UNIVERSIDAD NACIONAL AUTÓNOMA

DE MÉXICO

FACULTAD DE CONTADURÍA Y ADMINISTRACIÓN

ANÁLISIS DE RIESGO DE LA POLÍTICA BYOD EN DISPOSITIVOS ANDROID

T E S I S

QUE PARA OBTENER EL TÍTULO DE:

LICENCIADO EN INFORMÁTICA

P R E S E N T A:

ALEJANDRO GARCÍA SOLÓRZANO

DIRECTOR DE TESIS:

DR. CARLOS FRANCISO MÉNDEZ CRUZ

México D.F. 2014

UNIVERSIDAD NACIONAL AUTÓNOMA

DE MÉXICO

FACULTAD DE CONTADURÍA Y ADMINISTRACIÓN

ANÁLISIS DE RIESGO DE LA POLÍTICA BYOD EN DISPOSITIVOS ANDROID

T E S I S

ALEJANDRO GARCÍA SOLÓRZANO

México D.F. 2014

Índice de contenido

Agradecimientos

A mi familia, por el apoyo que me dieron para el desarrollo de este trabajo.

A mi hermosa novia Gaby, que me dio todo su apoyo y cariño para lograr terminar este gran proyecto, que sin ella no lo había podido lograr.

A mi asesor Carlos Francisco Méndez Cruz, por su guía y su apoyo para la realización de esta tesis.

A mis compañeros de trabajo, Yolanda, Rita, Juan Manuel, Edgar, Carolina, José Luis, por guiarme y darme un apoyo y orientación.

A mis amigos y en especial a Carlos, Samuel, Rafael, Enrique, por apoyarme y motivarme para terminar este ciclo.

A mis amigos del grupo de japonés, me gustaría agradecerles por su forma de ser y de actuar, ya que me han inspirado y motivado durante el tiempo que compartimos juntos, que a pesar de que no fue mucho. Me han recordado, que la edad o la carrera que uno estudie no son determinantes, y que lo que importa es la pasión, el orgullo, el esfuerzo que uno demuestra en todo lo que hace. Me han enseñado, que el trabajo duro es el camino para alcanzar las metas y sueños que uno se proponga.

A mí amada alma máter la Universidad Nacional Autónoma de México, por brindarme su cobijo todos los años que fui estudiante.

A mí querida facultad, Facultad de Contaduría y Administración que me formó profesionalmente.

> As of now, computer networks are still in their infancy, but as they grow up and become sophisticated, we will probably see the spread of 'computer utilities' which, like present electric and telephone utilities, will service individual homes and offices across the country (Kleinrock, 1969)

Introducción

Antecedentes

El hombre siempre busca la necesidad de hacer su vida más fácil, por lo que ha creado herramientas, fabricado máquinas, desarrollado teorías, creado fórmulas, etcétera. Tan sólo en la última década, la evolución de la telefonía celular; el surgimiento de sistemas operativos para dispositivos móviles como Android, Windows Phone, BlackBerry OS, Symbian OS y IOS; el desarrollo de paradigmas computacionales como Cloud Computing; los bajos costos en la renta del servicio de internet; y la fácil adquisición de equipo electrónico, han logrado cambiar el modo de vida del hombre, entrando a una nueva era digital.

Actualmente ha surgido una nueva tendencia conocida como BYOD (*Be Your Own Device*, por sus siglas en inglés). Esta tendencia consiste en que los empleados utilicen sus dispositivos móviles personales para desempeñar sus labores en las organizaciones, argumentando que con sus propios equipos son más eficientes en comparación con los proporcionados por la organización. Por otra parte las empresas al no tener que adquirir equipo para sus empleados ni proporcionar soporte, les resulta atractiva esta nueva tendencia.

Sin embargo, esta nueva tendencia que se está dando dentro de las organizaciones puede traer consecuencias por ser un elemento nuevo que no se tiene contemplado en ninguna política de las organizaciones, además al ser equipos de cómputo están sujetos a ser blancos de *Blackhats*, *Crakers* y similares.

Planteamiento del problema

Con la reducción de los costos del equipo de cómputo, la gran portabilidad de los mismos, el fácil uso del sistema operativo Android y los servicios proporcionados en la nube, se ha generado un gran aumento de usuarios con equipos portátiles que utilizan sus dispositivos en su vida tanto personal como laboral.

Esta portabilidad y fácil acceso han sobrepasado la barrera de control de los administradores de tecnologías de información (TI). Estos equipos, al no pertenecer a la empresa, no son regidos bajo las mismas normas que los equipos de la organización, permitiéndoles a los empleados ocuparlos como ellos quieran. Sin embargo, sin una cultura de la seguridad informática, el uso descuidado de estos dispositivos puede generar varias amenazas y riesgos que no se tenían contempladas en los esquemas de seguridad desarrollados por el área de TI.

Por lo tanto, el problema que aborda esta tesis es el conjunto de riegos que implica el uso descontrolado de las tecnologías de los dispositivos móviles en las organizaciones.

Preguntas de investigación

Las preguntas de investigación que plantea esta tesis son:

¿Cuáles son los riesgos que conlleva el aceptar la política de BYOD en las empresas?

¿Existe un modelo que pueda implementarse para contrarrestar los riesgos de la implementación de la política BYOD en una empresa?

Objetivos de investigación

Los objetivos que propone este trabajo son:

- Detectar los riesgos al aceptar la política BYOD en las empresas.
- Proponer un modelo de seguridad para contrarrestar los riesgos de la implementación de la política BYOD en las empresas.

Alcances y límites

Esta es una investigación sobre los problemas a los que se están enfrentando los administradores de TI con el aumento masivo de los dispositivos móviles y el paradigma de *Cloud Computing*. Además se busca proponer un modelo de seguridad que sea de utilidad y pueda ser implementado en el futuro.

A pesar de que el tema de BYOD no sólo se encuentra en empresas, sino también en organizaciones gubernamentales y educativas, esta tesis solo abarcará el enfoque empresarial y de organizaciones gubernamentales. Además, sólo se orientará a dispositivos móviles que utilicen el sistema operativo Android cuyas versiones sean Gingerbread, Ice Cream y Sandwich Jelly Bean, por ser las versiones más usadas hasta el momento según la comunidad de desarrolladores de Android.

Mucha de la información mostrada en esta tesis hará referencia al país de Estados Unidos, por ser uno de los países donde se encuentra más avanzada esta tendencia. Sin embargo, se buscará mantener un enfoque nacional pensando en que esta tesis pueda servir a los administradores de TI de organizaciones mexicanas.

Aportaciones

La siguiente tesis se desarrolló tomando en cuenta los riesgos y beneficios que presenta la adopción de una política BYOD en las organizaciones. Se espera que esta investigación sobre el *Análisis de riesgo de una política BYOD* mejore la administración de los dispositivos móviles en las organizaciones, además de concientizar a los usuarios sobre los peligros que existen sobre el uso descuidado de los dispositivos móviles.

También se pretende que esta investigación sirva como apoyo para los administradores de TI en el desarrollo de nuevos modelos de administración y seguridad para las organizaciones. Además de cambiar la ideología de los administradores de TI sobre la participación de los usuarios en los modelos de seguridad.

Asimismo esta investigación también pretende ser una fuente de información para los hispanohablantes, debido a que actualmente no existe mucha información sobre este tema en el idioma español.

Metodología

La metodología de investigación que se ocupará en esta tesis será la siguiente.

1. Buscar información sobre el funcionamiento del sistema operativo Android así como sus vulnerabilidades.
2. Analizar el impacto que han tenido los dispositivos móviles en las organizaciones y sus empleados.

1.1. Investigar sobre la tendencia de BYOD

1.2. Investigar sobre el software para administración de dispositivos móviles.

3. Recabar información sobre el paradigma de cómputo en la nube.
4. Buscar casos donde se hayan implementado la política BYOD así como las medidas de seguridad que se utilizaron.
5. Analizar la información obtenida en las etapas anteriores.
6. Elaboración de una propuesta de seguridad.

Estructura capitular

Este trabajo de investigación está estructurado de la siguiente manera. El primer capítulo se enfocará en los temas de *Seguridad informática*, *dispositivos móviles, administración de los dispositivos móviles y cómputo en la nube.* Donde se muestran los conceptos *riesgo*, *amenaza*, *vulnerabilidad, Android, BYOD, MDM*, entre otros.En el segundo capítulo, llamado *Análisis de riesgo de la política BYOD,* se desarrollarán los problemas que surgen al implementar una política BYOD en las organizaciones. Revelando que existen dos grandes problemas al momento de adoptar esta política dentro de las organizaciones.

En el tercer capítulo, llamado *Propuesta para prevenir riesgos de la política BYOD,* con base en la investigación realizada, se propondrá un modelo para una dependencia de la UNAM, en el cual se abarcó una sección dedicada a las recomendaciones que deben de seguir los trabajadores, así como la mejora de la red de telecomunicaciones y la instalación de dos servidores virtuales para administrar los dispositivos y controlar la fuga de datos.

Por último, en el cuarto capítulo, dedicado a las conclusiones, se reflexionará tanto en los problemas como en los beneficios que causa esta política en las organizaciones.

Resumen

El presente trabajo consiste en la investigación de los riesgos que existen al adoptar una política BYOD dentro de las organizaciones y como esta pueden afectar a las mismas. Tiene como objetivos detectar los riesgos al aceptar esta política dentro de las organizaciones, así como proponer un modelo de seguridad para contrarrestar los riesgos de la implementación de esta.

En esta tesis se hablará de conceptos de seguridad en los dispositivos móviles, malware, cómputo en la nube, entre otros. Además se mencionará la popularidad que han ganado los dispositivos móviles y la evolución que ha tenido el malware hacia los mismos, asimismo las malas costumbres que tienen los empleados frente a los datos personales y a la organización. También como las empresas y los empleados han empezado a adoptar BYOD por las prestaciones y beneficios que ellos perciben, además de cómo han reaccionado los administradores de TI frente a esta nueva tendencia.

Por otra parte también se mencionarán las ventajas y los riesgos que causa el aceptar esta política dentro de las organizaciones, y como se debe de generar nuevas políticas para no perder el control o causar pérdidas a las organizaciones. Además se realizó una propuesta para una dependencia de la UNAM para mitigar ciertos riesgos encontrados al realizar esta tesis.

1 Marco conceptual

1.1 Seguridad

La seguridad es un tema que cubre una amplia variedad de áreas, tan solo en el ámbito de la tecnología se pueden mencionar a la seguridad informática, la seguridad de la información o seguridad de las tecnologías de la información. A pesar de ser una gran variedad de áreas tiene un objetivo en común.

De acuerdo a la Real Academia Española define de la siguiente manera: "Libre y exento de todo peligro, daño o riesgo.", pero esta solo es una falacia, no existe nada que este exento de alguno de estos elementos. Debido a eso el propósito de la seguridad no es llegar a este objetivo, sino más bien lograr la reducción de estos elementos hasta niveles aceptables.

Para lograr este propósito se han creado organizaciones encargas de crear estándares, políticas y normas. No solo enfocadas a la seguridad sino también a la tecnología y al uso a adecuado de esta.

Algunas de estas organizaciones son ENISA (por sus siglas en inglés European Union Agency for Network and Information Security), IEC (por sus siglas en inglés International Electrotechnical Commission) e ISO (por sus siglas en inglés International Organization for Standardization). A continuación se presentarán las siguientes definiciones fundamentales para complementar el tema.

1.1.1 Tecnologías de la información y Comunicación

De acuerdo a Cabrero (1998) las Tecnologías de la información y comunicación (TIC), son aquellas tecnologías que giran en torno a los medios básicos: la informática, la microelectrónica y las telecomunicaciones, pero no sólo de una forma aislada, sino lo que es más significativo de manera interactiva e interconectadas, lo que permite conseguir nuevas realidades comunicativas.

Con base en la definición anterior, se puede decir que son tecnologías para el almacenaje, la recuperación, el procesamiento y la comunicación de la información.

1.1.2 *Seguridad* de las tecnologías de la información

Es la capacidad que tienen los sistemas de TI para proteger la confidencialidad y la integridad de la información, así como ser capaces de poder proporcionar la disponibilidad de los sistemas y posteriormente de la información procesada (Opensecurity Architecture, 2014).

De igual manera ENISA[1] (2013) lo define como: Todos los aspectos relacionados para lograr mantener la confidencialidad, la integridad, la disponibilidad, la autenticidad y fiabilidad de los datos. Se logra que un producto, sistema o servicio se considere que es seguro en la medida en que sus usuarios puedan confiar que funciona de la forma prevista. Para aclarar un poco la definición a continuación se describen los aspectos mencionados anteriormente.

1. Confidencialidad: Garantiza que la información sea accesible sólo para entidades autorizadas proponiendo una serie de reglas que limiten el acceso a cierto tipo de información.
2. Integridad: Se debe de garantizar la consistencia y precisión de los datos durante todo el ciclo de vida. Por lo cual los datos, no deben de sufrir ningún cambio por entidades no autorizadas durante su transferencia por los canales de comunicación.
3. Disponibilidad: Garantiza que los usuarios autorizados tengan acceso a la información y a los recursos relacionados con la misma en cualquier momento que estos lo requieran.

1.1.3 *Tipos de seguridad*

La seguridad se puede clasificar de la siguiente manera:

1. Seguridad física. Engloba lo relacionado con los soportes físicos de la información, por ejemplo, las medidas que se deben de tomar en caso de incendio, sobrecargas eléctricas, inundaciones, accesos físicos a equipos donde sólo personal autorizado tiene acceso, etcétera.
2. Seguridad de la información. Abarca lo que es la preservación de la información frente a amenazas externas o internas. Tomando en cuenta las siguientes características :

[1] ENISA: The European Network and Information Security, es una agencia de la union europea dedicada a la prevensión y orientación de la seguridad de las redes y los problemas de seguridad de la información (tomada de http://searchcloudsecurity.techtarget.com/definition/ENISA-European-Network-and-Information-Security-Agency consultada 29 marzo 2014)

a. Confidencialidad: Garantiza que la información sea accesible sólo para entidades autorizadas proponiendo una serie de reglas que limiten el acceso a cierto tipo de información
b. Integridad: Se debe de garantizar la consistencia y precisión de los datos durante todo el ciclo de vida. Por lo cual los datos no deben de sufrir ningún cambio por entidades no autorizadas durante su transferencia por los canales de comunicación
c. Disponibilidad: Garantiza que los usuarios autorizados tengan acceso a la información y a los recursos relacionados con la misma en cualquier momento que estos lo requieran.

1.1.4 Impacto

El impacto es el resultado de un incidente de seguridad de la información, provocado por una amenaza que afecta a los bienes de la organización, además este puede provocar la destrucción de los bienes, daño a los sistemas de TIC, y comprometiendo la confidencialidad, integridad, disponibilidad, autenticidad y confiabilidad, (ISO, 2011).

1.1.5 Vulnerabilidad

ISO (2009) define vulnerabilidad de la siguiente manera: Una debilidad de un bien o grupo de bienes que puede ser explotada por una o más amenazas. Por otro lado el Instituto Nacional de Normas y Tecnología (NIST por sus siglas en inglés, National Institute of Standards and Technology) la define como: Una falla o debilidad en los procedimientos de seguridad de los sistemas, en el diseño, en la implementación o en los controles internos que pueden ser ejecutados accidentalmente o intencionalmente. Lo cual resulta en una brecha o en una violación de las políticas de seguridad.

Además las vulnerabilidades asociadas a los bienes incluyen debilidades en la organización, la administración, los procedimientos, el personal, la dirección, el hardware, el software o en la información.

Sin embargo estas en sí mismas no causa daño si no es meramente una condición o conjunto de condiciones que pueden permitir a una amenaza afectar a un bien.

Por otro lado SANS Institute lo define como: Un defecto, el cual puede convertirse en una vulnerabilidad, si este presenta un comportamiento que puede ser aprovechado por un tercero, permitiéndole un acceso no autorizado, un escalamiento de privilegios o una denegación de servicio. Tomando en cuenta las anteriores definiciones, se considera que se debe mostrar el ciclo de vida de las vulnerabilidades el cual es propuesto en el artículo de "Windows of vulnerability: a case study analysis."

- Nacimiento: La etapa donde se denotan la creación de las vulnerabilidades en el proceso de desarrollo.
- Descubrimiento: Es la etapa donde se conoce la existencia de la o las vulnerabilidades.
- Divulgación: Se considera ingresada a esta etapa una vez que la vulnerabilidad es conocida por un tercero, la cual pude ser divulgada en su totalidad y públicamente en sitios como *Bugtraq*[2] o en negociaciones entre *Black Hats*.[3]
- Corrección: La fase consiste, en el análisis del desarrollador sobre las vulnerabilidades del sistema las cuales posteriormente solucionará y publicará.
- Publicidad: La fase consiste, en la publicación de la vulnerabilidad.
- Scripting: La fase inicia cuando es generado un programa o se utiliza una herramienta para explotar la vulnerabilidad.
- Muerte: La fase inicia cuando el número de sistemas vulnerados es reducido a una cantidad insignificante. Lo cual sucede por la aplicación de los parches de seguridad, la actualización de los sistemas o la falta de interés de los *Black Hats*.

1.1.6 Bienes

Son todos aquellos conjuntos de recursos (bienes, derechos y servicios) propiedad de una entidad, incluidos los recursos informáticos que apoyan a la misión de la organización, (ISO, 2009).

---

[2] BUGTRAQ: Es una lista de correo electrónico dedicada a temas de seguridad informática. Teniendo como temas, vulnerabilidades en los programas, anuncios de los vendedores sobre temas de seguridad, métodos de explotación y como solucionar estos (tomado de http://www.securityfocus.com/archive consultada el 1 de abril del 2014)

[3] Search Security define Black Hat: como un término usado para describir a los hackers(o crackers) los cuales violan la seguridad de los sistemas computacionales con fines maliciosos, (tomado de http://searchsecurity.techtarget.com/definition/black-hat consultada el 1 de abril del 2014)

Los bienes no sólo son objetos tangibles que la organización puede fácilmente clasificar en términos de valor monetario. La información producida por la organización, las relaciones de confianza y la reputación, son ejemplos de bienes intangibles. Ejemplos de estos son los siguientes:

- Bienes físicos (ej. .Equipo computacional, instalaciones de comunicación, etcétera)
- Información (ej., Documentos, bases de datos, etcétera)
- Software
- Servicios

Por otro lado ISO 27005 los divide en las siguientes categorías:

- Bienes primarios
- Bienes de apoyo

El primero, comprende la información y los procesos de negocio mientras que el segundo comprende el software, hardware, redes, personal y lugares.

1.1.7 Amenaza

Las amenazas tienen la capacidad de causar daño a un bien y por lo tanto a la organización. Este puede suceder por un ataque a la información que se maneja por un sistema o servicio de TIC (Tecnologías de la información y la comunicación), dentro del propio sistema o por otros medios, causando por ejemplo, accesos no autorizados, destrucción, modificaciones, revelación de información, corrupción de información, accesibilidad o perdida de información.

Asimismo surgen a partir de la existencia de vulnerabilidades, que puedan ser aprovechadas por un tercero, e independientemente de que se comprometa o no la seguridad del sistema. Estas mismas pueden originarse desde el medio ambiente o por el hombre, y en este último pueden ser de forma accidental o de manera deliberada (ISO, 2009). A continuación en la **Tabla 1** se muestran algunos ejemplos.

Tabla 1
Tipos de Vulnerabilidades

Humanos		Ambientales
Deliberado	**Accidentales**	
Modificación de información Hackeo de sistemas Códigos Maliciosos Robo	Errores y omisiones Eliminación de archivos Accidentes físicos	Terremotos Inundaciones Incendios Tormentas Eléctricas

Nota: Recuperada de ISO 13335-1 (2009).

Algunas amenazas pueden afectar más que otras a los bienes. Además estas pueden causar diferentes impactos dependiendo del bien afectado. Por ejemplo, un equipo de escritorio sin red que es infectado por un virus informático puede tener un impacto limitado, por otra parte si el equipo se encuentra en una red el impacto puede ser más amplio.

Además existen grupos de amenazas que cambian constantemente con el tiempo y sólo se conocen algunas. De la misma manera, el ambiente cambia con el tiempo y estos cambios pueden impactar la naturaleza de las amenazas y probablemente sus concurrencias.

1.2 Uso de redes inalámbricas públicas

El auge de las tecnologías de la información y comunicación ha cambiado varios paradigmas, como sociales, tecnológicos y de negocios, por mencionar algunos. Permitiendo así ofrecer nuevos servicios o ventajas tecnológicas.

Tan sólo en México en un estudio realizado por CISCO (2012) reveló que el consumidor mexicano de banda ancha cuenta con 2.85 de dispositivos móviles. Donde el 83% tiene una computadora portátil.

Además se ha mostrado un incremento en los teléfonos inteligentes con un 64%, superando a los teléfonos tradicionales los cuales tienen un 55%. Sin embargo, sólo el 30% cuenta con la capacidad de utilizar tecnologías como 3G y 4G.

Un factor interesante, es el comportamiento de los usuarios, la mayoría al momento de comprar un dispositivo móvil llámese; tableta, computadora portátil o teléfono inteligente, buscan que cuente como mínimo con la capacidad de conectarse a redes inalámbricas WIFI. Asimismo los usuarios tienden a preferir conectarse a estas redes que ocupar su conexión de telefonía móvil como se puede ver en la ***Figura* 1**.

También se observa que esta preferencia es significativa en la mayoría de los dispositivos móviles, excepto en el teléfono inteligente donde el uso de una conexión móvil es casi igual al de la red inalámbrica, posiblemente a la portabilidad del mismo.

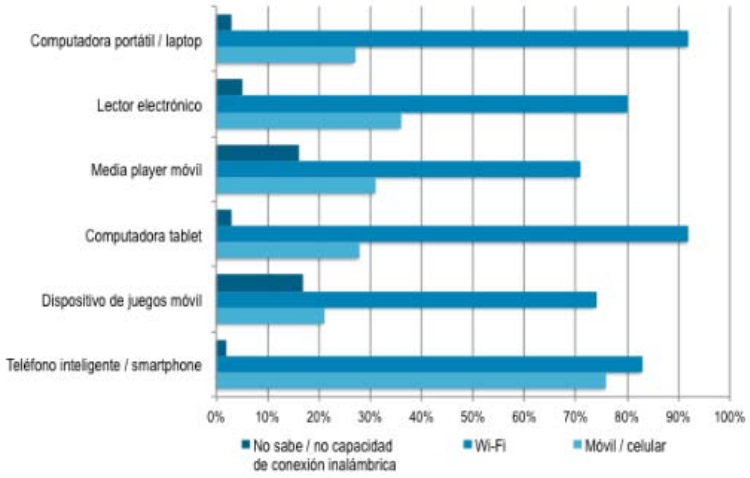

***Figura* 1. Uso de redes inalámbricas**

Nota. Recuperado de CISCO (2012)

Por otro lado los usuarios prefieren las redes inalámbricas WIFI en donde se ofrezca el servicio de manera gratuita, a las que se deba pagar por utilizarlas, como se muestra en la **Tabla 2**. También se puede observar los teléfonos inteligentes como los más utilizados en comparación con los otros dispositivos.

Tabla 2
Porcentaje de conexiones a redes inalámbricas

	Home Wi-Fi	Free Public Wi-Fi	Paid Public Wi-Fi	Any Public Wi-Fi
Laptop etc	82%	42%	11%	45%
MacBook	96%	55%	17%	58%
Laptop/Macbook	84%	44%	12%	67%
IPad	93%	63%	18%	67%
Other Tablet	87%	56%	12%	59%
Any Tablet	91%	62%	16%	69%
Smartphone	82%	64%	12%	67%
iPhone	90%	72%	15%	74%
Smartphone/iPhone	85%	69%	13%	71%
Any Mobile Device	88%	70%	15%	73%

Nota: Recuperado de Kaspersky (2013)

Esta tendencia de los usuarios representa un riesgo tanto para ellos como para las organizaciones. Debido en parte a la configuración de la infraestructura de red del proveedor de este servicio, la cual está orientada a sólo proporcionar el acceso a internet sin preocuparse por la seguridad de los usuarios de su red y por otro lado a las configuraciones de los equipos de los usuarios que tampoco se preocupan por esta.

Este tipo de malas prácticas por parte del usuario posiblemente se deban al desconocimiento de los riesgos que existen o a la falta de conocimiento en el uso del equipo.

Finalmente está es una combinación ideal para un atacante. Donde este puede ingresar a los recursos compartidos de los equipos de los usuarios, monitorear su actividad en la red o falsificar un sitio web, tan sólo por mencionar algunos ejemplos.

1.2.1 Riesgo

Es la posibilidad de que una o múltiples amenazas pueda aprovechar una o múltiples vulnerabilidades de un bien o grupo de bienes y causen daños a la organización, ISO (2009). Los objetivos pueden ser de diferentes aspectos, por ejemplo, financieros, de salud, seguridad, etcétera. De igual manera aplican a diferentes niveles como productos, proyectos o a toda la organización.

También el riesgo se caracteriza por una combinación de dos factores, la probabilidad de que ocurra un suceso y su impacto. Cualquier cambio en los bienes, amenazas, vulnerabilidades y en los propios procedimientos de seguridad puede tener efectos significativos en los riesgos. Tomando en cuenta estas definiciones, ENISA considera los elementos del riesgo en un diagrama que se muestra en la Figura 2.

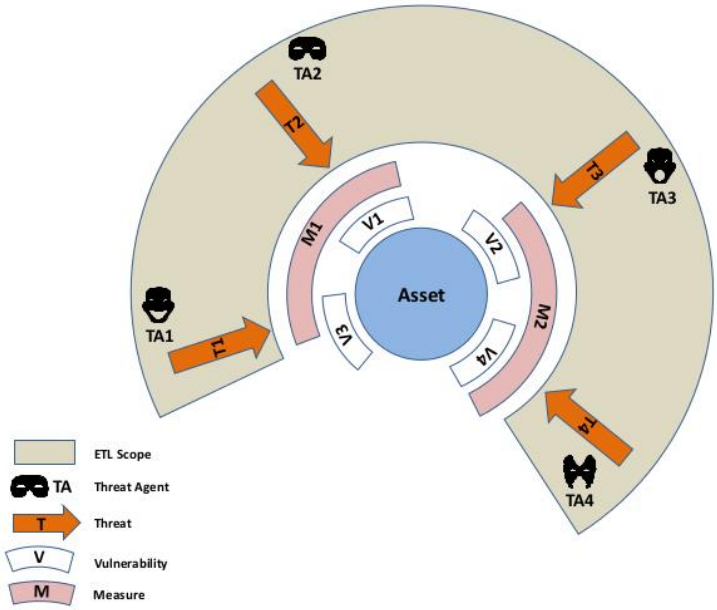

Figura 2. Elementos del riesgo

Nota. Recuperado de ENISA (2013).

En el cual se muestran los actores de las amenazas (TA), el despliegue de las amenazas (T), las cuales intentan explotar alguna vulnerabilidad (V) en los activos de las empresas, la implementación de medidas de seguridad (M) por el propietario de los activos, el cual elimina los efectos negativos de las amenazas.

1.2.2 Políticas de seguridad informática

Las políticas de seguridad informática son un conjunto de reglas y prácticas que regulan la manera en que se deben de dirigir y proteger los recursos de una organización. Teniendo estas como objetivo la implementación de una serie de leyes, normas, estándares y prácticas que garanticen la confidencialidad, seguridad y disponibilidad de la información, además de ser entendidas y ejecutadas por todos aquellos miembros de la organización a quienes van dirigidas.

La RFC 1244 (1991) define Política de Seguridad como: una declaración de intenciones de alto nivel que cubre la seguridad de los sistemas informáticos y que proporciona las bases para definir y delimitar responsabilidades para las diversas actuaciones técnicas y organizativas que se requerirán.

1.3 Dispositivos móviles

El desarrollo de las TIC ha permitido avances en diversas áreas como, son los dispositivos móviles y la telefonía móvil. Permitiendo así ofrecer aplicaciones más sofisticadas y con un mejor proceso de desarrollo para la creciente demanda de los consumidores.

Tal es la importancia que están teniendo estos dispositivos en la sociedad actual, que han empezado a cambiar paradigmas tanto en las personas como en las organizaciones.

A continuación se desarrollará uno de estos paradigmas además de las herramientas que se han desarrollado para lograr una mejor administración y control del mismo.

1.3.1 BYOD

1.3.1.1 Introducción

En el mundo de los teléfonos inteligentes y las tabletas, ha aparecido un nuevo paradigma conocido como “Bring Your Own Device” (BYOD, por sus siglas en inglés), que ha llevado a los dispositivos móviles hacia un uso más empresarial. Este consiste en que los empleados llevan sus dispositivos móviles personales a sus lugares de trabajo y los utilicen para desempeñar sus labores cotidianas como: consultas de correos electrónicos, lectura de documentos, edición, carga y descarga de archivos, entre otros.

Pillay, Diaki y Nham (2013) lo mencionan como la estrategia que permite tanto a los empleados, socios comerciales y otros usuarios utilizar un dispositivo móvil elegido por ellos para ejecutar aplicaciones y acceder a recursos de la empresa.

Estos dispositivos móviles llámense teléfonos inteligentes, tabletas o phablets combinan varias características, como son la facilidad de transporte, la capacidad de conectarse a redes inalámbricas, la reproducción de archivos multimedia, el envío de documentos y por supuesto el poder realizar llamadas o videollamadas, sólo por mencionar algunas. Estas características han logrado crear un ambiente perfecto para el desarrollo diario de la vida laboral permitiendo realizar diversas tareas en cualquier momento y lugar.

Los usuarios actualmente compran un dispositivo móvil no sólo para utilizarlo de manera personal sino también como apoyo para desempeñar sus actividades laborales en las organizaciones sin importarles si cuentan o no con el soporte del departamento de TI. En un estudio realizado por la empresa Forrester, muestra que el 33% de los usuarios adquieren un dispositivo móvil en específico para ayudarles a desempeñar mejor su trabajo. Tokuyoshi (2013) .

Además se creé que en el 2016, un billón de consumidores cuenten con un teléfono inteligente. Tan sólo en Estados Unidos se cuentan con 257 millones de teléfonos inteligentes y 126 millones de tabletas. Asimismo en el 2016, se espera que 350 millones de empleados puedan utilizar su teléfono inteligente en el trabajo. Actualmente solo 200 millones pueden utilizarlo (Disterer & Kleiner, 2013).

Por otro lado BYOD ha ganado fuerza rápidamente, debido a que explota los intereses tanto de los empleados como de las compañías. Por un lado el empleado ya no tiene la necesidad de llevar ambos dispositivitos al trabajo (el teléfono inteligente de la empresa y el personal), además cuenta con la libertad de escoger el dispositivo que se adecué mejor a sus necesidades. De igual manera las empresas ya no tienen la obligación de adquirir y dar soporte a pequeños dispositivos de bajo costo que son fácilmente rotos o perdidos por los empleados.

1.3.1.2 Beneficios

1.3.1.2.1 Reducción de costos

Los empleados al empezar a llevar sus propios dispositivos móviles a las organizaciones, han permitido a estas traspasar los costos de adquisición de hardware a ellos. Además los empleados tienden a actualizar su hardware para estar con lo último en tecnología (Calder, 2013). Siendo esta una de las principales razones para que las organizaciones hayan empezado a migrar a un ambiente BYOD.

Por otra parte, en un estudio conducido por HDI se reveló que el 40% de 844 organizaciones en 35 industrias no proporcionan el soporte para los dispositivos BYOD de sus empleados y estos requieren contactarse directamente con el proveedor para el soporte. (Rains, 2012).

1.3.1.2.2 Accesibilidad

El auge de las TIC ha permitido comunicar a las personas de forma instantánea sin importar dónde se ubiquen, por medio de grandes canales de comunicación y dispositivos electrónicos, que pueden ser tan pequeños como un reloj.

Los dispositivos BYOD de los empleados han aprovechado su portabilidad y estos canales de comunicación para acceder a información de la empresa sin tener la limitante de una ubicación fija.

Una mejor comunicación y accesibilidad de la información proporciona a las organizaciones la capacidad de mejorar sus productos y sus servicios ofrecidos, además de aumentar su valor para los clientes (Calder, 2013).

De igual manera con la evolución de las telecomunicaciones y la portabilidad de los dispositivos móviles, ha mejorado la comunicación en tiempo real entre los empleados y las organizaciones, logrando así mejorar la eficiencia operativa (Management Services, 2012) .

1.3.1.2.3 Satisfacción y productividad de los empleados

La implementación de una política BYOD en las organizaciones, ha empezado a cambiar los hábitos de trabajo de los empleados, debido en parte a la libertad de poder llevar sus propios dispositivos a la oficina y escoger la tecnología que mejor satisfaga sus necesidades Por ejemplo, un ejecutivo de

ventas puede llevar su MacBook, mientras que un representante de ventas puede preferir usar una tableta para tomar notas en una reunión.

Esta libertad les permite utilizar sus dispositivos después de las horas de trabajo o durante periodos fuera de la oficina para realizar tareas básicas, las cuales reducen los tiempos de espera y permiten una resolución más rápida de las tareas. Tiempos de respuestas más cortos y operaciones de negocio más fluidas conducen a una mejor productividad (Alleau & Desemery, 2013).

De acuerdo a Mont (2012), cuando la política BYOD es implementada en una organización, los empleados tienden a cuidar más su dispositivo, debido a la existencia de un sentimiento personal de propiedad, permitiendo así a las organizaciones disminuir los costos de hardware y mantenimiento.

Además en un ambiente BYOD, los empleados no tienen la necesidad de llevar múltiples dispositivos como: el personal y el de la organización. Estos se sienten más confortables trabajando con sus propios equipos, logrando así aumenta su nivel de satisfacción en el trabajo. De acuerdo a un estudio realizado por Alleau & Desemery (2013), 19% de las empresas percibían a BYOD como una manera de permitir la satisfacción de los empleados, mientras que el 17% sintió que BYOD podría mejorar la productividad en las áreas de trabajo.

De acuerdo a Mont (2012) el 64% de los empleados de empresas multinacionales en toda Asia y la región de Australia había aumentado su productividad debido a la eficiencia y a la facilidad de uso de los dispositivos móviles personales con fines de trabajo que a su vez conducen a la satisfacción y felicidad del empleado. Además al utilizar sus dispositivos personales añaden un extra de 240 horas laborales que los que no lo hicieron (Alleau & Desemery, 2013).

1.3.1.3 Peligros

La implementación de la política BYOD en las organizaciones, como se ha mencionado en puntos anteriores ofrece grandes beneficios para ambas partes. Pero a su vez existen problemas y peligros que si no son tomados en cuenta pueden provocar más dificultades que ventajas.

De acuerdo a Singh (2012), BYOD disminuye los activos y los costos de hardware, pero aumenta la suma de dinero que se debe de gastar para solucionar los problemas de seguridad. Debido a que después de implementar esta política, los datos de la empresa son más propensos a ser robados en los dispositivos de los empleados.

De igual manera en estudio realizado por la empresa Forrester reveló que aunque el gasto de la compra y el soporte de los dispositivos para el usuario final se redujeron cuando BYOD fue implementado, el costo de las aplicaciones de seguridad, la infraestructura back-end y el incumplimiento de las normas tendieron a aumentar (Pillay, Diaki, & Nham, 2013).

Asimismo Kaspersky Lab, una firma de seguridad digital, reveló que una de cada tres organizaciones permite el uso de teléfonos inteligentes sin ninguna restricción a los recursos de la misma. Por otra parte, una de cada cinco empresas en el mismo estudio admitió que perdieron información, después de que un dispositivo móvil fuera perdido o robado (Ackerman, 2013).

Con base en los anteriores estudios, se observa como uno de los grandes problemas de implementar la política BYOD, es la falta de control en el contenido de los dispositivos de los empleados.

Además otro elemento que debe de tomarse en cuenta es la seguridad en redes inalámbricas, debido a la tendencia de los usuarios a conectarse a redes públicas sin utilizar ninguna medida de protección. Que puede poner en riesgo la información de la organización (Tokuyoshi, 2013).

1.3.1.3.1 Fuga de Datos

La fuga de datos es uno de los problemas más relevantes de BYOD, debido a la falta de educación de los usuarios al momento de utilizar sus dispositivos para desempeñar sus actividades. Descargas de documentos, correos electrónicos o contraseñas, son algunos de los datos almacenados en estos equipos, en donde el usuario no toma en cuenta la sensibilidad de los mismos y no implementa alguna medida de protección.

De acuerdo a Pillay, Diaki & Nham (2013) la pérdida o robo de dispositivos BYOD es el principal riesgo, no solo por la pérdida de los datos, sino también porque estos son perdidos en tiempos cruciales, dificultando generar una ventaja competitiva sobre los demás competidores.

Asimismo un estudio realizado en el Reino Unido, menciona que cuando los empleados cambian o venden sus dispositivos móviles para actualizarlos por unos más recientes, la información sensible y confidencial es transmitida a usuarios no autorizados (Pillay, Diaki, & Nham, 2013).

Además de la pérdida o robo de los dispositivos BYOD otro factor que afecta a las organizaciones, es la dificultad para determinar el origen de la fuga de datos. Si esta es detectada a tiempo se podría tomar medidas para minimizar el impacto.

Gwen Hassan, administradora del corporativo Navistar afirma que el problema se intensifica cuando los ejecutivos ocupan sus propios dispositivos móviles para manejar datos de la compañía sin entender sobre tecnología, originando la fuga de datos sin darse cuenta (Mont, 2012).

1.3.1.3.2 Falta de control sobre los datos y los dispositivos

Uno de los problemas en las organizaciones ha sido la falta de control sobre los empleados, algunos de estos intencionalmente pasan por alto las políticas y las normas de seguridad para poder así utilizar sus dispositivos de una manera libre y en consecuencia pone en riesgo los bienes de las organizaciones.

Además los empleados con conocimientos técnicos pueden saltar más fácilmente las restricciones establecidas por los administradores de TI (Potts, 2012). Por ejemplo el acceso a sitios restringidos como Facebook o Twitter a través de un proxy.

Por otra parte, en un estudio realizado por Deloitte (2013) encontró que el incremento del uso de los dispositivos móviles en el área de trabajo, se considera como el segundo mayor riesgo para la seguridad de las organizaciones.

De igual manera el 91% de las empresas considera la seguridad de los datos como su prioridad número uno, por otro lado el 21% no cuenta con una política para protegerse contra el intercambio de datos a través de plataformas públicas (Khanna, 2013).

Servicios como iCloud de Apple, OneDrive de Microsoft o Dropbox, además de ofrecer almacenamiento en sus servidores cuentan con la funcionalidad de auto-sincronización de carpetas y archivos, permitiendo cargar estos mismos de una manera más rápida y transparente para el usuario.

Esta funcionalidad para las organizaciones representa un riesgo y una violación en el control de los datos, debido a que la información de estas ya no se encuentra bajo su control. Además el riesgo aumenta cuando esta información no se encuentra bien administrada y supervisada (Howie, 2012).

Por lo tanto cuando los empleados evaden las políticas establecidas, y sus equipos son robados, los datos no pueden ser eliminados remotamente (Potts, 2012).

1.3.1.3.3 Malware

El rápido aumento del uso de los dispositivos móviles y la amplia variedad de aplicaciones que son desarrollados para estos. Han logrado atraer la atención de cibercriminales que aprovechan por un

lado las vulnerabilidades tanto de los dispositivos como de las aplicaciones para sustraer información que puede ser personal, laboral o financiera. Y por otro por medio de desarrollo malware.

Osterman (2012) menciona que existe una mayor probabilidad de infección por malware, especialmente para los dispositivos Android. Además F-Secure (2012) en los primeros cuatro meses del 2012 reveló un incremento de 10% a 37% en el número de familias y variantes de malware para este sistema operativo, además el número de software maliciosos enfocado a las aplicaciones de este sistema había aumentado de 139 a 3096 (Osterman, 2012).

De igual manera TrendLabs (2012) identificó 5000 aplicaciones Android con código malicioso que fueron encontradas en los primeros cuatro meses del 2012. Las investigaciones también revelaron que fueron descargadas 700,000 veces antes de ser removidas por Google de su tienda (Google Play).

Actualmente, los tipos más comunes de malware en dispositivos móviles son encontrados en versiones gratuitas que son proporcionadas en sitios no oficiales. Estas aplicaciones al ser descargadas e instaladas por los empleados en sus dispositivos móviles, crean vulnerabilidades en los mismos haciéndolos propensos a ataques y no sólo poniendo en riesgo su información sino también la de la organización. Por otro lado el incremento en el número de aplicaciones para dispositivos móviles también incrementa la probabilidad de que algunas tengan código malicioso o huecos de seguridad (EY, 2013).

1.3.2 Administración de dispositivos móviles

1.3.2.1 Introducción

Con el rápido aumento de los dispositivos móviles y la aparición de paradigmas como BYOD. Las organizaciones y más específicamente el área de TI han empezado a tomar en cuenta los riesgos que contrae el acceso sin restricciones a estos nuevos elementos.

Desarrollando nuevas herramientas para facilitar el control y la administración de estos elementos. Por ejemplo Mobile Device Management (MDM, por sus siglas en inglés) y Mobile Applications Management (MAM, por sus siglas en inglés), orientadas para la administración de los dispositivos móviles que ingresan a recursos de la organización, cada uno con un mayor o menor impacto en el usuario. En la siguiente sección se desarrollaran las dos soluciones mencionadas.

1.3.2.2 Mobile Device Management (MDM)

1.3.2.2.1 Introducción

Mobile Device Management es considerado esencial para la administración en el área TI, porqué este se enfoca tanto en la seguridad como en la administración de los dispositivos móviles, permitiendo a los administradores de TI generar nuevas políticas para la gestión de los dispositivos móviles.

1.3.2.2.2 Definiciones

A continuación se presentaran algunas definiciones sobre MDM.

Gartner (2013) lo define de la siguiente manera, administración de dispositivos móviles (MDM, por sus siglas en inglés) es un software que proporciona las funciones de distribución de software, administración de políticas, administración de inventarios, administración de seguridad y administración de servicios para los teléfonos inteligentes y tabletas.

Por otra parte Steele (2013) lo define como un tipo de software que permite asegurar, monitorear y administrar dispositivos móviles sin importar el operador de telefonía o proveedor de servicios. Además permiten realizar instalaciones de aplicaciones, sincronización de archivos, acceso a dispositivos, rastreo y localización de equipos de manera remota.

1.3.2.2.3 Características

Algunas de las características más representativas de acuerdo a Ford (2014) son:

- Despliegue de opciones que incluyen locales, cloud y SaaS.
- Soporte para una gran cantidad de plataformas.
- Supervisión del uso de las aplicaciones.
- Administración de contenido y documentos.
- Administración de la red (uso de WIFI, uso de datos, bloqueo de servicios, etcétera.).
- Administración de servicios de monitoreo y administración del soporte técnico.
- Administración de aplicaciones (listas negras y blancas).
- Borrado parcial o total de los dispositivos remotamente.
- Capacidad de localización y bloqueo remoto de los dispositivos.
- Configuración de monitoreo y auditoria de los dispositivos.

1.3.2.3 Mobile Application Management (MAM)

1.3.2.3.1 Introducción

Con el auge de la política BYOD, las organizaciones han empezado a implementar medidas para controlar la información almacenada por los empleados en sus dispositivos móviles pero sin dañar las ventajas que esta política ofrece tanto a ellas como a sus empleados.

Mobile Application Management (MAM por sus siglas en inglés) se centra en el bloqueo de las aplicaciones de los dispositivos móviles, permitiendo un acceso a la información más segura y controlada, además da la capacidad a los administradores de TI de administrar y controlar el uso de aplicaciones que son específicas para el desempeño de las labores de los empleados. A continuación se presentan algunas definiciones sobre MAM.

1.3.2.3.2 Definiciones

De acuerdo a Rouse (2014), es el desarrollo y administración de software empresarial para los usuarios finales de las empresas y sus dispositivos personales.

Por otro lado Janssen (2014) lo define como un tipo de herramienta de administración de la seguridad orientada al uso específico de aplicaciones móviles.

1.3.2.3.3 Características

Algunas de las características más representativas del MAM de acuerdo a Gruman (2011) son las siguientes.

- Instalación de aplicaciones
- Actualización de aplicaciones
- Monitoreo de rendimiento de las aplicaciones
- Autenticación de usuarios
- Reportes de errores
- Control de acceso para usuarios y grupos
- Administración del mantenimiento.
- Configuración de la aplicación
- Reportes y seguimientos

- Análisis de uso
- Borrado de aplicaciones.

1.4 Sistema Operativo Android

1.4.1 Introducción

Android es un sistema operativo para dispositivos móviles basado en el núcleo del sistema operativo GNU/Linux inicialmente en su versión 2.6 y desarrollado por la empresa estadounidense Google. Este sistema operativo es utilizado en más de mil millones de dispositivos en todo el mundo, desde teléfonos inteligentes y tabletas hasta relojes, televisiones y automóviles.

Además permite a sus usuarios acceder a una vasta cantidad de aplicaciones para sus dispositivos, además de las aplicaciones principales de dicha compañía como Gmail. YouTube y Google Maps.

Este sistema operativo se encuentra estructurado en varias capas, las cuales serán detalladas en los siguientes apartados.

1.4.2 Estructura del sistema operativo

El sistema operativo Android, se encuentra estructurado en forma de pila, dividido en cinco capas principales. Este tipo de estructura permite tanto a desarrolladores como a fabricantes trabajar de forma independientemente. Como se observa en la ***Figura* 3**.

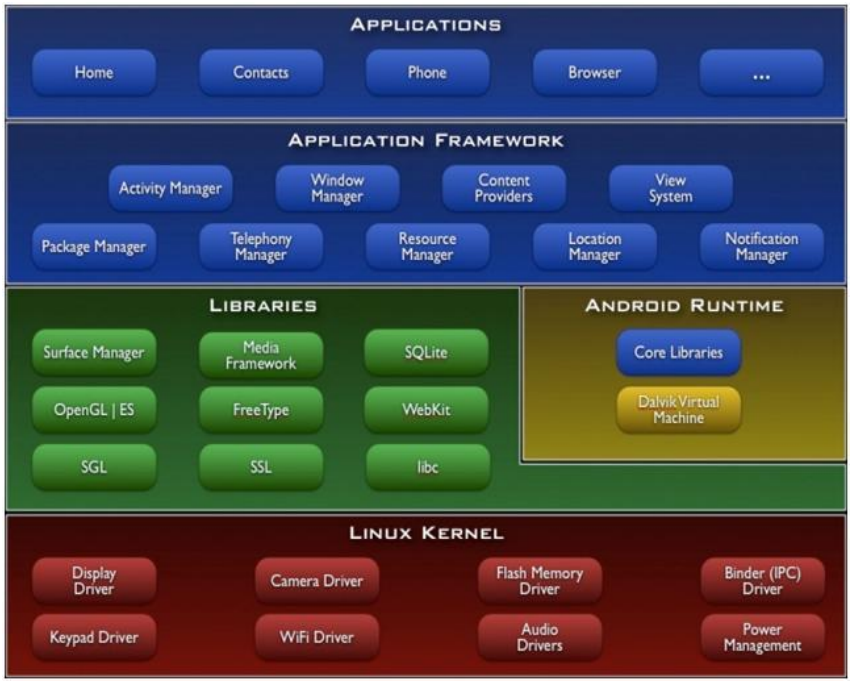

***Figura* 3. Estructura de Android**

Nota. Recuperado de Gupta (2014)

1.4.2.1 Kernel

En la base, se encuentra un Kernel de Linux el cual ha sido modificado para mejorar el rendimiento en dispositivos móviles. Inicialmente el sistema operativo Android se basó en la versión 2.6 del Kernel de Linux. Actualmente se encuentra basado en la versión 3.1.

El Kernel de Linux interactúa directamente con los componentes de hardware. Como resultado, los controladores que son escritos en el espacio de Kernel de Linux operan más rápido que los escritos fuera de él. Algunas de las funciones que controla, son: el sintonizador de la radio, la cámara, la carga de la batería, botones del dispositivo, entre otros (Gupta, 2014).

1.4.2.2 Frameworks de Aplicaciones

El sistema operativo Android, proporciona a los desarrolladores las herramientas y la capacidad para el desarrollo de aplicaciones, además de permitirles ofertarlas en la Google Play Store.

Los desarrolladores cuentan con acceso a la misma [4]API (por sus siglas en inglés, Application Programming Interface) que es usada dentro del núcleo de las aplicaciones, además del acceso a todas las bibliotecas de java que existen para el desarrollo de las aplicaciones de Android (Gupta, 2014).

1.4.2.3 Bibliotecas

Este nivel se encuentra dividido en dos partes: las bibliotecas nativas del sistema operativo Android y Android Runtime.

Las bibliotecas son compiladas y preinstaladas en binarios C/C++ que el sistema operativo depende. En la siguiente sección se listan algunas de las bibliotecas más representativas del sistema operativo Android (Gupta, 2014)

1.4.2.4 Surface Manager

Es la encargada de componer los diferentes elementos de navegación de pantalla. Gestiona también las ventanas pertenecientes a las distintas aplicaciones activas en cada momento. (Cancela García & Ostos Gutiérrez)

1.4.2.5 SQLite

Es una base de datos usada para la información persistente a través de las sesiones de un dispositivo Android. La base de datos SQLite es almacenada dentro del dispositivo, así como en la tarjeta SD y puede ser intercambiada sin sufrir perdida de datos (Gupta, 2014).

1.4.2.6 WebKit

Permite a HTML hacer rendered[5] y mostrarlo en Android más rápidamente y eficientemente. Este es el motor del navegador por defecto en el sistema operativo Android y está disponible para las aplicaciones de terceros (Gupta, 2014).

---

[4] Techterms lo define como. Como un conjunto de comandos, funciones y protocolos que utilizan los programadores para el desarrollarlo software de un sistema operativo en específico.
(tomado de http://www.techterms.com/definition/api consultada el 1 de Julio del 2014)

[5] Thefreedictionary lo define como: Computer Science to convert (graphics) from a file into visual form, as on a video display. (tomado de http://www.thefreedictionary.com/render)

1.4.2.7 OpenGL/ES

OpenGL es el motor de los procesos gráficos del sistema operativo Android. OpenGL permite hacer render tanto a Objetos en 2D y 3D en el sistema Android. Además permite realizar aceleraciones de hardware en dispositivos que cuenten con un chip dedicado a los gráficos (Gupta, 2014).

1.4.2.8 Android Runtime

Dentro del Android Runtime se encuentran dos componentes principales: El núcleo de las bibliotecas de Java que proporcionan el sistema Operativo Android, y la máquina virtual Dalvik. La máquina virtual Dalvik es una implementación de java realizada por Google, optimizada para dispositivos móviles (Gupta, 2014)

1.4.2.9 Aplicaciones

En la parte más alta se encuentran las aplicaciones, estas son las herramientas que todos los usuarios utilizan diariamente. El S.O Android proporciona un conjunto amplio de aplicaciones robustas que soportan todas las necesidades de un teléfono inteligente, como son: mensajes de texto, correo electrónico, navegadores web y una amplia cantidad de aplicaciones de terceros.

Las aplicaciones son principalmente escritas en Java y son distribuidas a través de varios medios. El más común y seguro es Google Play Store (anteriormente conocido como Android Marketplace). Además el sistema operativo Android, también permite instalar aplicaciones a través de una conexión USB o por una tarjeta SD (Gupta, 2014).

1.4.3 Versiones de Android

1.4.3.1 Astro (1.0)

Fue la primera versión del sistema operativo Android, lanzada como beta en noviembre del año 2007 y lanzada al público en septiembre del año 2008 para el HTC Dream (conocido como Google Phone) (Gupta, 2014).

1.4.3.2 Cupcake (1.5)

Fue lanzada el 30 de abril del año 2009. Cupcake fue basada en el Kernel de Linux 2.6.27 esta versión incluía nuevas características para los usuarios y los desarrolladores. Los mayores cambios fueron el soporte para teclados virtuales, soporte para widgets[6] sobre la pantalla de inicio, animaciones en distintos lugares y auto emparejamiento (Gupta, 2014).

1.4.3.3 Donut (1.6)

Lanzada el 15 de septiembre del año 2009, con esta versión se actualizó el Kernel de Linux de la versión 2.6.24 a 2.6.29, además de nuevas características y soporte para dispositivos. Las características más representativas fueron búsquedas por medio de voz y texto en la libreta de direcciones y en la web, el soporte para resoluciones WVGA y mejoras en la funcionalidad y velocidad de la cámara (Gupta, 2014).

1.4.3.4 Éclair (2.0/2.1)

Fue lanzada el 26 de octubre del 2009. Éclair siguió utilizando la versión 2.6.29 del Kernel de Linux. Esta incluía varios cambios en la interfaz del sistema operativo, además de mejoras significativas en la velocidad de respuesta de las aplicaciones.

El 3 de diciembre del año 2009, Google actualizó la versión de Android 2.0.1 para solucionar algunas fallas menores y además actualizó la API para los desarrolladores. No fue hasta el 12 de enero del año 2010 que el sistema operativo Android fue actualizado a la versión 2.1. Igual que la actualización de diciembre, la versión 2.1 incluía actualizaciones para la API y la solución de errores (Gupta, 2014).

1.4.3.5 Froyo (2.2.x)

Froyo fue lanzado el 20 de mayo del año 2010, con el Kernel 2.6.32. Google Nexus fue el primer dispositivo en el mercado en tener la versión de Froyo. Se agregaron nuevas características

[6] Thefreedicctionary lo define como: un programa que realiza alguna simple función, como proporcionar el reporte del tiempo o el estado de la bolsa, y puede ser accesado desde el escritorio de una computadora, una página web o un teléfono móvil. (tomado de http://www.thefreedictionary.com/widgets consultado el 4 de abril del 2014)

significativas como el soporte para Adobe Flash, C2DM (por sus siglas en inglés, Android Cloud to Device Messaging)[7], funcionalidad para WIFI hotspot y optimización del rendimiento (Gupta, 2014).

Tres actualizaciones para esta versión de Android: 2.2.1 el 18 de enero del 2011, 2.2.2 el 22 de enero del 2011 y la 2.2.3 el 21 de noviembre del 2011. Estas actualizaciones fueron principalmente para solucionar errores menores y realizar actualizaciones de seguridad.

1.4.3.6 Gingerbread (2.3.x)

Fue lanzada el 6 de diciembre del año 2010, se basó en la versión 2.6.35 del Kernel de Linux. Las características principales de Gingerbread fueron: soporte para WXGA y otras resoluciones extra grandes, mejoras para el teclado virtual, soportes para sensores internos (giroscopios y barómetros), soporte para múltiples cámaras y cámaras frontales, y la capacidad para leer etiquetas NFC (por sus siglas en inglés, Near Field Communication) (Gupta, 2014).

Cinco actualizaciones fueron lanzadas para Gingerbread, 2.3.3-7 de febrero a septiembre del 2011. Con estas actualizaciones se incluyeron nuevas funcionalidades, además de la corrección de varios errores y problemas de seguridad. Una de las características más significativas fue la implementación de AOA (por sus siglas en inglés, Android Open Accesory), el cual permite comunicarse con un dispositivo Android a través de un cable USB o una conexión Bluetooth (Gupta, 2014).

1.4.3.7 Honeycomb (3.x)

Honeycomb fue lanzada en febrero del año 2012. Honeycomb fue la primera versión de Android lanzada para tabletas, teniendo como anfitrión a Motorola Xoom. Honeycomb fue ajustada para permitir una mejor experiencia en resoluciones grandes. Esto incluía un rediseño del teclado virtual, una barra de estado que permitiera el rápido acceso a las notificaciones y a la navegación, múltiples pestañas de navegación para permitir un uso más fácil y soporte para múltiples procesadores (Gupta, 2014).

---

[7] Google Developers lo define como: Un servicio que ayuda a los desarrolladores a enviar datos desde los servidores de sus aplicaciones en los dispositivos Android. El servicio proporciona un mecanismo sencillo y ligero para que los servidores puedan comunicarse con las aplicaciones móviles en busca de actualizaciones o datos de usuarios, (tomado de https://developers.google.com/android/c2dm/?hl=es consultada el 7 de abril del 2014)

Honeycomb tuvo seis actualizaciones. Estas incluían, soporte para accesorios USB como teclados, joysticks y otros dispositivos de interfaz humana (por sus siglas en inglés, HID´S) además de mejor compatibilidad con aplicaciones que no eran diseñadas para tabletas (Gupta, 2014).

1.4.3.8 Ice Cream Sandwich (4.0.x)

Ice Cream Sandwich (ICS) fue liberada el 19 de octubre del 2011, se basó en la versión del 3.0.1 del Kernel de Linux. ICS incluía mejoras y nuevas funcionalidades para la interfaz de usuario de Android. Algunas de las características que incluía eran: un lanzador personalizable, pestañas para el navegador web, desbloqueo del dispositivo por medio de reconocimiento facial, un editor fotográfico, aceleración de hardware para la interfaz de usuario y nuevos botones (Gupta, 2014).

Tuvo cuatro actualizaciones que fueron lanzadas en el periodo del mes de noviembre del 2011 al mes de marzo del 2012. Las actualizaciones principalmente mejoraron el rendimiento de la cámara, además de la solución de errores y parches de seguridad (Gupta, 2014).

1.4.3.9 Jelly Bean (4.1.x)

Fue liberado el 9 de julio del 2012, este se basó en la versión 3.1.10 del Kernel de Linux. Jelly Bean realizó mejoras en la interfaz de usuario y en el audio de los dispositivos Android (Gupta, 2014).

Jelly Bean tuvo dos actualizaciones que fueron liberadas en el periodo de noviembre del 2012 a julio del 2013, en las cuales se incluía cambio en la versión del Kernel de Linux de la 3.1.10 a la 3.4.0, se incluyó OpenGL ES 3.0 para mejorar el rendimiento de los gráficos de los juegos, actualización de los derechos digitales para la administración de las APIs, notificaciones expandibles, filtrado de notificaciones de aplicaciones específicas y multicanales de audio (Gupta, 2014).

1.4.3.10 KitKat (4.4.x)

KitKat es la versión más reciente del Sistema Operativo Android, liberada el 3 de septiembre del 2013. Esta incluyó optimización del rendimiento en dispositivos con poca RAM, capacidades de impresión inalámbrica, además de una nueva y experimental máquina virtual llamada ART, la cual reemplaza a la máquina virtual Dalvik.

1.4.4 Financiamiento

Google recolecta dinero a través de publicidad en los navegadores y en la Google Play Store. Google además tiene los derechos de autor de las aplicaciones en Google Play (Gupta, 2014).

Google obtiene miles de millones de dólares en ingresos a partir de la publicidad en los sitios de Google y en los sitios de redes sociales a través de AdSense. En el tercer trimestre del 2012, los ingresos totales de la publicidad de Google fueron de más de 14 mil millones de dólares.

1.4.5 Seguridad en el sistema operativo Android

Con la introducción del mercado de aplicaciones, el modelo de seguridad de Android ha crecido y se ha vuelto complejo. Por un lado Android debe asegurar sus propias aplicaciones y por el otro debe de proporcionar un nivel de seguridad para las aplicaciones de terceros. Además su sistema de seguridad debe de ser lo suficientemente simple para que el usuario pueda comprenderlo, además de permitir decidir a los usuarios si desea o no utilizar las aplicaciones (Gupta, 2014).

Android solucionó este problema con el uso de permisos. Con el fin de tener acceso a determinadas funciones del dispositivo debe de registrarse en el permiso correspondiente. Por ejemplo para que la aplicación pueda utilizar el servicio de datos o de WI-FI, esta debe de ser registrada para tener permiso de internet.

Otra sección en la parte de seguridad de las aplicaciones, es la separación de información entre las aplicaciones. Si una aplicación pudiera interactuar libremente con otra dentro del dispositivo, sería un gran problema. El sistema de mensajerías interna de aplicaciones de Android utiliza el concepto de intentos para transmitir información a través del sistema operativo.

Un intento es simplemente un mensaje de forma libre producida por una aplicación y entregada a Android. Este mensaje puede contener distintos tipos de datos. Existen dos tipos, una intención implícita y otra explicita. La intención implícita es un mensaje que existe para cualquier aplicación pueda acceder a esta. Por ejemplo al hacer clic en un enlace este mostrará una ventana permitiendo escoger entre todas las aplicaciones disponibles que puedan visualizar el enlace. En el fondo la aplicación ejecutó una intención implícita y esta fue trasmitida a todas las aplicaciones disponibles capaces de visualizar la petición.

Intención explicitas, por otro lado se orienta a aplicaciones específicas, donde la intención sólo puede ser vista y manejada únicamente por la aplicación para la cual había sido hecha.

Las aplicaciones de terceros también operan como usuarios independientes en el sistema operativo. Lo cual significa que las aplicaciones de terceros no pueden acceder a los archivos y a los recursos que otras aplicaciones poseen. La excepción a esto es con las aplicaciones nativas del sistema operativo. Las aplicaciones del sistema pueden acceder a todas las secciones del dispositivo que se requieran para la operación.

Android proporciona varias funciones de seguridad para garantizar la seguridad de los usuarios y sus datos. Algunas de las funciones que ofrece Android son las siguientes: Bloqueo de pantalla, cifrado de textos y correo electrónico, múltiples tipos de contraseñas y contraseñas adicionales para acceder a determinadas secciones del dispositivo.

También se han desarrollado aplicaciones por parte de terceros para garantizar la seguridad de los dispositivos. Existen aplicaciones que pueden encontrar el dispositivo si este es perdido o robado, borrado de datos del teléfono, bloqueo del teléfono de forma remota por mencionar algunas.

1.5 Cómputo en la nube

Con la evolución de las TIC, surge un nuevo paradigma, conocido como cómputo en la nube (*Cloud Computing*), este no es una nueva tecnología, sino la combinación de varias tecnologías ya existentes que han madurado de diferentes maneras y de diferentes formas, permitiendo crear un ecosistema idóneo para la creación de este nuevo paradigma.

Teniendo como base la abstracción y la virtualización, aunque originalmente NIS contemplaba cómputo en la nube sin la virtualización, con el tiempo ha decidido aceptarlo por las posibilidades que ofrece la virtualización.

Cómputo en la nube ofrece varias ventajas como son: la reducción de costos de infraestructura de TI, una amplia capacidad de almacenamiento, misma que se puede acceder desde cualquier lugar y en cualquier momento, elasticidad, cómputo distribuido y web 2.0, además de modelos de negocio como pay as you go.

1.5.1 Definición

Existen varias definiciones sobre lo que es el cómputo en la nube. A continuación se citarán algunas de estas. El instituto nacional de estándares y tecnología (NIST, por sus siglas en inglés) lo define de la siguiente manera:

"Un modelo que permite el acceso oblicuo, simple y bajo demanda a un grupo compartido y configurable de recursos de computación (como por ejemplo: servidores, almacenamiento, aplicaciones y servicios) que pueden ser rápidamente aprovisionados y liberados con el mínimo esfuerzo administrativo o intervención del proveedor que da dichos servicios" (NIST, 2011).

Por otra parte Gartner (2008) la define de la siguiente manera:

"Un estilo de computación en donde, de forma masiva y escalable, las capacidades de las tecnologías de la información son proporcionadas como un servicio a clientes externos usando la tecnología de internet".

1.5.2 Características del cómputo en la nube

El paradigma de cómputo en la nube cuenta con las siguientes cinco características:

- Multi-arrendamiento: En el modelo de cómputo en la nube, no sé asignan recursos específicos a un solo usuario a la vez, como se hacía en los antiguos modelos de negocio, sino que se comparte el mismo recurso con múltiples usuarios al mismo tiempo. Los recursos compartidos pueden ser tanto a nivel de red, de almacenamiento o de aplicación.
- Gran escalabilidad: En la actualidad las organizaciones cuentan con cientos o miles de equipos operando dentro de sus instalaciones. El modelo de cómputo en la nube proporciona la capacidad de adquirir equipo de cómputo dependiendo de las necesidades de la empresa y las capacidades de infraestructura a nivel de telecomunicaciones con que cuente la organización.
- Elasticidad: Un usuario puede rápidamente incrementar o reducir sus recursos computacionales dependiendo de sus necesidades, así como liberar recursos de otros cuando estos no sean necesarios
- Pago por uso: Los usuarios pueden aumentar o disminuir sus recursos computacionales dependiendo de sus necesidades, así como liberar los recursos si es que otro usuario los necesita.

- Auto-suministro de recursos: El usuario solamente paga los recursos computacionales que está utilizando y por el tiempo que este los requiera.

1.5.3 Modelos de cómputo en la nube.

The U.S. National Institute of Standars and Technology (NIST, por sus siglas en inglés), divide en dos categorías los modelos del Cómputo en la nube: modelos de implementación y modelos de servicio. El primero consiste en la ubicación y la administración de la infraestructura de la nube, el segundo consiste en los tipos de servicios que el usuario pueda acceder dentro de una plataforma de nube. A continuación se definirán las dos categorías mencionadas.

1.5.4 Modelos de implementación

Los diferentes modelos de implementación varían dependiendo en su ubicación y distribución física. Estos son clasificados como públicos, privados, comunitarios e híbridos. La mayoría de estos consiste en servicios confiables proporcionados por centros de datos que cuentan con tecnologías de virtualización. Teniendo como requisito la disponibilidad de una infraestructura de red. Además de permitirles ser accesibles desde cualquier lugar.

A continuación se detallaran los modelos mencionados.

1.5.4.1 Nube Pública

La nuble pública se encuentra orientada hacia el público en general. Esta proporciona servicios a múltiples clientes o inquilinos a través de una infraestructura en común, además esta puede ser poseída, administrada y operada tanto por organizaciones comerciales como de gobierno o una combinación de estas. Además de poder existir tanto dentro como fuera de las instalaciones (NIST, 2011).

En este modelo los usuarios no necesitan adquirir hardware, software o infraestructura, esta es proporcionada por los proveedores. Siendo estos los administradores y propietarios de este servicio. (Sabharwal & Shankar, 2013).

De acuerdo a Arbrust y Fox (2010) una nube pública es cuando esta adopta el modelo de negocio *pay-as-you-go o pago por el consumo,* para el público en general y este servicio es inicialmente vendido como una utilidad computacional.

1.5.4.2 Privada

Sabharwal y Shankar (2013) definen nube privada como un modelo en donde la infraestructura de la nube es operada solamente por la organización y esta puede existir tanto dentro de la organización como fuera de ella.

De igual manera Mather, Kumaraswamy & Latif (2009) mencionan. Los modelos de nubes privadas difieren de las nubes públicas principalmente a que toda la infraestructura de red, cómputo y almacenamiento se encuentra asociada a las nubes pertenecientes a cada organización.

Asimismo NIST (2011) menciona que esta es proporcionada para el uso exclusivo de una sola organización, compuesta de varios consumidores. Además esta puede ser poseída, administrada y operada por una empresa, un tercero o una combinación de estos.

1.5.4.3 Hibrida

En este modelo la infraestructura en la nube se compone de dos o más nubes (privada, comunitaria o pública) que si bien son entidades únicas, estas se encuentran vinculadas por tecnologías estandarizadas o por una propia que permite la portabilidad de datos y aplicaciones (CISCO, 2009).

Además las aplicaciones pueden coexistir dentro de las dos nubes, por ejemplo, una organización puede usar normalmente una nube privada para aplicaciones pero si las cargas de las aplicaciones se empiezan a incrementar rápidamente, se puede utilizar la nube pública para administrar la carga extra. Esto se le conoce como Cloud bursting[8] (Rajaraman, 2014).

Un ambiente de nube hibrida consta de varios proveedores internos y/o externos. Con una nube hibrida las organizaciones puede ejecutar aplicaciones descentralizadas en una nube, mientras que se mantiene el núcleo principal de las aplicaciones y los datos sensibles dentro de la empresa en una nube privada Mather, Kumaraswamy y Latif (2009).

---

[8] Es un modelo de implementación de aplicaciones en la cual una aplicación se ejecuta en una nube privada o centro de datos y explota en una nube pública cuando lo demandan los picos de la capacidad de cómputo.
(tomado de http://www.techopedia.com/definition/26438/cloud-burst consultada eñ 10 de abril del 2014)

1.5.4.4 Comunitaria

En un modelo de nube comunitaria más de un grupo con intereses en común y necesidades específicas comparten la infraestructura de la nube, Williams (2012). Por ejemplo, un grupo de universidades puede decidir cooperar e interconectar su infraestructura de cómputo y crear una nube comunitaria, la cual puede ser accedida por cualquiera de sus miembros. La infraestructura de la nube puede ser administrada por cada institución participante Rajaraman (2014).

1.5.5 Modelos de Servicio

Cómputo en la nube ha permitido a las organizaciones mediante la implementación de algún modelo de nube crear nuevos modelos de servicios que varían dependiendo del giro de la organización, por ejemplo STaaS (Storage as a Service), IdaaS (Identify as a Service), CmmaS (Compliance as a Service), etcétera.

Sin embargo sólo son reconocidos mundialmente los siguientes:

- Infraestructura como servicio (IaaS).
- Plataforma como servicio (PaaS)
- Software como servicio (SaaS)

Estos tres modelos de servicios juntos son conocidos como modelo SPI de cómputo en la nube. A continuación se describen cada uno de ellos.

1.5.5.1 SaaS

El Software como Servicio se puede describir como aquellas aplicaciones consumidas a través de Internet, normalmente a través del navegador cuyo pago está condicionado al uso de la misma y en la lógica de la aplicación, así como los datos residen en la plataforma del proveedor. Algunos ejemplos de SaaS son: Salesforce, Zoho, Google App, entre otros Martínez & Galán (2010).

Además SaaS (por sus siglas en inglés de *Software as a Service*) al ser un modelo *Operational expenditure* (OpEx) el cliente no compra el software, lo renta por un determinado tiempo dependiendo de sus necesidades. Enfocándose en la manera de como el cliente utiliza el software de la organización para realizar sus procesos.

Al contrario de los modelos tradicionales de compra de software como *Capital expenditures* (CapEx) en donde el cliente debe de instalar el software en su equipo, pagar una licencia para su uso y además comprar el soporte para el software adquirido, como: parches de seguridad, actualizaciones, entre otros.

La ventaja de este modelo es que el cliente no tiene que adaptar su infraestructura para el uso de las aplicaciones, ya que en este modelo de negocio se incluye la infraestructura y el soporte del sistema. Además las organizaciones al utilizar a un tercero para la administración y el almacenamiento de aplicaciones pueden reducir los costos del software, por ejemplo: la compra de servidores, licencias, infraestructura y de personal necesario para la administración de los equipos Sabharwal & Shankar (2013).

1.5.5.2 IaaS

La Infraestructura como un servicio (IaaS por sus siglas en inglés) y en ocasiones Hardware como servicio (HaaS, por sus siglas en inglés) es un modelo de aprovisionamiento en el cual una organización coloca fuera de ella el equipo usado para soportar operaciones, estos pueden incluir el almacenamiento de la información, el hardware, los servidores y los componentes de la red (Martínez & Galán (2010).

En este tipo de modelo se proporciona a los usuarios finales recursos de infraestructura para las áreas de TI como son, el poder de procesamiento, el almacenamiento, la infraestructura de redes, y otros recursos computacionales fundamentales. Los cuales el cliente puede ocuparlos para la instalación de software como sistemas operativos y aplicaciones Sabharwal & Shankar (2013).

Además, Martínez y Galán (2010) mencionan que la ventaja más evidente de utilizar un modelo IaaS es la capacidad de transferir hacia el proveedor problemas relacionados con la administración de equipos de cómputo. Así como la reducción de costos como ocurre en general en las tecnologías asociadas al cómputo en la nube al pagar únicamente por el servicio consumido. Asimismo este modelo permite la escalabilidad prácticamente automática y transparente para el usuario.

1.5.5.3 PaaS

Plataforma como un servicio (PaaS, por sus siglas en inglés) es un modelo donde el vendedor ofrece un ambiente de desarrollo para el diseño de aplicaciones. Los desarrolladores ofrecen esas aplicaciones a través de la plataforma del proveedor (Sabharwal & Shankar (2013).

El proveedor, además de resolver problemas en la infraestructura de hardware también se encarga del software (Martínez & Galán (2010). El cliente que hace uso de este tipo de soluciones no necesita instalar, configurar ni dar mantenimiento a sistemas operativos, bases de datos y servidores de aplicaciones ya que todo esto es proporcionado bajo esta plataforma.

Asimismo el proveedor normalmente desarrolla kits de herramientas, estándares para el desarrollo de las aplicaciones y canales de distribución y pago. Este recibe un pago por proporcionar la plataforma y las ventas por los servicios de distribución, lo que permite una rápida propagación de las aplicaciones desarrolladas, logrando el bajo costo en la entrada y el aprovechamiento de los canales para la adquisición de los productos.

Por otro lado los desarrolladores pueden desarrollar aplicaciones web sin la necesidad de instalar ningún programa en sus equipos, y asimismo pueden distribuir estas aplicaciones sin tener conocimientos especiales en la administración de sistemas (Sabharwal & Shankar (2013).

Según Martínez y Galán (2010), una plataforma como servicio (PaaS) resuelve más problemas si se compara con una solución que sólo ofrece una infraestructura como servicio (IaaS), ya que presenta muchas limitaciones relacionadas con el entorno de ejecución. Entre éstas se encuentran el tipo de sistema, el lenguaje de programación (en algunos casos las bibliotecas que éstos podrán utilizar), el manejador de bases de datos, entre otros.

Empresas como Amazon, eBay, Google, iTunes y YouTube son algunas de las que emplean este modelo y hacen posible acceder a nuevas capacidades y nuevos mercados a través del navegador Web. Las PaaS ofrecen un modelo más rápido y ventaja costo-beneficio para el desarrollo de aplicaciones y entrega.

1.5.6 Ventajas del cómputo en la nube

El cómputo en la nube ofrece importantes ventajas a las organizaciones tanto para los sectores públicos como privados, según se describe en los siguientes puntos:

- Reducción de costos: Las organizaciones pueden reducir o eliminar los gastos de capital de TI al disminuir los gastos operativos corrientes y pagar únicamente los servicios que utilizan. Además de poder reducir o reubicar al personal de TI.
- Facilidad de implementación: Ya no es necesario comprar hardware, licencias de software o contratar servicios de implementación. Una organización puede implementar el cómputo en la nube de forma rápida.
- Escalabilidad: Las organizaciones que utilizan el cómputo en la nube no tienen que preocuparse para obtener hardware y software adicionales de alto nivel cuando aumentan las cargas de los usuarios, sino que pueden agregar y restar capacidad según lo determinen las cargas de la red.
- Acceso a funciones de TI de alto nivel: En especial para las organizaciones más pequeñas, el cómputo en la nube permite el acceso a hardware, software y personal de TI de más alto nivel que el que pueden atraer o proporcionarse por sí solas.
- Enfoque en las principales competencias: Cabe sostener que la capacidad para operar centros de datos y desarrollar y administrar aplicaciones de software no es necesariamente una competencia principal en la mayoría de las organizaciones. Mediante la computación en la nube es posible reducir o eliminar estas funciones, gracias a lo cual las organizaciones pueden concentrarse en problemas fundamentales como políticas y planificación para la mejora continua del entorno de aprendizaje.
- Sostenibilidad: Hoy se comprende que la baja eficiencia energética de la mayoría de los centros de datos es a causa de su diseño deficiente o del uso poco eficaz de los recursos. Los proveedores de servicios en la nube al utilizar economías de escala y tener capacidad para administrar recursos de computación con más eficiencia pueden consumir mucho menos energía y otros recursos, que los operadores de centros de datos tradicionales.

1.5.7 Desventajas del cómputo en la nube

El cómputo en la nube no sólo ofrece ventajas a las organizaciones sino también existen desventajas como se muestran en los siguientes puntos:

- Requiere constante conexión a internet: Cómputo en la nube es imposible si no se puede conectar a la red porque el uso de internet es indispensable para conectarte a cualquier

aplicación y documento. Si no se tiene conexión a internet no se puede acceder a nada incluso si son documentos propios.

- No se trabaja bien con conexiones lentas: Las aplicaciones basadas en web normalmente requieren un amplio ancho de banda para poder funcionar, así como para descargar documentos de gran tamaño.
- Seguridad en la nube: A pesar de que los proveedores utilicen las más recientes y sofisticadas técnicas en seguridad, todavía hay serios problemas de seguridad que los hackers pueden atacar para vulnerar los sistemas. Además a medida que los servidores están interconectados en la nube, un hacker puede romper un sistema y luego dar paso a otros sistemas conectados.

2 Análisis de riesgo de la política BYOD

En este capítulo se analizarán los riesgos que se presentan en la adopción de la política BYOD en dispositivos Android, y los problemas que se enfrentarían los administradores de TI.

La implementación de la política BYOD en las empresas presenta un reto para los administradores de TI, dado que esta cambia el paradigma de la administración y seguridad de las empresas. Como se observa en la ***Figura* 4** esta política añade elementos nuevos los cuales están fuera del control de los administradores de TI, tales como: el uso de dispositivos móviles en la organización y las tecnologías como *Cloud Computing.*

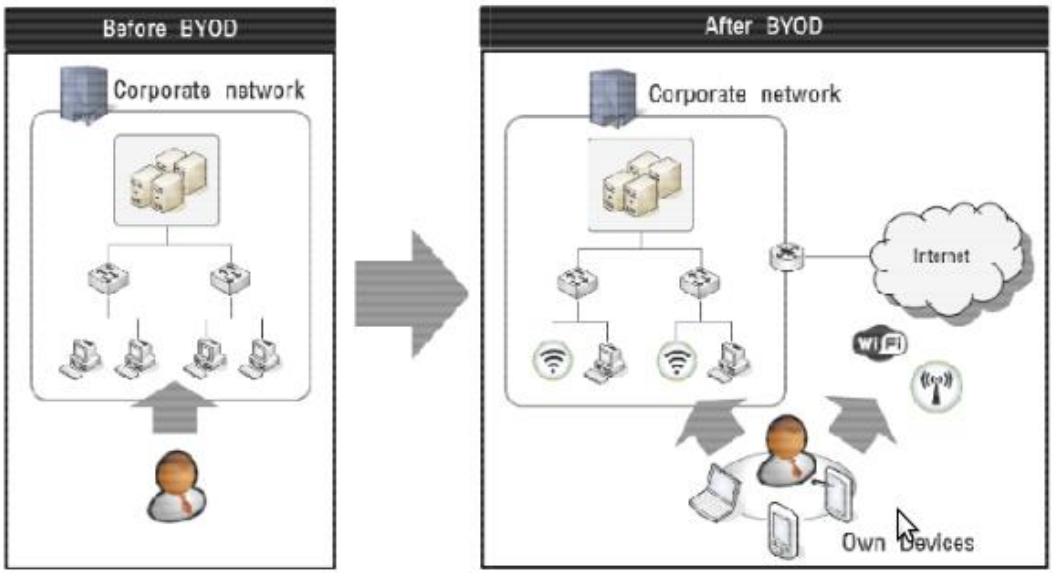

***Figura* 4. Ambiente BYOD**

Nota. Recuperado de Kang (2013)

Anteriormente se tomaban medidas de seguridad ya estandarizadas en las cuales sólo se protegía la red y la infraestructura de la empresa esto permitía tener un control sobre los equipos de la organización, pero con la implementación de la política BYOD esto ha cambiado, ahora el usuario/empleado juega un papel importante en la seguridad de la empresa. En la **Tabla 3** muestran algunas de las tareas realizadas antes y después de BYOD.

Tabla 3

Comparación antes y después de la implementación de la política BYOD

Antes de BYOD	Después de BYOD
Los usuarios se limitaban a usar equipos de la empresa para el desempeño de sus labores.	Los usuarios utilizan equipos tanto de la empresa como de su propiedad para el desempeño de sus labores.
Se realizaban configuraciones personalizadas en los equipos de la organización.	Los dispositivos son propiedad de los usuarios, lo cual no permite una configuración basada en las normas de la organización.
Instalación de software específico y controlado.	Los dispositivos son propiedad de los usuarios, estos deciden qué instalan y qué no.
Instalación de parches de seguridad y actualización de software.	El dispositivo al pertenecer al usuario, no lo obliga a instalar parches de seguridad y actualizaciones de sus equipos.
Instalación de software antimalware (antivirus, antispyware, etc.)	El equipo pertenece al usuario, él decide si instala o no el software.
Se ocupan marcas y modelos específicos de equipos en la organización.	Existen variedades de marcas y modelos de equipos usados por los empleados.
Soporte técnico a los equipos.	Este depende de un tercero, en la mayoría de los casos es el proveedor de los dispositivos.

Nota. Elaboración propia

Con la implementación de BYOD, los administradores de TI han empezado a preocuparse sobre ciertas áreas que anteriormente no se tenían contempladas como una amenaza. Esto lo demuestra un estudio realizado por Lookout (2013), el cual menciona las preocupaciones de los administradores de TI ante diversas amenazas, las cuales se muestran en la ***Figura* 5**.

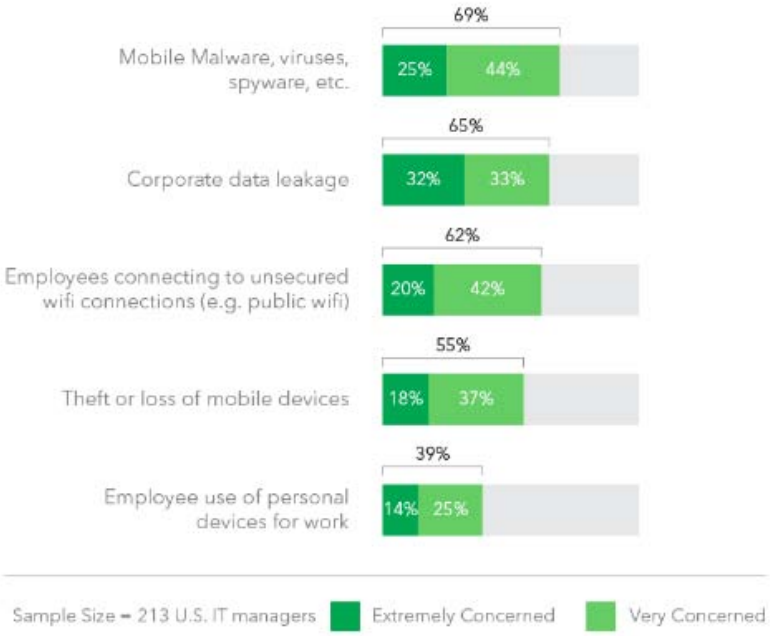

***Figura* 5. Amenazas en dispositivos móviles**

Nota. Recuperado de Lookout (2013)

Tal como se observa en la ***Figura* 5**, las preocupaciones más grandes de los administradores son el malware y la fuga de datos. En las subsecciones siguientes se comentan cada una de ellas y se agregan otras no incluidas en esta ***Figura* 5,** que se consideran importantes.

2.1 Malware en los dispositivos móviles

El malware en los teléfonos celulares existía desde el año 2000 con el primer virus registrado llamado Timofonica (Coursen, 2007). Estos tipos de malware no resultaban tener un gran impacto como sus contrapartes en equipos de escritorio ya que estos sólo se orientaban en el envío de cadenas por mensajes SMS.

Posteriormente, en el año 2004 se empezó a registrar un incremento del malware, teniendo como principal objetivo de ataque el sistema operativo Symbian. Como se muestra en la ***Figura 6*** en el periodo del 15 de agosto del 2005 al 15 de agosto del siguiente año, se observa un incremento de más del 300% y aún sigue en aumento.

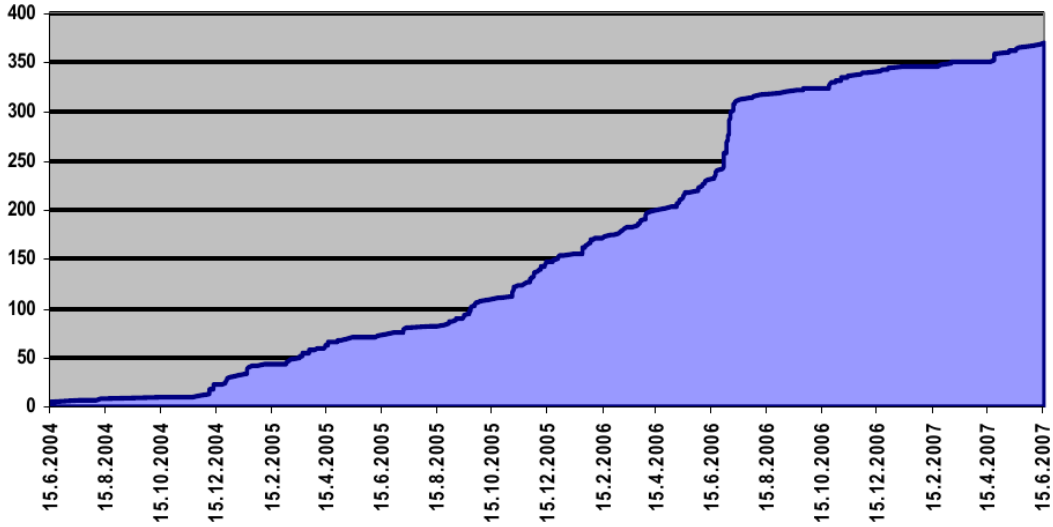

Figura 6. **Incremento del malware**

Nota. Recuperado de F-Secure (2012)

El gran aumento de teléfonos celulares en el mercado, la evolución de estos a teléfonos inteligentes y posteriormente el desarrollo de otros dispositivos como tabletas y phabets, sumándole a estos, las tecnologías Cloud Computing, han logrado llamar la atención de los Black Hats o Crackers para orientar sus ataques a estas plataformas.

Tan sólo en el año 2012 las familias de malware para dispositivos móviles tuvieron un incremento del 58% en comparación con el año 2011. Actualmente se presenta el 59% de todo el malware Symantec (2013). Lo anterior nos hace reflexionar sobre la importancia que se debe tomar frente a los dispositivos móviles.

Por otra parte, los dispositivos móviles como tabletas, phablet y teléfonos inteligentes, por sus características físicas reducidas, no pueden compararse con equipos como laptops o computadoras de escritorio. La arquitectura de estas últimas soportan software más robusto para combatir malware, como antivirus, firewalls, anti-spyware, por mencionar algunos.

Es cierto que existen versiones de estos programas para dispositivos móviles, pero algunas solamente funcionan si el dispositivo tiene activada la cuenta de administrador del sistema (dispositivo rooteado).

Sin embargo, esta opción es una "arma de doble filo", por un lado el dispositivo se presta para la implementación de nuevas medidas de seguridad que no serían posibles con la cuenta de un usuario limitado, un ejemplo de esto sería el uso de un *firewall* basado en *iptables.* Si no se toman en cuenta ciertas medidas de seguridad, el malware puede tomar ventaja de tales privilegios y comprometer no solo el dispositivo móvil si no también la red en la que se puede conectar.

Además, un reciente estudio realizado por Kaspersky Lab (2013) menciona que en términos de sistemas operativos para dispositivos móviles, Android es el sistema operativo más atacado teniendo un 98.05% del malware conocido.

Un estudio realizado por AV-Test (2013) a veintidós antivirus para el sistema operativo Android, reveló que tan sólo uno apenas logró pasar las pruebas de calidad. Lo cual es algo preocupante al no contar con herramientas especializadas para poder proteger los equipos.

El malware en dispositivos Android ha estado en constante evolución desde la primera detección en agosto del 2010 (Sophos, 2014). Un ejemplo de este malware es el troyano *Ginmaster,* el cual fue detectado en China. Este actualmente cuenta con 6000 variantes conocidas (Yu, 2013). Este malware tiene la facultad de evadir las detecciones de los antivirus por medio del uso de técnicas de Polimorfismo las cuales le permiten ocultar su código malicioso. Además, este malware tiene la capacidad de robar información confidencial y enviarla a un sitio web remoto, así como instalar aplicaciones sin la interacción del usuario.

En la evolución del malware para los dispositivos móviles "no se inventa el hilo negro", sino que se ha aprovechado la experiencia en equipos de escritorio. Tal es el caso de las aplicaciones tipo RAT, por sus siglas en inglés de *Remote Access Control* o *Remote Access Trojan* (Rouse, 2009). Este tipo de aplicación infecta a la víctima con un malware del tipo *Trojano*, con el cual tiene el control total del equipo de la víctima, permitiéndole realizar las siguientes tareas.

- Monitoreo del comportamiento del usuario a través de *keyloggers* o cualquier otro programa del tipo spyware.
- Encendido de equipos como micrófonos y webcams.
- Tomar capturas de pantalla.
- Distribución de malware.
- Eliminar, alterar o descargar archivos del sistema.
- Formateo de las unidades del equipo.

Este tipo de aplicaciones originalmente sólo eran ocupadas en sistemas operativos de escritorio tales como Windows, GNU/Linux, MAC OSX, por mencionar algunos. Hoy en día con la gran popularidad que ha tenido Android, era de esperarse que este tipo de herramientas también empezaran a surgir en esta plataforma.

El primer programa de este estilo fue publicado en los foros del "bajo mundo" de forma gratuita con el nombre de AndroRAT (Android.Dandro), en noviembre del 2012 (Lelli, 2013). A su vez, también fue la primera herramienta del tipo *Binder*[9], esta facilita la tarea a los *Black Hats* para infectar aplicaciones legítimas con malware de una forma sencilla.

Actualmente se pueden observar imitaciones de este malware o versiones mejoradas. Una de estas versiones es *Dendroid,* recientemente descubierta por Symantec. Esta es vendida por 300 dólares, lo peculiar en esta herramienta es el hecho de contar con características innovadoras, como: el soporte técnico 24/7 el cual es proporcionado una vez que fue adquirida a través de cryptodivisas como Bitcoins o Litecoin; la evasión de los sistemas de detección de malware en la tienda de Google (Google Play), entre otros (Coogan, 2014).

Otras de las características que ofrece son las siguientes:

- Borrado del historial de llamadas.
- Realizar una llamada.
- Abrir páginas web.
- Grabar llamas.
- Interceptar mensajes de texto.
- Tomar fotos y video.
- Abrir aplicaciones.
- Realizar ataques de denegación de servicio (DoS sus siglas en inglés) por un periodo de tiempo.

En la ***Figura 7*** se muestra el panel de administración de la herramienta donde se observan las opciones citadas anteriormente, además de información sobre el dispositivo infectado, las

[9] TechTarget lo define como un software que permite combinar dos o más archivos en uno solo (tomado de http://searchwindowsserver.techtarget.com/definition/binder consultada el 24 de marzo de 2014).

coordenadas del dispositivo (posiblemente proporcionadas usando la API[10] de Google Maps), el número telefónico y la versión de la API que usa el dispositivo. En este caso se observa que se trata de las versiones 18 y 17, lo que quiere decir que se encuentran usando la versión 4.3 y la 4.2.x de Android (Android, 2014).

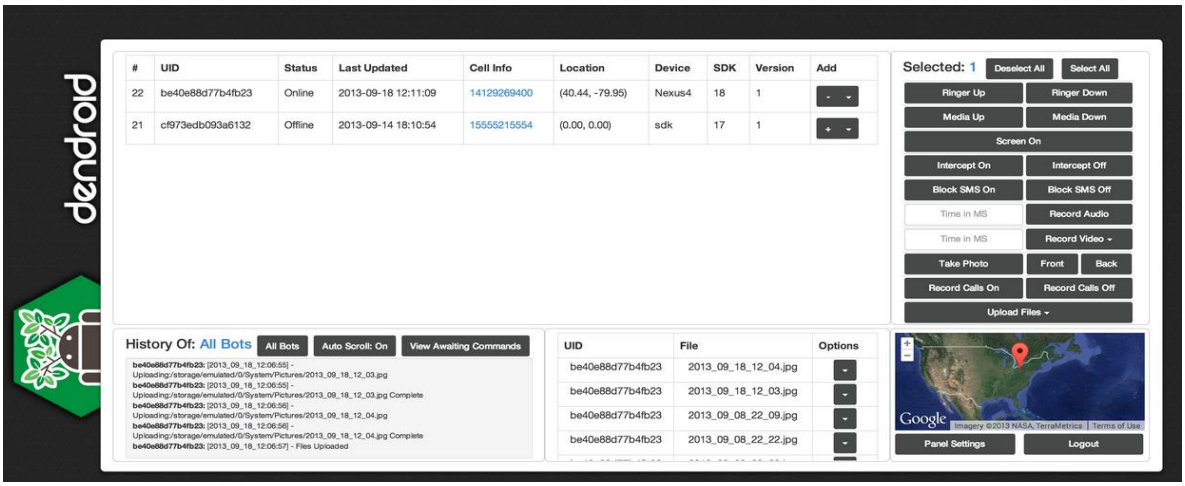

***Figura* 7. Plataforma de control Dendroid**

Nota. Recuperado de Khan (2014)

El malware no solo se ha orientado en el área (RAT), en donde puede obtener un control total de los dispositivos móviles, además ha incursionado en otras como: el adware[11], robo de datos, descargas maliciosas, herramientas de hacking y abuso de servicios premium.

Un estudio realizado por TrendLabs (2013) indica que el área de control remoto no es una de las más explotadas, esta se encuentra en cuarto lugar. La más rentable actualmente es el abuso de servicios premium como se puede ver en la ***Figura* 8**.

[10] TechTerms define una API (*Application Programming Interface*) como un conjunto de comandos, funciones y protocolos con el cual el programador puede construir software para un específico sistema operativo (tomado de http://www.techterms.com/definition/api, consultado el 24 de marzo de 2014).

[11] Tech Target lo define como un software en el cual se muestran anuncios publicitarios mientras el programa se encuentra ejecutándose. Los adware son criticados porque usualmente incluyen código para el rastreo de información del usuario la cual es trasmitida a un tercero (tomado de http://www.techterms.com/definition/adware, consultado el 24 de marzo de 2014).

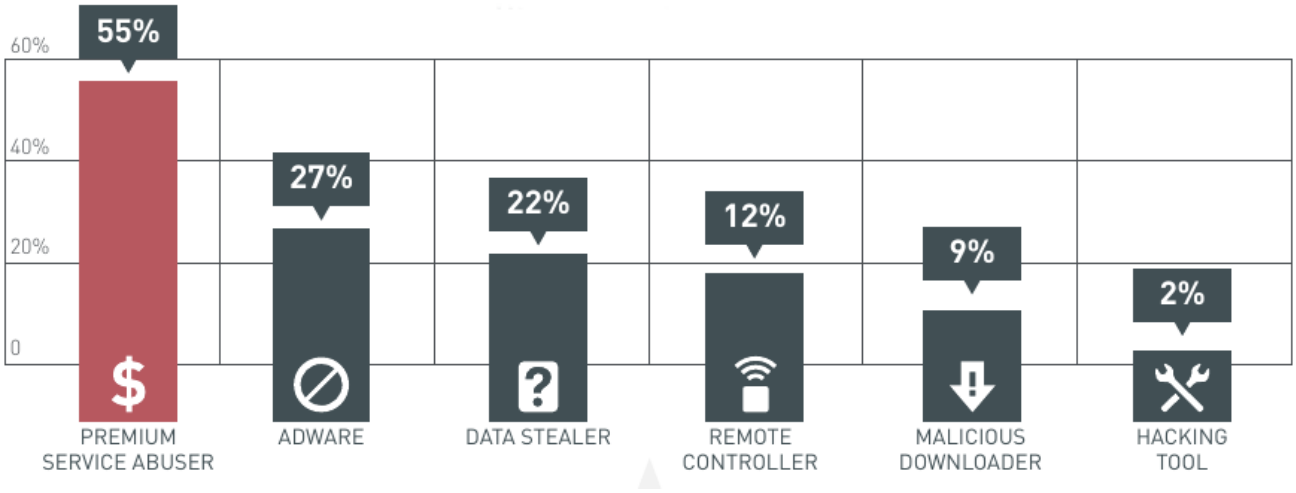

***Figura* 8. Distribución de las amenazas**

Nota. Recuperado de TrendLabs (2013)

El abuso de servicios Premium, es un método útil y sencillo en la obtención de dinero. El modo de operación es el siguiente: el dispositivo es infectado a través de la descarga de aplicaciones en repositorios no oficiales, foros, blogs, redirecciones de páginas, enlaces de *spam,* etcétera. Una vez que la app es instalada, esta envía mensajes de texto de forma secreta y programada a sitios de servicios premium o de pago, reduciendo el saldo de la víctima.

Además tiene acceso a la tarjeta de memoria del dispositivo, la lista de contactos de la víctima, acceso a los mensajes de texto y la localización del dispositivo (Trend Micro, 2013).

2.2 Uso de aplicaciones no autorizadas

Los empleados no sólo utilizan los recursos de la empresa para desempeñar sus labores, sino también los ocupan para uso personal. Utilizan aplicaciones o servicios no autorizados, como: clientes de correo electrónico, banca en línea, pago de cuentas, compras en línea y mensajería instantánea, por mencionar algunos. El uso de estas aplicaciones o servicios pone en riesgo la información de la empresa porque no son monitoreadas o no se basan en los estándares de seguridad de la organización. El estudio realizado por Cisco System (2008) revela lo siguiente:

- 78% de los empleados acceden a sus correos personales a través de las computadoras de las empresas.
- 63 % de los empleados admite que usa la red de la empresa para uso personal.
- 83% de los empleados admite que usa de vez en cuando el equipo de la empresa para uso personal.

2.3 Conclusiones preliminares

La evolución del malware hacia los dispositivos móviles ha crecido a un ritmo acelerado, en donde los antivirus y herramientas de detección de *Google,* no han sido capaces de proteger en su totalidad a los dispositivos móviles. Lo anterior no quiere decir que no se utilicen estas herramientas, dado que también se encuentran en constante evolución, logrando frenar parte del malware que existe.

Además el malware orientado a dispositivos móviles, se considera más peligros en comparación con la versión de computadoras de escritorio. Esté cuenta con similitudes de su contraparte de escritorio y añade ventajas para el *Black Hat,* como el hecho de ser un dispositivo portable permitiéndole ampliar sus horizontes.

Por lo tanto se considera a la capacitación de los usuarios finales como el elemento clave para poder combatir este mal. El contagio de malware en su mayoría es exitoso por la falta de cultura de los usuarios en la instalación de las aplicaciones. El usuario puede reducir el contagio de malware evitando descargar aplicaciones de forma de paga o gratuita en lugares no oficiales donde en su mayoría son aplicaciones alteradas con algún malware.

2.4 Fuga de información

La información dentro de las organizaciones se podría considerar como uno de los activos más importante que estas poseen. No importa si es física o digital, si son secretos comerciales o estrategias empresariales. La información junto con la propiedad intelectual es el principal motor de los ingresos de una organización. Además permite distinguir una organización de otra y esta es una de las razones principales para el consumo de sus productos o servicios. Sin embargo, se encuentran bajo un riesgo constante: la fuga de información.

Gordon (2007) define la fuga de información de la siguiente manera: es la transmisión no autorizada de datos o información dentro de una organización a un destino externo. Este puede ser por un medio electrónico o físico. Existiendo diferentes tipos de información dentro de las organizaciones que pueden ser propensos a la fuga de datos.

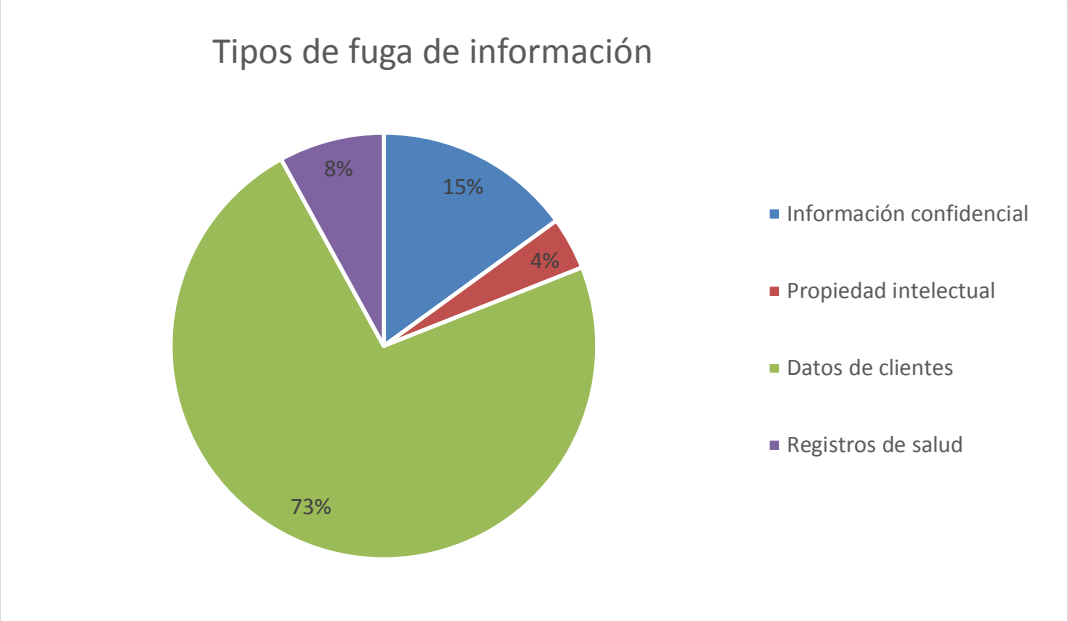

Figura 9. **Tipos de fuga de información en las organizaciones**

Nota. Recuperado de Gordon (2007)

Como se puede observar en la ***Figura 9***, la información mayormente sustraída de las organizaciones, es el conjunto de datos de los clientes y la información confidencial. Esto es posiblemente debido al fácil acceso que los empleados tienen a esta, dado que la utilizan para desempeñar sus labores. La fuga de datos o información puede ocurrir de varias maneras: errores humanos, fallas tecnológicas, malas configuraciones, vulnerabilidades aprovechadas por *black hats*, empleados disgustados y empleados que violan las políticas de seguridad de la organización. Por lo que se puede considerar las siguientes divisiones que se desarrollarán en los siguientes apartados.

2.4.1 Internas

2.4.1.1 Los empleados

En un principio se pensará en los *black hats* como los principales responsables en el tema del robo de propiedad intelectual o fuga de datos, pero un elemento menos obvio en un inicio, es el empleado, el cual tiene el mayor índice de fuga de datos. Lo anterior los convierte en *Frenemy*[12].

Un estudio realizado por *Epic.org y PerkingsCoie.com* muestra que el 52% de las brechas de seguridad son originadas desde el interior de las organizaciones (Gordon, 2007). Esto es debido a que los empleados tienen la capacidad de manipular la información de la organización, moverla, compartirla o eliminarla, según sea necesario para desempeñar su trabajo.

La motivación de los empleados para realizar este tipo de acciones es variada, por ejemplo, pueden ser por espionaje corporativo, alguna recompensa, altercados con su jefe o simplemente desconocían lo que estaban haciendo.

Por otra parte, el 50% de los encuestados, de acuerdo al estudio anterior, respondió que se ha llevado información de la organización consigo una vez que termina de laborar. Además, el 40% de estos mismos respondió que la ocupan en sus futuros trabajos.

Los empleados en las organizaciones suelen buscar alternativas para satisfacer necesidades que las organizaciones no les permiten, como la consulta de redes sociales, acceso a sitios web no permitidos en las políticas de la organización o algún otro elemento que no sea esencial para realizar su labor. En su mayoría son los empleados con conocimientos técnicos los que realizan las evasiones a las políticas de la empresa.

En la ***Figura 10***, se observa que un porcentaje significativo de los empleados son conscientes de que están evadiendo las políticas de seguridad de la organización. Pero a la vez no son conscientes de que evadiendo estas políticas afectan la seguridad de la empresa y ellos mismos se ponen en riesgo.

[12] Persona que es amigo y enemigo a la vez.

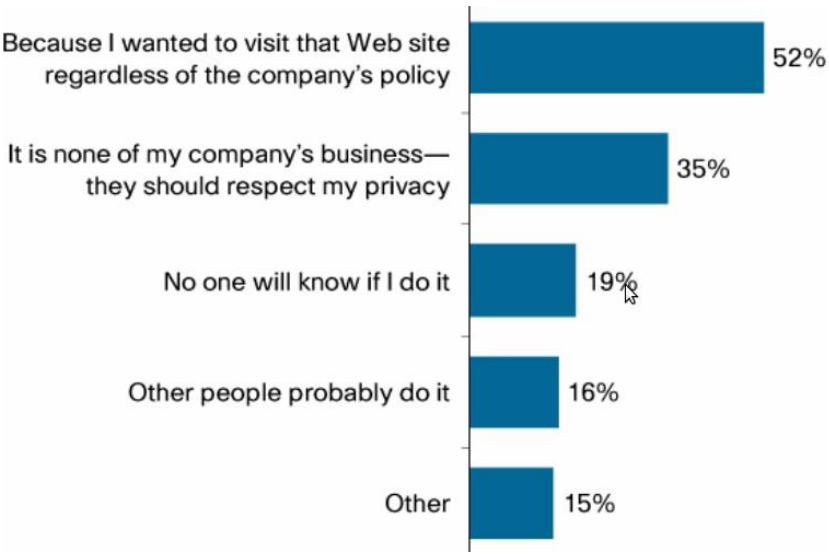

Figura 10. **Razones por la que los empleados evaden las políticas de seguridad.**

Nota. Recuperado de CISCO (2014).

Otro factor importante a considerar, es si existe descontento por parte del empleado con su trabajo, disgusto con su superior o algún sentimiento vengativo. Esto puede ocasionar una amenaza interna que consecuentemente causará algún daño o robo de datos.

Por lo anterior es recomendable no olvidar el factor humano al momento de diseñar políticas de seguridad para mantener la integridad de las organizaciones.

2.4.1.2 Almacenamiento en medios

Con al avance de la tecnología en materia de almacenamiento, contar con grandes capacidades de carga para transportar datos se ha vuelto verdaderamente sencillo.

Como se muestra en la **Tabla 4**, los usuarios suelen almacenar todo tipo de información en sus dispositivos móviles, desde datos personales hasta información de la organización donde estos laboran.

Tabla 4
Información almacenada en los dispositivos móviles

Device	iPad	Other Tablet	Other Mobile	Smartphone	iPhone	Blackberry
Base	**1720**	**864**	**750**	**2337**	**1639**	**504**
Photos/videos/music/created by you	78%	65%	71%	76%	81%	59%
Personal email message	73%	61%	55%	64%	78%	59%
SMS or MMS	25%	23%	66%	72%	70%	74%
Password to personal & email	20%	23%	26%	22%	24%	21%
Work email message	33%	28%	31%	32%	41%	65%
Files for work use	29%	29%	16%	20%	18%	32%
Files for personal use	43%	50%	24%	34%	33%	25%
Address book/phone contacts	59%	40%	80%	82%	87%	81%
PIN codes/passwords for online banking	10%	10%	18%	11%	14%	16%
Other banking details	13%	10%	13%	11%	16%	13%
Passwords for corporate / work accounts	9%	9%	12%	7%	11%	17%
Coursework, study materials	3%	3%	2%	2%	3%	1%
Any of the above	95%	88%	96%	96%	98%	97%

Nota. Recuperado de Kaspersky (2013)

De acuerdo a un estudio realizado por Karspersky Lab (2013), los hogares promedio son propietarios de 4.5 de dispositivos móviles, los cuales son utilizados para diversas tareas. Su uso va desde consultas de correo electrónico, estados de redes sociales, transferencias bancarias, compra de servicios, lectura de documentos, por mencionar algunos.

Por otro lado, el 50% de los empleados admitió que se auto envía información de la empresa (documentos, imágenes, etc.) a sus correos personales y dispositivos móviles. Asimismo, el 41% respondió que realiza esta tarea al menos una vez a la semana (Symantec, 2013).

Al mismo tiempo esta práctica aumenta por el uso de servicios en la *nube,* tales como *Dropbox* y *Google Docs,* que son utilizados sin el conocimiento de las organizaciones. Asimismo los datos compartidos a través de estos servicios rara vez son eliminados por los empleados una vez que han terminado de ocuparlos.

2.4.2 Externas

2.4.2.1 Robo o pérdida de dispositivos

Actualmente la tecnología para los dispositivos móviles ha evolucionado al grado de transformar el modo en que se accede a la información. Cada vez más personas confían en sus dispositivos para almacenar todo tipo de información y realizar una variedad de tareas. Esto propicia que la fuga de información sea más fácil, dado que los empleados tienden a guardar información tanto personal como de la organización en sus dispositivos móviles.

Además la mayoría de los usuarios no tienen una educación sobre la seguridad y los riesgos que pueden tener al perder sus dispositivos. Esto lo demuestra un estudio realizado por Karspesky Lab (2013) en donde el 50% de los encuestados respondió que una vez que ha perdido su dispositivo bloquea la tarjeta SIM, 43% cambia las contraseñas de sus servicios en línea, 41% utiliza alguna aplicación para bloquear su dispositivo remotamente, el 24% utiliza aplicaciones que le permitan borran toda información sensible del dispositivo móvil y el 12% toma una fotografía de la cara del ladrón que posteriormente envía a la policía.

La pérdida de los dispositivos móviles o el robo de los mismos se ha vuelto para las organizaciones una gran amenaza, dado que la información contenida en los dispositivos móviles ya no sólo es de los propietarios de los dispositivos sino también de las organizaciones, por lo cual se puede poner en riesgo la imagen de la empresa y causar pérdidas financieras.

Asimismo, el robo a dispositivos móviles es mayor en un 7% que el robo o pérdida de tarjetas de crédito que cuenta con un 6%, billeteras con un 5% y relojes, llaves de hogares y pasaportes con un 3%.

Otro estudio realizado por Karspesky Lab (2013) revela que uno de cada seis consumidores ha experimentado pérdida o robo de alguno de sus dispositivos móviles en los últimos doce meses.

2.4.2.2 Falta de educación en los empleados

Los empleados no piensan que transferir libremente datos de la compañía a través de sus dispositivos móviles o la nube esté mal. Symantec (2013) en un estudio menciona que el 30% de los empleados se encuentran a favor de compartir y subir información a sus dispositivos móviles o a la nube, alegando que esto está bien mientras no se reciban ganancias, el 50% de ellos piensa que no está haciendo algún daño a la empresa al realizar esta actividad.

Esta falta de conciencia por parte de los empleados es una de las principales causas de la fuga de información y contagio de algún malware, el cual puede esparcirse por la red de la empresa si esta no se encuentra debidamente protegida.

Por otro lado, las compañías no cuentan con estrictas políticas para la protección de la propiedad intelectual. Esto sugiere que los empleados no reconocen o desconocen el rol de los datos confidenciales de la compañía (Symantec, 2013).

2.4.2.3 Mal uso de contraseñas y autentificaciones

Uno de los métodos de autenticación más utilizados desde hace cientos de años, y que aún se sigue ocupando hasta la época actual, es la contraseña. Esta es un procedimiento sencillo para salvaguardar la información, pero también es considerada como la más débil de las formas de protección. Su debilidad radica en la forma en que esta es creada, la mayoría de las veces se ocupan palabras fáciles de recordar, por ejemplo: fechas de cumpleaños, números telefónicos, números de seguro social, entre otros.

Este tipo de formas es lo que hace fácil el descifrar las contraseñas, y algunas veces sin la necesidad de utilizar programas especiales. Además de ocupar contraseñas con una complejidad mínima, las personas tienden a preocuparse poco sobre la seguridad de sus equipos, lo cual es demostrado por un estudio realizado por CISCO (2008):

- 1 de cada 3 empleados mencionó que deja su equipo sin bloquear cuando se aparta para ir a comer o a su hogar.

- 1 de cada 5 empleados almacena la contraseña y el usuario para acceder a su equipo, escribiendo los mismos debajo de su equipo o escribiéndolo en un papel el cual deja al lado de su equipo o lo almacena en gabinetes sin cerrojo.

Estos tipos de comportamientos generan riesgos de seguridad. Donde no solo se compromete a la empresa, sino también puede resultar afectado el usuario.

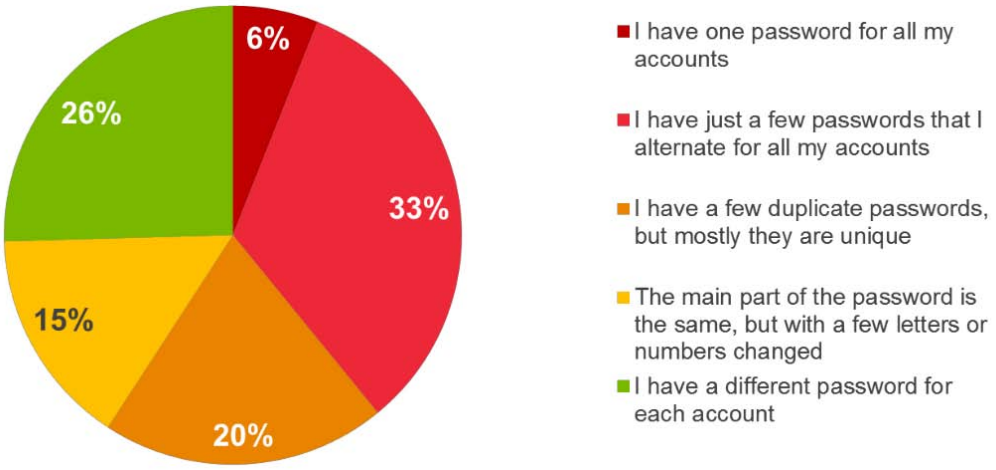

Figura 11. **Uso de contraseñas en los usuarios.**

Nota. Recuperado de Kaspersky Lab (2013).

Como se puede observar en la ***Figura 11***, el 39% de los encuestados respondió que sólo tiene una contraseña o unas cuantas contraseñas que alternan para todas sus cuentas. El 15% dijo que usa una contraseña base, a la cual sólo le modifica algunos caracteres. Prácticamente la mayoría de los usuarios, con un 54%, utilizan una o algunas contraseñas para acceder a sus cuentas.

De ese estudio, sólo 6% de los usuarios utiliza programas para generar contraseñas seguras. Esos otros encuestados respondieron que no confían en sus memorias y almacenan las contraseñas en medios no seguros. El 16% lo almacena en una libreta de notas, 11% en un documento en su computadora o un papel que regularmente se encuentra cerca de su computadora.

Por otro lado este tipo de comportamientos no es exclusivo de cierto tipo de empresas o países en específico, más bien es un comportamiento que se repite en todo el mundo. Por ejemplo en un

estudio realizado por Cisco System (2008), reveló que el 28% de los empleados en China almacena en sus equipos de trabajo datos personales, como usuarios y contraseñas de sus cuentas financieras.

De igual manera en países como Italia, India, Francia y Reino Unido el 10% de los empleados escriben notas con las contraseñas de acceso a sus equipos de trabajo mismas que dejan en lugares visibles. Además el 5% de los empleados de Francia y Reino Unido también deja a la vista las contraseñas de acceso a sus sistemas financieros.

La mayoría de los usuarios como se ha mostrado, no tiene cuidado al momento de generar una contraseña y además utiliza la misma para todos los sitios. Esto lo vuelve un objetivo bastante fácil no sólo para los *black hats*, sino también para cualquier persona que quiera afectar o dañar a la víctima.

Los usos que se pueden dar a este tipo de información son muy variados, por ejemplo, accediendo a la computadora de la víctima la pueden convertir en un "*zombie o bot*[13]" para realizar ataques de *DDoS*[14]o podrían sustraer datos importantes que podrían dañar no solamente la parte financiera sino también la imagen de la víctima hasta llegar al robo de identidad. Este último es más peligroso si se combina con ingeniería social porque se podría conseguir acceso a lugares donde sólo la victima puede acceder, por ejemplo correos del trabajo, acceso a sitios restringidos, cuentas bancarias, tan sólo por mencionar algunas. Lo anterior ya no sólo afectaría a la víctima, si no también a la empresa donde esta labora.

2.4.3 Conclusiones preliminares

Las amenazas siguen incrementándose cada vez más. Dispositivos móviles, internet y hasta los propios usuarios representan riesgos que amenazan a las organizaciones, por lo que se deben de tomar en cuenta estos elementos para el desarrollo de nuevas estrategias para poder mitigar el riesgo.

---

[13] TechTarget lo define como: Una computadora bajo el control de un intruso es conocida como zombie o bot. Obtenido de http://searchsecurity.techtarget.com/definition/distributed-denial-of-service-attack Visitada el 31/10/2014.
[14] TechTarget lo define como: Un ataque distribuido de denegación de servicio por sus siglas en inglés (Distributed Denial of Service) es donde un grupo de sistemas comprometidos atacan un sistema en particular, causando denegación de los servicios para los usuarios del sistema víctima. La gran cantidad de los mensajes recibidos por el sistema víctima es tanta que se ve obligado a cerrar el servicio incluso para los usuarios legítimos, (obtenido de http://searchsecurity.techtarget.com/definition/distributed-denial-of-service-attack. consultada el 31 de octubre del 2014).

Muchas empresas solamente se enfocan en desarrollar la parte tecnológica, dejando de lado la parte humana. Creen que comprando un equipo o software de seguridad será suficiente para salvaguardar su información. Pero el hecho es que se deben de desarrollar estrategias, políticas y educación, resolviendo el problema de una manera holística.

Las organizaciones deben de evaluar los comportamientos de los empleados y los riesgos asociados, basados en factores como el lugar y el panorama de la amenaza. La educación sobre las amenazas, el entrenamiento sobre seguridad y los procesos de negocios deben de ser recalcados, casi esculpidos.

Algunos puntos que se pueden sugerir para lograr prevenir la fuga de datos, son los siguientes:

- Conocer los datos de la organización y tener una buena administración.
- Tener un cuidado especial con los datos.
- Imponer estándares de conducta en la organización.
- Fomentar una ambiente de franqueza y verdad en la organización.
- Establecer conciencias sobre la seguridad y educación en la empresa.
- Educar a los empleados sobre el tema de seguridad en la organización.
- Desarrollar planes de contingencias e incidentes.

Algunas de las recomendaciones que se dan para lograr mejorar la forma de crear contraseñas, serían las siguientes.

- Generar contraseñas mayores a ocho caracteres y ocupar: letras, números, caracteres especiales y símbolos.
- No utilizar patrones de uso cotidiano como: números telefónicos, direcciones, fechas de cumpleaños, códigos postales, etcétera.
- Generar contraseñas dinámicas, donde se tenga un tiempo limitado de uso.
- Utilizar frases junto con caracteres especiales o símbolos.

3 Propuesta para prevenir riesgos de la política BYOD

En el capítulo 2, se presentaron los riesgos de adoptar una política BYOD. Ahora, en este capítulo se presenta la propuesta desarrollada durante la investigación de esta tesis para prevenir estos riesgos y amenazas. Se propone una serie de recomendaciones y un esquema de seguridad para mejorar la administración de los dispositivos móviles que ingresen a una organización.

Este capítulo se dividirá en secciones. En la primera de ellas, se expondrán las recomendaciones para el uso de dispositivos móviles, que los usuarios de los mismos podrían adoptar ante una política BYOD. En la segunda, se describirá una propuesta técnica para adoptar una política de este tipo.

3.1 Recomendaciones para el uso de dispositivos móviles

Los dispositivos móviles, como se ha mencionado a lo largo de esta tesis, son un elemento importante para mejorar la eficiencia de los empleados dentro de las organizaciones, pero si no se tiene una correcta administración de estos pueden volverse un riesgo para las mismas.

La administración no sólo implica la parte tecnológica de BYOD si no también se debe de hacer hincapié en la educación de los empleados sobre las ventajas y los riesgos que existen por el uso de esta política. Por lo anterior, y después de haber hecho un análisis de los riesgos de adoptar esta política, a continuación se presentan una serie de recomendaciones para el uso de los dispositivos móviles. Estas recomendaciones se listan a continuación y se explican en apartados posteriores.

- Bloqueo de pantalla.
- Cifrado de datos.
- Conexiones a redes públicas.
- Asignación de contraseñas.
- Borrado remoto.
- Desactivación de bluetooth.
- Copias de seguridad.
- Administración de aplicaciones.
- Actualización de Sistema operativo.
- Cargar la batería de dispositivos móviles en computadoras

3.1.1 Bloqueo de pantalla

Uno de los métodos más básicos de seguridad que existen en los dispositivos móviles, es el bloqueo de pantalla. Este funciona de la siguiente manera: después de un determinado tiempo de inactividad, el dispositivo se bloquea negando el acceso al mismo. El dispositivo seguirá bloqueado hasta que se ingrese uno de los siguientes elementos: código, patrón, contraseña, gesto o botón y en algunos de los dispositivos más modernos por métodos biométricos (huella digital o reconocimiento facial).

Es recomendable para mejorar la protección de los dispositivos móviles tener activada esta función con algunas de las opciones mencionadas anteriormente, excepto la opción de desbloqueo por botón o por gesto. La opción de bloqueo por medio de gesto o botón haría totalmente ineficiente este método de seguridad en el dispositivo por el hecho de que cualquier persona pueda acceder al dispositivo móvil sin mayor problema.

3.1.2 Cifrado de datos

El cifrado del dispositivo móvil es uno de los métodos más seguros para salvaguardar la confidencialidad de la información contenida dentro de los dispositivos móviles, permitiendo sólo descifrarla por medio de un PIN (Personal Identication Number, por sus siglas en inglés) que es utilizado como llave.

Este método es soportado por las versiones más recientes del sistema operativo Android (a partir de la versión 2.2).

3.1.3 Conexiones a redes públicas

Conectar el dispositivo móvil a una red pública es una de las prácticas más comunes hoy en día. Actualmente se puede tener acceso a internet desde cualquier lugar, por ejemplo: cafeterías, centros comerciales, parques, librerías, tan sólo por mencionar algunos.

Pero como se ha mencionado anteriormente, estos dispositivos son equipos sencillos que no cuentan con los parámetros mínimos de seguridad (regularmente se instalan con las configuraciones de fábrica). Además si no se cuentan con las precauciones mínimas de seguridad, un tercero puede fácilmente interceptar la información que se transmite, consiguiendo datos personales o del trabajo, lo que podrían ser secretos empresariales o financieros.

Por lo anterior, se recomienda tener las siguientes precauciones al momento de conectarse a una red pública.

- No conectarse a servicios bancarios o similares.
- Verificar el cifrado de los sitios web utilizados (HTTPS).
- No transmitir documentos o información sensible, especialmente del trabajo.

3.1.4 Asignación de contraseñas.

Como se ha mencionado en apartados anteriores, el uso de contraseñas es una de las formas más antiguas de proteger algo y el acceso a sitios web o programas es fundamental en estos días, por lo que se recomienda tener en mente los puntos de la siguiente **Tabla 5**.

Tabla 5
Recomendaciones para crear contraseñas seguras

Puntos	Descripción
Usar una contraseña diferente para el acceso a sitios o programas	Se debe de tener en mente que ocupar una contraseña para todos los sitios implica un gran riesgo por qué una vez descubierta esta por un tercero este tiene acceso a todos los sitios y programas donde se utilizó.
No usar nombres, apellidos, fechas de nacimiento	Mientras más difícil sea una contraseña más difícil será descifrarla. Utilizar contraseñas que impliquen nombres, apellidos, fechas de nacimiento, números telefónicos, entre otros, son realmente fáciles de descifrar sin la necesidad de programas especiales, tan sólo es necesario un poco de ingeniería social.

Puntos	Descripción
Las contraseñas deben de tener caracteres alfanuméricos, caracteres especiales y una longitud mínima de 8 caracteres	Al diseñar una contraseña se debe de tener en mente que existen diccionarios en línea y cada vez procesadores más poderosos capaces de descifrar contraseñas en cuestión de segundos, que tengan sólo números o sólo letras. Además mientras tenga una mayor longitud más difícil será de descubrir.
Cambio frecuente de contraseñas	Ninguna contraseña es totalmente irrompible, ya sea por software o ingeniería social. Utilizar una misma contraseña por mucho tiempo implica un riesgo. Se recomienda un cambio de contraseña como mínimo cada 3 meses.

Nota. Elaboración propia

3.1.5 Borrado remoto

Los dispositivos móviles como teléfonos inteligentes, tabletas o phablets hoy en día contienen una gran cantidad de información, como cuentas de correo electrónico, documentos de la organización, fotografías personales, números telefónicos, acceso a sitios restringidos, etc. Si el dispositivo es robado o perdido por el usuario, se podría comprometer no sólo al usuario sino también a la organización.

El borrado remoto garantiza que la información almacenada dentro del dispositivo móvil no vaya a ser accedida por un tercero, previniendo la fuga de información o accesos a recursos de la organización por personal ajena a esta. Este borrado remoto puede implementarse mediante un servicio contratado con una empresa o mediante software instalado en el dispositivo. Algunas de los proveedores más conocidos son el mismo Google con la solución empresarial (Google Apps Bussines), Samsung con Find my mobile y Apple con iCloud.

3.1.6 Desactivar bluetooth

Actualmente todos los dispositivos móviles cuentan con una antena bluetooth integrada, la cual les permite realizar transferencias de archivos entre dispositivos que cuenten con esta misma tecnología.

Además los dispositivos más modernos cuentan con versiones mejoradas de esta tecnología, como corregir vulnerabilidades y mejoras en transferencias de información.

Sin embargo, pese a las nuevas versiones y correcciones el hacking de bluetooth es algo bastante sencillo. En algunos casos solamente es necesario que se acepte el dispositivo del atacante para poder tomar el control del dispositivo de la víctima y otras más avanzadas ocupan herramientas en donde sólo es necesario el nombre del dispositivo.

Teniendo en cuenta esto se recomienda tomar las siguientes acciones:

- Desactivar la antena de bluetooth si no se va a utilizar.
- Mantener el dispositivo en modo oculto o invisible.
- No aceptar archivos de dispositivos desconocidos.
- Asignar contraseñas fuera de los estándares, como por ejemplo (0000, 1111,2222, etc).
- No aceptar dispositivos desconocidos.

3.1.7 Copias de seguridad

La información almacenada dentro de los dispositivos móviles es susceptible a diferentes factores. El robo o pérdida del dispositivo no son los únicos factores que afectan la integridad de la información almacenada, una falla eléctrica, golpes o caídas al agua son algunos de los riesgos susceptibles que son puestos a los dispositivos móviles.

El respaldo de información es fundamental, ya sea por medio de la nube o a un medio extraíble. Realizando esto se garantiza que en alguna catástrofe se pueda recuperar la información dentro del dispositivo. Este respaldo puede ser implementado mediante la ayuda de software.

3.1.8 Administración de aplicaciones

A pesar de la existencia de tiendas en línea como Google play o Apple store, para la adquisición de software estas no son las únicas opciones que el usuario tiene para poder instalar aplicaciones. Se puede instalar aplicaciones configurando tiendas no oficiales en el dispositivo, por ejemplo GetJar o SlideMe o descargado de la aplicación directamente de alguna página o por alguna transferencia.

La mayoría de estos usuarios son motivados por la premisa de que el software es gratis o que ha recibido algún tipo de alteración para conseguir funciones extras. Pero este tipo de programas por lo general puede contener algún malware oculto dentro de la aplicación permitiéndole a un black hat conseguir información o control del dispositivo móvil como se ha mencionado a lo largo de esta tesis.

Asimismo tampoco se puede confiar plenamente en tiendas oficiales debido a la gran cantidad de aplicaciones ofrecidas en tiendas con un porcentaje de aplicaciones con contenido malicioso. Dado esto, no se debe de confiar en su totalidad. Si una aplicación es ofrecida en una tienda oficial no implica que esté libre de código malicioso. Por eso se recomienda tener en cuenta las siguientes acciones:

- Verificar los comentarios y la reputación de las aplicaciones antes de instalarlas, mientras más baja sea la calificación más cuidado hay que tener.
- Verificar los permisos que desea obtener del dispositivo móvil una vez instalada. Aplicaciones con demasiados requisitos o extraños pueden contener algún código malicioso oculto.

Por otra parte, ningún software es totalmente seguro, siempre existirá alguna falla o vulnerabilidad que pueda ser explotada por un black hat, teniendo esto en mente es recomendable mantener las aplicaciones importantes o más populares con la última actualización.

3.1.9 Actualización de Sistema operativo

Una nueva versión del sistema operativo implica nuevos cambios y funcionalidades, además de la corrección de problemas y vulnerabilidades del anterior sistema. Si el dispositivo móvil soporta el nuevo sistema operativo sin que este pierda rendimiento se recomienda actualizarlo para evitar ser víctima de posibles fallos de seguridad.

3.1.10 Cargar batería de dispositivos móviles en computadoras

Los dispositivos móviles actuales tienen la ventaja de utilizar un cable y puerto USB estándar para poder comunicarse o cargarse. Esta ventaja es un riesgo porque por omisión al conectar un dispositivo móvil a una computadora esta lo reconoce como un medio de almacenamiento masivo o una cámara digital, permitiéndole manipular archivos dentro del dispositivo. Esta funcionalidad es aprovechada por los *black hats* como un medio para infectar dispositivos sin la necesidad de que los usuarios descarguen algún software.

3.2 Propuesta de implementación

En la sección anterior se presentó una propuesta para prevenir riesgos de la política BYOD basada en una serie de recomendaciones. Ahora, en esta sección se hará una propuesta técnica y de carácter práctico para realizar la implementación de una propuesta para mejorar la administración y la seguridad de las organizaciones, y como se ha mencionado a lo largo de esta investigación están siendo afectadas por el fenómeno de BYOD.

La implementación de la propuesta ayudará a observar su viabilidad en un ámbito real. Afortunadamente, se contó con el apoyo de una dependencia de la Universidad Nacional Autónoma de México (UNAM) para realizar esta investigación aplicada. La propuesta será diseñada para la Dirección General de Incorporación y Revalidación de Estudios (DGIRE). La propuesta se dividirá en cuatro secciones: la primera será la de una breve descripción de la dependencia, la segunda será la reestructuración de la red de cómputo, la tercera será la implementación de un sistema MDM y la cuarta será la implantación de un sistema de almacenamiento de archivos.

3.2.1 Estructura de la DGIRE

La Dirección General de Incorporación y Revalidación de Estudios (DGIRE) es una dependencia de la UNAM orientada al ambiento académico. Esta se enfoca principalmente en las escuelas incorporadas a la UNAM. Tiene como principales actividades el control de los historiales académicos de los alumnos de todas las escuelas del sistema incorporado, así como de las becas y exámenes extraordinarios, además de la expedición de certificados académicos.

Las principales áreas se encuentran organizadas como se observa en la ***Figura* 12.** Además las principales áreas se describen en la **Tabla 6.**

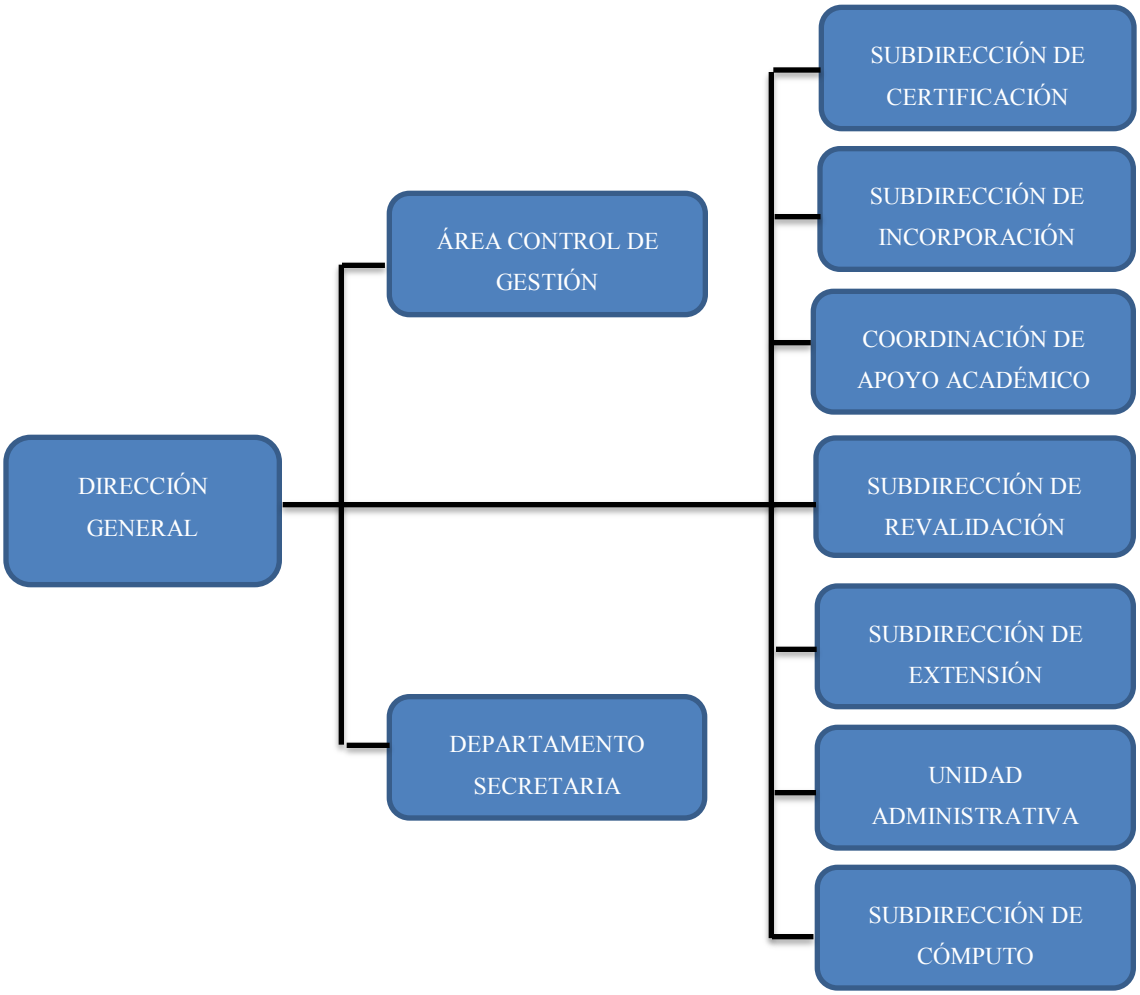

***Figura* 12. Organigrama DGIRE,** en el siguiente organigrama se presentan las áreas más importantes de la organización.

Nota. Recuperado de DGIRE (2014)

Tabla 6

Descripción de las principales áreas de la DGIRE

Área	Descripción
Dirección General	"Asegurar el cumplimiento de las normas y políticas universitarias aplicables a las instituciones con estudios incorporados a la UNAM, así como dar validez e incorporar los estudios que se realicen en otros establecimientos educativos nacionales o extranjeros".

Área	Descripción
Coordinación de Apoyo Académico	"Coordinar las actividades para la formación, superación y actualización integral del personal docente del SI, a fin de incrementar la calidad de los servicios que ofrecen las instituciones".
Subdirección de Certificación	"Vigilar la aplicación de la Legislación Universitaria en los procesos de registro, avance escolar y certificación de estudios de alumnos de las ISI".
Subdirección de Cómputo	"Atender y dar respuesta a los requerimientos de información e información en general, necesarios para el cumplimiento de las funciones de la dependencia".
Subdirección de Extensión y Vinculación	"Extender a las instituciones con estudios incorporados, los beneficios de la oferta extracurricular de la UNAM"
Subdirección de Incorporación	"Vigilar el cumplimiento del proceso de incorporación de planes de estudio de enseñanza media superior, superior y de posgrado de la UNAM, mediante la supervisión del desarrollo académico y de la planta docente de las instituciones con estudios incorporados".
Subdirección de Revalidación y Apoyo Académico	"Proponer el dictamen de revalidación y equivalencia de promedio de calificaciones de estudios realizados fuera del Sistema Educativo Nacional y gestionar la equivalencia de títulos y grados obtenidos en el extranjero".
Unidad Administrativa	"Administrar eficientemente los recursos humanos, financieros y materiales asignados, así como proporcionar los servicios generales de apoyo, cumpliendo con las políticas establecidas por la Administración Universitaria".

Nota. Recuperado de DGIRE (2014)

3.2.2 Estructuración de la red

3.2.2.1 Red física

Se propone utilizar VLANS para aislar las áreas. Esto mejorará la administración de los equipos y balanceará el tráfico de los paquetes generados, además de limitar la expansión de un malware a las demás áreas. La configuración de las direcciones IP que se propone se muestra en la **Tabla 7**.

Tabla 7
Propuesta de la configuración de la red cableada

Red	Descripción	Número de equipos
Dirección	192.168.10.0/28	16
Cómputo	192.168.11.0/26	60
Unidad Administrativa	192.168.12.0/25	128
Extensión y Vinculación	192.168.13.0/26	128
Certificación de Estudios	192.168.14.0/25	60
Revalidación de Estudios	192.168.15.0/25	128
Servidores	192.168.20.0/27	32

*Nota***.** Elaboración propia

Como se observa en la **Tabla 7**, se utilizarán direcciones IP de clase C, con máscaras variables dependiendo de la necesidad de cada área. Para la asignación de direcciones IP, se establecerán de forma estática para cada usuario, además de limitar el acceso por dirección MAC.

3.2.2.2 Red inalámbrica

Para la administración de la red inalámbrica se proponen las siguientes configuraciones descritas en la **Tabla 8**.

Tabla 8
Propuesta de la configuración de la red inalámbrica

Red	Descripción	Número de equipos
Dirección	192.168.110.0/26	64
Cómputo	192.168.111.0/26	64
Extensión y Vinculación	192.168.113.0/26	64
Certificación de Estudios	192.168.114.0/26	64
Revalidación de Estudios	192.168.115.0/26	64

Nota. Elaboración propia

Para una mejor administración de los equipos inalámbricos que se conecten a la red, se propone asignar un segmento diferente para cada punto de acceso, dependiendo del área a la que se proporcione el servicio. Se utilizarán direcciones IP de clase C, con una máscara para 64 equipos. Para la seguridad de la red inalámbrica se propone utilizar las siguientes configuraciones de acuerdo a la **Tabla 9.**

Tabla 9
Parámetros de seguridad en la red inalámbrica

Parámetros	Descripción
Firewall	Activo
Seguridad	WPA2 personal
Encriptación	TKIP o AES
Difusión de SSID	NO
Modo de red	Mixto (soporta los 802.11. b,g,n)
Modo de administración	Vía web por HTTPS

Nota. Elaboración propia

3.2.2.3 Servidor MDM (WSOS2)

Actualmente la dependencia cuenta con una infraestructura de nube (IaaS) basada en SUSE Cloud 13.1. Está tecnología se aprovechara para crear una máquina virtual e instalar el servidor de MDM (WSO2 EMM) dentro de la misma.

Esta tecnología de virtualización permite que el servicio de MDM sea escalable, transportable y modificable dependiendo las circunstancias. En la **Tabla 10** y **Tabla 11** se muestran los valores con los cuales se configuró el equipo virtual.

Tabla 10
Características físicas de máquina virtual

Características	Descripción
Procesadores	2
Arquitectura	X86_64
Memoria RAM	3 Gb
Disco Duro	20 GB
Interfaz de red	10/100/1000

Nota. Elaboración propia

Tabla 11
Software requerido para la instalación de un MDM

Software	Versión
JAVA (JDK, JRE)	1.7
MySQL	5.6.1
MySQL Connector	5.1.2
GIT	1.8.7
Eclipse Juno 4.0	4.0
Android SDK	17
Apache Ant	1.7.0
Apache Maven	3.0.2

Nota. Elaboración propia

Tabla 11
Software requerido para la instalación de un MDM

Software	Versión
JAVA (JDK, JRE)	1.7
MySQL	5.6.1
MySQL Connector	5.1.2
GIT	1.8.7
Eclipse Juno 4.0	4.0
Android SDK	17
Apache Ant	1.7.0
Apache Maven	3.0.2

Nota. Elaboración propia

3.2.3 Administración de MDM (WSO2)

Una vez instalado el software WSO2 EMM en el sistema operativo, se crearán los usuarios administradores y los usuarios locales. Dependiendo el tipo de usuario se aplicarán las siguientes políticas, las cuales se dividirán en dos ramas: Hardware y Software. Estas se mostrarán en la **Tabla 12** y **Tabla 13**.

Tabla 12
Configuraciones para el uso de los dispositivos móviles

Parámetro	Descripción
Cifrado de dispositivo	Se cifrará el contenido de los dispositivos móviles para evitar la fuga de información en caso de que el dispositivo sea robado o perdido.

Borrado remoto del dispositivo	Permitirá borrar el dispositivo móvil remotamente a través del servidor MDM.
Bloqueo de pantalla por contraseña	▪ Longitud de la contraseña (teniendo como mínimo ocho caracteres) ▪ Forzar la utilización de caracteres alfanuméricos. ▪ Establecer el mínimo de caracteres complejos (ej. @, #, etcétera). ▪ Histórico de contraseñas (no se permite repetir la misma contraseña)

Nota. Elaboración propia.

Tabla 13
Configuraciones para el uso del software

Parámetros	Descripción
Administración de WIFI	Se configurarán los parámetros de la red inalámbrica de la organización como el SSID y la contraseña a través del servidor de MDM de acuerdo al área del usuario.
Administración del correo electrónico	Se realizará la configuración de las cuentas de correo electrónico de la organización.
Administración de aplicaciones.	Se establecerá una lista negra de las aplicaciones prohibidas.

Nota. Elaboración propia.

La **Tabla 14** muestra las aplicaciones permitidas. Estas dependerán del usuario y del área a la que este pertenezca.

Tabla 14
Aplicaciones permitidas en los dispositivos móviles

Aplicaciones permitidas	Descripción
Unamsi	Programa de la dependencia

K-9 Mail	Cliente de correo electrónico
Sol Calendar	Agenda
Google Calendar	Agenda
Droid Wall	Firewall
Chrome	Navegador
Firefox	Navegador
Cliente Mysql	Cliente para conexiones a servidores MySQL
Andftp	Cliente para conexiones a servidores FTP
Any.Do	Organizador de tareas
Evernote	Organizador de tareas
Firefox	Navegador
Irssiconnectbot	Cliente para conexiones a servidores SSH
Pdfreader	Lector de PDF
Youtube	Visor de contenido

*Nota***.** Elaboración propia

3.2.4 Almacenamiento de archivos (OwnCloud)

OwnCloud es un software de código abierto para el almacenamiento de archivos, similar al servicio conocido como Dropbox. Teniendo como principal diferencia el uso de una licencia de código abierto AGPL (*Affero General Public Licence*), les permite a los usuarios la capacidad de operar, editar y configurar el software de acuerdo a sus necesidades. Además, al no depender de un servidor privado, no se tiene la limitante del almacenamiento o el número de clientes que se pueden conectar a él.

Como se mencionó en la sección anterior se bloqueará el uso de aplicaciones de terceros que no son indispensables para el desarrollo de la actividad laboral diaria. Pero también se es consciente de que algunos de los servicios ofrecidos por estas aplicaciones podrían mejorar el rendimiento de los empleados si estas son correctamente administrados y supervisados.

OwnCloud al ser un software con licencia AGPL, se considera como una opción para ser implementada en la DGIRE. Este les permitirá a los empleados la capacidad de almacenar documentos de régimen laboral en un servicio de nube privada. Además de mejorar el rendimiento de los empleados al permitirles compartir, modificar y administrar documentos desde la nube, eliminaría la fuga de datos generada por los empleados que utilizan algún software de terceros en donde la organización no tiene un control sobre los datos que se almacenan.

Para determinar el espacio requerido en el servidor y la cuota que se va a proporcionar a cada usuario, se elaboró un estudio del personal que labora en la dependencia. Como se muestra en la ***Figura* 13** la dependencia se encuentra dividida en tres grandes ramas: personal de base, personal de confianza y funcionarios.

El personal de base, a pesar de ser mayoría en la dependencia, no cumple con los requisitos para poder utilizar el sistema debido a que las actividades que desempeña de acuerdo a sus puestos no implican el uso de documentos o no son actividades de alta importancia. En cambio los funcionarios y el personal de confianza realizan actividades de una mayor importancia de acuerdo por los puestos que algunos de estos desempeñan, por ejemplo jefaturas o coordinaciones por lo que son considerados como los mejores candidatos para el uso de este servicio.

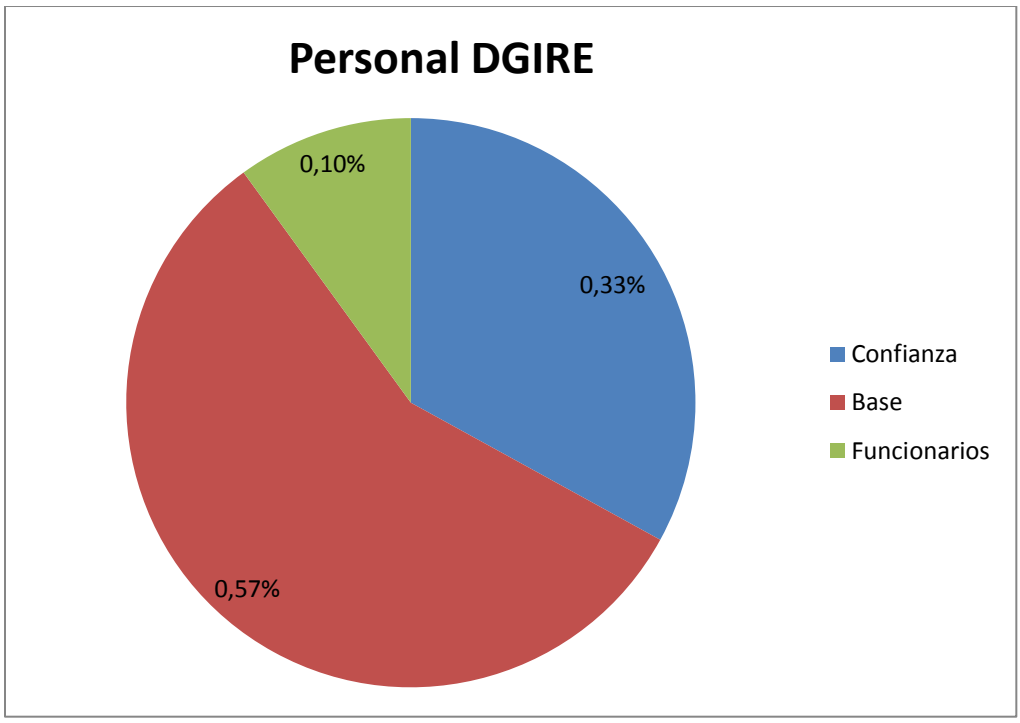

***Figura* 13. Estructura del personal que labora en la dependencia.**
Nota. Elaboración propia.

Con base en el estudio anterior se determinó un espacio de almacenamiento de 2GB por usuario. Asimismo se concluyó que el tamaño máximo de carga para un archivo sea de 20 MB como máximo salvo en algunos casos especiales donde se requiera una mayor capacidad de carga. Tomando en cuenta el tamaño de cuota por cada usuario se determinó que el espacio de almacenamiento destinado para este servicio sea de 3 TB en disco duro.

3.2.4.1 Infraestructura

Aprovechando la infraestructura de nube de la dependencia, se realizará la instalación del servicio de almacenamiento de archivos OwnCloud en un ambiente virtual, de igual manera que el servicio de MDM mencionado en apartados anteriores. A continuación, la **Tabla 15** y **Tabla 16** muestran las características de la máquina virtual destinada para OwnCloud.

Tabla 15
Características físicas del equipo virtual

Características	Descripción
Procesadores	4
Arquitectura	64 Bits
Memoria RAM	5 GB
Disco Duro	3 TB
Interfaz de red	10/100/1000

Nota. Elaboración propia.

Tabla 16
Software instalado en el equipo virtual

Características	Detalles
Sistema Operativo	SUSE Linux Enterprise Server 11, Service Pack 3 (SLES11SP3)
Dirección IP	172.168.10.2 /24
Usuarios	Root, Ownadm
Servicios	Servidor Secure Shell, Servidor HTTP con PHP y Servidor MySQL

Nota. Elaboración propia

3.2.4.2 Grupos

Se crearon los siguientes grupos que se muestra en la **Tabla 17**, tomando como base a las áreas de la dependencia. Se optó por esta estructura para poder mantener una mejor administración y control sobre los usuarios registrados en el sistema y en una posible auditoría determinar donde se realizó la fuga.

Tabla 17
Lista de grupos permitidos en el servidor virtual

Grupos	
• Dirección • Unidad de control de gestión • Incorporación • Supervisión académica • Estudios y proyectos • Control Docente • Extensión y vinculación • Actividades académicas • Actividades culturales • Actividades deportivas • Revalidación	• Certificación • Registro y control escolar • Revisión de estudios y certificación • Unidad Administrativa • Presupuesto y contabilidad • Personal • Bienes y suministros • Cómputo • Sistemas • Procesos • Seguridad

Nota. Elaboración propia

3.2.4.3 Usuarios

Para el caso de los usuarios estos se crearán de acuerdo a los siguientes lineamientos:

- Las cuentas deberán de utilizar una contraseña con una longitud de 9 caracteres como mínimo, además de contener por lo menos una letra mayúscula, una minúscula, un carácter y un número.
- Las cuentas de los usuarios solamente podrán subir como máximo 20 MB por archivo (excepto casos especiales en donde se solicite una mayor capacidad de carga).
- La cuota de los usuarios será de 2 GB.
- Los ID de los usuarios serán establecidos de acuerdo a los lineamientos establecidos en la dependencia para el uso de cuentas.
- Los usuarios deben de pertenecer al grupo de su área correspondiente.
- Los usuarios sólo pueden compartir archivos entre su mismo grupo (excepto en casos especiales donde necesite enviarlo a otras áreas).

4 Conclusiones

4.1 Resumen de los capítulos

En el presente trabajo se han analizado los diferentes elementos que se relacionan con la política BYOD y sus riesgos al momento de ser implementada. En esta tesis se decidió iniciar con un apartado dedicado a la *Seguridad informática*, en donde se muestran los conceptos de seguridad de acuerdo a instituciones o agencias gubernamentales. Además de los significados de las palabras *riesgo*, *amenaza* y *vulnerabilidad*, cuyo significado debe de estar muy claro para el desarrollo de modelos de seguridad.

Por otra parte, en el apartado de *Administración de dispositivos móviles*, se ha mencionado la amplia propagación del servicio de internet gratuito y de pago, que se ofrece en diferentes lugares, permitiendo mantener una comunicación en todo momento y casi en cualquier lugar. En conjunto con los nuevos dispositivos móviles se ha logrado crear un ambiente perfecto para la nueva tendencia conocida como BYOD en donde la comunicación por medio de voz (telefonía) ha sido rebasada por los servicios ofrecidos en la nube, ocupando los mismos en una infinidad de tareas que van desde el envío de correos electrónicos hasta las transacciones bancarias, volviéndose parte fundamental de la vida cotidiana de las personas. Pero con el auge de esta tendencia también se han desarrollado herramientas para mejorar la administración y los dispositivos móviles como es el caso de MDM y MAM.

En el siguiente apartado se habló sobre el *Sistema operativo Android*, debido a su alta popularidad en el mercado de los dispositivos móviles. En esta parte se explicó su arquitectura y su funcionamiento, además de las versiones que se han creado hasta el momento con algunas de sus principales características para un mejor desempeño en el desarrollo de políticas. También se mencionaron los sistemas de seguridad que este sistema implementa.

Debido a que el paradigma de cómputo en la nube es uno de los pilares para el desarrollo de BYOD, este se desarrolla en el apartado de *Cómputo en la nube*. En este se describe qué es el cómputo en la nube, sus características, las diferentes versiones de ella, como son: nube privada, nube publica, nube hibrida y nube comunitaria. Además se mencionó la creación de modelos de servicio como son SaaS, IaaS o PaaS, y por ultimo las ventajas y desventajas que existen en este paradigma. Este paradigma ha cambiado el modo en que se realizan ciertas actividades especialmente en el comercio del software o la renta de infraestructura. Estos servicios que anteriormente sólo eran posibles

realizarlos con infraestructura física ahora es posible rentarlos a través de internet, logrando así abaratar los costos y ofreciendo nuevos servicios a los usuarios.

En el capítulo llamado *Análisis de riesgo de la política BYOD* se desarrollan los problemas que surgen al implementar una política BYOD en las organizaciones. Revelando que existen dos grandes problemas al momento de adoptar esta política, el primero es el malware que ataca a los dispositivos móviles y el segundo es la fuga de información que se realiza a través de los mismos.

El malware hacia los dispositivos móviles es uno de los riesgos que existen al aceptar la política BYOD debido a que este ha ido creciendo de manera exponencial en los dispositivos móviles desde el inicio de los mismos y se ha ido adaptando a las nuevas tecnologías haciéndose cada vez mejor y más eficiente. Programas para monitorear los teléfonos inteligentes, software que consume el saldo de los usuarios o programas para convertir un dispositivo en un soldado que posteriormente realizará ataques a blancos más específicos como pueden ser servidores de empresas, son cosas tan comunes, y mucho de este tipo de software se puede encontrar en la red.

La fuga de información es el otro elemento que afecta a las organizaciones, originado desde dentro de la empresa por los mismos empleados. Estos por su desconocimiento del uso de la tecnología en algunos casos o por problemas con sus superiores, entre otros realizan este tipo de actividad.

Con las nuevas tecnologías como son los dispositivos móviles, conexiones a redes inalámbricas y servicios en la nube, este tipo de actividad ha ido en aumento por la facilidad en que se puede sustraer información de las organizaciones. Tan sólo es necesario conectarse a una red inalámbrica y subir el archivo a un servicio en la nube como Dropbox para poder sustraer información de la organización. Por ello se recomienda educar a los empleados, de los riesgos que existen por el mal uso de la tecnología, dado que no sólo estarían afectando a la empresa sino también a ellos mismos.

En el capítulo llamado *Propuesta para prevenir riesgos de la política BYOD* con base en la investigación realizada, se propuso un modelo para una dependencia de la UNAM, en el cual se abarcó una sección dedicada a las recomendaciones que deben de seguir los trabajadores, así como la mejora de la red de telecomunicaciones y la instalación de dos servidores virtuales para administrar los dispositivos y controlar la fuga de datos.

4.2 Resumen de la propuesta

Con base en la información recabada se realizó una propuesta para implementar un modelo para la política BYOD el cual se encuentra desarrollado en el capítulo de *Propuesta para prevenir riesgos de la política BYOD*. Para mejorar el efecto de la propuesta realizada se evaluó un caso de una dependencia de la UNAM. En este se propuso hacer cambios en la estructura de la red, creando VLANS, mejorando las contraseñas, estableciendo un orden de direcciones IP por área. Además se propuso una seria de políticas que se sugieren que sigan los empleados para el uso de los dispositivos móviles.

Por otra parte, se aprovechó la infraestructura de nube con la que cuenta la dependencia para montar dos servidores virtuales. Uno de ellos contendrá el sistema de administración de dispositivos móviles y el otro alojara un sistema de almacenamiento de documentos. Con esto se pretende prevenir la propagación del malware dentro de la organización, además de mejorar la eficiencia de los empleados al limitar el uso de aplicaciones que pueden utilizar en sus dispositivos móviles en horas laborales. Asimismo también se controlaría la fuga de información que existe por usar aplicaciones de terceros como es el caso de Dropbox.

4.3 Revisión de preguntas de investigación

En este apartado se realizará la revisión de las preguntas de investigación planteadas en la primera etapa de esta tesis. Asimismo estas se expondrán nuevamente y además se responderá a las mismas.

- *¿Cuáles son los riesgos sobre aceptar la política BYOD en las empresas?*

Con base en la investigación realizada en este trabajo se determinaron los riegos que existen al utilizar una política BYOD en las organizaciones, revelando como principales riesgos el aumento en la fuga de información y el fácil contagio de malware en los dispositivos móviles de los empleados.

- *¿Existe un modelo que pueda implementarse para contrarrestar los riesgos de la implementación de la política BYOD en la empresa?*

No, en la investigación realizada en esta tesis, no se encontraron modelos que cubrieran en su totalidad los principales riesgos al momento de implementar una política BYOD en las empresas.

Por un lado, las ventajas tecnológicas no sólo son aprovechadas por las organizaciones y los usuarios para hacer su vida más cómoda, sino también son aprovechadas por los *Black hats, Hacker, Script-kits* entre otros, debido a que estos buscan algún tipo de beneficio el cual puede ser monetario o no.

Dada la carencia de un modelo, es que se hace una propuesta en esta tesis.

4.4 Revisión de objetivos

En este apartado se realizará la revisión de los objetivos planteados en la primera etapa de esta tesis, asimismo estos se expondrán nuevamente y además se mencionará el cumplimiento de los mismos.

- *Detectar los riesgos al aceptar la política BYOD en las empresas.*

  Este objetivo se cumplió debido a que, con base en la investigación realizada, se lograron detectar los riesgos a que son propensas las organizaciones al adoptar esta política. Estos riesgos fueron el aumento de la fuga de información y la fácil propagación del malware en dispositivos móviles.

- *Proponer un modelo de seguridad para contrarrestar los riesgos de la implementación de la política BYOD en las empresas.*

  Este objetivo se logró porque en base en la investigación realizada para el desarrollo de esta tesis, se lograron determinar los principales problemas que surgen con la adopción de una política BYOD en las organizaciones y con ello se consiguió proponer en el capítulo 3 un modelo para contrarrestarlas.

4.5 Desventajas o debilidades de la propuesta

Las desventajas y limitantes que considero que puede presentar mi trabajo de investigación, son las siguientes.

- *Falta de una estrategia para la capacitación de los empleados en materia de seguridad en cómputo.*
  - El diseño de una estrategia para la capacitación de los empleados reforzaría la propuesta de seguridad en el uso de BYOD.

- *Software de protección contra malware de dispositivos móviles.*
    - Esta propuesta no contempla un estudio más amplio de sistemas de detección de malware en los dispositivos móviles. Este hubiera permitido generar una mejora en la propuesta de seguridad de los equipos móviles.
- *Conexiones seguras para ser utilizadas fuera de las organizaciones.*
    - En el caso de estudio, la propuesta no involucró un sistema de conexiones cifradas, la cual hubiera permitido tener una mayor confiabilidad en el uso de los dispositivos móviles en zonas fuera de la organización.

4.6 Aportaciones de la propuesta

El siguiente trabajo aportó los siguientes puntos.

- *Se documentaron los riesgos que una organización enfrenta al adoptar una política BYOD.*
- *Una serie de recomendaciones para mejorar la administración de los dispositivos móviles al momento de adoptar una política BYOD en las organizaciones.*
- *Se resaltó la importancia de los empleados, así como el papel que juegan en este nuevo paradigma conocido como BYOD.*
- *Se resaltó la amenaza del malware que existen en los dispositivos móviles y los riesgos que estos pueden presentar a las organizaciones.*
- *Una propuesta de implementación para una entidad real en la que se pusieron en práctica las recomendaciones propuestas.*

4.7 Trabajo futuro

A lo largo del desarrollo de esta tesis han surgido futuras líneas de desarrollo que no fueron contempladas en las preguntas de investigación, pero se espera poder desarrollarlas en un futuro trabajo. A continuación se listarán estas.

- Expansión a otros sistemas operativos.

    La propuesta como se menciona a lo largo de esta tesis, se enfoca en dispositivos móviles con sistema operativo Android, por lo que se pretende que no se límite

solamente a ese sistema sino se expanda a otros sistemas operativos como IOS, Windows Phone y Black Berry.

- Mejorar la seguridad en dispositivos móviles.

  A lo largo de esta tesis se mencionaron las amenazas y riesgos que existen en los nuevos dispositivos móviles. Aunque se intentaron hacer recomendaciones para todos los aspectos documentados, se considera que en algunos se podrían mejorar. Por ejemplo con algún tipo de módulo de seguridad como SELinux.

- Desarrollo de varios SaaS en las organizaciones.

  En el caso de estudio se optó por utilizar un servicio de nube privada, en el cual se ofrecía un servicio de hosting para los empleados similar a Dropbox, logrando así controlar en parte la fuga de información generada por los empleados. Sin embargo, existen una variedad de SaaS que se pueden implementar dentro de una nube privada que pueden controlar la fuga de información dentro de las organizaciones.

- Mejorar la capacitación de los empleados en materia de tecnología y seguridad.

  Los empleados como se ha mencionado en este trabajo, son una de las principales causas de la fuga de información y del malware que afecta a los sistemas computacionales de las organizaciones. Por ello se cree que se podría desarrollar mejores sistemas de capacitación para que los empleados sean conscientes de los riesgos y peligros que pueden provocar por el uso descuidado de sus dispositivos, lo cual no sólo puede afectar a la organización sino también a ellos mismos.

4.8 Comentarios finales

Los peligros que existen en los dispositivos móviles por causa del malware, los *Black Hats*, *Scripts Kids* y similares se podrían considerar incluso más peligros que los que se orientan a equipos de escritorio o laptops. Esto es debido al ambiente perfecto que se ha dado gracias a los siguientes elementos: el paradigma de cómputo en la nube, las mejoras en materia de telecomunicaciones y el avance en los dispositivos móviles.

Los dispositivos móviles actualmente contienen todo tipo de información, por ejemplo: nuestros contactos telefónicos, nuestra ubicación física, fotografías, videos y documentos de toda índole, contraseñas, recordatorios, agendas, acceso a sitios web, que van desde redes sociales, bancos

y páginas internas de las organizaciones donde se labora, tan sólo por mencionar unos cuantos usos. Todo esto es utilizado de una manera descuidada por parte de la mayoría de las personas.

Además la mayoría del malware que existe por la red, se ha vuelto relativamente fácil de conseguir y de usar, solamente los más especializados se pueden conseguir como se mencionó en esta tesis, en el mercado negro. Lo anterior es altamente preocupante, pero por fortuna la mayoría de este tipo de software es orientado a afectar el mayor número de dispositivos, atacando valores y configuraciones ya preestablecidos o estándares, además los usuarios que lo consumen no se molestan en modificarlo para adaptarlo a objetivos más específicos, tal vez por desconocimiento o porque saben que existen más usuarios usando las configuraciones estándares. Así que realizando cambios en las configuraciones se puede evadir este tipo de programas.

El factor humano, en otras palabras los empleados, son el principal riesgo que existen en las organizaciones al no contar con una educación sobre los riesgos y peligros que pueden causar si violan las políticas de seguridad establecidas. Por lo anterior, se piensa que con una buena educación para el personal, sumado con técnicas, políticas y estándares, se podría aumentar los niveles de seguridad de las organizaciones. Asimismo se hace hincapié en la formación de los empleados sobre los peligros que ellos mismos pueden causar de forma consiente o no, debido a que no importa qué tan eficiente sea el sistema o modelo de seguridad que se diseñe, si el usuario no sabe los principios básicos de seguridad, lo anterior no servirá y más en este nuevo paradigma conocido como BYOD, en donde el empleado lleva su propio dispositivo al trabajo.

Bibliografía

P. Aronson, J., Brownlee, N., Byrum, F., & Nuno Ferreira, J. (Septiembre de 1997). *ietf*. Recuperado el 22 de Febrero de 2014, de https://www.ietf.org/rfc/rfc2196.txt

A Shepherd, S. (2003). Vulnerability Disclosure How do we define Responsible Disclosure. *SANS INSTITUTE Information Security Reading Room*, 21.

Ackerman, E. (23 de Agosto de 2013). The bring your own device dilema: Employees and businesses seek to balance privacy and security. Estados Unidos.

Alleau, B., & Desemery, J. (30 de Enero de 2013). Bring Your Own Device: It's all about Employee Satisfaction and Productivity, not Costs!

Anderson, H., Kaplan, J., & Smolinski, B. (Octubre de 2012). Capturing value from IT infrastructure innovation.

Android. (3 de Marzo de 2014). *Develope Android.* Recuperado el 24 de Marzo de 2014, de http://developer.android.com/about/dashboards/index.html

Arbaugh, W., Fithen, W., & McHugh, J. (2000). Windows of Vulnerability: a Case Study Analysis. *IEEE*.

Arbrust, M., & Fox, A. (2010). A view of cloud computing. *Communications of the acm*, 9.

AV-Test. (2013). AV-TEST Examines 22 Antivirus Apps for Android Smartphones and Tablets. *AV_TEST*, 6. Recuperado el 14 de marzo de 2014, de http://www.av-test.org/fileadmin/pdf/avtest_2013-01_android_testreport_english.pdf

Bye, R., & Schmidt, A. D. (2009). Static Analysis of Executables for Collaborative. *IEEE Communications Society*, 5.

Cabrero Almenera, J. (1998). Impacto de las nuevas tecnologías de la información y la comunicación en las organizaciones educativas. Sevilla, España.

Calder, A. (2013). Is the BYOD Movement Worth the Risk? *Credit Control*, p65-70.

Camacho Vargas, Á. (2012). Uso de cloud computing en el sistema nacional de archivos de Colombia: implementación del plan de gestión de documentos vitales. *Códice (Bogotá)*, 21.

Cancela García, L., & Ostos Gutiérrez, S. (s.f.). *Software de Comunicaciones.* Recuperado el 4 de Julio de 2014, de https://sites.google.com/site/swcuc3m/home/android/generalidades/2-2-arquitectura-de-android

CISCO. (2009). *CISCO*. Recuperado el 25 de Mayo de 2014, de http://www.cisco.com/web/LA/soluciones/strategy/education/connection/pdfs/Cisco_Campus_Technology_Whitpaper.pdf

CISCO. (2014). *Cisco Visual Networking Index: Global Mobile Data Traffic Forecast Update, 2013–2018*. Recuperado el 12 de Febrero de 2014, de http://www.cisco.com/en/US/solutions/collateral/ns341/ns525/ns537/ns705/ns827/white_paper_c11-520862.html?CAMPAIGN=MobileVNI2014&COUNTRY_SITE=us&POSITION=link&REFERRING_SITE=cisco+blog&CREATIVE=MobileVNI+2014

Cisco System. (2008). *Cisco.* Recuperado el 12 de Abril de 2014, de http://www.cisco.com/c/en/us/solutions/collateral/enterprise-networks/data-loss-prevention/white_paper_c11-499060.html

Comité de Seguridad de la Informacion. (2009). *Políticas de Seguridad de la Información* . Mar del Plata: Universidad Tecnológica Nacional Rectorado.

Coogan, P. (5 de Marzo de 2014). *Symantec.* Recuperado el 21 de Marzo de 2014, de http://www.symantec.com/connect/blogs/android-rats-branch-out-dendroid

Coursen, S. (2007). The future of mobile malware. *Network Security*, 7.

Curry, D., Kirkpatrick, S., Longstaff, T., & Hollingsworth, G. (Julio de 1991). *ietf*. Recuperado el 22 de Febrero de 2014, de http://www.ietf.org/rfc/rfc1244.txt

D. Dagon, T. M. (2004). Mobile phones as computing. *IEEE Pervasive Computing, IV*, 11–15.

Deloitte. (2013). TMT Global Security Risk Study.

DGIRE. (19 de 10 de 2014). *DGIRE*. Obtenido de http://www.dgire.unam.mx/contenido/acerca/manual_organizacion.pdf

Disterer, G., & Kleiner, C. (2013). BYOD Bring Your Own Device. *ScienceDirect*, 11.

ENISA . (11 de Diciembre de 2013). ENISA Threat Landscape 2013. Europa.

EY. (Septiembre de 2013). BYOD Security and risk considerations for your mobile device program.

Ford, G. (5 de Febrero de 2014). BYOD Consumer Demand and Information Security.

F-SECURE. (11 de Mayo de 2012). Mobile thread report Q1 2012.

García , A. (24 de Mayo de 2013). Esquema de red DGIRE. México, Distrito Federal, México.

Gartner. (3 de Junio de 2008). Assessing the security risk of cloud computing. Estados Unidos.

Gartner. (2013). *It-glossary.* Recuperado el 3 de 09 de 2014, de http://www.gartner.com/it-glossary/mobile-device-management-mdm/

Gelbstein , E. (2011). *Isaca.* Recuperado el 26 de Febrero de 2014, de http://www.isaca.org/Journal/Past-Issues/2011/Volume-6/Pages/Data-Integrity-Information-Securitys-Poor-Relation-spanish.aspx

Gest, J. (2013). Managing BYOD: How to mitigate the risk of using personal devices in the workplace. *SmartBusiness*, p20.

Google. (26 de Septiembre de 2012). *Google Developers.* Recuperado el 8 de Julio de 2014, de https://developers.google.com/android/c2dm/?hl=es

Gordon, P. (15 de Octubre de 2007). Data Leakage - Threats and Mitigation. Recuperado el 31 de Marzo de 2014, de http://www.sans.org/reading-room/whitepapers/awareness/data-leakage-threats-mitigation-1931?show=data-leakage-threats-mitigation-1931&cat=awareness

Gruman, G. (26 de Abril de 2011). *InfoWorld*. Obtenido de http://www.infoworld.com/article/2624028/application-security/mobile-application-management-without-the-heavy-hand.html

Gruškovnjak, J., Lombardo, A., & Taylor, S. (2012). *cisco*. Recuperado el 1 de Mayo de 2014, de http://www.cisco.com/web/about/ac79/docs/sp/SP_Wi-Fi_Consumer_Briefing-Doc_Mexico_SPANISH.pdf

Gupta, A. (2014). *Learning Pentesting for Android Devices.* Birmingham: Pack Publishing.

Howie, J. (2012). BYOD Security: Bring your own device – but secure it first! *Windows IT Pro*, p37-45.

ISO. (2009). IS/ISO/IEC 13335-1. India. Recuperado el 2 de Febrero de 2014

ISO. (1 de Junio de 2011). ISO/IEC 27005. Suiza.

Janssen, C. (8 de Agosto de 2014). *technopedia*. Obtenido de http://www.techopedia.com/definition/29717/mobile-application-management-mam

Jorba Esteve, J., & Suppi Boldrito, R. (2004). *Administración Avanzada de GNU/Linux.* Barcelona: Eureca Media, SL.

Kang, D. (12 de Noviembre de 2013). Ambiente BYOD. *A Study on Abnormal Behavior Detection in BYOD Enviroment*. corea.

Kang, D., Oh, J., & Im, C. (2013). A Study on Abnormal Behavior Detection in BYOD Enviroment. *International Journal of Enviromental, Earth Science and Engineering*, 4.

Kaspersky Lab. (10 de Diciembre de 2013). *http://www.securelist.com/en/.* Recuperado el 16 de Marzo de 2014, de http://www.securelist.com/en/analysis/204792318/Kaspersky_Security_Bulletin_2013_Overall_statistics_for_2013

Kaspersky Lab. (Agosto de 2013). *Kaspersky*. Recuperado el 10 de April de 2014, de http://media.kaspersky.com/pdf/Kaspersky_Lab_B2C_Summary_2013_final_EN.pdf

Khan , H. (8 de Marzo de 2014). *appsngizmo*. Recuperado el 24 de Marzo de 2014, de http://www.appsngizmo.com/dendroid-trojanizer-turns-apps-malware/

Khanna, R. (Agosto de 2013). Data breaches:the enemy within.

Krajci, I., & Cummings, D. (2014). *Android on X86.* Apress Open .

Lelli, A. (16 de Julio de 2013). *Symantec.* Recuperado el 22 de Marzo de 2014, de http://www.symantec.com/connect/blogs/remote-access-tool-takes-aim-android-apk-binder

Lookout. (2013). *Five key Business insights for mobile security in a BYOD worls.* San Francisco, CA.

Lucena Lopéz, M. (2008). *Criptografía y seguridad en computadores.* Jaén: Universidad de Jaén.

Management Services. (2012). Mobile technology for increased productivity and profitability. *Management Services*, p15-17.

Martínez, F. C., & Galán, B. V. (11 de Diciembre de 2010). *Cómputo en la nube: Ventajas y Desventajas*. Recuperado el 15 de Julio de 2014, de http://revista.seguridad.unam.mx/numero-08/c%C3%B3mputo-en-nube-ventajas-y-desventajas

Mather, T., Kumaraswamy, S., & Latif, S. (2009). *Cloud Security and Privacy.* United States of America : O'Reilly .

McCarty, B. (2003). *Firewalls.* Madrid: Anaya.

Miller, M. (2009). *Cloud Computing: Web-based applications that change the way you work and collaborate online.* Indiana: QUE.

Mont, J. (2012). The Risks and Benefits of Employee-Owned Devices. *Compliance and Technology*, p38-39.

Moore, C. (13 de Noviembre de 2013). *Macprices*. Recuperado el 12 de Febrero de 2014, de http://www.macprices.net/2013/11/13/ios-hits-new-record-android-pushes-past-80-market-share-and-windows-phone-shipments-leap-156-0-year-over-year-in-3q13-idc/

Moore, C. (13 de Noviembre de 2013). *Macprices*. Recuperado el 12 de Febrero de 2014, de http://www.macprices.net/2013/11/13/ios-hits-new-record-android-pushes-past-80-market-share-and-windows-phone-shipments-leap-156-0-year-over-year-in-3q13-idc/

Morrow, B. (2012). BYOD security challenges: control and protect your most sensitive date. *Network Security*, 4.

Navetta, D. (28 de Marzo de 2012). *InfoLawGroup.* Recuperado el 12 de Marzo de 2014, de http://www.infolawgroup.com/2012/03/articles/byod/the-security-privacy-and-legal-implications-of-byod-bring-your-own-device/

NIST. (Septiembre de 2011). *NIST.* Recuperado el 28 de 06 de 2014, de http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf

Opensecurity Architecture. (2014). *Opensecurity Architecture*. Recuperado el 15 de Febrero de 2014, de http://www.opensecurityarchitecture.org/cms/definitions/it-security

Osterman. (2012). Putting IT Back in Control of BYOD.

P.E, C. (2003). *A History of Modern Computing.*

Pallis, G. (2010). Cloud Computing: The New Frontier of Internet Computing. República de chipre.

Pereira García, J. (2012 de Mayo de 2012). *Androcode.* Recuperado el 6 de Julio de 2014, de http://androcode.es/2012/05/c2dm-notificaciones-push-parte-i/

Pillay, A., Diaki, H., & Nham, E. (2013). Does BYOD increase risk or drive benefits? Merlbourne, Victoria, Australia.

Ponemon Institude. (Mayo de 2013). 2013 Cost of Data Breach Study: Global Analysi. Michigan, Estados Unidos.

Potts, M. (Julio de 2012). The state of information security.

Powell, H. (s.f.). *Mcfee*. Recuperado el 31 de Marzo de 2014, de http://www.mcafee.com/uk/resources/white-papers/foundstone/wp-data-loss-prevention-program.pdf

Rains, J. (Marzo de 2012). Bring your own device (BYOD) Hot or Not.

Rajaraman, V. (2014). Cloud Computing. *RESONANCE*, 17.

redes, E. d. (1998). *Manual de Seguridad en Redes.* Buenos Aires: Subsecretaría de Tecnologías Informáticas Secretaría de la Función Pública.

Rogers, M. (6 de Marzo de 2014). *https://blog.lookout.com/.* Recuperado el 21 de Marzo de 2014, de https://blog.lookout.com/blog/2014/03/06/dendroid/

Rouse, M. (Octubre de 2009). *Search Security.* Recuperado el 22 de Marzo de 2014, de http://searchsecurity.techtarget.com/definition/RAT-remote-access-Trojan

Rouse, M. (11 de Octubre de 2010). *searchmidmarketsecurity.techtarget*. Recuperado el 20 de Febrero de 2014, de http://searchmidmarketsecurity.techtarget.com/definition/risk-analysis

Rouse, M. (Junio de 2014). *Techtarget.* Recuperado el 15 de Agosto de 2014, de http://searchconsumerization.techtarget.com/definition/mobile-application-management

Sabharwal, N., & Shankar, R. (2013). *Apache CloudStack Computing.* United Kingdome: Packt .

Sabharwal, N., & Wali, P. (2013). *Cloud Capacity Management.* Apress.

Singh, N. (Diciembre de 2012). B.Y.O.D. Genie is out of the bottle "Devil or Angel". Pune, India.

Sophos. (2014). *Sophos.* Recuperado el 20 de Marzo de 2014, de http://www.sophos.com/en-us/threat-center/security-threat-report.aspx

Sosinsky, B. (2011). *Cloud computing.* Indianapolis: Wiley Publishing.

Steele, C. (2013). *Mobile device management vs. mobile application management*. Obtenido de http://searchconsumerization.techtarget.com/feature/Mobile-device-management-vs-mobile-application-management

Steele, C. (2013). *Mobile device management vs. mobile application management.* Recuperado el 4 de Septiembre de 2014, de http://searchconsumerization.techtarget.com/feature/Mobile-device-management-vs-mobile-application-management

Stoneburner, G., Goguen, A., & Feringa, A. (2002). Risk Management Guide for Information Technology Systems. *Recommendations of the National Institute of Standards and Technology*, 56.

Symantec. (Abril de 2013). Recuperado el 19 de Marzo de 2014, de Symantec: http://www.symantec.com/security_response/publications/threatreport.jsp

Symantec. (6 de Febrero de 2013). *Symantec Corporation*. Recuperado el 1 de Abril de 2014, de https://symantec-corporation.com/servlet/formlink/f?kPugHuQYUAD&ACTIVITYCODE=157115&inid=GL_NA_WP_WhatsYoursIsMine-HowEmployeesarePuttingYourIntellectualPropertyatRisk_dai211501_cta69167_aid157115

The Internet Engineering Task Force. (Julio de 1991). *The Internet Engineering Task Force*. Obtenido de https://www.ietf.org/rfc/rfc1244.txt

Thomson, G. (2012). BYOD: Enabling the chaos. *Network Security*, 4.

Tokuyoshi, B. (Abril de 2013). The security implications of BYOD. Santa Clara, San Francisco, Estados Unidos.

Trend Micro. (16 de Septiembre de 2013). *About Threats.* Recuperado el 27 de Marzo de 2014, de http://about-threats.trendmicro.com/us/infographics/infograph/the-high-cost-of-premium-service-abusers

TrendLabs. (17 de Abril de 2012). Security in the Age of Mobility.

TrendLabs. (13 de Noviembre de 2013). *Trend Micro.* Recuperado el 26 de Marzo de 2014, de http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/reports/rpt-trendlabs-3q-2013-security-roundup.pdf

Universidad de Miami Leonardo M. Miller. (2008). *http://it.med.miami.edu*. Recuperado el 2014, de http://it.med.miami.edu/x904.xml

W. Miller, K. (2012). BYOD: Security and Privacy Consideration. *IEEE Computer society*, 3.

Williams, B. (2012). *The economics of cloud computing.* Indianapolis: Cisco Press.

Wood, A. (Agosto de 2012). *BCS*. Recuperado el 14 de Julio de 2014, de http://www.bcs.org/content/conWebDoc/47519

Yu, R. (2013). *Virusbtn.* Recuperado el 20 de Marzo de 2014, de http://www.virusbtn.com/conference/vb2013/abstracts/Yu.xml