en su posesión/responsabilidad una vez finalizado el acuerdo, contrato de prestación de servicios o actividades relacionadas con su contrato de empleo.

8.2 Clasificación de la información

Objetivo: Asegurar que la organización recibe un nivel apropiado de protección de acuerdo con su importancia para la organización.

Actividades de control del riego

8.2.1 Clasificación de la Información: La información debería clasificarse en relación a su valor, requisitos legales, sensibilidad y criticidad para la Organización.

8.2.2 Etiquetado de la información: Se debería desarrollar e implantar un conjunto apropiado de procedimientos para el etiquetado y tratamiento de la información, de acuerdo con el esquema de clasificación adoptado por la organización.

8.2.3 Manipulación de activos: Se deberían desarrollar e implantar procedimientos para la manipulación de los activos acordes con el esquema de clasificación de la información adoptado por la organización.

8.3 Manejo de medios de soporte

Objetivo: Prevenir la divulgación, la modificación, el retiro o la destrucción de información almacenada en medios de soporte.

Actividades de control del riego

8.3.1 Gestión de medios de soporte extraíbles: Se deberían establecer procedimientos para la gestión de los medios informáticos removibles acordes con el esquema de clasificación adoptado por la organización.

8.3.2 Eliminación de soportes: Se deberían eliminar los medios de forma segura y sin riesgo cuando ya no sean requeridos, utilizando procedimientos formales.

8.3.3 Soportes físicos en tránsito: Se deberían proteger los medios que contienen información contra acceso no autorizado, mal uso o corrupción durante el transporte fuera de los límites físicos de la organización

Dominio A.9 CONTROL DE ACCESO

9.1 Requisitos de negocio para el control de acceso

Objetivo: Limitar el acceso a información y a instalaciones de procesamiento de información.

Actividades de control del riesgo

9.1.1 Política de control de acceso: Se debería establecer, documentar y revisar una política de control de accesos en base a las necesidades de seguridad y de negocio de la Organización.

9.1.2 Control de acceso a las redes y servicios asociados: Se debería proveer a los usuarios de los accesos a redes y los servicios de red para los que han sido expresamente autorizados a utilizar.

9.2 Gestión de acceso de usuarios

Objetivo: Asegurar el acceso de los usuarios autorizados e impedir el acceso no autorizado a sistemas y servicios.

Actividades de control del riesgo

9.2.1 Gestión de altas/bajas en el registro de usuarios: Debería existir un procedimiento formal de alta y baja de usuarios con objeto de habilitar la asignación de derechos de acceso.

9.2.2 Gestión de los derechos de acceso asignados a usuarios: Se debería implantar un proceso formal de aprovisionamiento de accesos a los usuarios para asignar o revocar derechos de acceso a todos los tipos de usuarios y para todos los sistemas y servicios.

9.2.3 Gestión de los derechos de acceso con privilegios especiales: La asignación y uso de derechos de acceso con privilegios especiales debería ser restringido y controlado.

9.2.4 Gestión de información confidencial de autenticación de usuarios: La asignación de información confidencial para la autenticación debería ser controlada mediante un proceso de gestión controlado.

9.2.5 Revisión de los derechos de acceso de los usuarios: Los propietarios de los activos deberían revisar con regularidad los derechos de acceso de los usuarios.

9.2.6 Retirada o adaptación de los derechos de acceso: Se deberían retirar los derechos de acceso para todos los empleados, contratistas o usuarios de terceros a la información y a las instalaciones de procesamiento de información a la finalización del empleo, contrato o acuerdo, o ser revisados en caso de cambio.

9.3 Responsabilidades del usuario

Objetivo: Hacer que los usuarios rindan cuentas por la custodia de su información de autenticación.

Actividades de control del riesgo

9.3.1 Uso de información confidencial para la autenticación: Se debería exigir a los usuarios el uso de buenas prácticas de seguridad de la organización en el uso de información confidencial para la autenticación

9.4 Control de acceso a sistemas y aplicaciones

Objetivo: Prevenir el uso no autorizado de sistemas y aplicaciones.

Actividades de control del riesgo

9.4.1 Restricción del acceso a la información: Se debería restringir el acceso de los usuarios y el personal de mantenimiento a la información y funciones de los sistemas de aplicaciones, en relación a la política de control de accesos definida.

9.4.2 Procedimientos seguros de inicio de sesión: Cuando sea requerido por la política de control de accesos se debería controlar el acceso a los sistemas y aplicaciones mediante un procedimiento seguro de log-on.

9.4.3 Gestión de contraseñas de usuario: Los sistemas de gestión de contraseñas deberían ser interactivos y asegurar contraseñas de calidad.

9.4.4 Uso de herramientas de administración de sistemas: El uso de utilidades software que podrían ser capaces de anular o evitar controles en aplicaciones y sistemas deberían estar restringidos y estrechamente controlados.

9.4.5 Control de acceso al código fuente de los programas: Se debería restringir el acceso al código fuente de las aplicaciones software.

Dominio A.10 CRIPTOGRAFÍA

10.1 Controles criptográficos

Objetivo: Asegurar el uso apropiado y eficaz de la criptografía para proteger la confiabilidad, la autenticidad y/o la integridad de la información.

Actividades de control del riesgo

10.1.1 Política de uso de los controles criptográficos: Se debería desarrollar e implementar una política que regule el uso de controles criptográficos para la protección de la información.

10.1.2 Gestión de claves: Se debería desarrollar e implementar una política sobre el uso, la protección y el ciclo de vida de las claves criptográficas a través de todo su ciclo de vida.

Dominio A.11 SEGURIDAD FÍSICA Y AMBIENTAL

11.1 Áreas seguras

Objetivo: Prevenir el acceso físico no autorizado, el daño y la interferencia a la información y a las instalaciones de procesamiento de información de la organización.

Actividades de control del riesgo

11.1.1 Perímetro de seguridad física: Se deberían definir y utilizar perímetros de seguridad para la protección de las áreas que contienen información y las instalaciones de procesamiento de información sensible o crítica.

11.1.2 Controles físicos de entrada: Las áreas seguras deberían estar protegidas mediante controles de entrada adecuados para garantizar que solo el personal autorizado dispone de permiso de acceso.

11.1.4 Protección contra las amenazas externas y ambientales: Se debería diseñar y aplicar una protección física contra desastres naturales, ataques maliciosos o accidentes.

11.2 Seguridad de los equipos

Objetivo Prevenir la pérdida, daño, robo o compromiso de activos, y la interrupción de las operaciones de la organización.

Actividades de control del riesgo

11.2.3 Seguridad del cableado: Los cables eléctricos y de telecomunicaciones que transportan datos o apoyan a los servicios de información se deberían proteger contra la interceptación, interferencia o posibles daños.

11.2.4 Mantenimiento de los equipos: Los equipos deberían mantenerse adecuadamente con el objeto de garantizar su disponibilidad e integridad continuas.

11.2.5 Salida de activos fuera de las dependencias de la empresa: Los equipos, la información o el software no se deberían retirar del sitio sin previa autorización.

11.2.6 Seguridad de los equipos y activos fuera de las instalaciones: Se debería aplicar la seguridad a los activos requeridos para actividades fuera de las dependencias de la organización y en consideración de los distintos riesgos.

11.2.8 Equipo informático de usuario desatendido: Los usuarios se deberían asegurar de que los equipos no supervisados cuentan con la protección adecuada.

Dominio A.12 SEGURIDAD DE LAS OPERACIONES

12.1 Responsabilidades y procedimientos de operación

Objetivo: Asegurar las operaciones correctas y seguras de las instalaciones de procesamiento de información.

Actividades de control del riesgo

12.1.1 Documentación de procedimientos de operación: Se deberían documentar los procedimientos operativos y dejar a disposición de todos los usuarios que los necesiten.

12.1.2 Gestión de cambios: Se deberían controlar los cambios que afectan a la seguridad de la información en la organización y procesos de negocio, las instalaciones y sistemas de procesamiento de información.

12.1.3 Gestión de capacidades: Se debería monitorear y ajustar el uso de los recursos junto a proyecciones necesarias de requisitos de capacidad en el futuro con el objetivo de garantizar el rendimiento adecuado en los sistemas.

12.1.4 Separación de entornos de desarrollo, prueba y producción: Los entornos de desarrollo, pruebas y operacionales deberían permanecer separados para reducir los riesgos de acceso o de cambios no autorizados en el entorno operacional.

12.2 Protección contra código malicioso

Objetivo: Asegurarse de que la información y las instalaciones de procesamiento de información estén protegidas contra códigos maliciosos.

Actividades de control del riesgo

12.2.1 Controles contra el código malicioso: Se deberían implementar controles para la detección, prevención y recuperación ante afectaciones de malware en combinación con la concientización adecuada de los usuarios.

12.3 Copias de seguridad

Objetivo: Alcanzar un grado de protección deseado contra la pérdida de datos.

Actividades de control del riesgo

12.3.1 Copias de seguridad de la información: Se deberían realizar pruebas regulares de las copias de la información, del software y de las imágenes del sistema en relación a una política de respaldo (Backup) convenida.

12.4 Registro de actividad y seguimiento

Objetivo: Registrar los eventos relacionados con la seguridad de la información y generar evidencias.

Actividades de control del riesgo

12.4.1 Registro y gestión de eventos de actividad: Se deberían producir, mantener y revisar periódicamente los registros relacionados con eventos de actividad del usuario, excepciones, fallas y eventos de seguridad de la información.

12.4.2 Protección de los registros de información: Se debería proteger contra posibles alteraciones y accesos no autorizados la información de los registros.

12.4.3 Registros de actividad del administrador y operador del sistema: Se deberían registrar las actividades del administrador y del operador del sistema y los registros asociados se deberían proteger y revisar de manera regular.

12.5 Control del software Operacional

Objetivo: Garantizar la integridad de los sistemas operacionales para la organización.

Actividades de control del riesgo

12.5.1 Instalación del software en sistemas en producción: Se deberían implementar procedimientos para controlar la instalación de software en sistemas operacionales.

12.6 Gestión de la vulnerabilidad técnica

Objetivo: Evitar o prevenir la explotación o aprovechamiento de vulnerabilidades técnicas.

Actividades de control del riesgo

12.6.1 Gestión de las vulnerabilidades técnicas: Se debería obtener información sobre las vulnerabilidades técnicas de los sistemas de información de manera oportuna para evaluar el grado de exposición de la organización y tomar las medidas necesarias para abordar los riesgos asociados.

12.6.2 Restricciones en la instalación de software: Se deberían establecer e implementar las reglas que rigen la instalación de software por parte de los usuarios.

Dominio A.13 SEGURIDAD EN LAS COMUNICACIONES

13.1 Gestión de la seguridad en las redes

Objetivo: Evitar el acceso físico no autorizado, los daños e interferencias a la información de la organización y las instalaciones de procesamiento de la información.

Actividades de control del riesgo

13.1.1 Controles de red: Se deberían administrar y controlar las redes para proteger la información en sistemas y aplicaciones.

13.1.2 Mecanismos de seguridad asociados a servicios en red: Se deberían identificar e incluir en los acuerdos de servicio (SLA) los mecanismos de seguridad, los niveles de servicio y los requisitos de administración de todos los servicios de red, independientemente de si estos servicios se entregan de manera interna o están externalizados.

13.1.3 Segregación de redes: Se deberían segregar las redes en función de los grupos de servicios, usuarios y sistemas de información.

13.2 Intercambio de información con partes externas

Objetivo: Mantener la seguridad de la información que transfiere una organización internamente o con entidades externas.

Actividades de control del riesgo

13.2.1 Políticas y procedimientos de intercambio de información: Deberían existir políticas, procedimientos y controles formales de transferencia para proteger la información que viaja a través del uso de todo tipo de instalaciones de comunicación.

13.2.2 Acuerdos de intercambio: Los acuerdos deberían abordar la transferencia segura de información comercial entre la organización y las partes externas.

13.2.3 Mensajería electrónica: Se debería proteger adecuadamente la información referida en la mensajería electrónica.

13.2.4 Acuerdos de confidencialidad y secreto: Se deberían identificar, revisar y documentar de manera regular los requisitos para los acuerdos de confidencialidad y "no divulgación" que reflejan las necesidades de la organización para la protección de información.

Dominio A.14 ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE LOS SISTEMAS DE INFORMACIÓN

14.1 Requisitos de seguridad de los sistemas de información

Objetivo: Garantizar que la seguridad de la información sea una parte integral de los sistemas de información durante todo el ciclo de vida. Esto incluye los requisitos para sistemas de información que prestan servicios sobre redes públicas.

Actividades de control del riesgo

14.1.1 Análisis y especificación de los requisitos de seguridad: Los requisitos relacionados con la seguridad de la información se deberían incluir en los requisitos para los nuevos sistemas o en las mejoras a los sistemas de información ya existentes.

14.1.2 Seguridad de las comunicaciones en servicios accesibles por redes públicas: La información de los servicios de aplicación que pasan a través de redes públicas se deberían proteger contra actividades fraudulentas, de disputa de contratos y/o de modificación no autorizada.

14.1.3 Protección de las transacciones por redes telemáticas: La información en transacciones de servicios de aplicación se debería proteger para evitar la transmisión y enrutamiento incorrecto y la alteración, divulgación y/o duplicación no autorizada de mensajes o su reproducción.

Dominio A.15 RELACIONES CON LOS PROVEEDORES

15.1 Seguridad de la información en las relaciones con los proveedores

Objetivo: Asegurar la protección de los activos de la organización que sean accesibles a los proveedores.

Actividades de control del riesgo

15.1.1 Política de seguridad de la información para suministradores: Se deberían acordar y documentar adecuadamente los requisitos de seguridad de la información requeridos por los activos de la organización con el objetivo de mitigar los riesgos asociados al acceso por parte de proveedores y terceras personas.

15.1.2 Tratamiento del riesgo dentro de acuerdos de suministradores: Se deberían establecer y acordar todos los requisitos de seguridad de la información pertinentes a cada proveedor que puede acceder, procesar, almacenar, comunicar o proporcionar componentes de infraestructura de TI que dan soporte a la información de la organización.

15.1.3 Cadena de suministro en tecnologías de la información y comunicaciones: Los acuerdos con los proveedores deberían incluir los requisitos para abordar los riesgos de seguridad de la información asociados con la cadena de suministro de los servicios y productos de tecnología de información y comunicaciones.

Dominio A.16 GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN

16.1 Gestión de incidentes de seguridad de la información y mejoras

Objetivo: Asegurar un enfoque coherente y eficaz para la gestión de incidentes de seguridad de la información, incluida la comunicación sobre eventos de seguridad y debilidad.

Actividades de control del riesgo

16.1.1 Responsabilidades y procedimientos: Se deberían establecer las responsabilidades y procedimientos de gestión para garantizar una respuesta rápida, eficaz y ordenada a los incidentes de seguridad de la información.

16.1.2 Notificación de los eventos de seguridad de la información: Los eventos de seguridad de la información se deberían informar lo antes posible utilizando los canales de administración adecuados.

16.1.3 Notificación de puntos débiles de la seguridad: Se debería requerir, anotar e informar sobre cualquier debilidad sospechosa en la seguridad de la información en los sistemas o servicios tanto a los empleados como a contratistas que utilizan los sistemas y servicios de información de la organización.

16.1.4 Valoración de eventos de seguridad de la información y toma de decisiones: Se deberían evaluar los eventos de seguridad de la información y decidir su clasificación como incidentes.
16.1.5 Respuesta a los incidentes de seguridad: Se debería responder ante los incidentes de seguridad de la información en atención a los procedimientos documentados.
16.1.6 Aprendizaje de los incidentes de seguridad de la información: Se debería utilizar el conocimiento obtenido del análisis y la resolución de incidentes de seguridad de la información para reducir la probabilidad y/o impacto de incidentes en el futuro.
16.1.7 Recopilación de evidencias: La organización debería definir y aplicar los procedimientos necesarios para la identificación, recopilación, adquisición y preservación de la información que puede servir de evidencia.

Dominio A.17 ASPECTOS DE LA SEGURIDAD DE LA INFORMACIÓN EN LA GESTIÓN DE LA CONTINUIDAD DE NEGOCIO

17.1 Continuidad de la seguridad de la información

Objetivo: La continuidad de seguridad de la información se debe incluir en los sistemas de gestión de la continuidad de negocio de la organización.

Actividades de control del riesgo

17.1.1 Planificación de la continuidad de la seguridad de la información: La organización debería determinar los requisitos para la seguridad de la información y su gestión durante situaciones adversas como en situaciones de crisis o de desastre.
17.1.2 Implantación de la continuidad de la seguridad de la información: La organización debería establecer, documentar, implementar y mantener los procesos, procedimientos y controles para garantizar el mantenimiento del nivel necesario de seguridad de la información durante situaciones adversas.
17.1.3 Verificación, revisión y evaluación de la continuidad de la seguridad de la información: La organización debería verificar regularmente los controles de continuidad de seguridad de la información establecidos e implementados para poder garantizar su validez y eficacia ante situaciones adversas.

17.2 Redundancia

Objetivo: Garantizar la disponibilidad de las instalaciones de procesamiento de información.

Actividades de control del riesgo

17.2.1 Disponibilidad de instalaciones para el procesamiento de la información: Se debería implementar la suficiente redundancia en las instalaciones de procesamiento de la información y en correspondencia con los requisitos de disponibilidad.

Dominio A.18 CUMPLIMIENTO

18.1 Cumplimiento de los requisitos legales y contractuales

Objetivo: Evitar violaciones de las obligaciones legales, estatutarias, de reglamentación o contractuales relacionadas con seguridad de la información y de cualquier requisito de seguridad.

Actividades de control del riesgo

18.1.1 Identificación de la legislación aplicable: Se deberían identificar, documentar y mantener al día de manera explícita para cada sistema de información y para la organización todos los requisitos estatutarios, normativos y contractuales legislativos junto al enfoque de la organización para cumplir con estos requisitos.

18.1.2 Derechos de propiedad intelectual (DPI): Se deberían implementar procedimientos adecuados para garantizar el cumplimiento con los requisitos legislativos, normativos y contractuales relacionados con los derechos de propiedad intelectual y utilizar productos software originales.

18.1.3 Protección de los registros de la organización: Los registros se deberían proteger contra pérdidas, destrucción, falsificación, accesos y publicación no autorizados de acuerdo con los requisitos legislativos, normativos, contractuales y comerciales.

18.1.4 Protección de datos y privacidad de la información personal: Se debería garantizar la privacidad y la protección de la información personal identificable según requiere la legislación y las normativas pertinentes aplicables que correspondan.

18.1.5 Regulación de los controles criptográficos: Se deberían utilizar controles de cifrado de la información en cumplimiento con todos los acuerdos, la legislación y las normativas pertinentes.

18.2 Revisiones de la seguridad de la información

Objetivo: El objetivo es garantizar que se implementa y opera la seguridad de la información de acuerdo a las políticas y procedimientos organizacionales.

Actividades de control del riesgo

18.2.1 Revisión independiente de la seguridad de la información: Se debería revisar el enfoque de la organización para la implementación (los objetivos de control, los controles, las políticas, los procesos y procedimientos para la seguridad de la información) y gestión de la seguridad de la información en base a revisiones independientes e intervalos planificados o cuando tengan lugar cambios significativos en la organización.

18.2.2 Cumplimiento de las políticas y normas de seguridad: Los gerentes deberían revisar regularmente el cumplimiento del procesamiento y los procedimientos de información dentro

de su área de responsabilidad respecto a las políticas, normas y cualquier otro tipo de requisito de seguridad correspondiente.

18.2.3 Comprobación del cumplimiento: Los sistemas de información se deberían revisar regularmente para verificar su cumplimiento con las políticas y normas de seguridad dispuestas por la información de la organización.

4.4. Propuesta Política de Seguridad para implementaciones de BYOD

EMPRESA (XXXX)

POLÍTICA DE USO DE DISPOSITIVOS MÓVILES ANDROID

EN AMBIENTES(BYOD)

Ciudad - País.

Fecha: dd/mm/aaaa

Tabla de Contenido

POLÍTICA DE USO DE DISPOSITIVOS MÓVILES ANDROID

EN AMBIENTES(BYOD)

Código: (***XXXX)***
Versión: ***1(X)***
Fecha: ***dd/mm/aaaa***

1. Introducción

El servicio de BYOD - Bring Your Own Device – “Trae tu Propio Dispositivo” es un servicio proporcionado por el Área de Tecnología de (***la empresa XXXXX***), con el objeto de proveer el acceso de los dispositivos móviles con sistema operativo ANDROID, a los sistemas de información y facilitar la realización de las funciones laborales de los empleados y/o contratistas de las distintas áreas de la empresa en los procesos Estratégicos, Misionales, de Apoyo y/o los que se requieran. Los Términos de Uso que se describen a continuación, constituyen el acuerdo entre la Empresa y los Usuarios del servicio de BYOD, por lo tanto, es responsabilidad de la empresa socializar y dar a conocer ésta política, y asimismo es responsabilidad del usuario leerla, aceptarla, firmarla y respetarla, de tal manera que conozca plenamente las condiciones de uso y de revocatoria del servicio.

2. Terminología usada

A) Se le denomina “Usuario” a cualquier persona que se encuentre autorizada por la empresa para acceder a los servicios de BYOD, y ello implica su adhesión plena e incondicional a las Políticas de Uso del mismo.

B) Se denomina “Administrador” al rol encargado de crear, eliminar, y/o gestionar los servicios de BYOD, que para los efectos de la presente política de uso es asumido por el Área de Tecnología y/o (XXXXXX).

C) Se denomina “Área” a cualquier dependencia y/o equipo de trabajo que pertenezca a los distintos departamentos constituidos dentro y fuera de la empresa, los cuales conforman los procesos Estratégicos, Misionales y de Apoyo de la organización, así como también otras líneas de apoyo que tengan acceso a los servicios BYOD de la organización.

D) ACCESO BYOD GENERAL: Acceso para los dispositivos móviles con sistema operativo ANDROID, para los usuarios en general: Auxiliares administrativos, comerciales, analistas de proyectos, analistas de mesa de servicios, otros, estas

cuentas contaran con acceso a los servicios básicos de la compañía, según sus roles y necesidad del servicio.

E) ACCESO BYOD VIP: Acceso para los dispositivos móviles con sistema operativo ANDROID de los usuarios de tipo: Ejecutivos, Directivos de Área, Gerentes de Departamentos, Directores de Departamentos y/o cargos de Alta Dirección, estas cuentas contaran con acceso preferencial pero controlado a los servicios definidos por la compañía, según sus roles y necesidad del servicio.

F) Acceso a módulos administrativos, asignado exclusivamente a usuarios con rol de administrador de su respectivo modulo o aplicación, previa autorización escrita por el líder del proceso.

G) Otros Accesos BYOD: cualquier acceso que no corresponda a los accesos antes enunciados, por ejemplo, acceso de terceros a servicios internos, los cuales estarán aprobados y autorizados por el líder del respectivo proceso y estarán regidos por los acuerdos de confidencialidad y niveles de acceso controlado.

3. Política de uso de dispositivos móviles ANDROID

A) Los Usuarios son completamente responsables de todas las actividades realizadas con sus dispositivos móviles con sistema operativo ANDROID y accesos concedidos a estos por solicitud de su respectiva Área o proceso.

B) Es una falta grave facilitar y ofrecer su dispositivo móvil con sistema operativo ANDROID, a personas no autorizadas, su acceso es exclusivo del cargo, funcionario y/o dependencia y no es transferible; de llegar a presentarse y/o detectarse este tipo de situaciones, la empresa (XXXXXX) procederá a la revocatoria del servicio según la normatividad de la organización, acuerdos de confidencialidad, consentimiento informado, términos de uso de BYOD y/o lo estipulado en el contrato laboral.

C) Se permitirá el acceso a BYOD a los dispositivos móviles con sistema operativo ANDROID que cumplan con los siguientes requerimientos técnicos mínimos: Versión del Sistema Operativo: ANDROID (4.0), Requerimientos de Hardware: Procesador (X.X GHz), Memoria Ram: 1 GB, Almacenamiento interno: 1 GB “libre”, Instalación de Agente de herramienta MDM.

   NOTA: El almacenamiento del dispositivo móvil ANDROID, será ENCRIPTADO y protegido por contraseña, en caso de detectarse este evento. Las demás configuraciones que el área de TI defina, podrán ser enviadas remotamente a los dispositivos.

D) Está complemente prohibido que el sistema operativo de los dispositivos móviles ANDROID, se encuentre modificado o (rooteado).

E) El acceso por BYOD es una herramienta de trabajo para el intercambio de información corporativa, no es una herramienta para difusión de información de la organización.

F) No es permitido almacenar información corporativa en los dispositivos móviles, ni el acceso a otro tipo de información o "información sensible", diferente a la asignada a su rol. Si la empresa detecta la realización de alguna de estas prácticas, se procederá a la revocatoria del servicio según la normatividad de la empresa, acuerdo de confidencialidad, consentimiento informado, términos de uso de BYOD y/o lo estipulado en el contrato laboral.

G) Está completamente prohibida la instalación y el uso de las siguientes aplicaciones mientras el dispositivo se encuentre conectado a la red corporativa (Interna - Externa), o esté siendo usado con fines laborales. **Listado de Aplicaciones:** (XXXX, XXXX, XXXX, etc.) Si la empresa detecta la omisión de este apartado, se procederá a la revocatoria del servicio según la normatividad de la empresa, acuerdo de confidencialidad, consentimiento informado, términos de uso de BYOD y/o lo estipulado en el contrato laboral.

H) El usuario acepta cumplir las políticas y restricciones de uso en su dispositivo móvil para cada uno de los servicios a los cuales tendrá acceso, según su rol (correo electrónico, VPN, portales, aplicativos, CRM, acceso remoto, etc.).

I) El dispositivo móvil será cifrado o encriptado en su totalidad por parte del usuario antes de ingresar a BYOD, procedimiento que se realizará de forma manual o de forma remota por el administrador de los servicios BYOD de la empresa.

J) Los usuarios cuyos dispositivos móviles cuentan con acceso permitido a BYOD, deben asistir obligatoriamente a las campañas de sensibilización, capacitación y participar de las pruebas de seguridad que establezca la empresa.

K) Está expresamente prohibido a los usuarios deshabilitar los sistemas de seguridad, o agentes implementados por la organización en los dispositivos móviles.

L) El usuario de los servicios BYOD, acepta expresamente la política de la compañía sobre la RESTITUCIÓN de dispositivos móviles y gastos cubiertos por la compañía en caso de pérdida, daño total o parcial y/o robo.

M) Periódicamente el administrador de los dispositivos móviles revisará a través de los medios que estime pertinentes, la trazabilidad y seguimiento de las acciones realizadas por los usuarios y los dispositivos móviles, en los servicios BYOD, en caso de incumplimiento total o parcial de alguna de las políticas establecidas, se procederá a desactivar el acceso a BYOD, y se enviará una comunicación de las actividades realizadas al área responsable del usuario, para que se apliquen las acciones correspondientes, correctivos, expulsión del servicio, o hasta la destitución del cargo.

N) El uso inapropiado de los servicios suministrados por el Área de Tecnología, así como la violación e incumplimiento total o parcial de las políticas de uso descritas, tendrá como consecuencia el desarrollo de una investigación y/o castigo sujeto a la normatividad, acuerdo de confidencialidad, consentimiento informado, términos de uso de BYOD y/o lo estipulado en el contrato laboral.

O) En caso de pérdida o robo del dispositivo móvil, el usuario responsable del servicio BYOD, debe dar aviso inmediato a la compañía, usando los datos de soporte

asociados a la presente política, para que se realice el procedimiento de baja del dispositivo de la plataforma BYOD, y lanzar el proceso de borrado seguro de información del dispositivo.

P) BYOD A es suministrado por la compañía para proveer al Usuario, acceso a la información corporativa (en lo sucesivo el "contenido") así como a la utilización de los servicios proporcionados por la misma, (en lo sucesivo los "servicios"), para lo cual el Usuario acepta cumplir integra y completamente la presente política, de lo contrario su dispositivo móvil y su acceso será rechazado de los servicios BYOD.

4. Datos de Soporte

A) Atención telefónica:

XXX XX XX Ext. XXXX

B) Atención virtual:

Correo electrónico: XXXXX@XXXX.XXX

C) Mesa de Ayuda:

URL: http://xxxxxxxx.xxx.xx

5. Responsabilidades y Garantías

A) Cada Área o integrante de la misma es responsable de los procedimientos de copias de respaldo de su información, se sugiere que cada usuario haga Backup con una periodicidad mensual, como mínimo.

B) En caso de que el Usuario borre de forma accidental su información, el Área de Tecnología NO se hará responsable de la información perdida en este imprevisto. (Referirse al procedimiento de realización de Backup establecido por la empresa).

6. Seguridad

A) Si por cualquier motivo El Usuario sospecha o detecta que la seguridad de su dispositivo móvil se ve comprometida de cualquier forma, debe reportarlo de forma inmediata al Área de Tecnología. *Como mejor practica de seguridad se recomienda que la empresa solicite el cambio de las contraseñas de las cuentas, con una periodicidad mínima de 60 días.*

7. Confidencialidad

A) La empresa (XXXXX) se compromete a no ceder, ni vender a terceros la información privada que almacena, posee, trata, administra y demás de sus empleados, contratistas, proveedores, y/o demás partes, etc.

B) Cada usuario es responsable de su información personal y privada que trate, administre, almacene y divulgue por medio de sus dispositivos móviles.

NOTA: Por políticas de seguridad se requiere expresamente que el Password, la credencial, el patrón de acceso a los dispositivos móviles, se cambie cada 60 días, el cual debe estar acorde a las políticas de Password que la compañía ha establecido para este servicio.

5. Dispositivos de Gestión Mobile Device Management (MDM)

Son consolas, servidores o dispositivos dotados de un software especializado, cuya función primordial es centralizar la administración, gestión y monitoreo remoto de los dispositivos móviles, por medio de la instalación de un "agente" en los dispositivos móviles, que no es más que un pequeño programa o software específico de cada herramienta, el cual se encarga de conectarse y sincronizarse con la herramienta MDM, para informar qué se hace con los dispositivos, y permitir la gestión y control de lo que se puede o no, hacer con los mismos.

Este tipo de herramientas se encuentra en el mercado de acuerdo al fabricante, como suscripción de servicio (SaaS), o de forma perpetua con la adquisición de plataformas (PaaS) y de la respectiva licencia(s) de uso.

La implementación de proyectos de esta naturaleza debe cumplir con unas fases que se han descrito en otras palabras a lo largo del trabajo, pero que a continuación se presentan de forma específica y clara.

Ilustración 25 Fases de Implementación de Proyectos de Gestión de Infraestructuras Móviles

Fuente: http://www.3gmg.com/

5.1 Funcionalidades de los MDM

Algunas de las funcionalidades que ofrecen este tipo de herramientas a las organizaciones, a las áreas de tecnología y a los administradores, son:

- Por lo general son consolas únicas que se encargan de todo lo relacionado con los dispositivos móviles (según el fabricante de cada herramienta, ofrecen mayores o menores fortalezas y compatibilidad con determinados dispositivos móviles, tabletas y/o sistemas operativos de los mismos).
- Inventario de Software y Hardware de los dispositivos móviles.
- Datos de geolocalización, monitoreo de zonas permitidas y prohibidas.
- Instalación, desinstalación y bloqueo de aplicaciones.
- Información y configuración de Red.
- Histórico de eventos.
- Información de los dispositivos (Espacio disponible de almacenamiento, información de dispositivos rooteados o con Jailbroken, estado de batería, otros).
- Sincronización de archivos.
- Plantillas de configuración para el uso seguro de los dispositivos móviles, (permisos de acceso a redes, permisos de almacenamiento, aplicaciones permitidas o denegadas, acceso a correo personal o corporativo).
- Bloqueo de funciones de los dispositivos móviles.
- Borrado remoto de información.
- Cumplimiento de políticas, o desvinculación de los dispositivos.
- Envío de notificaciones (Alertas, consumo de datos o minutos, otros).
- Restablecimiento de contraseñas.
- Monitoreo y Auditoría.
- Catálogos de aplicaciones permitidas, para que los usuarios se aprovisionen de las mismas.
- Deshabilitar el acceso a tiendas de Aplicaciones.

5.2 Fabricantes de Herramientas de Administración de Dispositivos Móviles “MDM” en 2017

En el presente TFM a nivel de conocimiento general del mercado de herramientas MDM, se incluye un gráfico con información según Gartner, acerca de los diferentes fabricantes de

herramientas MDM en el mercado TI, el cual a su vez incluye la valoración de nivel de satisfacción del usuario, basados en comentarios de los usuarios acerca de las herramientas.

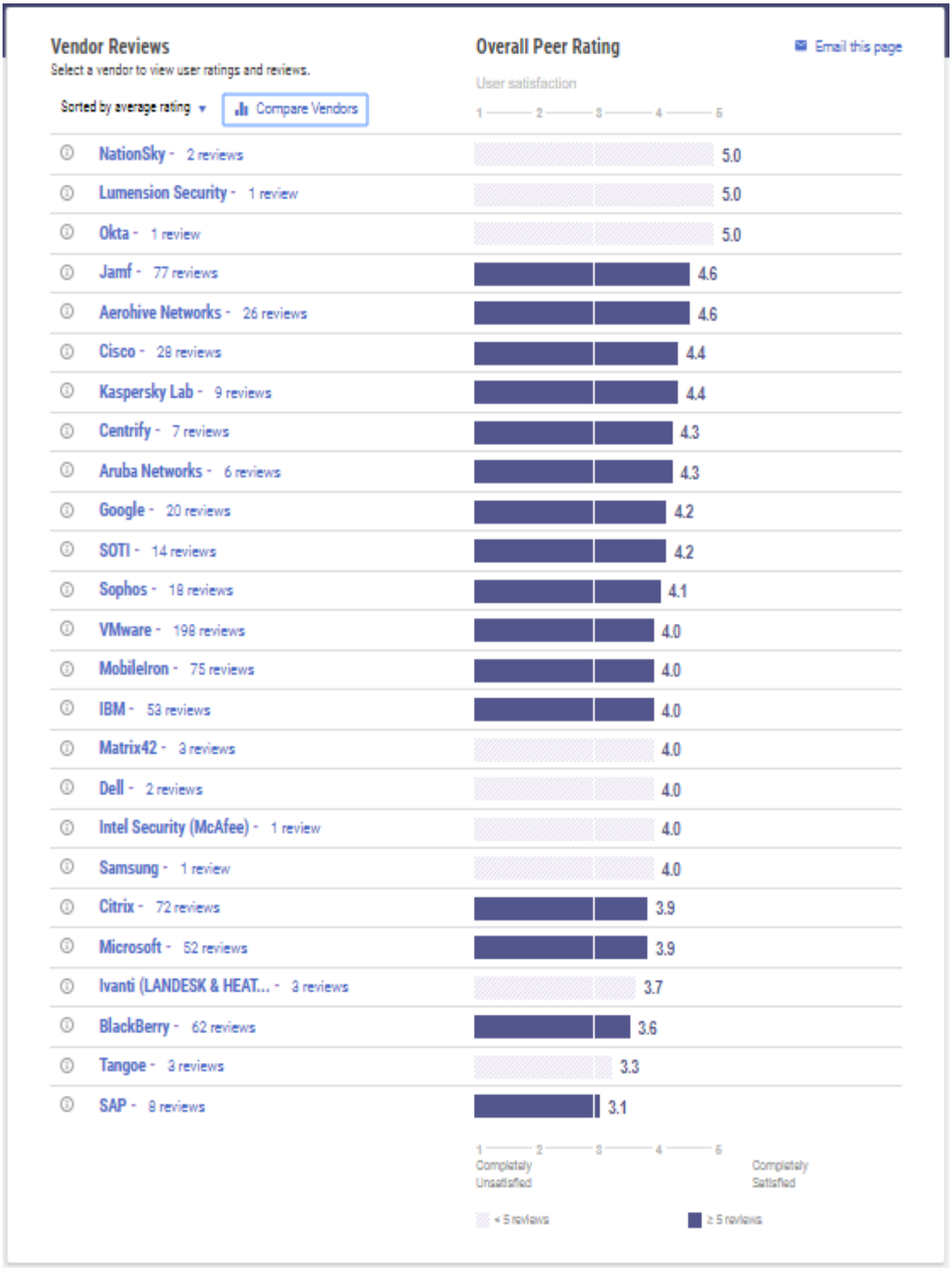

Ilustración 26 Fabricantes de dispositivos MDM - 2017

Fuente: https://www.gartner.com/reviews/market/enterprise-mobility-management-suites

5.3 Mejores Herramientas de Administración de Dispositivos Móviles “MDM” en el 2017

Dada la inminente necesidad de las organizaciones por realizar la implementación de adecuados niveles de control, gestión y seguridad para los dispositivos móviles, se ven enfrentados a elegir una herramienta MDM de entre la gran cantidad de fabricantes que existe en el mercado, para lo cual deben basarse en la información que ha sido recabada previamente por la organización, en cuanto al alcance que va a tener BYOD y el tipo de dispositivos móviles que se van a permitir, puesto que cada una de las herramientas MDM en el mercado, ofrece determinadas coberturas y funciones en cuanto a los sistemas operativos de los dispositivos móviles (Windows Phone, Kindle, BlackBerry, Symbian, IOS, Android, otros) que cada una de ellas puede gestionar, o también mayor integración con dispositivos móviles de determinado fabricante como por ejemplo Samsung, LG, Motorola, Apple, u otros.

Por lo anterior las áreas de tecnología, sus responsables y administradores, se ven abocados a realizar la elección de la herramienta que mejor cumpla con las necesidades propuestas por la organización y las partes interesadas, y de la misma forma que cumpla con las expectativas de seguridad, que garanticen que la organización no tendrá expuesta su información, ni la información de los usuarios.

Según uno de los artículos más recientes de la revista PCMag, publicado el 20 de Junio de 2017, por Paul Ferrill, en el cual presenta a los lectores, las mejores soluciones para la gestión de dispositivos móviles del 2017, según su fabricante, producto y un comparativo de funcionalidades entre estos mismos.

Name	SOTI MobiControl	VMware AirWatch	Citrix XenMobile	IBM MaaS360	ManageEngine Mobile Device Manager Plus	Amtel Telecom and Mobile Management	AppTec360 Enterprise Mobility Management	Microsoft Intune	Radia Endpoint Manager
Lowest Price	SEE IT	SEE IT	SEE IT	SEE IT	SEE IT	SEE IT	SEE IT	SEE IT	SEE IT
Editor Rating	●●●●◐ EC	●●●●◐ EC	●●●●○	●●●●○	●●●◐○	●●●○○	●●●○○	●●●○○	●●○○○
Windows Phone 8	✓	✓	✓	✓	✓	✗	✓	✓	✗
Windows Phone 10	✓	✓	✓	✓	✗	✗	✓	✓	✗
Android Version	✓	✓	✓	✓	✓	✓	✓	✓	✓
iOS Version	✓	✓	✓	✓	✓	✓	✓	✓	✓
User Self-Registration	✓	✓	✓	✓	✓	✓	✓	✓	✓
Remote Lock	✓	✓	✓	✓	✓	✓	✓	✓	✓
Remote Wipe	✓	✓	✓	✓	✓	✓	✓	✓	✓
Enterprise Wipe	✓	✓	✓	✓	✓	✗	✓	✗	✓
Role-Based Authentication	✓	✓	✓	✓	✓	✓	✓	✓	✓
Mobile Expense Management (MEM)	✓	✓	✗	✓	✗	✓	✗	✗	✗
Single Sign-On (SSO) for All Apps	✓	✓	✓	✓	✗	✓	✗	✓	✗
Geofencing	✓	✓	✓	✓	✗	✓	✓	✗	✓
Read Review	SOTI MobiControl Review	VMware AirWatch Review	Citrix XenMobile Review	IBM MaaS360 Review	ManageEngine Mobile Device Manager Plus Review	Amtel Telecom and Mobile Management Review	AppTec360 Enterprise Mobility Management Review	Microsoft Intune Review	Radia Endpoint Manager Review

Tabla 3 Comparativo de Características de las mejores soluciones de Administración de Dispositivos Móviles del año 2017

Fuente: http://www.pcmag.com/article/342695/the-best-mobile-device-management-mdm-software-of-2016

Tal y como se observó a lo largo de este documento, la penetración de los dispositivos móviles con sistema operativo ANDROID, en sus diferentes versiones a nivel mundial es muy elevada, lo cual motivó y enfocó la realización del presente Trabajo de Fin de Máster, y poniendo en el contexto del enfoque que cada uno de los fabricantes de soluciones de administración de dispositivos móviles ofrece, es evidente que todos soportan ANDROID desde versiones bastante obsoletas como la Versión 2.3, lo cual da un amplio nivel de cobertura para este sistema operativo y, asimismo ya se cuenta en el mercado con un adecuado nivel de madurez en el tratamiento y gestión de este tipo de dispositivos móviles, lo cual facilita la administración de los mismos, independientemente de que en las organizaciones no se pueda contar con un parque de dispositivos móviles homogéneo.

5.4 Configuración Mínima Recomendada para Herramientas MDM

CONFIGURACIÓN MDM	
Inventario	Se recopilará periódicamente el inventario de Hardware y Software de los dispositivos móviles, lo cual servirá como insumo de informes, histórico y auditoria de los dispositivos, asimismo será validado contra las listas Blancas y Negras que el administrador estime pertinente.
Configuración Inicial	Basados en las directrices de cada organización, se definirá cual es la configuración inicial que tendrán los dispositivos móviles para su uso en la empresa, en la cual se tendrá en cuenta la activación o desactivación de funciones de los dispositivos como (GPS, Cámara, otros), aplicaciones permitidas, aplicaciones requeridas, entre otras que aplique de acuerdo a cada organización.
Contenedores	Se debería incluir el uso de contenedores de información, para separar la información personal, de la información corporativa, lo cual será de gran importancia en la administración de la seguridad de la información.
Políticas	Las políticas son esenciales en este tipo de dispositivos, dado que se ven orientados al cumplimiento de éstas, o a la revocatoria automática del servicio en caso de incumplirlas, para no poner en riesgo la información, la red, la infraestructura, aplicativos y demás activos.
Seguridad	Habilitar zonas geográficas permitidas, modo de autenticación, medios de conexión, VPN, deshabilitar conexiones Wi-Fi públicas, encriptación de medios de almacenamiento, otras.
Aplicaciones	Implementación de listas Blancas y listas Negras de aplicaciones, instalación y desinstalación silenciosa de aplicaciones sin ninguna intervención del usuario, portal de auto aprovisionamiento de aplicaciones permitidas, gestionado por el usuario.
Estadísticas de Consumo	Es de gran utilidad a nivel de estadísticas la configuración de Consumos y tope máximo de consumos, envío de notificaciones, lo cual servirá para la toma de decisiones en la empresa y, asimismo para la realización de autorías y seguimiento de uso y consumo.

Tabla 4 Configuración mínima recomendada para herramientas MDM

Fuente: Elaboración Propia

6. Resumen de Riesgos Asociados al Uso de Dispositivos Móviles

6.1 Riesgos Asociados a los Dispositivos Móviles

- Extravío, daño o robo de los dispositivos móviles, que es una situación muy común y con una alta probabilidad de ocurrencia, en vista de su tamaño y de la facilidad que presenta este factor para que los delincuentes puedan acceder a estos dispositivos.

- Falta de actualizaciones de seguridad y de sistema operativo Android en los dispositivos móviles, las cuales no son proporcionadas en forma y tiempo adecuados por los fabricantes de los dispositivos móviles a sus clientes, o simplemente dejan de producir actualizaciones para los modelos o referencias obsoletas.

- Explotación de vulnerabilidades asociadas a las diferentes versiones de los sistemas operativos Android obsoletos, o que se encuentran sin las respectivas actualizaciones que de forma juiciosa, publica mensualmente el grupo de desarrollo de Android, lamentablemente para los usuarios, estas actualizaciones son producidas para los dispositivos propios de Google, y son puestas a disposición de los fabricantes, para que realicen sus respectivos ajustes y las publiquen a sus usuarios, que es lo que en ultimas ocurre muy lentamente, o no ocurre.

- Explotación de vulnerabilidades asociadas a la conexión e interceptación de Wi-Fi, NFC, Bluetooth, etc., estas interfaces tienen la capacidad de comunicarse con dispositivos cercanos, lo cual mantiene latente la posible interceptación de información que viaja por el aire, así como el ataque a las vulnerabilidades propias de cada una de estas interfaces.

- Explotación de vulnerabilidades como escucha pasiva, escucha activa, denegación de servicio, robo de información, modificación de información, eliminación, u otras, asociadas a arquitecturas de comunicaciones móviles 2G, 2.5G, 3G y 4G, que aunque han evolucionado y mejorado sus sistemas de seguridad, no significa que en la actualidad han logrado ser infalibles, por lo cual son una vulnerabilidad latente.

- Acceso de terceros a información guardada en medios de almacenamiento extraíble o interno de los dispositivos móviles, la cual puede ser copiada, robada, eliminada, modificada y/o almacenada en otros dispositivos o sistemas.

- Sistemas Operativos Android modificados o rooteados.

- Adquisición y uso de dispositivos móviles “usados”.

- Vulnerabilidades asociadas a modelos, series, partes y fabricantes de dispositivos móviles.

- Vulnerabilidades del uso de controles de seguridad Biométrica.

- Vulnerabilidades de los chips y de la arquitectura de hardware y software con el que vienen de fábrica los dispositivos móviles.

- Acceso de terceros a la información de los dispositivos móviles, vía interconexión de los dispositivos con otros sistemas y realización de sincronizaciones.
- Inadecuadas campañas de sensibilización en cuanto a seguridad y privacidad de la información por parte de los fabricantes de los dispositivos móviles, hacia los usuarios finales o consumidores de estos dispositivos.

6.2 Riesgos Asociados a Malas Prácticas de los Usuarios de los Dispositivos Móviles

- Ataques de Ingeniería Social enfocados a los usuarios, que requieren que los usuarios hagan tareas peligrosas en sus dispositivos móviles, como cambios en los permisos, o permitir la instalación de aplicaciones de terceros no firmadas, como es el caso de los falsos antivirus, o aplicaciones mágicas de optimización de dispositivos.
- Instalación indiscriminada de aplicaciones potencialmente peligrosas, que pueden tener código malicioso, el cual conlleva a robo de información y otras amenazas a la seguridad de la información contenida en los dispositivos móviles.
- Inadecuados o inexistentes controles de autenticación en los dispositivos móviles, los cuales por lo general son omitidos o configurados de forma débil por los usuarios.
- Almacenamiento de información privada y sensible, tanto personal como laboral, en los dispositivos móviles, sin adecuados controles de seguridad.
- Ataques por medio de direcciones URL falsas, códigos QR, URL en mensajes de texto, descarga y ejecución de archivos dañinos, entre otra gran gama de posibilidades de este tipo engañando al usuario, el cual es conocido como “phishing”.
- Uso inadecuado de los permisos para las aplicaciones, por lo general se da permiso a información sensible como los contactos, ubicación, galerías, multimedia, administración de configuración de los dispositivos, etc., con lo cual el usuario pierde el control de la seguridad de los dispositivos móviles.
- Ausencia de activación de cifrado de los medios de almacenamiento, para proteger de forma adecuada la información contenida en los dispositivos móviles en caso de robo, perdida u otro tipo de incidente de seguridad.
- Préstamo de los dispositivos móviles a terceras personas, cuyo resultado puede terminar en la perdida de privacidad, y de control de los dispositivos móviles.

- No se usan medios de conexión cifrados tipo VPN u otros, para el intercambio de información de forma segura, cuando el usuario requiere trabajar con información confidencial o sensible.

- Uso indiscriminado de redes inseguras, en especial los Wi-Fi públicos, en aeropuertos, restaurantes, hoteles, bares, etc., por medio de los cuales puede ser interceptada la información, lo cual es conocido como “sniffing”.

- Conexión permanente y habilitada de medios de conectividad inalámbrica que no se usan todo el tiempo en los dispositivos móviles, como es el caso del Wi-Fi, Bluetooth, NFC, lo que conlleva como consecuencia que se abran puertas traseras y vulnerabilidades relacionadas con estas interfaces de comunicación.

- Conexión de los usuarios de los dispositivos móviles a puntos de acceso Wi-Fi falsos, conocido como “spoofing”, en el cual son hábilmente engañados los usuarios por los delincuentes, para poder tener acceso a la información de los dispositivos móviles y pueden llegar hasta tomar el control remoto de los mismos.

- Conexión de los dispositivos móviles a otros sistemas como computadores en sitios públicos, accesorios, dispositivos de carga de baterías, en los cuales puede ocurrir intercambio bidireccional de información sensible, pérdida de control, robo de información, transmisión y ejecución de código malicioso, etc.

- Inadecuados niveles y controles de configuración de conexión a dispositivos conocidos, o seguros como es el caso de los dispositivos “Bluetooth” como parlantes, SmartWatch y demás dispositivos de confianza de esta naturaleza.

- Inadecuado uso de los sistemas de geolocalización o GPS en los dispositivos móviles, los cuales permiten el acceso y control de esta característica a aplicaciones potencialmente peligrosas, navegadores, cámara, redes sociales, entre otros que afectan o comprometen la seguridad física del usuario, de la información y permiten a los atacantes conocer los movimientos geográficos y perfiles de los usuarios.

- Ausencia de tratamiento adecuado y seguro de los metadatos que recopilan y envían los dispositivos móviles, por medio de archivos, correos, fotografías y demás de este tipo.

- La información personal y corporativa de los usuarios es un nuevo blanco económico para los ciberdelincuentes, tal es el caso, como robo de información bancaria, secuestro de información, variantes de ransomware, cuentas y contraseñas de acceso a redes sociales, correos electrónicos personales y corporativos, y la lista continúa extendiéndose, pues cualquier tipo de información que se pueda recopilar de una persona tiene un valor económico en la red.

- Acceso de los usuarios a aplicaciones potencialmente peligrosas o modificadas, las cuales se encuentran disponibles y son descargadas con confianza por los usuarios de los dispositivos móviles de la tienda oficial de Android “Google Play”, sin tener la plena certeza de que son aplicaciones seguras y no han sido modificadas por terceros.

- Rootear o modificar el sistema operativo Android, es un procedimiento que realizan los usuarios en los dispositivos móviles, para quitar todas las restricciones que vienen predefinidas de fábrica con los dispositivos y otorgar control total del sistema operativo, configuraciones, modificación de rendimiento, reemplazo de aplicaciones de sistema, de fabricante y de operador móvil, entre otros aspectos que otorgan a los usuarios el control total del dispositivo y del sistema operativo, pero asimismo, la consecuencia para el usuario es la perdida de seguridad de su dispositivo y su información, pues es un sistema modificado, que puede permitir a las aplicaciones la ejecución de código y acciones maliciosas sobre todo el dispositivo.

De acuerdo con la información antes mencionada en los numerales 6.1 y 6.2, a grosso modo podemos ver que los dispositivos y los usuarios de los dispositivos móviles, se encuentran expuestos a diario a listas muy extensas de riesgos y vulnerabilidades que día a día son aprovechadas y continúan en constante evolución por los ciberdelincuentes, por tal razón estas listas presentadas aquí no son la última palabra en cuanto a los riesgos que una organización enfrentará, asociada al uso de los dispositivos móviles de los usuarios en las redes y sistemas informáticos, pero de una manera amplia se trata de abordar los puntos clave, que deben ser considerados por una organización y por el área de TI.

A la información aquí presentada se debe sumar el estudio propio que realice cada organización en su momento, en cuanto a los nuevos riesgos que se hayan detectado a la fecha en que se realiza el análisis, y a los propios riesgos de cada organización.

7. Ventajas y Desventajas de BYOD

7.1 Ventajas

- Centralización de la información mediante el uso de contenedores seguros de información, servicios en la nube, o en un dispositivo móvil.
- Los usuarios deben llevar consigo menos cantidad de dispositivos, pues su propio dispositivo móvil, es también su herramienta de trabajo.
- Mayor productividad empresarial, se provecha el conocimiento de los usuarios en el manejo de sus propios dispositivos, herramientas y aplicaciones, se hace un mejor aprovechamiento del tiempo, debido a que pueden atender asuntos laborales en todo momento, lugar y hora, lo cual da un valor agregado de más horas de trabajo por empleado a las empresas.
- Aumento de la satisfacción de los empleados en la realización de sus actividades, debido a que trabajan con la tecnología escogida por ellos mismos.
- Menor inversión económica de las empresas en capacitaciones a sus empleados, en el manejo de nuevas tecnologías móviles, pues los usuarios están en constante evolución en el manejo de estas herramientas.
- Dispositivos de última tecnología adquiridos por los usuarios y puestos a disposición de las empresas, sin que ello represente una inversión económica y/o reemplazo de tecnologías, cuyo beneficio directo para las organizaciones es ahorro de dinero.
- Renovación constante del parque de dispositivos móviles, la cual está a cargo de los usuarios.
- Ahorro económico para las empresas, en cuanto a adquisición y renovación de licencias de software y de mantenimiento preventivo y correctivo de los dispositivos móviles.
- Ahorro económico para las empresas, en cuanto a adquisición de pólizas de seguros que amparen el parque de dispositivos móviles.
- Se abre una nueva posibilidad de uso de herramientas o aplicaciones libres o gratuitas, que sigue siendo un factor de ahorro económico para las empresas.
- Constante retroalimentación en cuanto a la seguridad de la información, por parte del personal de TI, contacto con grupos de interés relacionados, asesoría y capacitaciones de entidades gubernamentales y privadas, especializadas en el tema de seguridad de la información.

7.2 Desventajas

- Se requieren nuevas políticas, adecuadas, ajustadas y específicas para el correcto funcionamiento de BYOD y de la seguridad de la información.
- Revisión, actualización, modificación de las medidas y protocolos de seguridad de la información vigentes en las organizaciones.
- El uso de los dispositivos móviles supone a las organizaciones riesgos latentes con la seguridad de las redes, los sistemas de información, las infraestructuras y demás componentes tecnológicos y humanos, puesto que se pueden materializar nuevos riesgos que ingresen a éstas por medio de los dispositivos móviles.
- Constante actualización por parte del personal de seguridad y seguimiento a los informes, estadísticas, boletines de seguridad y de nuevas vulnerabilidades o amenazas relacionadas con dispositivos móviles.
- BYOD trae consigo un incremento elevado en el consumo de recursos de red para las organizaciones, puesto que la mayoría de servicios impacta directamente sobre dispositivos de conectividad y comunicaciones.
- Incremento de un nuevo servicio que requiere soporte, los "dispositivos móviles y sus aplicaciones", el cual demanda personal con conocimientos avanzados en este tipo de dispositivos, así como también la incorporación de este nuevo servicio en las plataformas de mesa de ayuda o help desk.
- Incremento de personal de las áreas de TI, para hacer frente a los nuevos retos administrativos, documentales, de sensibilización, de soporte y personal específico para la administración de las herramientas de gestión de dispositivos móviles, entre otras adicionales que puedan requerirse.
- Adquisición de herramientas específicas para la administración y gestión de los dispositivos móviles.
- Las organizaciones no tendrán un parque tecnológico de dispositivos móviles homogéneo, relacionado con versiones de sistema operativo, hardware, fabricantes y demás relacionados con la diversidad de dispositivos móviles.
- Se requiere consentimientos de autorización aceptados y firmados por los usuarios, para poder tener acceso a la gestión y administración de sus dispositivos móviles y de su información.
- Incrementa la exposición de la seguridad de la información y la posibilidad de explotación de vulnerabilidades en servicios web, aplicativos y demás activos con información de las organizaciones.

- Incremento de divulgación de información y campañas de sensibilización en seguridad de la información, para mantener a los usuarios actualizados, sensibilización en el manejo seguro de la información personal y laboral, para mitigar de forma preventiva la materialización de riesgos ocasionados por acciones imprudentes o por desconocimiento de los usuarios.

- Exposición total de las partes a la ciberdelincuencia (empresa y empleado), no solo los datos de los datos de los usuarios son de valor para los cibercriminales, también los datos corporativos son un blanco bastante atractivo para los ciberdelincuentes en la red, con lo que se concluye que hay una mayor exposición para ambas partes empresa y empleados, los cuales pueden ir desde simples bloqueos de cuentas de usuario, de correo, hasta fraudes y estafas millonarias a las organizaciones.

- Almacenamiento de información en la nube, es un nuevo factor de riesgo que surge del uso de BYOD y de los dispositivos móviles, en la actualidad para proveer el acceso a la información a los usuarios, esta debe ser publicada en servicios en la nube, el cual también requiere de protección adicional y constante monitoreo, de la misma forma los usuarios de los dispositivos móviles están resguardando su información en servicios en la nube como Google Drive para el caso específico de Android y otros servicios ofrecidos por terceros.

8. Conclusiones y Trabajo Futuro

En el presente trabajo de fin de master se abordó la investigación de la tendencia de BYOD desde su inicio hasta la fecha, en el cual las empresas dieron inicio al cambio de filosofía y mentalidad desde las áreas de tecnología, hasta la empresa por completo, para adaptarse a los cambios que se requieren para realizar implantaciones de este tipo.

Se evidenció a lo largo del TFM la gran penetración que han tenido y tienen los dispositivos móviles ANDROID a nivel mundial, por esta razón se eligió específicamente este tipo de dispositivos y de sistema operativo, y es de conocimiento general que los usuarios de dispositivos inteligentes van adquiriendo este tipo de tecnología y renovando sus dispositivos móviles a medida que avanza la tecnología y lanzan una nueva versión del Sistema Operativo ANDROID, o un nuevo modelo de Smartphone, por lo cual BYOD, cuenta con dispositivos en su mayoría de última generación que ofrecen mayores prestaciones a los usuarios.

La investigación arroja como resultado que los dispositivos móviles han desplazado ampliamente el uso de computadores tradicionales, ya que este tipo de dispositivos se han convertido en computadores de bolsillo, desde los cuales los usuarios pueden realizar la mayoría de actividades laborales como si estuvieran trabajando en un computador de escritorio, pero con la ventaja que también simultáneamente pueden realizar sus actividades personales, razón por la cual se ha convertido este tipo de dispositivos móviles, en herramientas necesarias en el día a día de la humanidad.

Debido a la gran versatilidad de los dispositivos móviles, los usuarios han obligado prácticamente a las empresas a permitir su uso para la realización de las actividades laborales con beneficios para las empresas, en cuanto a productividad y satisfacción en el trabajo por parte de sus empleados y colaboradores; pero de la misma forma las empresas han tenido que realizar grandes esfuerzos económicos y tecnológicos, para permitir dicha inclusión sin perder el control de la seguridad de sus sistemas y sin arriesgar completamente la información que es el activo más importante, de cualquier empresa y usuario.

A pesar de que BYOD se encuentra presente en el mercado con gran fuerza desde hace más de 5 años, aún muchos CIOS y empresarios, se niegan a esta transición, puesto que requiere cambios drásticos de mentalidad como de adaptaciones tecnológicas, de procesos y procedimientos internos y en algunos otros casos porque simplemente la misión de las empresas no requiere de este tipo de servicio.

El aporte general del presente TFM es una propuesta metodológica que se presenta de forma directa a los responsables de implementaciones BYOD, ofreciendo una forma sencilla de abordar la transición de los sistemas tradicionales a BYOD, mostrando los sistemas operativos más usuales en el mercado, las versiones más utilizadas, las principales vulnerabilidades, y se propone una lista de riesgos a tener en cuenta, así como una política de seguridad; lo anterior sin hablar, ni contemplar la elección, implementación y configuración de complejas herramientas de infraestructura, que se encarguen de la gestión de los dispositivos móviles, lo cual se convierte en una futura línea de investigación y de trabajo que complemente el presente TFM.

Se presenta una visión general a los responsables de tecnología, para ofrecer un punto de partida de fácil comprensión, que es adaptable a los procesos y procedimientos con los que trabaja la mayoría de organizaciones y empresas a nivel mundial. Se realiza una propuesta de evaluación de riesgos generales a los que se exponen los usuarios, los dispositivos y las empresas, la cual debe ser adaptada o modificada para el caso específico de cada empresa, pero que servirá como insumo para el planteamiento de la misma.

Teniendo los anteriores factores, se aborda el tema de controles de seguridad de la información en BYOD, proponiendo una serie de controles o salvaguardas que se deben implementar, los cuales fueron tomados de la norma ISO/IEC 27001:2013, que aplican no solo para BYOD, sino como mejores prácticas de seguridad de la información en general y también será una bondad adicional que se aporta en el presente TFM, puesto que las organizaciones con este importante insumo, pueden iniciar la ruta de certificación en seguridad de la información ISO/IEC 27001:2013.

Habiendo estructurado lo anterior, finaliza el aporte del presente TFM con la propuesta de una política de seguridad, abordando características usuales de cualquier organización o empresa, con lo cual los encargados o directores de las áreas de tecnología y sistemas pueden personalizar dicho insumo y adaptarlo al 100% a la misión del negocio.

La conclusión global de este trabajo es que los dispositivos móviles y BYOD son el futuro inmediato laboral que la humanidad va a enfrentar y asumir a nivel mundial en los próximos años, razón por la cual se debe perder el miedo a realizar la transición y centrarse en la mejor forma de convertir a BYOD en un aliado estratégico de negocio, en el cual todo es más productivo, oportuno y asequible.

Las futuras líneas de investigación son muy variadas, se pueden centrar en investigar y definir las bondades y alcance de las actuales herramientas del mercado para la gestión de

dispositivos móviles y profundizar en cuáles son las más adecuadas y precisas para cada empresa, según el alcance y tipo de dispositivos que se quiera permitir en BYOD.

Se podría aplicar la norma ISO/IEC 27017, específica en seguridad de la información para servicios CLOUD, y aplicarla directamente a los servicios que las organizaciones tienen en la nube y son accesibles a los usuarios por BYOD.

Plantear una línea de trabajo específica de concientización a los encargados de tecnología para abordar de forma puntual el tratamiento y resolución de los temas de seguridad en BYOD, para que se centren específicamente en los usuarios, que son el eslabón más débil de toda la cadena, aún hoy en día este sigue siendo uno de los más grandes problemas a atacar.

Cabe recalcar que hay muchos mecanismos de protección y de seguridad, pero por más esfuerzos que se realizan por securizar cualquier ambiente, siempre siguen existiendo brechas de seguridad y una gran mayoría está relacionada con las acciones de los usuarios por diversos factores, como por ejemplo instalación de aplicaciones no firmadas, acceso a enlaces fraudulentos en la red, ejecución de cualquier tipo de archivos, publicación de información en redes sociales, perdida de los dispositivos, en fin, la lista se hace más extensa, razón por la cual es un gran segmento para tratar, investigar y difundir información, para concienciar a los usuarios de los riesgos a los que están expuestos día a día.

Otra línea de trabajo futuro que puede ser propuesta, es que las soluciones de BYOD no se deban bazar en qué tipo de dispositivos y sistemas operativos manejan estos, se debe pensar en que BYOD admita cualquier tipo de dispositivo y que esté preparado para escalarse sin mayores esfuerzos, puesto que hoy en día, aún se debe estudiar a profundidad que tipo de dispositivos móviles serán los que se pueden permitir, y con los constantes avances de la tecnología móvil, en la cual los fabricantes están en constante desarrollo y evolución, es un tema que siempre estará en retroalimentación, actualización y será cambiante.

9. Bibliografía

Cisco Systems. (2013). Cisco Bring Your Own Device Device Freedom Without Compromising the IT Network. Cisco Systems, Inc.

International Standard. (2013). Information technology - Security techniques - Code of practice for information security controls. Switzerland: ISO/IEC.

Mathias, C. J. (enero de 2014). Como crear una política de BYOD. Recuperado el 21 de octubre de 2014, de http://searchdatacenter.techtarget.com/: http://searchdatacenter.techtarget.com/es/consejo/Como-crear-una-politica-de-BYOD

Fernando C., B. A. (2012). Modelo unificado para identificación y valoración de los riesgos de los activos de información en una organización. Cali: ICESI.

Martínez, E. A. (2012). redyseguridad.fi-p.unam.mx. Recuperado el 25 de 10 de 2014, de http://redyseguridad.fi-p.unam.mx/proyectos/criptografia/criptografia/index.php/3-gestionde-claves/31-politicas-de-gestion-de-claves?showall=&start=1

Software Engineering Institute. (2010). CMMI para Desarrollo, Versión 1.3. Carnegie Mellon University.

MAP., A. C. (s.f.). Herramientas para la Gestión de Proyectos. Recuperado el 27 de 11 de 2014, de PROJECT - TOOLS: projectools.wordpress.com/modelos-de-madurez-engestion-de-proyectos
International

Organization for Standardization. (2005). ISO/IEC 27001.
International Organization for Standardization. (2005). ISO/IEC 27001.
GOOGLE. (09 de 06 de 2014). OWR MOBILE PLANET. Obtenido de http://think.withgoogle.com/: http://think.withgoogle.com/mobileplanet/es/graph/?country=ar&country=br&country=ca&c
ountry=us&country=mx&category=DETAILS&topic=Q00&stat=Q00_1&wave=2011&wave=
2012&wave=2013&age=all&gender=all&chart_type=bar&active=gender

Cisco IBSG Horizons. (2012). BYOD y Virtualización.
Forrester Reseach. (2012). Forrsingts Workforce Employee Survey Q4 2012.
GARTNER. (01 de 05 de 2014). www.gartner.com. Obtenido de http://www.gartner.com: http://www.gartner.com/it/content/2538500/2538515/august_14_bring_your_own_device_b
yod_dwillis.pdf?userId=73210080

Ann Cavaukian, P. (11 de 12 de 2013). BYOD (Bring Your Ownd Device) Is Your Organization Ready? Ontario, Canadá.
ISACA. (s.f.). ISACA.ORG. Recuperado el 01 de 05 de 2014, de Information Systems Audit and Control Association: http://www.isaca.org/Blogs/282270/archive/2011/04/27/ProteccióndeActivosdeInformación.

aspx

Vera, E. (s.f.). ISO 27001. El inventario de activos en la implementación de la norma. Recuperado el 20 de 04 de 2014, de http://www.isotools.org: http://www.isotools.org/2013/12/05/en-inventario-de-activos-en-la-implementacion-de-lanorma-iso-27001/
International
Organization for Standardization. (2013). ISO/IEC 27001.

Ministerio de tecnologías de la Información y las comunicaciones. (14 de 03 de 2014). Boletín Trimestral de las TIC Banda Ancha Cifras Cuarto trimestre de 2013.
Chrissis, M. B. (2011). CMMI for Development: Guidelines for Process Integration and Product Improvement (3rd Edition ed.).

Miller, K. W., Voas, J., & Hurlburt, G. F. (2012). BYOD: Security and privacy considerations.It Professional,14(5), 53-55.

Miguel Angel Aranguren Romero, Haciendo Inteligente mi movilidad (Oct 2011), from http://sasorigin.onstreammedia.com/origin/isaca/LatinCACS/cacslat/forSystemUse/papers/123.pdf

Semer, L. (2013). Auditing the BYOD program: the growing business use of personal smartphones and other devices raises new security risks. Internal Auditor, 70(1), 23-26.

Especialista en administración de la seguridad. Recuperado el 22 de Septiembre del 2011. http://repository.unimilitar.edu.co/handle/10654/3215

Instituto Colombiano de Normas Técnicas y de Certificación ICONTEC , “NORMA -ISO-IEC 27001 Tecnología de la información : técnicas de seguridad. Sistemas de gestión de la seguridad de la información (SGSI). Requisitos / Icontec.,” *Repositorio Digital de documentación en materia de Gestión Documental*, revisado 7 de junio de 2017, http://www.archivogeneral.gov.co/normatividad/items/show/34.

De la Torre, M. L. (2012). Una aproximación al concepto de Sociedad Móvil: el smartphone: su expansión, funciones, usos, límites y riesgos. Revista Dialnet, Derecom,(11), 10.

Herrera-Mendoza, K. M., Rodríguez, M. P. A., & Vega, L. G. (2016). Motivación de jóvenes universitarios hacia el uso de teléfonos celulares/Motivation of youth students with use of cell phones. Revista Encuentros, 15(1).

El cifrado de la información es una tarea pendiente en la pyme. Recuperado el 20 de Febrero de 2012. http://www.tecnologiapyme.com/hardware/el-cifrado-de-informacion-es-una-tarea-pendiente-en-la-pyme

10. Otros Recursos Electrónicos

"WannaCry", "exploits", "ingeniería social": Acérquese a las complicaciones informáticas modernas
https://diarioemisordigital.wordpress.com/2017/05/19/wannacry-exploits-ingenieria-social-acerquese-a-las-complicaciones-informaticas-modernas/
BYOD: Security and Privacy Considerations
http://s3.amazonaws.com/academia.edu.documents/30666416/MVH2012.pdf?AWSAccessKeyId=AKIAIWOWYYGZ2Y53UL3A&Expires=1499445368&Signature=t8dO%2B22ZBiWFiwNr98INO16abXk%3D&response-content-disposition=inline%3B%20filename%3DBYOD_Security_and_Privacy_Considerations.pdf

Las 4 fases de un ciberataque en un dispositivo Android
http://mundocontact.com/las-4-fases-de-un-ciberataque-en-un-dispositivo-android/

The future of Enterprise Mobility
https://www.techgoondu.com/2017/05/22/the-future-of-enterprise-mobility/

Diez estadísticas de Movilidad Empresarial que pueden Sorprenderte
https://www.bixpe.com/blog/diez-estad%C3%ADsticas-de-movilidad-empresarial-que-pueden-sorprenderte

Aranda Mobile Device Management
http://arandasoft.com/aranda-mobile-device-management/

Gestión Bring Your Own Device
https://www.manageengine.com/es/mobile-device-management/gestion-bring-your-own-device-byod.html

TIB – Seguridad en la Información
https://www.isaca.org/chapters8/Montevideo/Events/Documents/presentacion%20-%20maximiliano%20alonzo%20-%20byod%20ventajas%20desventajas%20y%20consideraciones%20de%20seguridad.pdf

BYOD: Una perspectiva Global
http://www.cisco.com/c/dam/en_us/about/ac79/docs/re/byod/BYOD_Horizons-Global_ES.pdf

Qué es el BYOD, Ventajas y Desventajas
https://leyprotecciondedatos.files.wordpress.com/2013/01/quc3a9-es-el-byod.pdf

Definición Dispositivos móviles
http://revista.seguridad.unam.mx/numero-07/dispositivos-moviles

'Smartphones', el nuevo blanco predilecto de criminales cibernéticos
http://www.eltiempo.com/archivo/documento/CMS-15344197

Juan Manuel Gómez, de Citrix: "BYOD ha penetrado en Latinoamérica mucho más rápido que en otras regiones"
http://distribucion.itsitio.com/us/juan-manuel-gomez-de-citrix-byod-ha-penetrado-en-latinoamerica-mucho-mas-rapido-que-en-otras-regiones/

Informe de Amenazas CCN-CERT IA-21/13

https://www.ccn-cert.cni.es/informes/informes-ccn-cert-publicos/677-ccn-cert-ia-21-13-riesgos-y-amenazas-del-byod-1/file.html

IMS Mobile in Latam – Enero 2015
http://www.imscorporate.com/news/Estudios-comScore/IMS-Mobile-Study-Enero2015.pdf

Dispositivos Mobiles: Un riesgo de seguridad en las redes corporativas
https://revista.seguridad.unam.mx/node/2198

Seguridad, Cultura de prevención para TI
http://revista.seguridad.unam.mx/sites/revista.seguridad.unam.mx/files/revistas/pdf/21_RevistaSeguridad-JavayOtrasTecnologias.pdf

Enterprise Mobility Landscape Wave II
http://www.cisco.com/c/dam/en/us/solutions/collateral/enterprise-networks/mobile-workspace-solution/enterprisemobilitylandscapestudy-spring2014.pdf

Cost of Data Breach Study
https://www.ibm.com/security/data-breach/

Informe Mobile en España y en el mundo 2015
http://www.ditrendia.es/resumen-y-conclusiones-del-informe-mobile-en-espana-y-en-el-mundo-2015-de-ditrendia/

Roll Out Internacional de dispositivos móviles e integración en un MDM
https://contecconsulting.files.wordpress.com/2017/02/caso-de-c3a9xito-puig-rollout-internacional.pdf

MDM vs MAM, ¿qué estrategia de movilidad se adapta mejor a las necesidades de mi negocio?
http://www.revistabyte.es/tendencias-byte-ti/mdm-vs-mam-%C2%BFque-estrategia-de-movilidad-se-adapta-mejor-a-las-necesidades-de-mi-negocio/

Instituto Nacional de Ciber Seguridad – INCIBE - Nuestros datos y los smartphones. ¿Qué riesgos existen?
https://www.osi.es/es/actualidad/blog/2014/09/22/nuestros-datos-y-los-smartphones-que-riesgos-existen

Instituto Nacional de Ciber Seguridad – INCIBE - Lo que debes saber antes de rootear el smartphone
https://www.osi.es/es/actualidad/blog/2014/09/08/lo-que-debes-saber-antes-de-rootear-el-smartphone

Los riesgos de tener un Smartphone desactualizado o no actualizable
https://www.movilzona.es/2016/01/19/los-riesgos-de-tener-un-smartphone-desactualizado-o-no-actualizable/

Predicciones de ciberseguridad y pronóstico de amenazas para 2017
http://searchdatacenter.techtarget.com/es/cronica/Predicciones-de-ciberseguridad-y-pronostico-de-amenazas-para-2017

Malware e ingeniería social, la evolución del virus informático
https://www.ull.es/servicios/stic/2016/11/22/malware-e-ingenieria-social-la-evolucion-del-virus-informatico/