ESTADO DEL ARTE VULNERABILIDADES DE SEGURIDAD EN SISTEMAS OPERATIVOS MÓVILES ANDRIOID Y IOS

YAMIR ASMIRIO MUÑOZ CACERES

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BASICAS, TECNOLOGIAS E INGENIERIAS
ESPECIALIZACION EN SEGURIDAD INFORMATICA
BUCARAMANGA
2019

ESTADO DEL ARTE VULNERABILIDADES DE SEGURIDAD EN SISTEMAS OPERATIVOS MÓVILES ANDRIOID Y IOS

YAMIR ASMIRIO MUÑOZ CACERES

TRABAJO DE MONOGRAFÍA COMO REQUISITO DE GRADO PARA OPTAR EL TÍTULO DE ESPECIALISTA EN SEGURIDAD INFORMÁTICA

DIRECTOR DE PROYECTO: INGENIERO CHRISTIAN REYNALDO ANGULO

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BASICAS, TECNOLOGIAS E INGENIERIAS
ESPECIALIZACION EN SEGURIDAD INFORMATICA
BUCARAMANGA
2019

Nota de aceptación

_____

_____

_____

_____

_____

_____

Firma del presidente del jurado

_____

Firma del jurado

_____

Firma del jurado

Bucaramanga, _____

DEDICATORIA

Inicialmente a Dios y a mi familia, por su apoyo incondicional brindado durante el desarrollo de la especialización y a la Universidad Nacional Abierta y a Distancia UNAD por el apoyo brindado para el desarrollo de la presente monografía.

AGRADECIMIENTOS

A Dios Todopoderoso, por brindarme la fuerza y fortaleza para llevar a cabo este trabajo.

A mi familia, por su apoyo incondicional tanto el actual proceso formativo, así como en todos mis proyectos personales y profesionales.

A las personas asignadas por la Universidad Nacional Abierta y a Distancia UNAD para brindar asesoría en el desarrollo de la presente monografía, el Ingeniero Juan José Cruz y el Ingeniero Christian Reynaldo Angulo, por sus aportes y sugerencias brindadas durante el desarrollo de la presente monografía.

TABLA DE CONTENIDO

Pág

LISTA DE FIGURAS

Pág

LISTA DE TABLAS

Pág.

LISTA DE ANEXOS

Pág.

RESUMEN

El auge de los dispositivos móviles en la actualidad hace que muchas personas los consideren parte fundamental de sus labores diarias, tanto a nivel personal como a nivel laboral. Sus funcionabilidades, sus portabilidad y facilidad de uso, hacen que estos equipos hallan inundado el mercado de la tecnología en los últimos años. De la misma forma en que los usuarios de estas tecnologías se han incrementado exponencialmente, los riegos y amenazas a los que se encuentran expuestos estos equipos también se han incrementado en los últimos años.

En monográfico de seguridad en dispositivos móviles se considera:" Es evidente que los dispositivos móviles son cada vez más potentes y, de alguna forma, se parecen cada vez más a sus hermanos mayores -los ordenadores de sobremesa o los ordenadores portátiles- desde el punto de vista de las capacidades y funcionalidades que incorporan. Pero estas similitudes no terminan en sus capacidades o funcionalidades, sino que además están igualmente expuestos a amenazas similares"[1] Esto lleva a la conclusión de que, a pesar de su gran auge y características ofrecidas, las cuales los hacen más cercanas a sus competidores directos en el mercado, los dispositivos móviles están igual o en mayor porcentaje expuestos a inconvenientes de seguridad.

Independientemente del tipo de dispositivo utilizado bien sea portátiles o móviles, una de las principales preocupaciones de los usuarios al hacer uso de sus dispositivos es la seguridad. Partiendo de esta premisa, Flores[2] plantea que, a pesar de los riesgos existentes de ataques de virus o software malicioso en los dispositivos móviles, la mayoría de los usuarios no hacen uso de ningún tipo de software antivirus, dando más importancia a su privacidad que a la seguridad de los mismos frente a posibles ataques maliciosos.

[1] Monográfico de seguridad en dispositivos móviles [en línea]. Instituto Nacional de Tecnologías de la Comunicación [Consultado:15 de Marzo de 2018]. Disponible en Internet: https://www.firma-e.com/wp-content/uploads/2013/03/monografico_seg_disp_moviles.pdf

[2] FLORES, Javier. ¿Qué es lo que más preocupa a quienes usan Smartphone Android? [en línea]. Revista Muy Intersante.párr.1.[Consultado: 15 de Abril de 2018].Disponible en Internet: https://www.muyinteresante.es/curiosidades/preguntas-respuestas/ique-es-lo-que-mas-preocupa-a-quienes-usan-smartphones-android

La empresa de seguridad danesa SPAMfighter plantea en uno de sus estudios que “El 59 por ciento de los usuarios de Android no hace uso de antivirus, ya sea en sus Smartphone o en sus tabletas. De hecho, los usuarios, a pesar de que conocen la existencia de oleadas de ataques de spam, no lo consideran un problema a tener en cuenta. Solo un 25,5 por ciento de los usuarios de Smartphone se preocupa por el riesgo de navegar sin herramientas que garanticen la seguridad”[3].

El trabajo de monografía está enfocado en desarrollar una investigación acerca de las vulnerabilidades o fallas identificadas en dispositivos móviles con sistemas operativos Android y IOS. Respecto a este tema, Pacheco y Piazza plantean “la problemática de seguridad en dispositivos móviles se incrementa tanto por el desconocimiento de los inconvenientes de seguridad como las contramedidas o soluciones que se ofrecen por los fabricantes frente a estas amenazas”[4].

Para llevar a cabo este objetivo, se tendrán en cuenta las siguientes actividades que nos ayudarán a desarrollar el objetivo inicialmente propuesto: realizar estudio acerca de las vulnerabilidades más comunes en los sistemas operativos móviles Android y IOS, determinar fallas de seguridad que se presentan en sistemas operativos móviles Android y IOS y la forma de mitigarlas e identificar los principales errores que cometen los usuarios de dispositivos móviles relacionados con aspectos de seguridad.

Como parte introductoria al presente trabajo, se abarcará el tema de arquitecturas de los sistemas operativos móviles conceptos y clasificación de dispositivos móviles. Para el caso de Android, se describen elementos como: aplicaciones, framework de aplicaciones, librerías, y Run Time de Android. Por otro lado, haciendo referencia a los modelos IOS, su trabajo de arquitectura se basa en capas las cuales se pueden describir como: Core OS, capa de servicios principales, capa de media y Cocoa Touch Layer.

---

[3] Ibid.,p. 13.

[4] PACHECO SEBASTIAN, Exequiel Y PIAZZA ORLANDO Carlos Damián. Estudio y análisis de seguridad en dispositivos móviles. BYOD y su impacto en las organizaciones [en línea]. Tesis presentada para optar al título de Licenciatura en Sistemas. La Plata, Argentina. Universidad Nacional de la Plata. Facultad de Informática, 2016. p. 8. [Consultado; 16 de abril de 2018]. Disponible en Internet: http://sedici.unlp.edu.ar/bitstream/handle/10915/58591/Documento_completo.%20y%20Piazza%20Orlando,%20C.%20Estudio%20y%20an%C3%A1lisis%20de%20seguridad%20en%20dispositivos%20m%C3%B3viles.pdf-PDFA.pdf?sequence=4&isAllowed=y

Los riesgos, ataques y amenazas que están vinculadas con aplicaciones móviles en las plataformas Android y IOS también son tratados en la monografía, con el objeto de conocerlos y brindar recomendaciones a cerca de procedimientos a llevar a cabo para mitigar este tipo de situaciones. En esta parte de la investigación también se aborda el tema del estado de arte de los ataques a dispositivos móviles en la región y en país.

Adicionalmente a lo anterior, se llevará a cabo una consulta acerca de herramientas que se enfocan en el tratamiento de aspectos se seguridad en dispositivos móviles. Se lleva a cabo una clasificación dependiendo de las plataformas sobre las cuales funcionan dichas herramientas. Complementando la información anterior, se brindan algunas recomendaciones a la hora de hacer uso de Smartphones con el objeto de mitigar problemas de seguridad que se puedan presentar.

Seguidamente, se lleva a cabo una investigación acerca de cómo se comporta el mercado de teléfonos móviles en cuanto a la cantidad de usuarios que hacen uso de las principales plataformas. Esta información se plasma en tablas o gráficos de tal manera que sea más sencillo para los lectores analizar sus proyecciones a futuro. Como parte final de la monografía se identifican lo errores de seguridad más comunes a los cuales se exponen este tipo de dispositivos.

INTRODUCCIÓN

En esta monografía se pretende mostrar un análisis de vulnerabilidades que se presentan en los sistemas operativos para móviles más populares en el mercado. Inicialmente se propone ahondar un poco en la historia de los dispositivos móviles incluyendo algunas generalidades y explicando los tipos de dispositivos existentes. Luego se tratan las plataformas Android y IOS, plasmando sus principales características y arquitecturas. Seguidamente se muestran las diferentes vulnerabilidades o fallas encontradas en los sistemas operativos y la forma en que ellas se pueden mitigar o atacar.

El surgimiento que se ha presentado en los últimos tiempos de los dispositivos móviles es una realidad. Existen características que los hacen muy llamativos a los usuarios, principalmente la movilidad que brinda la posibilidad de tener información necesaria en cualquier lugar y momento, tendiendo los accesos a redes requeridas para hacer uso de ellas. La reducción en sus costos es otra de las barreas que se han superado en la actualidad. Solo teniendo en cuenta estas dos variables, es normal que el usuario final empiece a considerarlo como elemento primordial en su vida diaria, en campos como académicos, laborales y profesionales. El tipo de información que se maneja y almacena en ellos empieza a ser de vital importancia para cada uno de sus propietarios. Es allí donde entra el concepto de seguridad de dispositivos a jugar a papel preponderante.

A pesar de que no existen en el mundo de las tecnologías de la información ambientes totalmente seguros, y que el de los dispositivos móviles no se escapa a esta situación. El paso inicial para empezar a analizar formas para mitigar las fallas de seguridad en este tipo de dispositivos es tener conciencia de que para mantener un nivel de seguridad mínimo de nuestra información almacenada en los equipos móviles debemos identificar inicialmente los riegos y amenazas a los que estamos expuestos con el uso de este tipo de dispositivos y tener en cuenta una serie de pautas o acciones que nos ayudarán a salvaguardar de alguna forma nuestros datos que generalmente son de carácter confidencial y personal.

Algunos de los objetivos que se tratan logar con la investigación se encuentran: Identificar los errores que cometen los usuarios de dispositivos móviles en cuanto a aspectos de seguridad los cuales aumentan las posibilidades de accesos indebidos o malware a los dispositivos, identificar al momento de configurar los equipos aspectos de seguridad disponibles para los diferentes plataformas

existentes, determinar fallas de seguridad que presentan los plataformas IOS y Android y formas de mitigar dichas fallas.

La temática a tratar en la investigación será: Historia y evolución de los dispositivos móviles, arquitecturas de los dispositivos basados en Android y OIS, identificación de vulnerabilidades detectadas en los sistemas operativos abordados en la investigación y como se han tratado de mitigar, y recomendaciones para reducir la posibilidad de ataques en las plataformas de dispositivos móviles Android y IOS.

1. DEFINICIÓN DEL PROBLEMA

1.1 ANTECEDENTES

El auge de los dispositivos móviles en la actualidad hace que muchas personas los consideren parte fundamental de sus labores diarias, tanto a nivel personal como a nivel laboral. Sus funcionabilidades, sus portabilidad y facilidad de uso hacen de estos equipos hallan inundado el mercado de la tecnología en los últimos años.

De la misma forma en que los usuarios de estas tecnologías se han incrementado exponencialmente, los riegos y amenazas a los que se encuentran expuestos estos equipos también se han incrementado en los últimos años.

Según se plantea en artículo de la compañía Kaspersky “Aunque el malware dirigido a atacar dispositivos móviles no llega aún al nivel de las PC en términos de volumen y complejidad, estudios están identificando tipos de malware más específicos dirigidos a dispositivos móviles cuyo fin es atacar las funciones de los teléfonos y las vulnerabilidades de las tablets”[5]

1.2 FORMULACIÓN DEL PROBLEMA

Toda esta problemática nos lleva a una plantearnos la siguiente pregunta: ¿Que tan segura puede estar nuestra información almacenada en los equipos móviles con Sistemas Operativos Android y OIS?

[5] Amenazas de seguridad móvil dirigidas a dispositivos Android [en línea]. Kaspesky Latinoamérica. Consultado: [1 de Septiembre de 2018]. Disponible en Internet: https://latam.kaspersky.com/resource-center/threats/mobile

1.3 DESCRIPCIÓN DEL PROBLEMA

Hoy en día, los dispositivos móviles se han convertido en elementos comúnmente encontrados en los quehaceres diarios de las personas. Su incursión en el ámbito laboral y personal ha puesto a las organizaciones a tomar mucho más en serio los inconvenientes de seguridad que los afectan debido al uso de estos dispositivos. Con el desarrollo de nuevas funcionabilidades, tales como redes sociales, banca electrónica, correo, están llevando a los Smartphone como punto de ataque de delincuentes informáticos, que buscan tener acceso a información personal crítica y de esta forma llevarse a cabo infracciones del tipo suplantación de identidad y accesos no autorizados.

Los usuarios de las aplicaciones móviles no son conscientes del riesgo y por ende no toman medidas mínimas en los temas de seguridad de sus dispositivos móviles. Según Informe de reporte Anual sobre amenazas para la seguridad en Internet publicado por la empresa Symantec "La cantidad de nuevas variantes de malware para dispositivos móviles aumentó un 54% en 2017, en comparación a 2016".[6]

Siguiendo el informe anteriormente citado se indica "Los usuarios de dispositivos móviles también enfrentan riesgos de privacidad generados por aplicaciones de grayware, que no son totalmente malintencionadas, pero pueden ser problemáticas. Symantec identificó que el 63% de las aplicaciones de grayware filtran el número de teléfono del dispositivo. Con el aumento de grayware en un 20% en 2017, este problema simplemente no desaparecerá"[7].

Con el objeto de aclarar el concepto expuesto por la Symantec, Kovacs[8] define grayware como un programa que a pesar de no ser malicioso puede resultar bastante molesto. Los avisos tipo pop-pup, tan comunes en este tipo de

[6] Informe sobre amenazas para la seguridad en Internet [en línea]. Symantec. [Consultado; 20 de Abril de 2018]. Disponible en Internet: https://www.symantec.com/content/dam/symantec/mx/docs/reports/istr-23-executive-summary-mx.pdf

[7] Ibid.,p.19.

[8] KOVACS, Nadia. ¿Qué es Grayware, Adware y Madware ? [en línea]. Norton Protection Blog. 7 de abril de 2016, párr. 2. Consultado: [20 de abril de 2018]. Disponible en Internet: https://community.norton.com/es/blogs/norton-protection-blog/%C2%BFqu%C3%A9-es-grayware-adware-y-madware

aplicaciones, pueden afectar el desempeño del acceso a Internet, así como llevar a cabo un registro de páginas o lugares visitadas.

2. JUSTIFICACIÓN

En la actualidad los dispositivos móviles están más cerca de los usuarios. Aquellas épocas en las que la variable precio entraba a jugar papel importante en la decisión de adquirir el Smartphone preferido quedaron atrás. La forma de utilizar la tecnología ha cambiado drásticamente con la inclusión en el mercado de estos dispositivos. Redes sociales, accesos a internet, transacciones bancarias, entre otros servicios se pueden llevar a cualquier lugar sin ningún tipo de inconvenientes.

Es normal pensar que, debido a su gran crecimiento a nivel mundial, se hayan incrementado los ataques a estos dispositivos. El Centro de Estudios, Respuesta y Tratamiento de Incidentes de Seguridad en Brasil[9], plantea que los riegos que se han presentado con el uso de los Smartphone son: filtrado de información, invasión de privacidad, instalación de aplicaciones maliciosas, propagación de código malicioso, y posibilidad de pérdida o robo. Además, ESET[10] plantea en su artículo, que se debe tener en cuenta que cada vez los usuarios de dispositivos móviles almacenan información considerada sensible, lo que los convierte en un campo de acción bastante importante para los cibercriminales, quienes, buscando principalmente beneficios económicos, han incrementado los ataques haciendo uso de ataques que contienen códigos maliciosos.

Un punto adicional es la gran variedad de plataformas existentes haciendo casi imposible la creación o estandarización de políticas en temas de seguridad que mitiguen los ataques a los cuales están expuestos estos dispositivos.

Estadísticas de Kaspersky Lab revelaron que “los usuarios en América Latina han recibido un total de 677,216,773 ataques de malware durante los primeros ocho

[9] Seguridad en los Dispositivos Móviles [en línea]. Centro de Estudios, Respuesta y Tratamiento de Incidentes de Seguridad en Brasil. [Consultado 15 de Abril de 2018]. Disponible en Internet: https://cartilla.cert.br/fasciculos/dispositivos-moviles/fasciculo-dispositivos-moviles-slides.pdf

[10] Guía de Seguridad para usuarios de Smartphones. [en línea]. ESET Latinoamérica [Consultado: 20 de Abril de 1918]. Disponible en Internet: https://www.welivesecurity.com/wp-content/uploads/2014/01/documento_guia_de_seguridad_para_usuarios_de_smartphone_baj.pdf

meses (1ero. de Enero a 31 de Agosto del 2017). Esta cifra es significativamente mayor a los 398 millones que se registraron durante el mismo periodo en 2016, lo que representa un aumento de 59%. Para ponerlo en contexto, esto significa que cada hora, los usuarios en Latinoamérica son sujetos a 117,572 ataques de malware o 33 ataques por segundo"[11].

Es importante poner en consideración que los riesgos existentes en la actualidad en aspectos de dispositivos móviles no son los mismos que en años anteriores. Por esta razón en relevante que en este trabajo se planteen los riegos actuales a los que se encuentran expuestos dichos dispositivos.

La monografía se lleva a cabo porque es importante conocer las fallas identificadas en los sistemas operativos Android y IOS, así como plantear soluciones para solucionar algunas de ellas. Los usuarios de los dispositivos móviles no conocen las mininas normas de seguridad que se les pueden aplicar a sus equipos móviles, con el objeto de reducir la posibilidad de ataques a los mismos. Es importante que ellos mismos conozcan las herramientas disponibles para mitigar los riesgos de seguridad existentes en los diferentes sistemas operativos.

Abordando la plataforma Android, Skyvor[12] en su escrito publicado en la página de Avast indica que las principales amenazas a las cuales se encuentran expuestas este tipo de dispositivos son: descargadores, los cuales hacen referencia a las diferentes métodos o tácticas utilizadas por los cibercriminales para lograr instalar en dispositivos Android aplicaciones las cuales lanzan ejecutan malware o programas maliciosos al sistema una vez que están instalado. En segundo lugar, se encuentran las amenazas de banca móvil, seguidamente se ubican los ransomware móvil y por último el auge de las aplicaciones falsas.

[11]33 ataques por segundo: Kaspersky Lab registra un aumento del 59% en ataques de malware en América Latina [en línea].Kaspersky Latinoamérica. [Consultado: 25 de abril de 2018]. Disponible en Internet: https://latam.kaspersky.com/about/press-releases/2017_33-attacks-per-second-increase-in-malware-attacks-in-latin-america

[12] SKVOR, Michael. Keeping your Android safe this year [en línea] Blog Avast. 24 de Enero de 2018. Párr. 4. [Consultado:30 de Abril de 2018]. Disponible en Internet: https://blog.avast.com/keeping-your-android-safe-this-year

Por los lados de IOS, las amenazas no son ajenas a este tipo de dispositivos. De acuerdo con el portal de noticias SearchMobileComputing[13] a pesar de ser más cuidadosos a la hora de actualizar sus aplicaciones para así evitar ataques externos, todavía hay muchos errores que los usuarios cometen que pueden afectar la seguridad de Apple IOS. Los ataques de phishing, en los cuales se envían enlaces engañosos a sitios web que instalan malware o engañan a los usuarios para que renuncien a su información personal, expone Edmon[14], se encuentra en primer lugar en cuanto a las amenazas de ataques en esta plataforma. Le siguen falta de códigos de acceso, que tiene que ver con que los usuarios desactiven la protección de contraseña en sus dispositivos. Por último, la existencia de aplicaciones maliciosas, a pesar del control que brinda su tienda de aplicaciones.

El impacto social que puede tener este trabajo de monografía es que las personas del común conozcan los riesgos a los cuales pueden estar expuestos sus dispositivos móviles y la forma de mitigar algunos ataques que se presentan frente a ellos, independientemente del ámbito en donde se encuentre. En este punto es importante hacer hincapié que las características de estos dispositivos ya no son de uso exclusivo familiar, y se han convertido en herramientas de trabajo en las organizaciones.

Cuando enfocamos el concepto de seguridad informática a la seguridad de dispositivos móviles debe ser vista como un conjunto de medidas que debemos seguir o tener en cuenta para llevar a cabo la labor de navegación en Internet a través de los dispositivos móviles de forma segura y, de esta manera, evitar las amenazas que podrían afectar e infectar nuestro equipo o dispositivos móviles.

Según información obtenida del blog Andalucía es digital “El uso masivo del correo electrónico, las redes sociales, el comercio electrónico, la descarga de aplicaciones móviles, los juegos online o los sistemas de mensajería instantánea (WhatsApp, Telegram) han traído consigo un aumento de los peligros en Internet y

[13] EDMOND , Ramin Users are biggest impediment to Apple iOS security.[en línea]. SearchMobileComputing.(31 de julio de 2017), párr. 5. [Consultado: 1 de septiembre de 2018]. Disponible en Internet: https://searchmobilecomputing.techtarget.com/news/450423643/Users-are-biggest-impediment-to-Apple-iOS-security

[14] Ibid.,p.23.

la necesidad de estar más vigilantes que nunca con nuestra seguridad informática".[15].

[15] Guía de Seguridad Informática. En Internet, el mejor sistema de seguridad eres tú ¡protégete! [en línea]. Blog Andalucía es digital.30 de noviembre de 2016, párr. 2. [Consultado: 1 de Septiembre de 2018].Disponible en Internet: https://www.blog.andaluciaesdigital.es/guia-de-seguridad-informatica/

3. OBJETIVOS

3.1 OBJETIVO GENERAL

Realizar un estudio investigativo acerca de las vulnerabilidades identificadas en dispositivos móviles con sistemas operativos Android y IOS.

3.2 OBJETIVOS ESPECÍFICOS

1. Realizar estudio acerca de las vulnerabilidades más comunes en los sistemas operativos móviles Android y IOS.

2. Determinar fallas de seguridad que se presentan en sistemas operativos móviles Android y IOS, definir forma de mitigarlas e investigar a cerca de herramientas de seguridad disponibles en las plataformas Android y IOS.

3. Identificar los principales errores que cometen los usuarios de dispositivos móviles relacionados con aspectos de seguridad.

4. MARCO REFERENCIAL

4.1 MARCO TEÓRICO

4.1.1 Generación de dispositivos móviles: La evolución de la tecnología ha incursionado en el campo de la telefonía móvil, influenciada principalmente por los medios de trasmisión y las tecnologías utilizadas en cada una de sus generaciones. A continuación, se abordarán las diferentes generaciones de dispositivos móviles junto a sus características que las identifican.

La primera generación de dispositivos móviles se caracterizó por el gran tamaño y peso de los dispositivos. Según Betancur y Erazo[16] la transmisión funcionaba de manera analógica, haciendo uso de ondas de radio para la trasmisión y recepción de datos. Solo podían ser utilizados para trasmisión de voz y el concepto de seguridad no existía.

Pasando a la segunda generación, esta etapa marcó un paso importante de telefonía analógica a digital, con lo cual la calidad de las llamadas mejoró ostensiblemente. Según publicación Evolución de la red de comunicación móvil[17] La tecnología GSM (Sistema Global para Comunicaciones Móviles) surgida en esta generación fue la pionera en facilitar voz y datos digitales, así como roaming internacional lo que les permitió a los usuarios desplazarse de un lugar a otro sin perder sus llamadas de contacto. Los conceptos de retención, transferencia, y bloqueo de llamadas tomaron fuerza en esta generación de móviles.

Continuando con la evolución de la telefonía móvil la tercera generación se caracterizó según anota Betancur y Erazo [18] por mostrar cómo podían trabajar de manera mancomunada voz, datos, acceso inalámbrico a Internet, aplicaciones

[16] BETANCUR JARAMILLO, Oscar y ERAZO HANRRYR, Sonia Elizabeth. Seguridad en dispositivos móviles Android [en línea]. Monografía presentada para optar el título de: Especialista en Seguridad Informática. Universidad Nacional Abierta y a Distancia – UNAD. Escuela de Ciencias Básicas, Tecnología e Ingeniería,2015. p.17. [Consultado: 12 de Enero de 2018]. Disponible en Internet: https://stadium.unad.edu.co/preview/UNAD.php?url=/bitstream/10596/3614/1/59836994.pdf

[17] Evolución de la red de comunicación móvil, del 1G al 5G.[en línea].Universidad Internacional de Valencia.[Consultado el 1 de Septiembre de 2018]. Disponible en Internet: https://www.universidadviu.com/evolucion-la-red-comunicacion-movil-del-1g-al-5g/

[18] BETANCUR JARAMILLO. Op. Cit., p. 26.

multimedia y altas transmisiones de datos. Se trabajan con protocolos que soportan mayores velocidades para facilitar el trabajo de aplicaciones más allá de la voz tales como audio (MP3), vídeo en movimiento, vídeo conferencia, sólo por nombrar algunos.

El siguiente nivel de generaciones, plantea Universidad Internacional de Valencia[19] en su escrito, se caracteriza por "Proporcionar alta velocidad, alta calidad, alta capacidad, seguridad y servicios de bajo coste para servicios de voz y datos, multimedia e internet a través de IP. Para usar la red de comunicación móvil 4G, los terminales de los usuarios deben ser capaces de seleccionar el sistema inalámbrico de destino"

En la cuarta generación, Conde[20] indica que con la aparición de las redes IP (protocolo de Internet), se logró una confluencia entre redes cableadas e inalámbricas. Todos los datos eran transmitidos a través de paquetes conmutados con una velocidad que estará por encima de 1 GBps, además de mejorar el ancho de banda con el cual trabajaba en esos momentos.

Por último, la quinta generación de dispositivos móviles surgió a partir del año 2010. Vora expone en su escrito que esta generación "se caracterizó por ser altamente compatible con WWWW (World Wide Web inalámbrico), alta velocidad y capacidad de procesamiento, proporcionaba una gran transmisión de datos en Gbps. calidad de televisión de alta definición (HD), transmisión de datos más rápida que la de la generación anterior, incremento en memoria del teléfono y mayor claridad en audio / video".[21]

4.1.2 Evolución Sistema Operativo Android: Es el momento de hacer historia de la forma como surgió el sistema operativo para móviles más popular en el momento.

[19] Evolución de la red de comunicación móvil, del 1G al 5G. Op. Cit., p. 26.

[20] CONDE, Rita. Redes de telefonía celular ¿Qué significan 1G, 2G, 3G y 4G? [en línea]. About Español. (24 de abril de 2016), párr. 17. [Consultado: 1 de Septiembre de 2018]. Disponible en Internet: https://www.aboutespanol.com/redes-de-telefonia-celular-que-significan-1g-2g-3g-y-4g-580779

[21] VORA,Lopa. Evolution of mobile generation technology: 1G to 5G and review of upcoming wireless technology 5G [en línea]. En: International Journal of Modern Trends in Engineering and Research. Octubre de 2015, vol 2, no 10, p 4. [Consultado: 1 de Septiembre de 2018]. ISSN: 2349-9745.Disponible en Internet: https://pdfs.semanticscholar.org/4dfd/40cc3a386573ee861c5329ab4c6711210819.pdf

Rodríguez [22] afirma que su primera versión surgió para los años 2008, la cual incluía su tienda de Apps, y funcionaba sincronizado con las aplicaciones populares en el momento: calendario, google contact y Gmail entre otros. Además, contaba con reconocimiento de *bluetooth, wifi* y marcación de voz. A partir de allí surgieron actualizaciones como la 1.1 *Petit Four*, 1.5 *Cupcake* y 1.6 *Donut*. Estas mejoraron en parte las características del sistema tales como subir videos a YouTube, girar pantalla y la aparición de widgets.

Según publicación de la organización Spinfold[23] ,una de las versiones más populares del sistema operativo Android fue Android 2.0 / 2.1 (Eclair), la cual fue liberada en Octubre del 2009. Se introdujeron características orientadas a mejorar el manejo de su cámara (flash, zoom digital, efectos de colores entre otros), así como el mejoramiento de interfaces de usuarios, soporte a aplicaciones flash, y aparición de Android Cloud. De esta etapa también hacen parte Android 2.2 *Froyo* y Android 2.3 *Gingerbread.*

Como tercera versión difundida en este tipo de dispositivos aparece Honeycomb, la cual trae consigo algunas características planteadas por De Looper:[24]entre las cuales se encuentran: que estaba dirigida a tablets, proporcionó algunas claves de diseño sobre lo que aparecería en futuras versiones de Android (por ejemplo, cambio en el color ofrecido por defecto), además de eso, en lugar de que los usuarios tuvieran que elegir los widgets de la pantalla de inicio de una lista , se ofrecían vistas previas para los widgets individuales.

La primera gran revolución en Android, anota Rodríguez [25] apareció con el surgimiento de Android 4.0 *Ice Cream Sandwich* en Octubre 2011. Sus principales características fueron la edición de fotos en y grabación de video en formato mucho más alto. Android 4 tuvo 4 actualizaciones importantes, Android 4.1 *Jelly*

[22] RODRIGUEZ MOLINA, Carlos. Evolución de Android desde su creación a Android 8.0 [en línea]. Tu experto Tecnología. (4 de Agosto de 2017), párr.3. [Consultado: 13 de Mayo de 2018].Disponible en Internet: https://www.tuexperto.com/2017/08/04/evolucion-de-android-desde-su-creacion-a-android-8-o/

[23] Evolution of Android OS [en línea].Spinfold.[Consultado:1 de Septiembre de 2018]. Disponible en Internet: http://www.spinfold.com/evolution-of-android-os/

[24] DE LOOPER,Christian. From Android 1.0 to Android 7.0, here's how the top mobile OS has evolved over the years [en línea]. Yahoo Finance (4 de Septiembre de 2018), párr. 21.[Consultado:3 de Septiembre de 2018] . Disponible en Internet: https://finance.yahoo.com/news/android-1-0-android-9-192746756.html

[25] RODRIGUEZ MOLINA, Op.cit,.p.28.

Bean, Android 4.2 *Jelly Bean* (*Gummy Bear*), Android 4.3 *Jelly Bean (Michel)* y Android 4.4 *KitKat*.

Luego nos encontramos con el sistema de Google, Android 5 *Lollipop* en donde, según artículo publicado en Cnet, "Google revisó completamente su estética con una interfaz plana conocida como Material Design. Las notificaciones aparecieron en la pantalla de bloqueo o como alertas emergentes. El sistema operativo también tenía modo de prioridad, soporte multiusuario, fijación de pantalla y las aplicaciones recientes se renombraron como Información general"[26].

La versión siguiente para los equipos con sistema Android, expone Bagchi[27], se conoció en el mercado como Marshmallow, y trajo consigo el soporte para huellas dactilares así como un modo para ahorrar batería mientras el teléfono estaba en espera. En el campo de las aplicaciones, esta versión permitía que los permisos de las mismas podían otorgarse individualmente en tiempo de ejecución.

Android 7.0 Nougat, según Bagchi[28], fue compatible con múltiples ventanas para operar dos aplicaciones a la vez. La capacidad incorporada permite utilizar dos o más idiomas al mismo tiempo. En la versión 8 del sistema Android (Oreo), indica Chung[29], se introdujo una forma para que todos los íconos tuvieran una forma consistente cuando se muestran. Otro de los cambios propuestos por esta versión fue que el botón de todas las aplicaciones fuera reemplazado por el gesto de deslizar hacia arriba del teclado para mostrar las aplicaciones instaladas.

La más reciente versión de Android (Android Pie) fue liberada en Agosto del 2018. Entre las nuevas características ofrecidas Raphael expone en su artículo "que incluye un sistema universal de respuesta sugerida para notificaciones de mensajes, un método más eficaz de administración de capturas de pantalla y

---

[26] LYN, La. Android through the years [diapositivas].Cnet.22 de Febrero de 2016, diapositiva 11. [Consultado: 2 de Septiembre de 2018]. Disponible en Internet: https://www.cnet.com/pictures/google-android-versions-history/

[27] BAGCHI, Apeksha. The evolution of Android [en línea].Yaabot.(1 de Junio de 2017).párr.15.[Consultado:14 de Octubre de 2018]. Disponible en Internet: https://www.yaabot.com/30831/the-evolution-of-android/

[28] Ibid.,p.29.

[29] CHUNG, Ek. Evolution of Android Homescreen and Navigation [en línea].Google Design.(15 de Mayo de 2018).párr. 14.[Consultado:14 de Octubre de 2018]. Disponible en Internet: https://medium.com/google-design/evolution-of-android-homescreen-and-navigation-bad189d536f2

sistemas más inteligentes para la administración de energía y el control del brillo de la pantalla"[30].

Esta versión también trae consigo, según Raphael[31], mejoras en el campo de la seguridad y privacidad, así como avances en el manejo de ajustes visuales, y formas más inteligentes de manejar puntos de acceso Wi-Fi. A continuación, se muestra grafica de evolución de este sistema operativo:

Figura 1.Evolución Sistema Operativo Android en la historia

Fuente: MATHEUS, Abraham. Evolución Sistema Operativo Android en la historia [imagen]. Android 1.0 to Android M, The story Android Evolution.2015. p.1. [Consultado: 20 de Mayo de 2018].Disponible en Internet: https://www.cubettech.com/blog/android-1-0-to-android-m-the-story-of-mobile-evolution/

4.1.3 Evolución Sistema Operativo IOS: Después de haber tratado el tema de la evolución en la historia del Sistema Android, a continuación, se brindarán conceptos relacionados con la historia del Sistema IOS producido por la compañía Apple. Según escrito publicado en la revista Enter por Arias[32] para el año 2007, este sistema revolucionó el mundo de la telefonía móvil, gracias a su gran jugador titular: el IPhone. Fue considerado como un cambio radical para la época, pues los

[30] JR,Raphael. Android versions: A living history from 1.0 to Pie [en línea].Computerworld.(7 de Agosto de 2018),párr.14..[Consultado:13 de Octubre de 2018]. Disponible en Internet: https://www.computerworld.com/article/3235946/android/android-versions-a-living-history-from-1-0-to-today.html?page=2

[31] Ibid.,p.30.

[32] ARIAS, Ximena. Del 1 al 8: La evolución del sistema operativo IOS [en línea]. En: Revista Enter..17 de Septiembre de 2014), párr. 2. [Consultado: 23 de Mayo de 2018]. Disponible en Internet: http://www.enter.co/especiales/vida-digital/del-1-al-8-la-evolucion-del-sistema-operativo-ios/

teclados de los dispositivos desaparecieron para darles paso a teclado táctil, y sobre todo por su interfaz de usuario amigable. Algunas de las aplicaciones que traían incorporadas eran su navegador Safari, Google Maps, y los servicios de SMS, de los cuales fueron pioneros.

Abordando el tema de la versión 2.0 del sistema IOS, Hein [33]afirma que en Julio de 2008 Apple presento su tienda digital dirigida a trabajar con sus dispositivos móviles (Apple Store). Otras características notables que aparecieron en iOS 2.0 incluyen: opción de apertura de documentos elaborados en Microsoft Office, captura de pantallas y almacenamiento de fotos en Safari en la aplicación Fotos, aparición del ícono de Contactos, creación de controles dirigido a contenidos no aptos para menores y la creación de listas de reproducción.

Siguiendo el recorrido por los avances en el sistema IOS de Apple, Moreaw[34], editor de Computerworld, expone que la versión 3.0 de esta plataforma trae consigo avances importantes en el posicionamiento de la Compañía. Tal es el caso de traer al mundo de los móviles los conceptos de copiar cortar y pegar, tan comunes en el mundo de la tecnología, control de voz y mensajería multimedia, entre otras opciones que modificaron su aspecto inicialmente propuesto.

Con el surgimiento de la versión 4 de IOS, indica Van Allen[35] en artículo publicado en Cnet, el dispositivo trajo consigo algunas características al mundo del IPhone por ejemplo: fondos de pantallas personalizados, introdujo el concepto de video conferencia FaceTime, y la aparición de IBook, producto desarrollado por la compañía para soportar EBooks o librerías digitales, además de permitir a sus usuarios personalizar sus ambientes de trabajo creando carpetas en la pantalla de inicio de sus equipos.

[33] HEIN, Buster. The evolution of iOS: From iPhone OS to iOS 11 [en línea].Cult of Mac.(24 de Mayo de 2017),párr. 7. [Consultado:2 de Septiembre de 2018].Disponible en Internet: https://www.cultofmac.com/488454/ios-evolution-iphone-os/

[34] MOREAU, Sean. The evolution of iOS [diapositivas].Computerworld.6 de Junio de 2018,diapositiva 4.[Consultado:23 de Mayo de 2018].Disponible en Internet: https://www.computerworld.com/article/2975868/apple-ios/the-evolution-of-ios.html#slide4

[35] VAN ALLEN,Fox. The evolution of Apple iOS [diapositivas].Cnet.1 de Julio de 2017,dispositiva 7.[Consultado: 25 de Mayo de 2018]. Disponible en Internet: https://www.cnet.com/pictures/the-evolution-of-apple-ios/8/

Al revisar las siguientes versiones de IOS encontramos las versiones 5 y 6 del dispositivo. En la primera de ellas, Hein[36] expone que el principal anuncio fue que sus equipos se hicieron independientes de la PC al introducir la sincronización inalámbrica. Otras de sus puntos que se tuvieron en cuenta fueron: la aparición de iMessage, su integración con twitter, y por ultimo sus nuevas características ofrecidas como el Notification center, y la aparición de Siri , el asistente personal para usuarios IOS el cual se caracterizaba por utilizar procesamiento de lenguaje natural para poder interactuar con el usuario del dispositivo móvil. En la versión 6 expone Saxena[37], sobresalieron las siguientes características: desarrollo su propia aplicación para manejo de mapas, aunque no tuviera su mejor acogida, capacidad de hacer llamadas a través de FaceTime a través de su red celular, y la aparición de su aplicación Passbook (cartera virtual).

Continuando con la evolución del sistema operativo de equipos IPhone, a mediados del año 2013 surgió la versión 7, la cual trae consigo mejoras en aspectos de su rediseño visual. Sin embargo, Hein afirma que “IOS 7 no solo fue un bonito trabajo de pintura: la compañía también agregó algunas características increíblemente importantes. El muy esperado Centro de control les dio a los usuarios una forma rápida de cambiar entre Wi-Fi, Bluetooth, modo avión y otras configuraciones, así como también lanzar la linterna, la calculadora y la cámara del iPhone.” [38]

Saxena[39] plantea que el iOS 8 trajo consigo el Family Sharing, característica que brindaba a los usuarios de Apple la posibilidad de compartir contenido descargado de iTunes, adema de la opción de envió para mensajes de audio y video en la aplicación de mensajería propia de Apple, junto con la aparición de widgets que permitían compartir datos y funciones entre aplicaciones IOS y agregó iCloud Drive, que ofrece almacenamiento en la nube.

[36] HEIN. Op. cit., p. 31.

[37] SAXENA,Sobhit. Evolution from iPhone OS 1 to iOS 10 – Journey of iOS [en línea]. Mobiloitte Technologies.(14 Septiembre de 2016), párr. 7. [Consulado: 2 de Mayo de 2018]. Disponible en Internet: https://www.mobiloitte.com/blog/evolution-iphone-os-1-ios-10-journey-ios/

[38] HEIN, Op. cit., p. 31.

[39] SAXENA, Op.cit., p.32.

En la versión 9 de IOS, plantea Heisler[40], en vez de dedicarle tiempo desarrollo de características adicionales, sus desarrolladores se enfocaron en estabilizar el funcionamiento de su plataforma. Algunos de los aportes importantes que se implementaron en esta versión, según Hiesler fueron: mejoras en sus aplicaciones Siri y Passbook (ahora llamado billetera), así como la inclusión de nuevas aplicaciones de música y noticias.

Figura 2.Evolución Sistema Operativo IOS en la historia

Fuente: LONG, Joshua. Evolución Sistema operativo IOS en la historia [imagen]. The Evolution of iOS Security and Privacy Features.2016.p.27.[Consultado: 2 de 27 de Mayo de 1018].Disponible en Internet: https://www.intego.com/mac-security-blog/the-evolution-of-ios-security-and-privacy-features/

A pesar de no aparecer referenciados en la gráfica anterior, en conveniente tratar el tema de la versión de IOS 10, y 11 por ser los más recientes en aparición. La versión 10 según Hein[41] muestra cambios a primera vista los cuales se observan en la pantalla de inicio y en el centro de notificaciones. Pero no todo se detiene ahí. Se creó una nueva tienda de aplicaciones, se agregaron características a la aplicación Stock Photos en las cuales se hace uso de inteligencia artificial dependiendo del tiempo o lugar en que las fotos sean tomadas estas se organizan y se permite crear mini películas con ellas.

Por último, la versión 11, liberada en Junio de 2017, se caracterizó indica Smith[42] porque abría la posibilidad de que las fotos en vivo se convirtieran en gif, haciendo cambiar de posición o rotar en el momento deseado, Apple cambió el formato de

[40] HEISLER, Yoni. The history and evolution of iOS, from the original iPhone to iOS 9 [en línea]. Brg.(12 de Febrero de 2016),párr. 26.[Cosultado:29 de Septiembre de 2018]. Disponible en Internet: https://bgr.com/2016/02/12/ios-history-iphone-features-evolution/

[41] HEIN,Op.cit.,p.31.

[42] SMITH, Dave, The 13 most useful features in iOS 11 [en línea].Business Insider.(16 de Mayo de 2018), párr..2.[Consultado: 2 de Septiembre de 2018].Disponible en Internet: https://www.businessinsider.com/apple-ios-11-best-features-2017-7

compresión en iOS 11, permitiendo mayor almacenamiento de fotos y videos en sus dispositivos, Siri viene equipado con características de inteligencia artificial y aprendizaje automático, el teclado incorporado de Apple sugerirá palabras que haya visto en su teléfono, y por ultimo todas sus notificaciones, tanto recientes como almacenadas, están en un solo lugar no distribuidas como en sus versiones anteriores.

4.2 MARCO CONCEPTUAL

4.2.1 Dispositivo móvil: Un dispositivo móvil es esencialmente una computadora de mano. Aunque la categoría de dispositivo móvil parezca incluir cualquier dispositivo electrónico lo suficientemente pequeño como para transportarse, el término implica comunicaciones inalámbricas y la capacidad de computación general. Entre los ejemplos más comunes de dispositivos móviles se encuentran: Smartphone, teléfonos inteligentes, PDA (asistente digital personal) o agendas personales, tabletas, reproductores portátiles de música, entre otros.

4.2.2 Características de dispositivo móvil: En la mayoría de los casos, un dispositivo móvil se caracteriza por contar con una serie variables que lo distinguen de otros dispositivos que, aunque a pesar pertenecer a la misma categoría, carecen de algunas de las características de los dispositivos móviles “reales”. Estas características son:

- Conectividad a internet mediante redes WIFI: A pesar de existir el riego de accesos no autorizados a los equipos, este tipo de redes son muy utilizadas debido a su gran distribución y a su facilidad de acceso.

- Una batería, según artículo de Medina[43], permite tener el dispositivo disponible o encendido durante varias horas. En los últimos años se ha convertido en factor de investigación y la mayor parte de las casas productoras de equipos móviles han realizado grandes inversiones en aras de ofrecer mayor duración de tiempo de carga de sus baterías en cada uno de sus equipos. Las baterías de iones de litio en su mayoría aguantan hasta 1.000 ciclos de carga y

[43] MEDINA, Edgar. Cinco mitos y verdades sobre la batería de su celular [en línea].En El Tiempo.(16 de Febrero de 2017).párr.1.[Consultado: 23 de Agosto de 2018].Disponible en Internet: https://www.eltiempo.com/tecnosfera/tutoriales-tecnologia/cinco-mitos-y-verdades-sobre-la-bateria-de-su-celular-59543

descarga antes dar muestra de desgaste. Un nuevo desarrollo, llevado a cabo por científicos de la Universidad de Harvard promete que la batería solo perderá uno por ciento de su capacidad tras esos mismos 1.000 ciclos.

- Movilidad: Morillo[44] plantea que este concepto es asociado con la facilidad de un dispositivo para ser movido sin dificultad. Esto significa que debe funcionar sin presentar inconvenientes mientras nos encontremos en movimiento, sin importar la proximidad de una fuente de energía (enchufe) o de una conexión a Internet.

- Tamaño reducido: Esto hace que fácilmente puedan ser transportados o intercambiados entre personas. Esta característica marca diferencia a la hora de comparar los móviles con las tabletas. A pesar de que la variable movilidad puede aplicarse a cada uno de los anteriores dispositivos descritos, el tamaño hace que los usuarios a la hora de utilizarlos escojan la segunda opción.

- Interacción con personas: Según lo planteado por Morillo esto se entiende como una especie de relación existente entre usuario-móvil "se entiende por interacción el proceso de uso que establece un usuario con un dispositivo. Entre otros factores, en el diseño de la interacción intervienen disciplinas como la usabilidad y la ergonomía".[45]

- El ingreso de información al dispositivo: Se lleva a cabo a través de un teclado físico o en pantalla ofrecida por los dispositivos. Al igual los computadores de escritorio, este elemento es considerado como el dispositivo de entrada por defecto.

- Un asistente virtual: Según afirma Viswanathan en escrito algunos ejemplos de estos asistentes son: Siri, Cortana o Google Assistant. "Estos son principalmente utilizados por usuarios, para para llevar a cabo consultas o búsquedas haciendo uso de su voz. Como característica adicional se puede considerar la capacidad ofrecida de descargar datos de Internet, incluidas aplicaciones y libros, entre otros."[46]

4.2.3 Sistema operativo*:* Conjunto de programas encargados de la administración eficiente de recursos de máquina. El propósito de un sistema operativo, según

---

[44] MORILLO POZO, Julián David. Introducción a los dispositivos móviles [en línea].Universidad Abierta de Cataluña [Consultado:2 de Septiembre de 2018].Disponible en Internet: https://www.exabyteinformatica.com/uoc/Informatica/Tecnologia_y_desarrollo_en_dispositivos_moviles/Tecnologia_y_desarrollo_en_dispositivos_moviles_(Modulo_2).pdf

[45] Ibid.,p.35.

[46] VISWANATHAN, Pryya. What Is a Mobile Device?[en línea].Lifewire.(13 de Mayo de 2018),párr.2.[Consulado: 26 de Mayo de 2018].Disponible en Internet: https://www.lifewire.com/what-is-a-mobile-device-2373355.

artículo publicado en la BBC es “controlar la operación general de una computadora y proporcionar una manera fácil de interactuar con las computadoras y ejecutar aplicaciones”.[47]

4.2.3.1 Sistemas operativos usados por Smartphones: Teniendo en cuenta el auge de los dispositivos móviles y la necesidad de gestionar estos equipos, brindando la posibilidad de instalar y administrar aplicaciones en los mismos, la industria ha desarrollado programas encargados de facilitarle este tipo de tareas a los usuarios. Dentro de los principales sistemas para móviles se encuentran:

Android: Informática Hoy[48], expresa en su escrito, que Android es un sistema operativo desarrollado por la compañía Google, basado en sistema operativo Linux, y cuyo mercado de acción principalmente son las tabletas y los teléfonos inteligentes. Desde sus inicios fue considerado un sistema de distribución libre y código abierto, lo cual repercute en su gran cantidad de usuarios debido a su flexibilidad.

IOS: Sistema Operativo desarrollado por Apple, cuyo código es propietario o cerrado, y se encuentra codificado en lenguajes de programación en C, C ++ y Objective C. A pesar no manejar el mayor porcentaje de ventas, principalmente debido a su alto precio comparado con su competencia, sus aspectos de seguridad los hace una buena opción para los usuarios.

Windows Phone: Algunas de las características de este sistema operativo son planteadas por Padhya, quien afirma “Windows Phone es un sistema operativo móvil desarrollado por Microsoft Corporation y diseñado principalmente para dispositivos con pantalla táctil como teléfonos inteligentes y tabletas. Fue lanzado inicialmente el 8 de noviembre de 2010. Windows Phone es una fuente cerrada o sistema operativo propietario. Windows está programado en lenguajes de

[47] Operating Systems [en línea]. BBC.[Consultado en: 3 de Septiembre de 2018].Disponible en Internet: https://www.bbc.com/bitesize/guides/ztcdtfr/revision/1

[48] Cuál es el mejor sistema operativo para un smartphone?[en línea].Informática hoy.[Consultado: 3 de Septiembre de 2018].Disponible en Internet: https://www.informatica-hoy.com.ar/soluciones-moviles/Cual-es-el-mejor-sistema-operativo-para-un-smartphone.php

programación C, C ++. Su última versión conocida como Windows 10 fue liberada el 20 de noviembre de 2015".[49]

Blackberry: Singh[50] plantea que es un sistema operativo desarrollado por Research in Motion (RIM). Su primera versión fue liberada en el año 1999.Su incompatibilidad y ausencia de modelos comerciales lo han relegado a posiciones secundarias en la búsqueda del dominio del mercado de los dispositivos móviles. Posee un sistema de código cerrado y es considerado un sistema inmune y confiable.

Symbiam: Nokia, afirma Singh[51], es el propietario de este sistema operativo. Debido a la gran popularidad de los sistemas Android y IOS, su existencia en el mercado es cada vez más difícil, debido a la falta de acogida de sus modelos. Es usado principalmente en equipos considerados de gama baja.

4.2.4 Jailbreak: Cassavoy[52] afirma que es proceso que se aplica a equipos IPhone el cual se encarga de "liberarlos de las limitaciones impuestas por su fabricante (Apple) y su operador. Luego de llevar a cabo un jailbreak, el dispositivo puede hacer cosas que antes no podía, como instalar aplicaciones no oficiales y modificar configuraciones y áreas del teléfono que anteriormente estaban restringidas."

4.2.5 Rootear: De acuerdo con Gordon[53], rootear es un proceso por medio del cual se le brindan o asignan permisos de superusuario a un dispositivo Android. A través de estos permisos se puede tener acceso a configuraciones especiales del

[49] PADHYA, Bhargavi y DESAI, Prasad. Comparison of Mobile Operating Systems [en línea].En: International Journal of Innovative Research in Computer and Communication Engineering.Agosto, 2016.vol 4 no 8, p.2.[Consultado: 3 de Septiembre de 2018]. Disponible en Internet: http://www.ijircce.com/upload/2016/august/132_Comparison.pdf . ISSN: 2320-9798.E-ISSN: 2320-9801

[50] SINGH, Arpit. Top 15 Mobiles Phones Operating Systems 2018 [en línea].Digital SEO Guide.(6 de Julio de 2018), párr..9.[Consultado:3 de Septiembre de 2019].Disponible en Internet https://www.digitalseoguide.com/technology/top-mobile-phones-operating-systems-os/#7_Blackberry_OS

[51] Ibid.,p.37.

[52] CASSAVOY, Lianne. What Does It Mean to Jailbreak an iPhone?[en línea].Lifewire.(12 de Mayo de 2018), Párr.1. [Consultado: 20 de Mayo de 2018].Disponible en Internet: https://www.lifewire.com/what-is-jailbreaking-an-iphone-577591

[53]GORDON, Whitson. Everything You Need to Know About Rooting Your Android Phone [en línea].Lifehacker.(9 de Abril de 2013). Párr.4.[Consultado:2 de Septiembre de 2018].Disponible en Internet: https://lifehacker.com/5789397/the-always-up-to-date-guide-to-rooting-any-android-phone

dispositivo, ejecutar aplicaciones que requieren de dicho permiso, así como agregar características adicionales al dispositivo.

5. DESARROLLO DE LA INVESTIGACIÓN

5.1 ESTUDIO ACERCA DE LAS VULNERABILIDADES MÁS COMUNES EN LOS SISTEMAS OPERATIVOS MÓVILES ANDROID Y IOS

5.1.1 Arquitectura sistema operativo Android: Según Pisuwala[54] la arquitectura de aplicaciones móviles es un conjunto de patrones y técnicas que deben seguirse para construir una aplicación móvil completamente estructurada. Estas técnicas y patrones están formulados teniendo en cuenta los requisitos del proveedor y los estándares de la industria.

El sistema operativo Android sigue un enfoque de arquitectura en capas. Todas estas capas son responsables de los diferentes roles y características que se discuten a continuación.

5.1.1.1 Kernel de Linux: Según se plantea en Android OS Documentation,[55] esta capa es la base de la plataforma Android. Está formado por el sistema operativo Linux Versión 2.6. Contiene todos los controladores de bajo nivel para el soporte de varios componentes de hardware. El kernel de Linux actúa como capa de abstracción o interfaz entre hardware y el resto de la pila de software.

5.1.1.2 Run Time de Android: Está basado en el concepto de máquina virtual utilizado en Java. Para entender un poco este concepto afirma Alarcón56, debemos referirnos a la forma en que los lenguajes de programación de alto nivel permiten la comunicación entre computadores y los mismos seres humanos haciendo uso de los compiladores. El compilador generalmente es entendido como el elemento que se encarga de traducir las instrucciones ejecutadas a través del lenguaje de programación a lenguaje entendible por las maquinas. Puesto de

[54] Pisuwala, Ubaid. Everything You Need to Know About Mobile App Architecture[en línea].Movile Zone.(27 de Mayo de 2017),parr.4. [Consultado: 15 de Marzo de 2018].Disponible en Internet: https://dzone.com/articles/everything-you-need-to-know-about-mobile-app-archi

[55] Android OS Documentation[en línea].Read the Docs.[Consultado:7 de Abril de 2018[.Disponible en Internet: https://media.readthedocs.org/pdf/androidos/latest/androidos.pdf

[56] ALARCON,Jose Manuel. ¿Qué es la máquina virtual de Java o Java Virtual Machine? [en línea] Campus MPV. (23 de Octubre de 2017),párr. 2. [Consultado:23 de Agosto de 2018].Disponible en Internet: https://www.campusmvp.es/recursos/post/que-es-la-maquina-virtual-de-java-o-java-virtual-machine.aspx

otra manera, cuando compilamos un programa en C++ lo que obtenemos es un programa ejecutable, por ejemplo, para Windows (por ejemplo), que este sistema operativo es capaz de ejecutar directamente contra el procesador, en un lenguaje que sea entendible por el mismo.

Continuando con su aporte, Alarcón[57] expresa, que esto no debe ser considerado como novedad, pues hace tiempo su concepto fue concebido de la misma manera. La novedad aparece en los lenguajes de programación considerados modernos (C++, Java, por ejemplo), quienes mantienen este concepto, pero introducen un paso adicional que aparece como intermedio entre el lenguaje de máquina entendido por los equipos de cómputo y el código de alto nivel entendido por los humanos. Este elemento adicional tiene el nombre de Byte Code. Entre el Byte Code y el sistema operativo se coloca un componente especial llamado Máquina virtual que es el que realmente va a ejecutar el código.

Para culminar la idea de máquinas virtuales, Alarcón[58] afirma que, en el caso de Java, Java Virtual Machine o JVM toma el código Byte Code resultante de compilar tu aplicación Java y lo compila a su vez a código nativo de la plataforma en la que se está ejecutando, bien sea Windows, Linux, o cualquier otro sistema operativo. La ventaja principal de este esquema planteado es que es relativamente sencillo crear un programa en Java y que luego éste se puede ejecutar en cualquier sistema operativo para el cual exista una implementación de la JVM.

Concretamente, Bansal define el Runtime de Android (ART) “como un entorno de tiempo de ejecución de la aplicación utilizado por el sistema operativo Android. En reemplazo de Dalvik, la máquina virtual de proceso originalmente utilizada por Android, ART realiza la traducción del código de bytes de la aplicación a instrucciones nativas que luego se ejecutan en el entorno de ejecución del dispositivo[59]”. En el mismo artículo, Bansal[60] indica que ART fue introducido a partir de la versión 4.4 de Android (KiteKat).

---

[57] Idib., p.39.

[58] Idib., p.39.

[59] BANSAL,Gaurav. Android Runtime Improvements [en línea].MindOrks.(9 de Mayo de 2018),párr.1. [Consultado: 1 de Octubre de 2018]. Disponible en Internet: https://medium.com/mindorks/android-runtime-improvements-e69bf7c1d10c

[60] Ibid.,p.40.

5.1.1.3 Librerías: Librería de software es definido por Techopedia como “un conjunto de datos y código de programación utilizado para desarrollar programas y aplicaciones de software. Está diseñado para ayudar tanto al programador como al compilador del lenguaje de programación en la creación y ejecución del software. “[61].

Las librerías son consideradas por Vanegas[62], como bibliotecas nativas de Android escritas en lenguajes C y C++, las cuales tienen como función entablar comunicación entre la capa de abstracción de hardware con las API (Application Programming Interface - Interfaz de Programación de Aplicaciones) y las aplicaciones mismas. Se caracterizan por tener la extensión ".so", y funcionan de la misma forma a los archivos ".dll" en Windows.

Según expone Vanegas en el mismo artículo, entre las principales librerías de Android se encuentran:

- Surface manager: encargado de la gestión de las ventanas gráficas.
- OpenGL/ES: librerías para soportar gráficas 3D.
- SGL: librerías gráficas 2D.
- Media framework: bibliotecas para manejo de multimedia.
- Freetype: permite manejar diferentes fuentes de mapas de bits.
- SSL: capa de seguridad Andriod.
- SQLite: base de datos relacional.
- Webkit: plataforma de aplicaciones para navegadores.
- Libc: librerías de C. [63]

5.1.1.4 Framework de aplicaciones: En términos generales, afirma Gutiérrez, un framework se puede considerar como “una aplicación genérica incompleta y configurable a la que podemos añadirle las últimas piezas para construir una

[61] Software Library [en línea].Techopedia.[Consutado:25 de Agosto de 2018].Disponible en Internet: https://www.techopedia.com/definition/3828/software-library

[62] VANEGAS, Carlos Alberto. Android…. De que me hablan?[en línea]Revistas Udistrital.(Agosto de 2013).pár.5. [Consultado:16 de Marzo de 2018].Disponible en Internet: http://revistas.udistrital.edu.co/ojs/index.php/vinculos/article/view/8022/9631%20una

[63] Ibid.,p.41.

aplicación concreta "[64]. Adicionalmente el autor plantea que lo que se busca con el uso de estos framework es principalmente acelerar procesos de desarrollo, reutilización de código existente y hacer uso de buenas prácticas de desarrollo.

Desde el punto de vista del desarrollador de aplicaciones, afirma Azokan[65], esta es la capa más importante, pues contiene todas las API´s- Application Programming Interface (Interfaz de Programación de Aplicaciones) y librerías de Java utilizadas para desarrollar una aplicación. Dentro de las API´S disponibles se encuentran aquellas que se encargan de administrar el conjunto de labores o actividades, gestionar lo que se visualizará en pantalla, construcción interfaces de usuario, comunicación de eventos sucedidos en la aplicación, posición geográfica del dispositivo, entre otras.

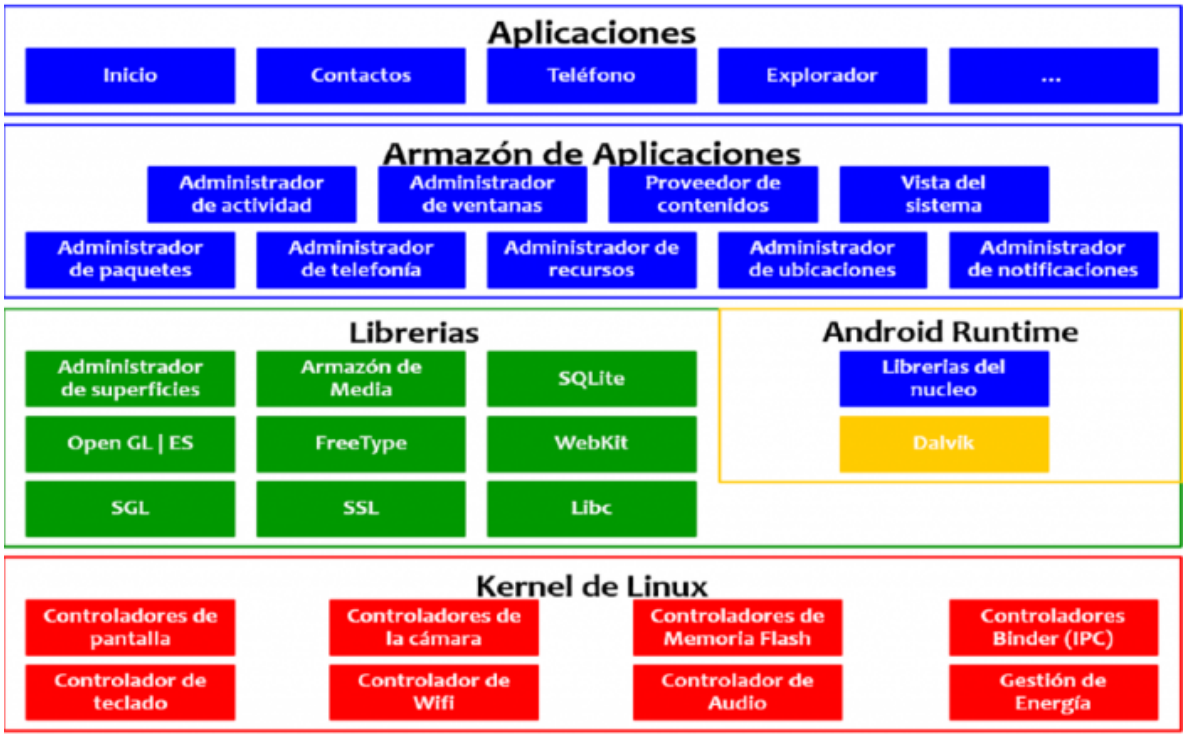
5.1.1.5 Aplicaciones: En esta última capa, expone Vanegas[66], se encuentran todas las aplicaciones del dispositivo. Cuando de hace uso del término "todas" se hace referencia aquellas que tienen interfaz de usuario como las que no, así como las nativas y las administradas. Las aplicaciones nativas son aquellas que son programadas en C o C++ y las administradas aquellas que son desarrolladas en Java, las aplicaciones que vienen preinstaladas en el dispositivo y aquellas que el usuario ha descargado. En esta capa se encuentran los siguientes elementos: Home (Inicio), Contacts (Contactos), Browse (Navegador) Phone (Teléfono) y otras aplicaciones.

[64] GUTIERREZ, Javier J. Qué es un framework web [en línea].Universidad de Sevilla. España.[Consultado: 2 de Mayo de 2028]. Disponible en Internet: http://www.lsi.us.es/~javierj/investigacion_ficheros/Framework.pdf

[65] AZOKAN,Ajin. Android Architecture From a Developer's Perspective [en línea].ApkChef.(23 de Diciembre de 2016),párr.28 . [Consultado:3 de Mayo de 2018].Disponible en Internet: https://www.apkchef.net/2016/12/android-architecture.html

[66] VANEGAS.Op.cit.,p.41.

Figura 3. Arquitectura sistema Android



Fuente: Arquitectura Sistema Android[imagen]. Sistemas Android-Fundamentos (2/2),2016,p.2.[Consultado:3 de Abril de 2018]. Disponible en Internet: http://webipedia.es/2016/12/19/introduccion-a-android-22/

Algunas de las ventajas identificadas de la plataforma Android son descritas a continuación:

- Código Abierto: Según publicación de la compañía Rishabh Software[67], esta característica ofrecida por los dispositivos Android permite a sus usuarios hacer uso del Kit de desarrollo de software (SDK) sin preocuparse con aspectos de licenciamiento. Esto se puede considerar punto fundamental a la hora llevar a cabo desarrollo de aplicaciones.

[67] 5 Major Benefits of Android App Development For Your Business [en línea]. Rishbash Software Blog.12 de Diciembre de 2017.párr.4.[Consultado:26 de Agosto de 2018].Disponible en Internet: https://www.rishabhsoft.com/blog/5-advantages-of-android-app-development-for-your-business

- Además del código abierto, Rishbash [68]expone que las aplicaciones basadas en Android son altamente personalizables y más fáciles de administrar. Al ser considerada una plataforma de código abierto, permite a los desarrolladores convertir sus ideas y aplicaciones innovadoras o creativas en un ámbito desde lo único que los restringe es el nivel de creatividad.

- Una de las ventajas que tiene la plataforma Android, según Rishbash[69], son sus diferentes canales de venta. Significa que no tiene que depender de un solo mercado para distribuir sus aplicaciones. Además de usar Google Play Store y otros mercados de aplicaciones de terceros, se pueden crear canales de distribución y ventas propios.

- Debido a la rápida expansión y gran acogida del lenguaje de programación Java hace que los desarrolladores construyan sus aplicaciones en plataformas Android más fácilmente. Es importante anotar que Java es el lenguaje nativo que utiliza Android.

- Estabilidad y seguridad: Tomando como base su lenguaje nativo, los dispositivos que usan plataforma Android heredan del lenguaje Java su estabilidad y niveles de seguridad. Otra característica que añade seguridad a esta plataforma es su arquitectura basada en Linux Kernel, el cual trae consigo niveles de alta seguridad en cuanto a las operaciones ejecutadas por usuarios o aplicaciones.

Por otra parte, las desventajas con las cuales deben lidiar los usuarios de la plataforma de Google son:

- Existen muchas casas fabricantes debido a su código abierto de desarrollo. Esto trae consigo inconvenientes a la hora de integración de hardware/software. Otro inconveniente relacionado con este tema es que la tienda de aplicaciones de Android en su mayoría no está exenta de malware o programas maliciosos que afectan el funcionamiento de los dispositivos.

[68] Ibid.,p.43.

[69] Ibid.,p.43,

- El hecho de mantener un alto porcentaje de ventas en el mercado de los dispositivos móviles a nivel mundial hace que los ataques del tipo malware se hallan incrementado en esta plataforma.

- La duración de la batería de los dispositivos Android, expone Rawat [70], puede verse afectada debido a la cantidad de procesos que se ejecutan en segundo plano cuando se ejecutan la mayoría de las aplicaciones.

- Los anuncios de publicidad siempre estarán presentes en el momento de descargar aplicaciones consideradas gratuitas, además de correr el riesgo de los interminables virus que afectan este tipo de dispositivos móviles.

5.1.2. Arquitectura sistema operativo IOS: La arquitectura de iOS , según plantea Intellipaat[71], se distribuye en capas. En el nivel superior, iOS funciona como un interlocutor entre el hardware subyacente y las aplicaciones desarrolladas por usuarios.

Las aplicaciones se comunican con el hardware a través de un conjunto de interfaces del sistema bien delimitadas o definidas. Estas interfaces hacen más sencilla la tarea de desarrollar aplicaciones en dispositivos que cuentan configuraciones de hardware diferentes.

Las capas inferiores brindan los servicios básicos en los que se basa toda la aplicación y su capa superior proporciona gráficos sofisticados y servicios relacionados con la interfaz. La arquitectura de iOS se puede dividir en cuatro capas distintas:

[70] RAWAT, Inder. Advantages And Disadvantages Of Android Phones [en línea]. OneWorldNews.(23 de Febrero de 2017).párr.11.[Consultado:30 de Septiembre de 2018].Disponible en Internet: http://www.oneworldnews.com/advantages-and-disadvantages-of-android-phones/

[71] iOS Architecture [en línea].Intellipaat.[Consultado:28 de Agosto de 2018].Disponible en Internet: https://intellipaat.com/tutorial/ios-tutorial/ios-architecture/

5.1.2.1 Cocoa Touch Layer: Según escrito de Apple Developer[72], es la capa responsable de la apariencia de las aplicaciones y su capacidad de respuesta a las acciones de los usuarios. Además, en esta capa se implementan muchas de las funciones que definen la experiencia del usuario de OS X, como el Centro de notificaciones, el modo de pantalla completa y el guardado automático.

5.1.2.2 Media Layer: Cuando la compañía Apple produce un nuevo dispositivo, propone Ray73, surge a la mente de sus usuarios trabajos importantes o mejoras en aspectos referentes a lo conocido como media. Este campo abarca temas del tipo creación de grafico complejos, calidad de audio y video, inclusión de gráficos 3D. Esta capa es la encargada de administrar todo lo relacionado con este tema.

De la misma manera que en la capa anterior, Ray[74] expresa que los desarrolladores encuentran una serie de frameworks que pueden utilizar a la hora de llevar a cabo desarrollo de aplicaciones en esta plataforma. Algunas de ellas son encargadas de administrar la reproducción y edición de sonido y video considerados complejos (Av Foundation Framework), otras ofrecen a desarrolladores capacidades avanzadas de procesamiento de imágenes y video a sus aplicaciones (Core Image Framework), también existen aquellas que se utilizan cuando se requiere hacer uso de características de dibujo 2D(Core Graphics Framework) y cuando es necesario el procesamiento de texto móvil(Core Text Framework).

5.1.2.3 Core Service Layer: Proporciona la mayor parte de la base sobre la cual se construyen las capas antes mencionadas. Según Smiyth[75], algunas de las características ofrecidas por frameworks en esta capa son los siguientes: acceso a

[72] Cocoa Applicatuion Layer. Apple Developer.[Consultado 28 de Agosto de 2018]. Disponible en Internet: https://developer.apple.com/library/archive/documentation/MacOSX/Conceptual/OSX_Technology_Overview/CocoaApplicationLayer/CocoaApplicationLayer.html

[73] RAY,Jhon. Sam Teach Yourself IOS 8 Application development in 24 hours.[en línea] Indiana.USA: Pearson.2015,p.121.[Consultado:1 de Septiembre de 2018].Disponible en Internet: https://books.google.com.co/books?id=FS75BgAAQBAJ&pg=PA120&lpg=PA120&dq=Cocoa+Touch+Layer&source=bl&ots=SjAJJmydTc&sig=j9DEa8ZAY3Mx7y-2FlF_A9gqtBg&hl=es&sa=X&ved=2ahUKEwj_yNS6gJHdAhVJ2lMKHUgSDyw4ChDoATAGegQIBBAB#v=onepage&q=Cocoa%20Touch%20Layer&f=true

[74] Ibid.,p. 46.

[75] SMYTH, Neil.IPhone IOS4. Devepment essentilas [en linea].4 ed.2011.[Consultado 4 de Septiembre de 2018].Disponible en Internet: https://books.google.com.co/books?id=QhDpbQJERd4C&pg=PA28&lpg=PA28&dq=Cocoa+Touch+Layer&source=bl&ots=-dxqrCB0ZP&sig=YLuTnAkA9AmHLfXyj-ifhjkg9LI&hl=es&sa=X&ved=2ahUKEwjT4KbPz5DdAhVOzVMKHfKXDrgQ6AEwCHoECAIQAQ#v=onepage&q=Cocoa%20Touch%20Layer&f=false

la base de datos de contactos de la libreta de direcciones de IPhone, acceso al protocolo de red TCPIP a través de interfaz basa de en lenguaje C, creación de modelo de datos de una aplicación haciendo uso de datos relacionales basado en SQLittle, facilitar las transacciones comerciales entre aplicaciones y la App Store de Apple, entre otras.

5.1.2.4 Core OS Layer: Este nivel, expresa Ramnath y Loffing[76], contiene el sistema operativo y los servicios sobre los cuales se construyen las otras tecnologías. Dentro de estos servicios se describen los siguientes:

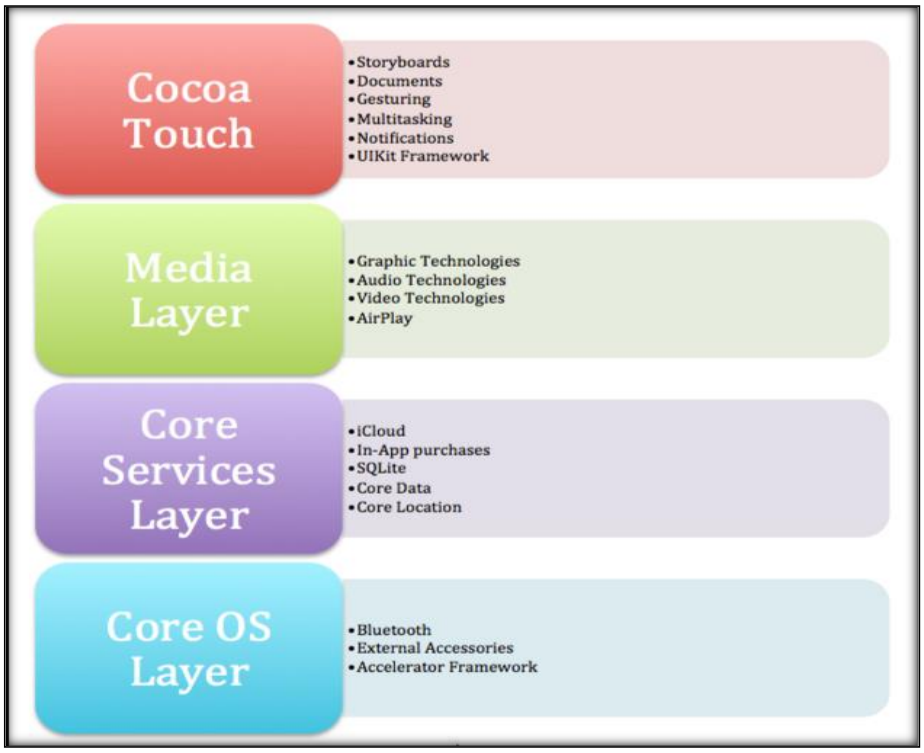
- Procesamiento de imágenes y señales digitales.
- Algebra lineal – principalmente la matemática de las operaciones con matrices utilizada para el dibujo vectorial.
- Acceso bluethooth.
- Conexiones de dispositivos de terceros al puerto serial.
- Dispositivos genéricos de seguridad.
- Servicios de redes y sistemas y manejo del sistema de archivos.

Gondi[77] expone en su artículo que se puede hacer uso de esta capa cuando se requiera buen sea implementar funciones de seguridad o comunicarse con un accesorio de hardware externo.

[76] RAMNATH, Rajib y LOFFING, Cheyney. Beginning IOS Programming For Dummies[en línea].New Jesey. 2014,p.14.[Consylado:1 de Septiembre de 2014].Disponible en Internet: https://books.google.com.co/books?id=8tIsAwAAQBAJ&pg=PA14&lpg=PA14&dq=core+os+layer&source=bl&ots=DCjP-btpm_&sig=fBWxkvI98Bd5zfYU--zX_m7jJI8&hl=es&sa=X&ved=2ahUKEwiegKrntpXdAhVrs1kKHSi2DNk4ChDoATAGegQIBBAB#v=onepage&q=core%20os%20layer&f=false

[77] GONDI, Tilakkumar. IOS – Architecture [en línea]. Tilakgondi Page.(14 de Enero de 2015).,párr. 5.[Consultado:13 de Octubre de 2018].Disponible en Internet: https://tilakgondi.wordpress.com/2015/01/14/ios-architecture/

Figura 4.Arquitectura sistema IOS



Fuente: GONDI, Tilakkumar. Arquitectura sistema IOS[imagen]. IOS – Architecture. 2015.p.1.[Consultado:13 de Octubre de 2018].Disponible en Internet: https://tilakgondi.wordpress.com/2015/01/14/ios-architecture/

Algunas de las ventajas ofrecidas por este tipo de plataforma son:

- Elevados niveles de seguridad: Desde su primera aparición en el mercado, el sistema operativo iOS se ha enorgullecido de su eficiencia frente a las ciberamenazas o ataques externos. Para complementar esta característica, el Blog de BeMovil[78] expresa que "la última actualización el código de seguridad con el sistema típico de 4 dígitos se ha actualizado a 6 dígitos ".

[78] Ventajas e inconvenientes del sistema operativo iOS [en línea].Blog BeMovil.2 de Agosto de 2015, párr. 2.[Consultado: 11 de Septiembre de 2018].Disponible en Internet: https://www.bemovil.es/blog/ventajas-sistema-operativo-ios/

- Filtro y exclusividad dentro del mercado de aplicaciones Apple Store: Las aplicaciones para iOS tiene que cumplir por un proceso revisión manual por parte del equipo de Apple antes de estar disponibles en su tienda. Esto hace que las apps desarrolladas en esta plataforma se lleven a cabo con mayor cuidado y con un mayor índice de calidad que el exigido en la plataforma Android.

- Interfaz intuitiva: La mejora en la experiencia de usuario es una de las características en las cuales ha trabajado más fuertemente la plataforma IOS, ofreciendo opciones de configuración del equipo sencillas, y menús de navegación intuitivos.

- Elevada duración de la batería, lo cual se expresa como una gran ventaja frente a su inmediato competidor Android. Además de esto, la sincronización entre los diversos dispositivos de Apple ha sido una de las principales banderas de la marca de la manzana. Todas las fotos, videos e imágenes que se encuentren en su dispositivo Apple, pueden estar disponible en todos sus equipos. Algunos de los servicios involucrados en este tipo de sincronizaciones son: iTunes, iTouch y iCloud.

Las ventajas anteriormente descritas, se ven opacadas, en algunos casos por deficiencias o puntos en contra frente a su inmediato competidor en el mercado, los cuales se describen a continuación:

- Las opciones de personalización del equipo pueden catalogarse casi nulas. De esta forma los usuarios convencionales de Android verán frustrante esta restricción planteada para las versiones del sistema OIS. Tareas consideradas sencillas en otros ambientes tales como la creación de accesos directos, en esta plataforma no se encuentran disponibles o sería una labor mucho más tediosa llegar a habilitarlas en el caso de que sea posible su activación.

- El costo de estos equipos es muy superior al de su competencia. Es decir, a la hora de presupuesto, difícilmente esta opción puede ser viable para un usuario con ingresos considerados medios.

- Otro de los inconvenientes que trae su código cerrado, según Travis[79], es que a pesar de que se pueden elegir diferentes aplicaciones para usar, por ejemplo, un navegador diferente al instalado por defecto, no existe la forma de configurar ninguna aplicación como predeterminada.

- Pobre integración con hardware de terceros. Por tomar un ejemplo, afirma Bach[80], a la hora de hacer uso de teclados de terceros, estos pueden hasta cierto punto funcionar, pero a la hora de ingresar campos del tipo contraseña vuelve al teclado de iOS.

5.1.3 Comparativo arquitecturas sistema Android y IOS: La elección del procesador de un celular ha sido la característica que los usuarios tienen principalmente en cuenta para hacer la elección de sus equipos. En su escrito, Blas[81] expresa que el usuario moderno tiene claro que entre mejor desempeño tenga, su experiencia en cuanto al manejo del sistema operativo y sus aplicaciones mejorará ostensiblemente.

Adicionalmente al procesador, afirma Blas[82], el entorno de desarrollo es crucial a la hora de hacer uso de recursos, que de hecho son reducidos debido a su tamaño, permitiendo su administración efectiva de manera que permita mayor rendimiento del equipo con buena calidad, y es donde el entorno de desarrollo proporciona múltiples herramientas para cumplir con estos objetivos.

Por último, Blas expone en su blog que “la arquitectura de los dispositivos móviles se encuentra ligadas a las necesidades y requerimientos de cada dispositivo como lo son memoria, periféricos, batería, el tipo de buses, entre otras variables. Por otra parte, el entorno de desarrollo consiste en un editor de código, un compilador,

[79] TRAVIS,May. IOS, Android or Windows: what’s the best mobile operating system? [en línea]. The Whiz Cells.(17 de Febrero de 2017).párr.20.[Consultado:4 de Septiembre de 2018]. Disponible en: https://www.thewhizcells.com/ios-android-windows-whats-best-mobile-operating-system/

[80] BACH, Michael. IPhone vs. Android: What are the pros and cons?[en línea].Quora.(27 de Febrero de 2016), párr.8.[Consultado: 24 de Abril de 2018].Disponible en Internet: https://www.quora.com/IPhone-vs-Android-What-are-the-pros-and-cons

[81] BLAS,Erika. Arquitectura y Entorno de Desarrollo de Aplicaciones Móviles [en línea].Blog de Erika Blas. 26 de Mayo de 2014, párr.2.[Consultado:19 de Marzo de 2018].Disponible en Internet: http://erykabp.blogspot.com/2014/05/arquitectura-y-entorno-de-desarrollo-de.html

[82] Ibid.,p.50.

un depurador y un constructor de interfaz gráfica, pueden ser aplicaciones por si solas o ser aplicaciones existentes".[83]

Tabla 1. Comparativo arquitecturas Android y iOS

Característica	Android	IOS
Arquitectura del procesador	Soporte para EMR MISPS y X86	ARM
Arquitectura del Kernel	Versión modificada de Linux	XNU
Tipo de licencia	Open source, Android Open Source Project, Apache2 con extensions GPL v2	ASL Apple Public Source License
Sistema de ficheros del sistema operativo	EXT4 desde 2010	HFS
Formato de empaquetado de aplicaciones	APK	IPA
Políticas copias de seguridad	Permite realizar copia parcial de datos, que incluye: contraseñas WIFI datos de ajustes y aplicaciones. Para copia completa se requiere de aplicación de terceros	Permite realizar copia total de seguridad total de datos. También permite la utilización de herramientas de terceros

Fuente: Comparativo Arquitecturas Android y IOS[imagen].Comparativa entre arquitecturas móviles. 2016.p. 9.[Consultado: 21 de Marzo de 2018].Disponible en Internet: https://www.certsi.es/blog/comparativa-arquitecturas-moviles

El debate que se llevó a cabo hace unos años teniendo como participantes a los sistemas operativos de computadores personales Windows y Mac, se ha trasladado al ambiente de los dispositivos móviles con nuevos contrincantes. Las dos principales plataformas, tanto Android como IOS ofrecen una serie de características importantes de las cuales cada una hace alarde: se puede estar

[83] Ibid.,p.50.

tentado tanto por los diseños ofrecidos por el ambiente IOS, como por la gran variedad de hardware disponible en plataforma Android. Sin embrago existen una serie de variables adicionales a tener en cuenta a la hora de llegar a tomar una decisión por alguna de las principales opciones disponibles. A continuación, se analizarán algunas de estas variables y la forma en las que las plataformas se desempeñan en dichas evaluaciones.

Opción de hardware: Según expresa Hopping[84], en la actualidad no existe forma, por lo menos confiable de ejecutar un sistema operativo en los dispositivos de la otra plataforma, el software y el hardware viene como un paquete. Entendiendo este concepto, las dos plataformas ofrecen diferentes argumentos que los usuarios deben tener analiza con cuidado a la hora de seleccionar algunos de las plataformas. Por ejemplo, OIS ofrece tres características que los hacen invencible en esta categoría: velocidad, pantalla y cámara. Sin embargo, su inmediato competidor, Android, esta empezado a incursionar fuertemente en términos de equipos con atractivo visual y características innovadoras, aspectos en donde la marca Apple ha perdido terreno.

Hopping[85] agrega que Android también tiene la ventaja en términos de elección de equipos donde se encuentra instalada su versión. Si bien los usuarios de iOS están restringidos a un pequeño número de opciones en el mercado, hay cientos de dispositivos Android diferentes para elegir, con opciones para todos los gustos y presupuestos.

Diseño: En este aspecto, a pesar de que la plataforma Android ha mejorado sustancialmente su diseño comparando sus primeras versiones, Hopping expresa que “el sistema operativo de Apple es simplemente más atractivo y más intuitivo que cualquier cosa que Google pueda ofrecer. Permite a la mayoría de sus usuarios hacer todo lo que necesitan para hacer de manera rápida y fácil”[86]. En esta última parte se incluye el concepto de nivel usabilidad del dispositivo.

[84] HOPPING,Clare. Android vs iOS: which mobile OS is right for you? [En línea]. ITPRO Analysis Business Insigth.(31 de Agosto de 2018), párr. 5.[Consultado:7 de Septiembre de 2018],Disponible en Internet: http://www.itpro.co.uk/mobile/30409/android-vs-ios-which-mobile-os-is-right-for-you

[85] Ibid.,p.52.

.

[86] Ibid.,p.52.

Seguridad y privacidad: Debido al tipo de plataforma abierta trabajada en Android, esta es considerada más vulnerable a ataques y amenazas cibernéticas. En este respecto, Katariya [87] plantea que el hecho de contar con una gran cantidad de dispositivos (fragmentación), así como la apertura a aplicaciones de terceros, hacen que este sistema sea susceptible a inconvenientes de seguridad. A este respecto, IOS es más estricto a la hora de permitir acceso a sus aplicaciones, así como brindar información de contacto a sus aplicaciones.

Aplicaciones: Antes de empezar a analizar este punto es importante conocer el número de aplicaciones disponible para cada tienda de aplicaciones. Según datos obtenidos de escrito publicado por Hill[88], en el caso de IOS el número aproximado de aplicaciones asciende a 2.2 millones. Para Android este número está cerca a los 3,5 millones. Es importante acotar que la gran mayoría de aplicaciones usadas por los usuarios se encuentran disponibles en las dos plataformas.

Desde las primeras épocas de sus apariciones en el mercado de dispositivo móviles, expresa Hill[89], IOS ha sido considerada una plataforma más lucrativa para desarrolladores, razón por la cual se ha convertido en tendencia que las aplicaciones en primera instancia se encuentren disponibles en esta plataforma, pero esta premisa ha cambiado a medida que la participación en el mercado de Android continúa creciendo. A pesar de la variedad de aplicaciones gratuitas ofrecidas en su tienda, algunos de los juegos para móviles no se encuentran disponibles en la plataforma Android, solo se desarrollan para su competencia.

Estabilidad: Un informe publicado por Blancco Technology Group[90] reveló que para el segundo semestre de año 2017 la tasa de fallas de dispositivos Android en todo el mundo fue del 25 por ciento, que fue más del doble que la tasa de fallas de los dispositivos iOS (12 por ciento) en el mismo periodo.

---

[87]KATARIYA,Jayanti. Apple Vs Android - A comparative study 2017[En línea] Mobile Apps Channel.27 de Febrero de 2017.párr 7.[Consultado:12 ad Abril de 2018].Disponible en Internet: https://www.whatech.com/mobile-apps/blog/archive/267836-apple-vs-android-a-comparative-study-2017

[88] HILL, Simon. Android vs. iOS: Which smartphone platform is the best?[En línea].Digital Trends.(7 de Marzo de 2018),parr.5.[Consultado:8 de Septiembre de 2018].Disponible en Internet: https://www.digitaltrends.com/mobile/android-vs-ios/

[89] Ibid.,p.53.

[90] BLANCCO TECHNOLOGY GROUP. Trend Report: Q2 2017 State of Mobile Device Performance and Health [en línea]. Blancco (Septiembre de 2017), párr.6. [Consultado:11 de Septiembre de 2018].Disponible en Internet: https://download.blancco.com/download/en-rs-q2-2017-state-of-mobile-device-performance-report.pdf

En cuanto a los inconvenientes de la plataforma IOS, Blancco[91] plantea en su informe que las fallas se presentan principalmente en los equipos iPhone 7 y iPhone 7 plus con un 7 y 6 por ciento de fallas identificadas respectivamente. Blancco expone que los usuarios han expuesto fallas relacionadas con "poca duración de la batería, problemas de activación, mala calidad de la llamada telefónica / altavoz, y las aplicaciones de congelación / bloqueo y el 3D Touch dejaron de funcionar". [92]

Por su parte, Biancco[93] indica que en los equipos con sistema Android, las marcas que presentan mayores tasas de fallos son Samsung Galaxy S5, Galaxy S7 y S7 Edge, los cuales tienen un 6 por ciento de porcentaje de fallas respectivamente. Los problemas más comunes identificados por los usuarios de Android están relacionados con el desempeño y rendimiento, desconexión de Wi-Fi, fallas presentadas con la cámara de los dispositivos, entre otros.

5.1.4 Anatomía de un ataque a dispositivos móviles: Antes de abordar el tema de la forma como se llevan a cabo los ataques a dispositivos móviles, es conveniente conocer los diferentes vectores de ataques utilizados por los delincuentes para afectar este tipo de dispositivos.

Según expone Mendoza[94] , un vector de ataque es una técnica que usa un cibercriminal para acceder a un dispositivo o red inalámbrica con el objeto de inyectar código malicioso comúnmente llamado payload. Estos vectores son herramientas importantes para los atacantes a la hora de identificar vulnerabilidades en los sistemas. Gran parte de estos vectores aprovechan la parte humana involucrada en los sistemas, ya que es la parte del eslabón más vulnerable. Algunos de los vectores más comúnmente usados por los delincuentes informáticos son:

[91] Ibid.,p.53.

[92] Ibid.,p.53.

[93] Ibid.,p.53.

[94] MENDOZA,Azury. ¿A qué se le conoce como vectores de ataque en ciberseguridad y cómo puedes eliminarlos de tus ambientes digitales?[en línea]. GB Advisors.(2 de Mayo de 2018).párr.3.[Consultado:13 de Septiembre de 2018].Disponible en Internet: http://www.gb-advisors.com/es/vectores-de-ataque-en-ciberseguridad/

- Ingeniería social: IT Business Solutions[95] plantea que la ingeniería social es una estrategia basada en el engaño y está orientada a explotar las debilidades del factor humano. Consiste en obtener información confidencial de un usuario perteneciente a un sistema u organización. Este tipo de ataques pueden permitir a un atacante obtener acceso no autorizado, y de esta manera eludir los esquemas de seguridad que se hayan implementado en la compañía.

- Códigos maliciosos: Los códigos maliciosos o malware expone IT Business Solutions[96], son considerados una de las principales amenazas de seguridad para cualquier Entidad. Hace referencia a programas que causan algún tipo de daño o anomalía en los sistemas. Como ejemplo de este tipo de amenazas se pueden enumerar: los programas troyanos, gusanos, virus informáticos, spyware, backdoors, rootkits, keyloggers, entre otros.

- SQL Injection: Este tipo de técnicas, según IT Business Solutions[97] hacen uso de las vulnerabilidades del lenguaje de consulta estructurado (SQL) en cual es utilizado en las bases de datos relacionales para inhabilitar o accesar las bases de datos de las organizaciones. Los ataques de inyección SQL (SQL Injection) están dirigidos a afectar directamente una aplicación o en su defecto el funcionamiento lógico de la misma, exponiendo los datos almacenados a ataques por parte de cibercriminales.

- Denegación de servicio (DDoS) : Los ataques de denegación de servicio, expone Fernández[98], son un tipo de ataque informático a través del cual se reduce o anula principalmente la capacidad de servidores encargados de ofrecer servicios. Un ejemplo de una situación en la cual un sistema pueda verse afectado por este tipo de ataques es la saturación de servicios haciendo uso de envíos masivos de solicitudes o explotación de vulnerabilidades de programas o servicios que dejan de funcionar total o parcialmente.

Algunas de las consecuencias que traen este tipo de ataques son:

- Perdida de datos: En el momento que un dispositivo móvil es atacado por alguno de los vectores anteriormente citados o se le ha introducido un virus, el atacante tomará todos sus datos almacenados.

[95] IT BUSINESS SOLUTIONS. ¿Cuáles son los vectores de ataque que usan los delincuentes informáticos?[en línea].[Consultado:13 de Septiembre de 2017].Disponible en Internet: https://www.itbusiness-solutions.com.mx/vectores-de-ataque-de-ciberdelincuentes

[96] Ibid.,p.55.

[97] Ibid.,p.55.

[98] FERNANDEZ CASTRILLO, Alejandro. Medidas de protección frente ataques de denegación de servicio (DoS) [en línea]. Centro de Respuesta a incidentes de Seguridad e Industria CERTSI.España.(26 de Enero de 2018).párr.1[Consultado:11 de Septiembre de 2018].Disponible en Internet: https://www.certsi.es/blog/medidas-proteccion-frente-ataques-denegacion-servicio-dos

- Pérdida de reputación: En el caso de que el objetivo del ataque sea una cuenta de Facebook, o cuenta de correo electrónico, el atacante puede enviar mensajes falsos a sus contactos, socios comerciales y otros contactos afectando su reputación o de su empresa.

- Robo de identidad: Existen situaciones en las cuales se presentan robos de nombres, números de tarjeta de crédito, fotos, entre otros, los cuales pueden utilizarse para perpetrar un ilícito.

Un ataque móvil, expone lvdaqian,[99] contiene tres aspectos que se pueden considerar cruciales a la hora que los delincuentes busquen explotar vulnerabilidades para lanzar ataques hacia los equipos: el dispositivo, la red y el centro de datos, o una combinación de los anteriores.

Figura 5.Anatomía ataque móvil

Fuente: Viaforensics. Anatomía ataque móvil [imagen]. Anatomy of a Mobile Attack. Ensuring Security on Mobile Devices It is possible…right? 2010.p.26.[Consultado:1 de Septiembre de 2018].Disponible en Internet: https://www.nowsecure.com/wp-content/uploads/2012/05/viaForensics-AmericanBanker-CARDFORUM12-final.pdf

[99] LVDAQIAN ,Darwin. Mobile Security Primer[en línea]. GitHub, Inc.(3 de Marzo de 2017), párr. 2.[Consultado: 24 de Marzo de 2018].Disponible en Internet: https://github.com/nowsecure/secure-mobile-development/blob/master/en/primer/mobile-security.md

Los ataques basados en dispositivos, expone lvdaqian[100], hacen uso de diferentes puntos de entrada tales como Navegador, correo, mensajes SMS; aplicaciones de terceros, sistema operativo, Bluetooth y otros canales de comunicación.

Para DCIT[101], Las puertas de ingreso para los ataques de red son: Wi-Fi sin cifrado, punto de acceso no confiable, Sniffing, Man-inThe-Middle (MITM), secuestro de sesión, envenenamiento DNS, y certificados SSL falsos.

Por último, lvdaqian[102] indica que los atacantes se dirigen al centro de datos haciendo uso de dos puntos principales de entrada o ingreso: servidores web y las bases de datos. De la categoría de ataques y vulnerabilidades basados en servidores web hacen parte: Vulnerabilidades de la plataforma, mala configuración del servidor, Cross-Site Scripting (XSS), falsificación de solicitudes entre sitios (CSRF), validación de entrada débil, y ataques de fuerza bruta. En la categoría de bases de datos se encuentran: inyección de código SQL, ejecución del comando del sistema operativo, escalada de privilegios.

Luego de conocer las formas en que se puede llevar a cabo un ataque móvil, una pregunta que queda planteada es qué sucede cuando nuestro dispositivo móvil ha sido afectado por algún tipo de ataque. Lo primero que se pierde es la privacidad del usuario. Pero detrás de esto hay mucho más.

Según artículo publicado en TutotialsPoints “no solo es la privacidad del usuario y los contactos almacenados en el equipo, sino la posibilidad de tomar nuestros datos personales para llevar a cabo actividades ilegales (por ejemplo, Ataques DDOS), realizar pagos no autorizados, entre muchas otras labores”[103].

---

[100] Ibid.,p.56.

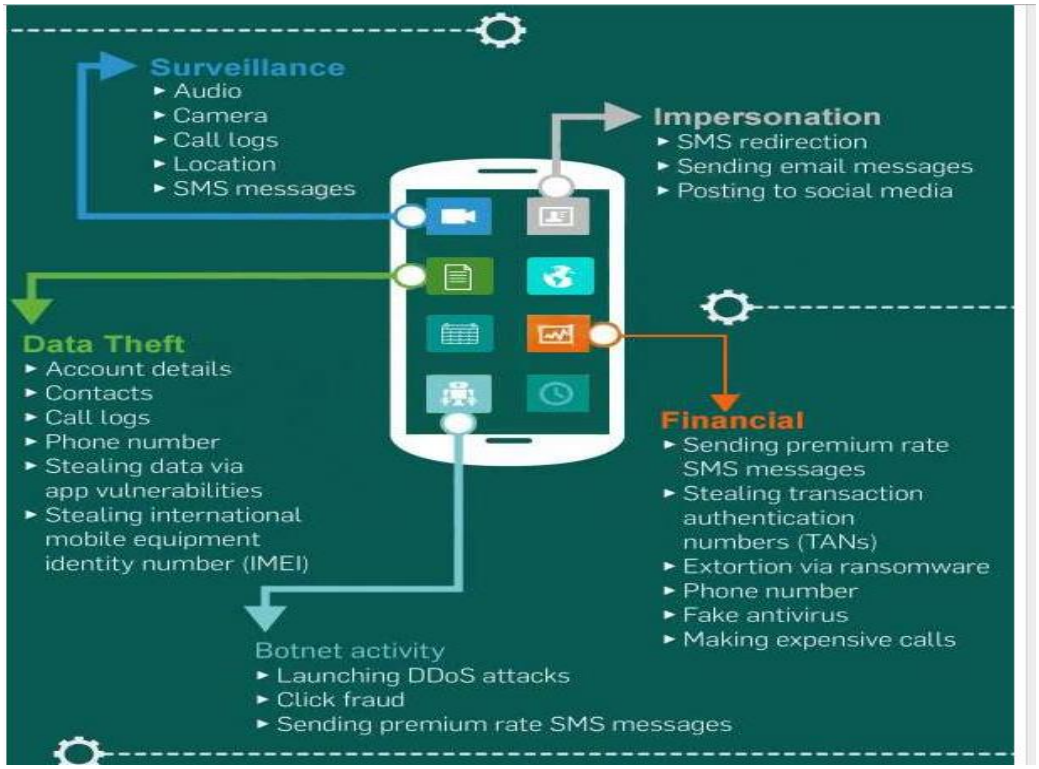
[101] DCIT. Security assesment of mobile applications (iOS, Android)[en línea].[Consultado:20 de Marzo de 2018].Disponible en Internet: https://www.dcit.cz/en/security/mobile-applications-security

[102] LVDAQIAN. Op. cit., p.57.

[103] Mobile Security - Attack Vectors [en línea].TutorialPoint. [Consultado: 5 de Abril de 2018]. Disponible en Internet: https://www.tutorialspoint.com/mobile_security/mobile_security_attack_vectors.htm

A continuación, se muestra un esquema que aborda los aspectos que están disponibles a los delincuentes informáticos cuando un dispositivo móvil es atacado. Estos aspectos se encuentran divididos en categorías tales como: vigilancia, interpretación, robo de datos y aspectos financieros.

Figura 6. ¿Cómo puede un pirata informático beneficiarse de un móvil con éxito comprometido?



Fuente: Tutorialspoint. ¿Cómo puede un pirata informático beneficiarse de un móvil con éxito comprometido?[imagen]. Mobile Security - Attack Vectors. p.10. [Consultado: 18 de Marzo de 2018]. Disponible en Internet: https://www.tutorialspoint.com/mobile_security/mobile_security_attack_vectors.htm

Según ilustración expuesta en Tutorialspoint[104], en la categoría de vigilancia (surveillance) se ubican dispositivos del tipo cámara, audio, llamadas y ubicación geográfica que están a merced de delincuentes a la hora de ser afectados por un ataque. En interpretación se pueden llevar a cabo labores como

[104] Ibid.,p.57.

redireccionamiento de mensajes SMS, y publicaciones fraudulentas en redes sociales. En robo de datos se puede tener acceso a contactos, registro de llamadas y acceso a datos personales a través de aplicaciones vulnerables.

Cuando los usuarios son atacados por cualquier tipo de vectores, concluye Tutorialspoint[105], también pueden caer en las manos de botnets (redes de computadores infectados con una variedad de malware) con las cuales se corre el riesgo de ataques de denegación de servicio. Por último, la parte financiera también se afecta cuando somos objeto de este tipo de ataques: extorciones via ransomware, robo de numero de autenticación de transacciones (TAN), antivirus falsos hacen parte de esta categoría.

5.1.5 Riesgos más importantes para aplicaciones móviles: Tomando como base la importancia que ha tenido el sector de los dispositivos móviles y su amplia difusión en la actualidad, y que sus aplicaciones forman parte de nuestras labores cotidianas, es importante resaltar el aspecto de la existencia de cierto nivel de seguridad que deban tener estas a la hora de ser liberadas en cualquiera de las plataformas existentes. Por esta razón, plantea Caballero [106], que el desarrollo de aplicaciones para dispositivos móviles debe ir mucho más allá de diseñar o presentar de una manera de manera intuitiva o atractiva una interfaz de usuario o resolver simples problemas descritos por clientes.

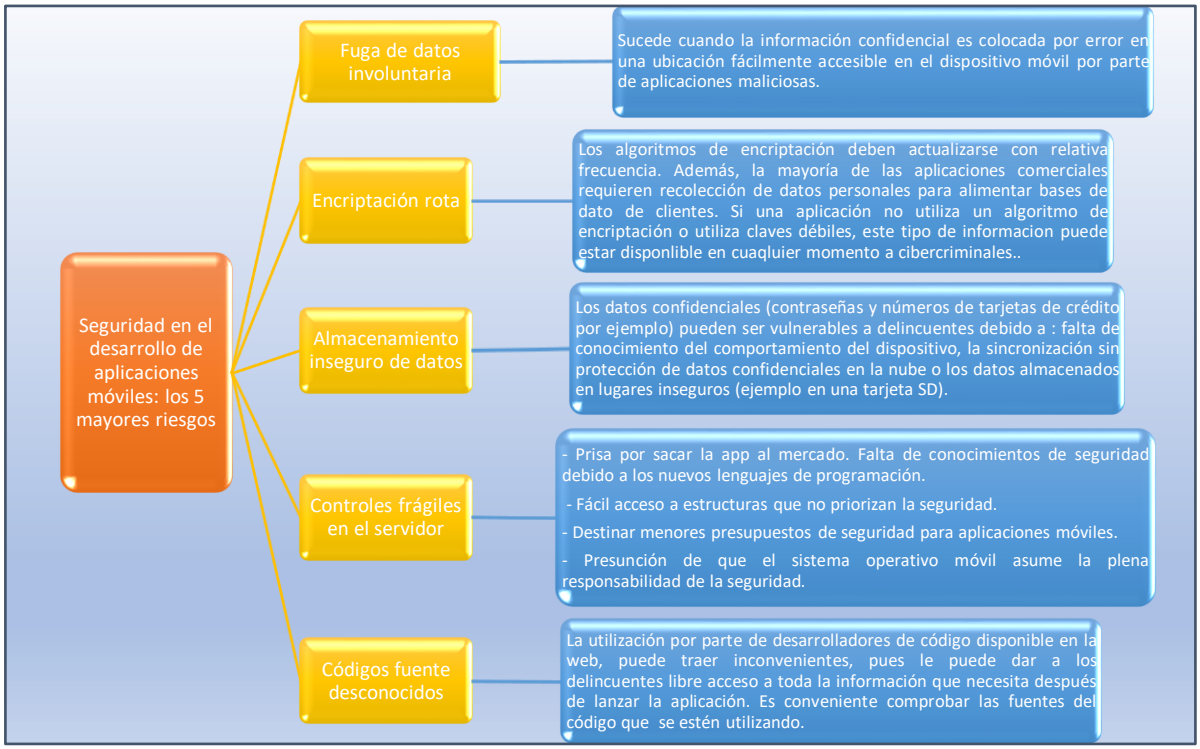
La seguridad en el desarrollo de aplicaciones móviles y la protección de datos expone Caballero “debe ser uno de los elementos más importante de los profesionales que buscan el crecimiento a largo plazo y la consolidación de su trabajo en esta industria. Mientras que el mundo móvil experimenta un crecimiento espectacular, se expone a importantes problemas de seguridad”[107].

[105] Ibid.p.,57.

[106] CABALLERO, Alejandro. Seguridad en el desarrollo de aplicaciones móviles: los 5 mayores riesgos [en línea]. Blog-seguridad-desarrollo-aplicaciones-moviles-mayores-riesgos.(8 de Marzo de 2018).[Consultado:3 de Abril de 2018].Disponible en Internet: https://kingofapp.es/blog/seguridad-desarrollo-aplicaciones-moviles-mayores-riesgos/

[107] Ibid.,p.59.

Figura 7.Mayores riesgos de seguridad en desarrollo de aplicaciones móviles



Fuente: CABALLERO, Alejandro. Mayores riesgos de seguridad en desarrollo de aplicaciones moviles[imagen]. Seguridad en el desarrollo de aplicaciones móviles: los 5 mayores riesgos.2018. p.5.[Consultado:12 de Septiembre de 2018].Disponible en Internet: https://kingofapp.es/blog/seguridad-desarrollo-aplicaciones-moviles-mayores-riesgos/#Almacenamiento_inseguro_de_datos

Tabla 2.Riesgos comunes de seguridad para Aplicaciones Móviles – MOBILE TOP 10 2016

Riesgo	Descripción
Uso inadecuado de la plataforma	Hace referencia al uso indebido de una característica de la plataforma y la falta de uso de controles de seguridad de la plataforma. Ejemplos: permisos de plataforma, uso indebido de características de reconocimiento biométrico.

Tabla 2. (Continuación)

Riesgo	Descripción
Comunicación insegura	Las comunicaciones inseguras exponen los datos de la aplicación a riesgos denominados de exposición, lo que puede causar una posible fuga de información sensible a través de la comunicación de la red. Este tipo de inconvenientes pueden presentarse por: versiones SSL incorrectas, o negociaciones débiles entre otras causas.
Autenticación insegura	Esta categoría identifica intentos de autenticación del usuario final o gestiones de sesión incorrectas. Los atacantes pueden comprometer contraseñas o claves con el objeto de suplantar la identidad de otros usuarios. El problema puede ser causado por la ausencia o la implementación incorrecta de los mecanismos de autenticación y la mala administración de sesiones.
Criptografía insuficiente	Los atacantes pueden robar o acceder a datos con niveles de protección bajos, debido a que no se utilizan adecuadamente las funciones criptográficas para encriptar activos de Información delicados.
Autorización insegura	Los atacantes pueden omitir el mecanismo de autorización y ejecutar la funcionalidad de privilegio excesivo. El problema puede ser causado por la falla de un servidor para aplicar correctamente la identidad y los permisos definidos por la aplicación móvil.

Tabla 2. (Continuación)

Riesgo	Descripción
Calidad del código del cliente	Las generaciones de código de clientes deficientes pueden generar vulnerabilidades, tales como desbordamientos de búfer y pérdidas de memoria al pasar entradas maliciosas a la aplicación móvil.
Manipulación de Código	Haciendo uso de formas maliciosas o aplicaciones falsas alojadas en ubicaciones de terceros de una aplicación, los delincuentes pueden modificar una aplicación original con el objeto de obtener ganancias personales o monetarias. Los delincuentes hacen uso del pishing para logar que sus aplicaciones se instalen en los equipos de las víctimas.
Ingeniería inversa	Los atacantes pueden hacer uso del análisis de núcleo binario de una app para determinar su código fuente, bibliotecas, algoritmos y otros activos con el buscando explotar vulnerabilidades, recolectar datos confidenciales o robar propiedad intelectual.
Funcionalidad Extraña	La etapa de desarrollo de una aplicación puede utilizarse para identificar o crear puestas traseras de la misma, y en el caso de su existencia en su versión de producción hacer uso de ellas para llevar a cabo acciones maliciosa.

Fuente: INFOSECK. Developing Secure Mobile App - Common Security Risks for Mobile App [en línea]. [Consultado: 10 de Septiembre de 2018]. Disponible en Internet: https://www.infosec.gov.hk/english/business/other_syma_3.html

5.1.6 Principales ataques y amenazas en Android y IOS: Los dispositivos móviles son herramientas consideradas fundamentales en los ambientes laborales tan comunes como las videoconferencias, correos electrónicos, o chats de servicio al cliente. Para las directivas de una compañía, plantea Arubanetworks[108], permitir que los empleados trabajen desde sus dispositivos móviles puede incluso aumentar la satisfacción, la productividad, la creatividad, la lealtad y el compromiso.

Sin embargo, estas ventajas traen consigo una amenaza que vienen con el uso de dichos dispositivos: las amenazas móviles. A menos que se desarrollen e implementen medidas de seguridad adecuadas, cada vez que un funcionario ingrese a través de su dispositivo móvil a información de la compañía pone en riego toda la red de la cual hace parte.

Para abordar el tema de amenazas que afectan dispositivos móviles , Ismail[109] expresa inicialmente que este tipo de dispositivos necesita dos tipos de protecciones: la ciberseguridad y la física. Para el caso de las protecciones de seguridad cibernética algunas de las amenazas que se pueden catalogar en esta categoría son: amenazas de malware y amenazas basadas en vulnerabilidades de dispositivos, entre otras.

Desde el punto de vista de la protección física expone Ismail[110], un teléfono móvil puede sufrir daños físicos de diferentes formas como humedad, exposición a temperaturas extremas entre otras. Otro tipo de este tipo de amenazas es el posible robo o extravío del dispositivo. Afortunadamente, existe software que permite ubicar equipos haciendo uso de geolocalización y funciones de bloque para contrarrestar este tipo de amenazas.

[108] Mobility, performance and engagement How CIOs can contribute to business performance by shaping the employee experience[en línea]. The Economist Intelligence Unit.[Consultado:17 de Septiembre de 2018].Disponible en Internet: https://www.arubanetworks.com/pdf-viewer/?q=/assets/EIUStudy.pdf

[109] ISMAIL, Nick. Common security vulnerabilities of mobile devices [en línea].InformationAge.(21 de Febrero de 2017),párr. 7.[Consultado:22 de Septiembre de 2018].Disponible en Internet: https://www.information-age.com/security-vulnerabilities-mobile-devices-123464616/

[110] Ibid.,p.63.

Por último, Ismail[111] indica que, si se presenta el caso de hacer uso de los dispositivos para propósitos de una compañía u organización, también existen otras amenazas como amenazas de usuarios no autorizados que acceden a la red de la empresa, así como amenazas de redes no seguras.

Según estadísticas publicadas por empresas del sector de la telefonía móvil, las amenazas en el ambiente de dispositivos móviles continúan creciendo a través de los años. En reporte de la Symantec[112], En 2017 hubo un 54 por ciento aumento en el número de nuevo variantes de malware. Este dato, adicionado al hecho de que los atacantes han desarrollado nuevos métodos de infección con el propósito de permanecer en dispositivos comprometidos el mayor tiempo posible, se ha convertido en un verdadero dolor de cabeza a la hora de identificarlos y promover medidas para no ser víctima de estas amenazas. Adicionalmente, plantea Symantec en su reporte que "se han creado una variedad de medios de generar ingresos a partir de dispositivos, desde ransomware a la minería de criptomonedas"[113]

Figura 8.Desafíos de seguridad en los dispositivos móviles

Fuente: RINALDI, Paola. Desafíos De Seguridad En Los Dispositivos Móviles [imagen]. Security challenges on mobile devices.2017.p.10. [Consultado: 17 de Septiembre de 2018].Disponible en Internet: https://www.le-vpn.com/security-challenges-on-mobile-devices/

[111] Ibid.,p.63.

[112] Internet Security Threat Report [en línea].Symantec. [Consultado:17 de Septiembre de 2018]. Disponible en Internet: https://www.symantec.com/content/dam/symantec/docs/reports/istr-23-2018-en.pdf

[113] Ibid.,p.64.

Como dato irónico, expone Symantec[114], mientras los ataques continúan evolucionando y mutando, muchos usuarios continúan para hacer la vida más fácil para los atacantes al no hacer uso de actualizaciones de sistemas operativos con parches liberados por fabricantes. En caso particular, Symantec indica que, solo 20% de dispositivos disponibles con sistemas Android en el mercado ejecutan la versión más actualizada del sistema.

Para CSO[115],sitio web que aborda temas ciberseguridad seguridad de la información y gestión de incidentes, los riesgos de seguridad móvil en el año 2018 estarán dirigidos a áreas que normalmente no se tiene en cuenta, y se enfocarán en los siguientes temas:

Fuga de datos: Pareciera de alguna forma una afirmación traída de épocas pasadas, pero, para CSO[116], la fuga de datos es vista como una de las amenazas más preocupantes para la seguridad empresarial. Lo que sucede es que normalmente este tipo de amenaza no es nefasto por naturaleza, más bien se trata de usuarios que no tienen ningún tipo de control a la hora de instalar aplicaciones en sus dispositivos.

Para ese tipo de amenazas, indica CSO que "las herramientas de prevención de pérdida de datos (DLP) pueden ser la forma más efectiva de protección. Dicho software está diseñado explícitamente para evitar la exposición de información sensible, incluso en escenarios accidentales" [117].

Ingeniería Social: A pesar de conocer su funcionamiento y de la difusión realizada acerca de los cuidados requeridos para evitar este tipo de amenazas, los ataques de este tipo siguen siendo bastante efectivos. El desarrollo de este tipo de ataques, expresa Lord[118], trae consigo un trabajo del orden psicológico desarrollado por parte

[114] Ibid.,p.64.

[115] JR, Rafael. 5 mobile security threats you should take seriously in 2018 [en línea]. CSO.(13 de Diciembre de 2017), párr.3.[Consultado:17 de Septiembre de 2018].Disponible en Internet: https://www.csoonline.com/article/3241727/mobile-security/5-mobile-security-threats-you-should-take-seriously-in-2018.html

[116] Ibid., p 65.

[117] Ibid., p 65.

[118] LORD,Nat, Social Engineering Attacks: Common Techniques & How to Prevent an Attack [en línea].DigitalGuardian.(19 de Septiembre de 2018),párr 2.[Consultado:21 de Septiembre de 2018].Disponible en Internet: https://digitalguardian.com/blog/social-engineering-attacks-common-techniques-how-prevent-attack

de los atacantes, habilidades sin las cuales, afirman las víctimas, no entregarían su información personal confidencial. El hecho de involucrar un elemento humano, culmina Lord, [119] hace que la prevención este tipo de ataques pueda ser más complejo para las empresas.

Wi-Fi inseguros: Normalmente se habla de que la seguridad de un dispositivo móvil está asociado al nivel de seguridad de la red sobre la cual se encuentra trasmitiendo los datos. Por esto es prudente, expone Tektonica [120], considerar el hecho de que, al estar conectados a redes públicas, hace que nuestra información se encuentre expuesta tanto a interceptación de tráfico que viaja por dichas redes, como al robo de información valiosa que se encuentre almacenada en nuestros equipos.

Puntos finales pasados por alto (Overlooked endpoints): Entendiendo los dispositivos móviles como parte de un sistema funcional, es importante tener claro que no son los únicos puntos de ataque donde los cibercriminales pueden tener acceso a datos confidenciales. Los puntos finales, como por ejemplo impresoras, expresa Teknotonica, aunque en algunos casos no parezca, también son consideradas amenazas de seguridad. "Si alguien usa un dispositivo móvil infectado e imprime en una impresora no segura, podría provocar una brecha importante que luego podría extenderse a toda la red." [121]

5.1.6.1 Categorías de ataques a Smartphones*:* Según lo expuesto por Syed Farhan[122] en artículo publicado en IJACSA, los ataques a dispositivos móviles se clasifican en dos categorías: los denominados antiguos, que son los más comunes y documentados hasta el momento y se caracterizan por estar presentes casi desde el momento de la aparición de los dispositivos móviles y los ataques nuevos, de los cuales hacen parte los ataques de control de flujo y ataques de fuerza bruta entre otros.

---

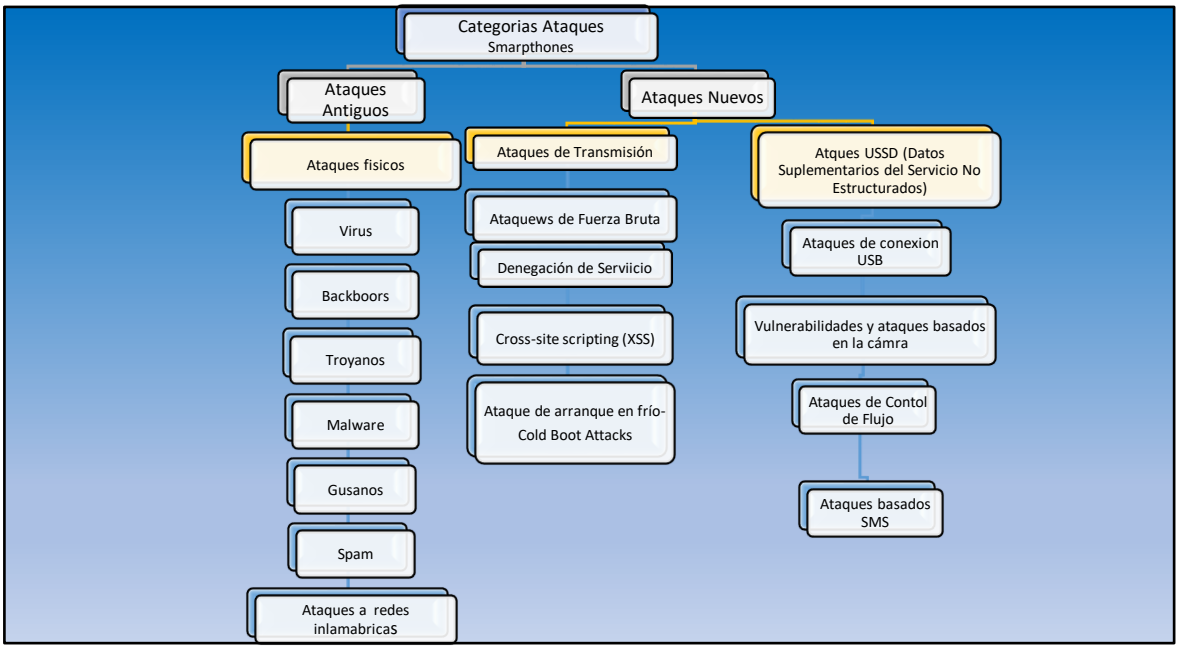
[119] Ibid.,p.65.

[120] 5 mobile threats you should shut down in 2018 [en línea].Tektonika.[Consultado:21 de Septiembre de 2018].Disponible en Internet: https://www.tektonikamag.com/index.php/2018/05/04/5-mobile-threats-you-should-shut-down-in-2018/

[121] Ibid.,p.66.

[122] SYED FARHAN, Alam Zaidi, et al. A Survey on Security for Smartphone Device [en línea]. En (IJACSA) International Journal of Advanced Computer Science and Applications,2016, Vol. 7, No. 4,p.210.[Consultado:27 de Septiembre de 2018].Disponible en Internet: http://thesai.org/Downloads/Volume7No4/Paper_26-A_Survey_on_Security_for_Smartphone_Device.pdf

Figura 9.Categorías de ataques a Smartphones



Fuente: SYED FARHAN, Alam Zaidi, et al. Categorías de ataques a Smartphones [imagen]. A Survey on Security for Smartphone Device Security challenges on mobile devices.2017.p.10.[Consultado: 27 de Septiembre de 2018]. Disponible en Internet: http://thesai.org/Downloads/Volume7No4/Paper_26-A_Survey_on_Security_for_Smartphone_Device.pdf

Ataques Antiguos: En esta categoría se ubican ataques del tipo: Malware, gusanos, Spam, virus entre otros. A continuación, se llevará a cabo una breve descripción de algunos de ellos:

Ataques físicos: Syed Farhan [123] expone en su artículo , que estos ataques están relacionados con la posibilidad de extravío o robo del dispositivo. La información almacenada en los dispositivos en estos casos puede ser manipulada, alterada o borrada.

[123] Ibid.,p.66.

Los ataques o riegos que pueden tener los equipos al no contar con los cuidados mínimos de uso también pueden ubicarse en esta clasificación, por ejemplo, daños por caídas.

Ataques a redes inalámbricas: En el mismo artículo Syed Farhan [124] expresa que es posible el acceso de intrusos a comunicaciones o información cuando se hace uso de redes inalámbricas pueden ser de dos tipos: Ataques activos (Spoofing, corrupción, bloqueo y modificación) y ataques pasivos (sniffing y escuchas).

Backdoors: Robert Siciliano[125] expone en su escrito que los backdoors se encuentran asociados con la posibilidad que tiene un ciberdelincuente de tener accesos no autorizados a un sistema al eludir los mecanismos de seguridad implementados en el mismo.

Ataques nuevos: Algunas de los ataques que se ubican en esta categoría son: ataques de transmisión, Cross-Site scripting (XSS), Ataques de arranque en Frio, ataques de control de flujo entre otros. A continuación, se hará una breve descripción de los mismos.

Ataques de trasmisión: Para entender el concepto es necesario hacer hincapié en el estándar utilizado para llevar a cabo transacciones de pago en tiendas móviles la cual es conocido como tecnología de comunicación de campo cercano (NFC-Near Field Communication). La importancia de esta tecnología, expone Darmon[126] radica a que requiere poca distancia entre la terminal de pago y el móvil, y sobretodo porque permite que la información que viaja a través de ella sea encriptada.

[124] Ibid.,p.66.

[125] SICILIANO; Robert. What is a Backdoor Threat?[en línea] McAfee.(12 de Mayo de 2014),párr.2.[Consultado: 24 de Septiembre de 2018*.Disponible en Internet: https://securingtomorrow.mcafee.com/consumer/identity-protection/backdoor-threat/

[126] DARMON,Luc. Protect Mobile In-Store Payments From Relay Attacks [en línea].Apparel Magazine.(12 de Septiembre de 2014).párr 4.[Consultado:22 de Septiembre de 2018].Disponible en Internet: https://apparelmag.com/protect-mobile-store-payments-relay-attacks

Sin embargo, a medida que se fue implementado esta tecnología, afirma Darmon[127] han surgido nuevos vectores de ataque. Este tipo de pagos pueden ser vulnerados por lo que se conoce como un "ataque de retransmisión" (Relay Attack).

> En un ataque de relevo o retransmisión, si alguien puede acceder a su teléfono móvil (o a su tarjeta de crédito con chip sin contacto), pueden usar su propio teléfono para suplantar el sistema de pago de una tienda y pasar datos de pago de su teléfono a otra persona, ubicado en una tienda real, para hacer la compra utilizando los detalles de su pago. Con dos teléfonos que actúan en conjunto para retransmitir la comunicación, el sistema de pago de la tienda y su teléfono creen que se están comunicando de forma segura.[128]

Cross-Site Scripting (XSS): Las secuencias de comandos entre sitios (XSS), son definidas por Kallin y Valbuena[129], como un tipo de ataque de inyección de código que le permite a un delincuente llevar a cabo la ejecución de JavaScript malicioso en el navegador de otro usuario.

Para Kallin y Valbuena[130], el atacante no afecta directamente a su víctima. En vez de ello, explota una vulnerabilidad en un sitio web que la víctima visita, para que el sitio web le envíe el JavaScript malicioso. Desafortunadamente, para el navegador usado por la víctima, el script infectado parece ser una parte legítima del sitio web y, por lo tanto, este se convierte en cómplice del atacante sin ser consciente de ello.

Cold Boot Attacks (Ataques de arranque en Frio): El portal Guías prácticas[131] expone que los ataques de arranque en frío son un tipo de ataques en el que un delincuente con acceso físico a una computador o dispositivo móvil, recupera las claves de cifrado del sistema operativo en ejecución, haciendo uso de un reinicio

---

[127] Ibid.,p.68.

[128] Ibid.,p.68.

[129] KALLIN Jakob y LOBO VALBUENA Irene. Excess XSS A comprehensive tutorial on cross-site scripting [en línea] Excess XSS. [Consultado: 23 de Septiembre de 2018]. Disponible en Internet: https://excess-xss.com/

[130] Ibid.,p.69.

[131] Ataque de arranque en frío (cold boot attack) [en línea]. Guías prácticas [Consultado: 21 de Septiembre de 2018]. Disponible en Internet: http://www.guiaspracticas.com/recuperacion-de-datos/ataque-de-arranque-en-frio-cold-boot-attack

en frío. ”El ataque de arranque en frío se basa en la persistencia de datos en la memoria RAM para recuperar su contenido, que sigue siendo legible después de que la energía se ha quitado, durante un período de entre decenas de segundos a varios minutos dependiendo del dispositivo de RAM físico”[132]

Ataques USSD: Según expone Achiary[133] en su artículo publicado en ESET Latinoamérica, los códigos USSD son utilizados tanto por compañías telefónicas como por empresas fabricantes de dispositivos móviles para desarrollar labores de soporte técnico y asistencia a los usuarios. Según el mismo artículo se afirma que “a través de esta vulnerabilidad, un equipo puede infectarse visitando una página web, ejecutando un código QR, a través de transmisión NFC o mediante un SMS; exponiéndose a la pérdida o robo de información contenida en el teléfono”. [134]

Ataques de control de Flujo: Según expone Davi[135] en su escrito, este tipo de ataques permiten que un delincuente altere el flujo de ejecución previsto de un programa explotando un error en el mismo. Un ejemplo de este inconveniente se presenta cuando un error de desbordamiento de búfer se explota para escribir datos más allá de los límites del búfer. Como la información de control de flujo guía el flujo de ejecución del programa, el delincuente puede llevar a cabo acciones como la instalación de puertas traseras inyectando un malware o accediendo a datos confidenciales. Los ataques de flujo de control se realizan en el tiempo de ejecución de la aplicación. Por tal razón, frecuentemente se hace referencia a ellos como exploits en tiempo de ejecución.

5.1.6.2 Amenazas sistemas Android: Según advierte Kim Komando[136], un programa de radio sobre tecnología de consumo producido en los Estados Unidos, las mayores amenazas de seguridad para los usuarios de Android en la actualidad son las siguientes:

---

[132] Ibid.,p.69.

[133] ACHIARI,Santiago. Ahora USSD Control está incluido en todos los productos de ESET [en línea].ESET Latinoamérica.(25 de Marzo de 2013),párr.3. [Consultado: 24 de Septiembre de 2018]. Disponible en Internet: http://www.somoseset.com/2013/03/25/ussd-control-incluido-productos-eset/

[134] Ibid.,p.70.

[135]DAVI, Lucas Vincenzo. Code-Reuse Attacks and Defenses [en línea].Tesis para obtener el título de Doctorado en filosofía (PHD). Duisburgo, Alemania. Universidad Técnica de Darmstadt. Departamento de Ciencias de la Computación,2015.p.19. [Consultado: 23 de Septiembre de 2018]. Disponible en Internet: http://tuprints.ulb.tu-darmstadt.de/4622/7/Davi-PhD-Code-Reuse-Attacks-and-Defenses.pdf

[136] 3 biggest security threats for Android users today [en línea]. Kim Komando.[Consultado:23 de Septiembre de 2018].Disponible en Internet: https://www.komando.com/tips/382348/3-biggest-security-threats-for-android-users-today

Software malicioso gooligan: Recientemente, expone Kim Komando[137] en su artículo, se descubrió un software malicioso que se presenta emulando auténticas aplicaciones para dispositivos Android. El malware conocido como Gooligan ha infectado casi 13,000 dispositivos Android desde Agosto de 2016. Según el mismo reporte, algunas de estas aplicaciones maliciosas se han identificado como: Perfect Cleaner, StopWatch y Wi-Fi Enhancer.

Continuando con el artículo de Kim Komando[138], las versiones que principalmente son atacadas por este software malicioso son Android 4 y 5, más conocidas como Android Jelly Bean, KitKat y Lollipop. Esto debido a los parches de seguridad diseñados para corregir estas fallas no se encuentran disponibles por ser versiones antiguas. El problema radica es que casi el 75 por ciento de usuarios de Android están haciendo uso de estos sistemas operativos.

Aplicaciones maliciosas: En cuanto a este tipo de amenazas, Kim Komando[139] indica que los estafadores están desarrollando aplicaciones falsas dirigidas a obtener información personal y bancaria de manera fraudulenta. Este tipo de aplicaciones tiene como finalidad obtener un pago por rescate del control de archivos de importancia para el usuario final. Así mismo, pueden hacer que el dispositivo funcione de forma errónea o incluso bloquearlos con el ransomware.

Un ejemplo de este tipo de ataques es Judy. Según publicación de TechAdvisory, "es una aplicación de Android, y aunque suena completamente inofensivo, este software está diseñado para infectar un dispositivo y activar un comando de auto-clic utilizado para campañas publicitarias maliciosas." [140]

[137] Ibid.,p.70.

[138] Ibid.,p.70.

[139] Ibid.,p.70.

[140] Mobile security threats in Android [en línea]. TechAdvisory.[Consultado:23 de Septiembre de 2018].Disponible en Internet: https://www.techadvisory.org/2017/06/mobile-security-threats-in-android/

Para complementar la lista de aplicaciones maliciosas, Valery[141] anunció la aparición del malware HummingBade en países como Colombia y México hacia el año 2016, el cual introdujo avisos publicitarios infectados e instala aplicaciones fraudulentas en el dispositivo del usuario. El malware expone Valery, "crea unrootkit (una puerta trasera que permite acceso total al dispositivo) persistente, por la que pueden colarse avisos que generan ingresos fraudulentos para el creador del virus a través de clics forzados, así como programas maliciosos."[142]

Los investigadores de Check Point[143] encontraron una variante del malware HummingBad oculta en más de 20 aplicaciones en Google Play. Esta nueva variante, llamada 'HummingWhale', incluye nuevas técnicas que le permiten realizar llevar a cabo el fraude publicitario de una mejor manera que su antecesor.

Ransomware: Según expone Avast, en su artículo, "el término Ransomware, (también conocido como como rogueware o scareware) restringe el acceso a un sistema informático y exige que se pague un rescate para que se elimine la restricción. Los ataques más peligrosos los han causado ransomware como WannaCry, Petya, Cerber, Cryptolocker y Locky."[144].

Adicionalmente a las amenazas anteriormente expuestas la empresa Komando, ZoneAlarm[145], compañía que ofrece soluciones de seguridad, propone algunas amenazas adicionales identificadas en la plataforma Android.

QuadRoot: QuadRoot según expone ZoneAlarm[146], es una vulnerabilidad que afecta a los dispositivos creados con los conjuntos de chips móviles de Qualcomm. Los hackers pueden usar las vulnerabilidades detectadas en estos

[141] VALERY, Yolanda. Qué es el virus HummingBad que afecta millones de teléfonos Android [en línea].BBC News.(6 de Julio de 2016),párr. 1 [Consultado: 23 de Septiembre de 2018]. Disponible en Internet: https://www.bbc.com/mundo/noticias-36726332

[142] Ibid.,p.72.

[143] A Whale of a Tale: HummingBad Returns [en línea].Checkpoint Blog. 23 de Enero de 2017.párr. 1.[Consultado:12 de Septiembre de 2018].Disponible en Internet: https://blog.checkpoint.com/2017/01/23/hummingbad-returns/

[144] Ransomware [en línea].Avast .[Consultado:30 de Septiembre de 2018].Disponible en Internet: https://www.avast.com/es-es/c-ransomware

[145] Android Threats [en línea].Zonealarm. [Consultado:12 de Septiembre de 2018]. Disponible en Internet: https://www.zonealarm.com/mobile-security/android/threats/

[146] Ibid.,p.72.

dispositivos para obtener un control total sobre su sistema operativo Android e información personal. Hay cuatro vulnerabilidades QuadRoot:

CVE-2016-2059

CVE-2016-2503

CVE-2016-2504

CVE-2016-5340.

Certifi-Gate : Certifi-Gate es definido por ZoneAlarm[147] como una vulnerabilidad que permite a los piratas informáticos tomar el control total de su dispositivo Android y robar todos sus datos personales. Para llevar a cabo este tipo de ataques se hace uso de herramientas de soporte remoto, que generalmente ya viene instaladas en el dispositivo. Los atacantes se centran en las vulnerabilidades de los métodos de autorización entre las aplicaciones y el sistema operativo. Para hacerle frente a esta vulnerabilidad se recomienda tener precaución al descargar herramientas de soporte remoto móvil, siempre use una fuente conocida.

En artículo publicado en Appknox, una comunidad de hackers éticos dedicado a la seguridad de aplicaciones móviles, Philips[148] expone que las siguientes son las principales amenazas que afectan esta plataforma Android:

Tabla 3. Principales amenazas que afectan a la plataforma Android

Amenazas	Descripción
StageFright	La explotación de esta vulnerabilidad implica un servicio de mensajería multimedia que se envía a los usuarios que contienen un video. Sin siquiera tener que abrir el video, el dispositivo se toma a través del mecanismo libStageFright que ayuda a Android a procesar videos.

[147] Ibid.,p.72.

[148] PHILLIPS Cassie. Five Immediate Threats to Android Security for 2016 and How to Eliminate Them [en línea].Appknox Blog.2016,párr.2.[Consultado:22 de Septiembre de 2018].Disponible en Internet: https://blog.appknox.com/five-immediate-threats-android-security-2016-eliminate/

Tabla 3. (Continuación)

Amenazas	Descripción
DDoS: Ataques Denegación de Servicio	Concretamente los ciberdelincuentes con este tipo de ataques buscan atacar un servidor con tráfico para cerrar un sitio web e impedir que los usuarios accedan a él. Pero debido al gran auge del internet móvil, esta amenaza está evolucionando de forma importante en este campo.
	En los últimos años se ha visto como los dispositivos móviles son secuestrados y convertidos en robots DDoS, permitiendo a los delincuentes informáticos aumentar la frecuencia y la intensidad de estos ataques de forma exponencial. La mejor manera de evitar ser víctima de esto es haciendo uso de aplicaciones que supervisan o controlan el tráfico en su dispositivo.
Pagos móviles	Datos como los números de tarjetas de crédito viajan a través de aplicaciones móviles, por esta razón no sorprende el interés de los atacantes estén enfocándose en estas áreas, ya que una vez superadas los niveles de seguridad, algunas veces ignorados por los usuarios de este tipo de plataformas, estos pueden ser víctimas de fraude, o extorsión.
Vulnerabilidades de la aplicación	La característica de la plataforma Android de código abierto le ha permitido desarrollarse y crecer con la libertad lo que ha llevado a su gran auge en cuanto a desarrollo de aplicaciones llevadas a cabo por usuarios. Desafortunadamente, este aspecto también ha demostrado ser una de las mayores debilidades de Android.
Vulnerabilidades de la aplicación	La falta de un proceso de verificación de aplicaciones disponibles pone a los usuarios de Android en un riesgo significativo. La naturaleza abierta del sistema también abre la posibilidad de amenazas de tipo tales como: inyecciones de código malicioso e incluso de secuestro remoto de dispositivos se puedan presentar en usuarios que hacen uso de la plataforma.

Fuente: PHILLIPS, Cassie. Five Immediate Threats to Android Security for 2016 and How to Eliminate Them [en línea].2016.p.6.[Consultado:23 de Septiembre de 2018]. Disponible en Internet: https://blog.appknox.com/five-immediate-threats-android-security-2016-eliminate/

5.1.6.3 Amenazas sistema IOS: Lacoom Mobile Security149 en su artículo expone las principales amenazas que deben tener en cuenta para los dispositivos IOS.

[149] Threats to iOS Mobile Devices [en línea] Laccon Movile Security.[Consultado: 24 de Septiembre de 2018].(Agosto de 2014),párr.1.Disponible en Internet: https://idency.com/wp-content/uploads/2014/08/Lacoon-White-Paper-iOS-Threats.pdf

Tabla 4.Principales amenazas que afectan a la plataforma IOS

Amenazas	Descripción
Troyanos de IOS de vigilancia remota y acceso móvil (mRAT)- Remote Access Troyans	Según expone Lacoom Security[150], estos ataques se basan en hacer uso de una característica que utilizan los usuarios de esta plataforma conocida como Jailbreak, en el cual el usuario puede modificar o tener acceso a características del equipo y aplicaciones que no se encuentran disponibles a través de la App oficial. Haciendo uso de esta característica, el atacante instala un software de vigilancia y un mRAT que le permite al delincuente acceder de forma remota a todo lo almacenado y que fluye a través del dispositivo.
Certificados de desarrollador o de Empresas falsos	Este tipo de ataques, indica Lacoom Security [151]usan certificados de distribución para cargar, no de la forma convencional, una aplicación (infectada con malware), lo cual la beneficia por no tener que pasar por el proceso de validación de la tienda Apple y poderse descargar directamente a dispositivo. Para entender mejor el concepto, se puede indicar que Apple proporciona dos tipos de certificados: • Certificados de desarrollador: Este tipo de certificados permite a desarrolladores probar sus aplicaciones antes de su publicación en la tienda oficial de aplicaciones. • Certificados Empresariales: Brinda a organizaciones la oportunidad de establecer su propio mercado interno para aplicaciones dedicadas. Cada aplicación en el sistema IOS debe estar firmada por un certificado de confianza antes de ser permitido. El inconveniente surge cuando un atacante obtiene de forma ilegal (robando, o comprando en el mercado negro) un certificado para su malware. El paso siguiente es atraer a usuarios para que descargaren su aplicación y de esta forma poder infectar sus dispositivos, sin tener dejar ningún tipo de sospecha, pues su aplicación cuenta con los “certificados” requeridos.

[150] Ibid.,p.74.

[151] Ibid.,p.74.

Tabla 4. (Continuación)

Amenazas	Descripción
Perfiles maliciosos de IOS	Según plantea La Porta, "los perfiles de iOS son utilizados por operadores de telefonía celular, soluciones de administración de dispositivos móviles e incluso aplicaciones móviles para configurar los ajustes de nivel de sistema de los dispositivos iOS. Estos incluyen configuración de Wi-Fi, VPN, correo electrónico y APN, entre otros."[152] . Los atacantes pueden hacer uso de estos perfiles para eludir el modelo de seguridad de Apple y poner en peligro el dispositivo de una víctima que perfiles infectados.
Wi-Fi Man in The Middle(MiTM)	Los ataques MitM , explica Umawing[153], involucran el uso ilegal de una red para explotar transacciones, conversaciones y transferencias de datos sobre la marcha. Los atacantes pueden hacer uso de estas exploraciones aprovechando las debilidades identificadas o desconocidas de una red o de cualquiera de sus elementos, como el software (navegador, VoIP, etc.).
Vulnerabilidades de WebKit	Estas vulnerabilidades permiten, según expone Mon Kywe[154], que el contenido web creado con fines malintencionados ejecute código arbitrario en dispositivos móviles. Los atacantes explotan las vulnerabilidades de un webkit para ejecutar sus propios scripts. Los delincuentes cibernéticos utilizan este tipo de vulnerabilidades como plataforma para llevar a cabo infecciones remotas a dispositivos móviles. Estos problemas se solucionan, explica Mon Kywe[155], con un mejor manejo de la memoria, validación de entrada, bloqueo y administración de estado.
Vulnerabilidades del sistema de día cero	Una amenaza de día cero es definida por Williams como "una vulnerabilidad que los desarrolladores e investigadores de seguridad han conocido durante menos de un día. En muchos casos, estas amenazas se identifican por primera vez mediante probadores de penetración y sombreros blancos (White Hat), lo que les da tiempo para emitir parches de emergencia.

[152] LA PORTA,Liarna. Malicious profiles – one of the most serious threats to IPhones [en línea].Wandera.(14 de Abril de 2018),párr. 1.[Consultado: 3 de Octubre de 2018].Disponible en Internet: https://www.wandera.com/malicious-profiles-come/

[153] UMAWING, Jovi. When three isn't a crowd: Man-in-the-Middle (MitM) attacks explained [en línea]. MalwareBytes Labs Bog.12 de Julio de 2018,párr. 5. [Consultado: 17 de Octubre de 2018].Disponible en Internet: https://blog.malwarebytes.com/101/2018/07/when-three-isnt-a-crowd-man-in-the-middle-mitm-attacks-explained/

[154] MON KYWE,Su. Mobile Threat Blog [en línea]. Appthority.32 de Mayo de 2018, párr. 1. [Consultado: 12 de Octubre de 2018].Disponible en Internet: https://www.appthority.com/mobile-threat-center/blog/ios-update-11-4-security-details/

[155] Ibid.,p.76.

Tabla 4. (Continuación)

Amenazas	Descripción
Vulnerabilidades del sistema de día cero	Expuesto de otra manera, estos ataques representan explotaciones de vulnerabilidades que se han descubierto pero que no han sido publicados.

Fuente: Threats to iOS Mobile Devices [en línea].2014. p.4. .[Consultado:25 de Septiembre de 2018].Disponible en Internet: https://idency.com/wp-content/uploads/2014/08/Lacoon-White-Paper-iOS-Threats.pdf

Si bien es cierto que probablemente sean aún más seguros que Android, la brecha se está reduciendo rápidamente. Según plantea Price[156], cuestiones como el pirateo de fotos de iCloud , la estafa de secuestro de Find My Phone y un número creciente de amenazas de malware han afectado la confianza en el sistema. Algunas de las amenazas más importantes planteadas en el artículo escrito por Price se describen a continuación:

XcodeGhost: Según expone Panda Security[157], este malware basa su ataque en la inclusión de código malicioso incluido en algunas aplicaciones confiables. En el mismo artículo se indica que XcodeGhost, "permite a los atacantes enviar notificaciones falsas a los usuarios con el fin de conseguir información personal y valiosa." [158].

Masque Attack: Price[159] indica que este tipo de ataques se lleva a cabo emulando y reemplazando aplicaciones legítimas previamente están instaladas en el dispositivo, involucrando los usuarios atraídos por la descarga de una aplicación aparentemente legítima desde el exterior de la App Store.

[156] PRICE, Dan. How to Fix 5 Common iPhone & iPad Security Threats [en línea].MakeUseOf.(26 de Enero de 2016), párr.1.[Consultado: 22 de Septiembre de 2018].Disponible en Internet: https://www.makeuseof.com/tag/fix-5-common-iphone-ipad-security-threats/

[157] XcodeGhost: qué es y cómo evitarlo. Fin de la invulnerabilidad de Apple [en línea].Panda Security.[Consultado:24 de Septiembre de 2018]. Disponible en Internet: https://www.pandasecurity.com/spain/mediacenter/noticias/xcodeghost-malware-apple/

[158] Ibid.,p.77.

[159] PRICE, Op.cit.,p.77.

Una vez el usuario hace clic en el enlace, el malware instalará una versión maliciosa de la aplicación sobre el original utilizando mismo identificador de paquete que la aplicación original, haciendo aún más complejo su proceso de detección.

Wirelurker: Para Pagannini[160] este código malicioso puede afectar dispositivos iOS, iPhone de Apple o iPad, robando los datos de usuarios y transfiriéndolos a servidores centrales. El ataque se inicia infectando el host del usuario (que en este caso puede ser una computadora de escritorio o portátil), el cual descargó el código malicioso de la web, y luego permanece oculto a la espera que un dispositivo Apple se conecte a través de USB.

Pagannini indica que el malware empieza a escanear aplicaciones instaladas en el dispositivo IOS una vez este es conectado, generalmente mediante USB, al equipo infectado. "Si WireLurker identifica que una aplicación de destino está presente, copia la aplicación del dispositivo móvil a la máquina, infecta su binario y luego la instala de nuevo en la unidad móvil"[161].

Defecto SSL: A principios de 2014, afirma Price[162], se descubrió una vulnerabilidad en el código SSL (capa de conexión segura) de Apple. SSL es una de las tecnologías utilizadas para crear conexiones seguras a sitios web. El problema surgió de un error de codificación, que se cree que se introdujo antes del lanzamiento de iOS 6.0. El error se basó en omitir un paso de validación de claves, permitiendo así que datos no encriptados se envíen a través de zonas Wi-Fi públicas.

Lock Screen Bypass- Derivación en bloqueo de pantallas: Esta vulnerabilidad, plantean Storm y Davidson[163] permite a cualquier persona eludir la pantalla de

[160] PAGANINI, Pierluigi. WireLurker, Masque: Every Apple iOS App Could Be Compromised [en línea]. Infosec Institute. (14 de Septiembre de 2018),párr.22.[Consultado:28 de Septiembre de 2018].Disponible en Internet: https://resources.infosecinstitute.com/wirelurker-masque-every-apple-ios-app-compromised/#gref

[161] Ibid.,p.78.

[162] PRICE , Op. cit., p. 77.

[163] STORM Darlene y DAVIDSON Michelle. Easy way to bypass passcode lock screens on iPhones, iPads running iOS 12 [en línea].(18 de Septiembre de 2018).párr.1. [Consultado:10 de Octubre de 2018]. Disponible en Internet: https://www.computerworld.com/article/3041302/security/4-new-ways-to-bypass-passcode-lock-screen-on-iphones-ipads-running-ios-9.html

bloqueo de código que se ejecuta en iPhones y iPads que tienen Touch ID. Con iOS 12 y versiones anteriores del sistema que hacen uso de la identificación dactilar, es posible pasar por alto la pantalla de bloqueo del iPhone y engañar a Siri para que permita el acceso al teléfono de una persona. El procedimiento es bastante sencillo, exponen Storm y Davidson "Presione el botón de inicio con un dedo no asociado con la autenticación de su huella digital, lo que provocará que Siri se despierte. Dile a Siri: Datos celulares. Siri luego abre la configuración de datos móviles donde puede desactivar los datos móviles".[164]

Es importante aclarar, expone Cluley[165] que, al ser una vulnerabilidad asociada a la pantalla de bloqueo del iPhone, es necesario que una persona no autorizada tenga acceso físico al equipo. Por esta razón no es considerada como agujero de seguridad que pueda ser explotado de forma remota.14181

5.1.7 Estado del arte ataques a sistemas móviles en la región y en el país: Antes de abordar el tema acerca de los ataques presentados en plataformas móviles en la región, es conveniente analizar estadísticas relacionadas con ataques cibernéticos que se presentaron el año 2017. Según reporte publicado por la compañía Kaspersky Lab[166], durante la Cumbre Latinoamericana de Analistas de Seguridad que se realizó en Buenos Aires, Argentina en el mes de Septiembre del año 2016, los ataques del tipo ransomware en Latinoamérica se han incrementado en un 30 % entre los años 2014 y 2016, y se pudo pronosticar que dicha tendencia se mantendría durante el año 2017.

Siguiendo con el mismo reporte, y teniendo como base el número de ataques asociados al secuestro de datos, Kaspersky[167] indica que los países que fueron más afectados por este tipo de ataques fueron en su orden Brasil con un 54,91 % de ataques identificados, seguido por México con un 23,40% y Colombia con el 5%.

---

[164] Ibid.,p.78.

[165] CLULEY, Graham. The latest iPhone lock screen bypass, and how to stop it [en línea].Integro (12 de Mayo de 2014).párr.7.[Consultado:26 de Septiembre de 2018].Disponible en Internet: https://www.intego.com/mac-security-blog/iphone-lock-screen-bypass/

[166] Kaspersky Lab: Brasil, México y Colombia lideran incidentes de secuestros digitales en América Latina [en línea] Kaspersky Lab Latinoamérica.(18 de Septiembre de 2017),párr.1.[Consultado:27 de Septiembre de 2018].Disponible en Internet: https://latam.kaspersky.com/about/press-releases/2017_kaspersky-lab-incidents-of-digital-kidnappings-in-latin-america

[167] Ibid.,p.79.

Según expone Santiago Pontiroli, analista de seguridad para Kaspersky Lab para América Latina

> la amenaza con mayor impacto en América Latina entre 2016 y 2017 ha sido, sin duda, el secuestro de datos. El incremento en la cantidad de ataques dirigidos ha sido notorio y no solo en la región, sino también en el resto del mundo, por lo que este ciberdelito se ha convertido en una epidemia global que ha causado pérdidas millonarias y daños irreparables en distintas industrias y que, por ahora, no parece detenerse[168]

Respecto al tema el periódico El Tiempo[169] consultó a Fabio Assolini, analista e investigador de la compañía, quien plantea que tomando como base de análisis la herramienta de correo electrónico el ataque más común es el phishing en el cual se envían mensajes los cuales se encargan de redirigir a paginas falsas que simulan ser originales. Además de esto, se deja claro que "los fraudes financieros, el ransomware y los ataques móviles son las amenazas cibernéticas más comunes que se presentan en América Latina" [170], para la época que se llevó a cabo dicha asamblea.

Según datos presentados por Kaspersky[171] durante la Octava Cumbre de Analistas de Seguridad para América Latina llevada a cabo en la ciudad de Panamá que se realizó el presente año, la región ha experimentado un considerable aumento en el número de amenazas cibernéticas, la mayoría de ellas orientadas al robo de dinero.

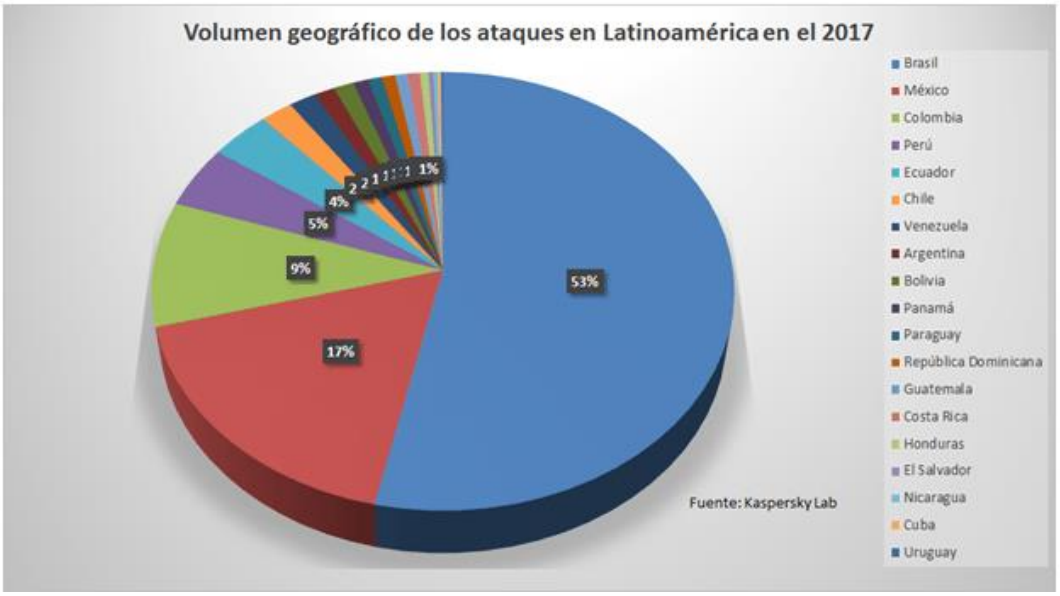
[168] Ibid.,p.79.

[169] Colombia es el tercer país de América Latina con más ciberataques [en línea]. En: El Tiempo.11 de Septiembre de 2017.párr.4.[Consultado:26 de Septiembre de 2018].Disponible en Internet: https://www.eltiempo.com/tecnosfera/paises-latinoamericanos-en-ciberseguridad-129604

[170] Ibid.,p.80.

[171]Kaspersky Lab registra un alza de 60% en ataques cibernéticos en América Latina [en línea].Blog Kaspersky Lab Latinoamérica.14 de Agosto de 2018. párr 1. [Consultado: 27 de Septiembre de 2018]. Disponible en Internet: https://latam.kaspersky.com/blog/kaspersky-lab-registra-un-alza-de-60-en-ataques-ciberneticos-en-america-latina/13266/

Figura 10.Volumen geográfico de ataques en Latinoamérica en el año 2017



Fuente: Volumen geográfico de ataques en Latinoamérica en el año 2017. [Imagen] 33 ataques por segundo: Kaspersky Lab registra un aumento de 59% en ataques de malware en América Latina.2017.p.5.[Consultado: 27 de Septiembre de 2018]. Disponible en Internet: https://latam.kaspersky.com/blog/33-ataques-por-segundo-kaspersky-lab-registra-un-aumento-de-59-en-ataques-de-malware-en-america-latina/11265/

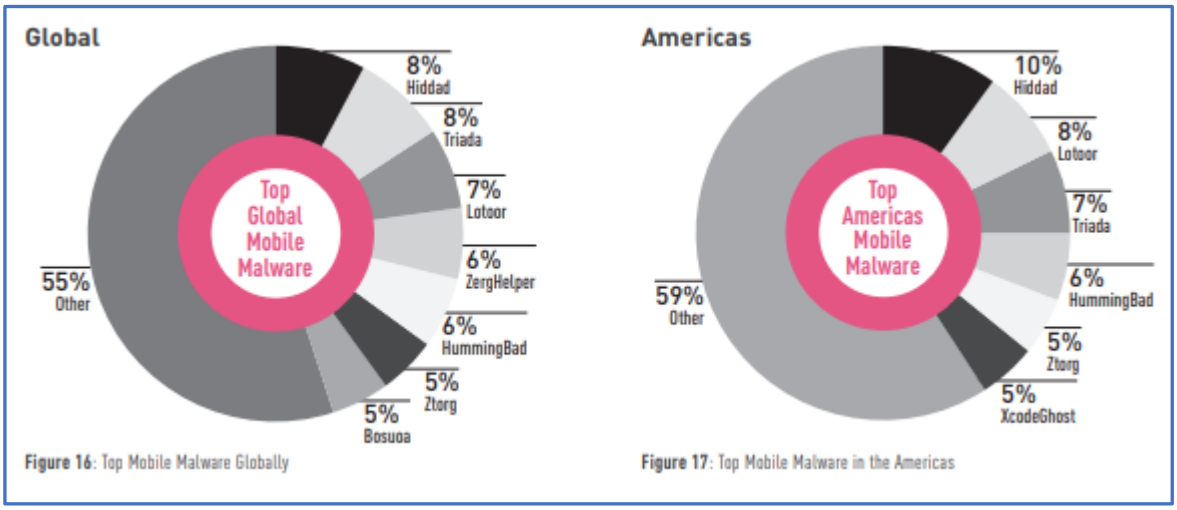
Dmitry Bestuzhev, Director del equipo de Investigación y Análisis para América Latina en Kaspersky Lab, indica que

> hubo un incremento del 60% en ataques cibernéticos en la región, donde Venezuela registra el mayor número de los ataques en proporción a su población con un total de 70.4%, seguido por Bolivia (66.3%) y Brasil (64.4%). Al igual que en 2017, Brasil continúa encabezando a los países latinoamericanos en términos de alojamiento de sitios maliciosos ya que 50% de los hosts ubicados en América Latina que se utilizaron en ataques a usuarios de todo el mundo está ubicado en este país. [172]

[172] Ibid.,p.80.

Uno de los mayores riesgos de seguridad para la región, expone Kaspersky[173] está representado por amenazas móviles. Durante el año 2017, y principios del año 2018 la compañía registró un incremento del 31.3% en los ataques enfocados a este tipo de dispositivos, la mayoría de dichas amenazas fueron desarrolladas para afectar equipos con plataforma Android. En mismo artículo se expresa que se detectó un descenso del 14.9% en los ataques a usuarios MacOS.

Figura 11.Principales malware móvil año 2017 a nivel global y Américas



Fuente: Principales malware móvil año 2017 a nivel global y Américas [imagen].2017 Global Cyber Attack Trends Report Checkpoint Research.2017.p.27.[Consulado:28 de Septiembre de 2018].Disponible en Internet: https://www.checkpoint.com/downloads/product-related/infographic/H2_2017_Global_Cyber_Attack_Trends_Report.pdf?mkt_tok=eyJpIjoiTW1FMlpXUTBaREZqWXpSbCIsInQiOiJTYzFzV1UxWVdTc2pOa24yeHh3aXZodEcwZ2czMnlOQnhHRlJcL3l6ZHI3YjRpUU9mbXpra1BtN3FjUnlNZzRGb3ByVDVWdzdhMythZjRWbThYQnk0dFFEQ1NyXC9JSWVcL1FzejZhcjRodzdlaE8zNExcL3FPeDlGSk5UMDRua2tGbTEifQ%3D%3D

[173] Gustavo. Kaspersky Lab registra un alza de 60% en ataques cibernéticos en América Latina [en línea]. Kaspersky Lab Latinoamérica.(14 de Agosto de 2018),párr.5.[Consultado:28 de Septiembre de 2018].Disponible en Internet: https://latam.kaspersky.com/blog/kaspersky-lab-registra-un-alza-de-60-en-ataques-ciberneticos-en-america-latina/13266/

La ilustración anteriormente expuesta permite identificar a nivel global y regional los malware móvil más importantes en el año 2017. Sin abordar en profundidad en tema, Checkpoint[174] afirma que Hiddad, malware de Android que es utilizado principalmente para mostrar anuncios, tuvo su aparición por primera vez en la primera mitad del año 2017, y desde ese momento se ha mantenido en la cima de la clasificación mundial y en las Américas.

En lo relacionado con vulnerabilidades identificadas en plataforma Android, expone Giusto Bilic,[175] ,que hasta Junio del presente año se habían identificado 322 fallos de seguridad, que corresponde a un 38% del total de vulnerabilidades reportadas para esta plataforma en 2017, año en el cual la cantidad de CVE marcó un pico histórico (842 fallos identificados).

Figura 12.Consolidado vulnerabilidades Sistema Android Latinoamérica

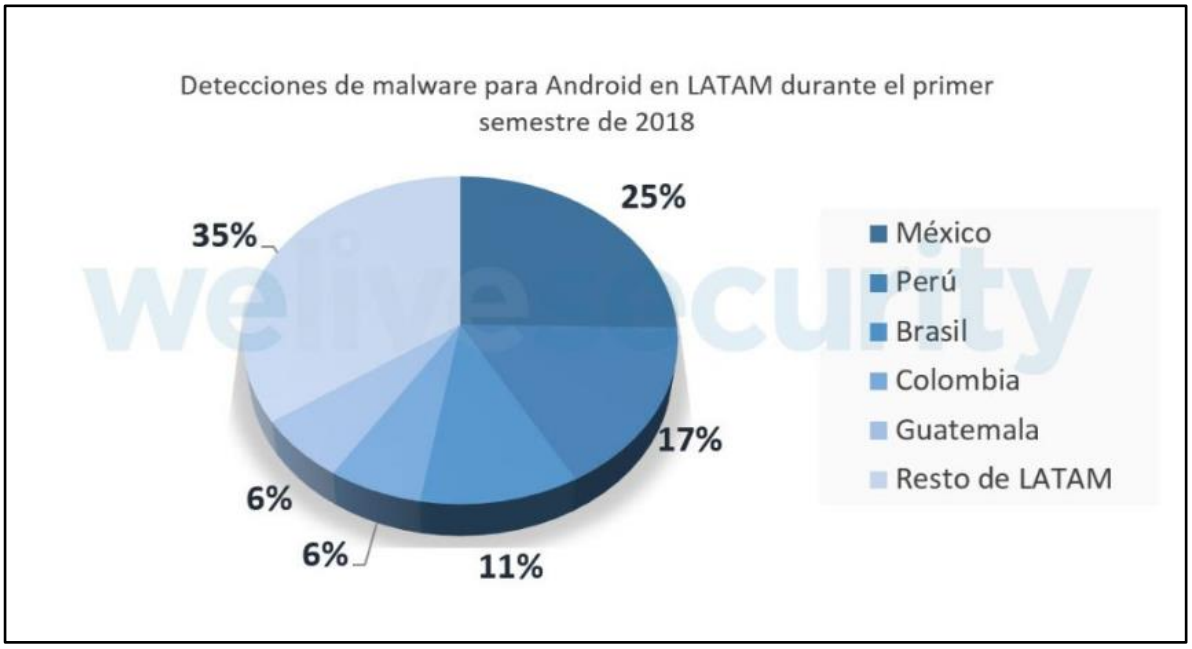
Fuente: GIUSTO BILIĆ, Consolidado vulnerabilidades Sistema Android Latinoamérica [imagen].Balance semestral de la seguridad móvil.2018.p.7.[Consulado:28 de Septiembre de 2018].Disponible en Internet: https://www.welivesecurity.com/la-es/2018/08/06/balance-semestral-seguridad-movil/

[174] Global Cyber Attack Trends Report[en línea].Checkpoint Research.[Consultado:28 de Septiembre de 2018].Disponible en Internet: https://www.checkpoint.com/downloads/product-related/infographic/H2_2017_Global_Cyber_Attack_Trends_Report.pdf?mkt_tok=eyJpIjoiTW1FMlpXUTBaREZqWXpSbCIsInQiOiJTYzFzV1UxWVdTc2pOa24yeHh3aXZodEcwZ2czMnlOQnhHRlJcL3l6ZHI3YjRpUU9mbXpra1BtN3FjUnlNZzRGb3ByVDVWdzdhMythZjRWbThYQnk0dFFEQ1NyXC9JSWVcL1FzejZhcjRodzdlaE8zNExcL3FPeDlGSk5UMDRua2tGbTEifQ%3D%3D
.

[175] GIUSTO BILIĆ, Denise. Balance semestral de la seguridad móvil [en línea].Welivesecurity.(6 de Agosto de 2018),párr.2.[Consultado:29 de Septiembre de 2018].Disponible en Internet: https://www.welivesecurity.com/la-es/2018/08/06/balance-semestral-seguridad-movil/

En su estudio publicado el presente año ESET Giusto Bilić,[176] afirma que las detecciones de malware para Android tomando en cuenta solamente detecciones en países latinoamericanos en el año 2018, los países con mayores detecciones fueron México (25%), Perú (17%) y Brasil (11%).

Figura 13.Malware identificado plataforma Android primer semestre 2018



Fuente: GIUSTO BILIĆ, Consolidado vulnerabilidades Sistema Android Latinoamérica [imagen]. Malware identificado plataforma Android primer semestre. 2018.p.7.[Consulado:28 de Septiembre de 2018].Disponible en Internet: https://www.welivesecurity.com/la-es/2018/08/06/balance-semestral-seguridad-movil/

Para el caso de la plataforma iOS, la misma autora expone que “se identificaron 124 vulnerabilidades en 2018, lo que representa un 32% de la cantidad de fallos encontrados para este sistema operativo en 2017 y menos de la mitad de las encontradas en Android durante el corriente año. El porcentaje de fallas criticas

[176] Ibid,p.83.

encontradas es similar al número detectado en la plataforma Android, con un 12% de vulnerabilidades críticas". [177]

Figura 14.Consolidado vulnerabilidades Sistema IOS Latinoamérica

Fuente: GIUSTO BILIĆ, Consolidado vulnerabilidades Sistema IOS Latinoamérica [imagen]. Malware identificado plataforma Android primer semestre 2018 . 2018.p.7.[Consulado:28 de Septiembre de 2018].Disponible en Internet: https://www.welivesecurity.com/la-es/2018/08/06/balance-semestral-seguridad-movil/

Para culminar el tema de vulnerabilidades identificadas en las principales plataformas en la región,[178] Giusto Bilić expresa que las detecciones de malware para plataforma IOS disminuyeron en un 15% con relación al primer semestre del año 2017, pero aumentaron un 27% con respecto al segundo semestre del mismo año.

[177] Ibid.,p.83.
[178] Ibid.,p.83.

En reporte publicado por Symantec, conocido como Informe Sobre las Amenazas para la Seguridad en Internet en su volumen 23, del año 2018, se reveló que "la cantidad de nuevas variantes de malware para dispositivos móviles creció 54% en 2017, en comparación con 2016."[179]

Abordando el tema empresarial, según datos obtenidos de ESET Security Report Latinoamérica 2017[180], solo el 12% de las empresas latinoamericanas hacen uso de alguna solución de seguridad para los equipos móviles utilizados en su empresa. Este dato contrasta con el crecimiento contante que han tenido los ataques de malware ocurridos en los últimos años.

La compañía de desarrollo de soluciones de seguridad en tecnología ESET, presentó su informe ESET Security Report 2018[181], en el cual se indica que la mayor preocupación para las empresas latinoamericanas es el ransomware. El documento recopiló la opinión de ejecutivos, técnicos y gerentes de más de 2.500 empresas de la región, dando como resultado "que al menos una de cada cinco compañías encuestadas fueron víctimas del secuestro de información" [182].

A continuación, se muestra una figura que resume parte de la información obtenida en el reporte de ESET Latinoamérica 2018.

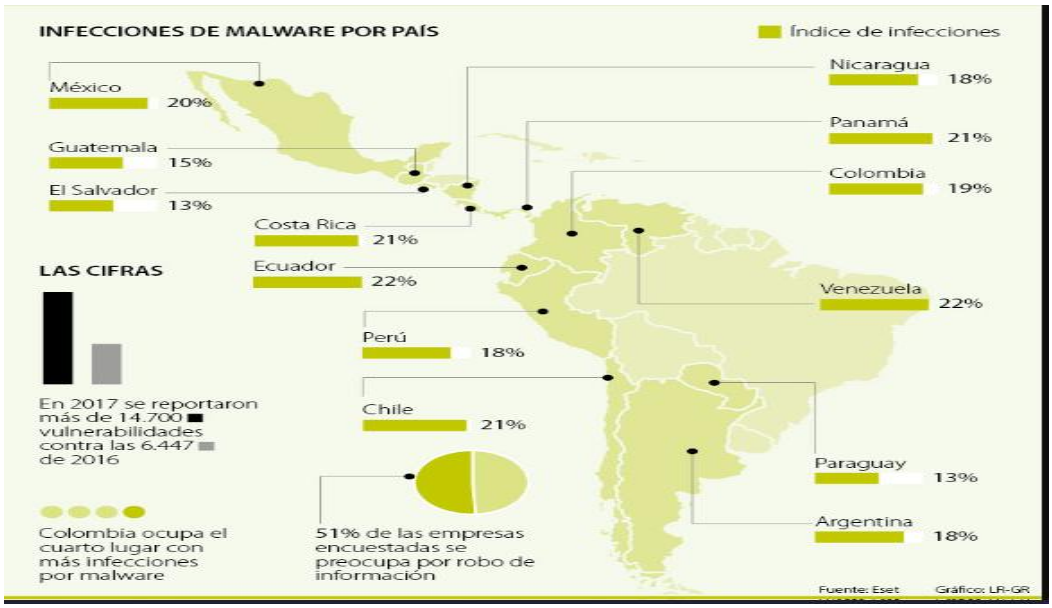
[179] Informe Sobre las Amenazas para la Seguridad en Internet Volumen 23[en línea].Symantec.[Consultado:27 de Septiembre de 2018].Disponible en Internet: http://images.mktgassets.symantec.com/Web/Symantec/%7B3eb3b2d7-76de-484e-951f-e903d31ea889%7D_ISTR23-FINAL_ES.pdf

[180] ESET Security Report Latinoamérica 2017 [en línea].ESET Latinoamérica.[Consultado: 27 de Septiembrre de 2018]. Disponible en Internet: https://www.welivesecurity.com/wp-content/uploads/2017/04/eset-security-report-2017.pdf

[181] ESET Security Report Latinoamérica 2018 [en línea]. [Consultado: 27 de Septiembrre de 2018]. Disponible en Internet: https://www.welivesecurity.com/la-es/2018/06/19/eset-security-report-2018-el-estado-de-la-seguridad-de-la-informacion-en-las-empresas-de-la-region/

[182] Ibid.,p.86.

Figura 15.Ataques cibernéticos a empresas de la región



Fuente: VENEGAS LOAIZA, Ataques Cibernéticos a Empresas de la Región [imagen]. Colombia, entre los países de la región en donde las compañías más sufren malware.2018.p.3. [Consultado: 29 de septiembre de 2018]. Disponible en Internet: https://www.larepublica.co/internet-economy/colombia-esta-entre-los-paises-en-donde-las-companias-mas-sufren-de-malware-2746737

Teniendo en cuenta el caso de nuestro país, y tomando como fuente la información publicada en el artículo del portal web Colombia[183], a continuación, se plantea un resumen de algunas de las principales amenazas y ataques que afectaron a Colombia en el año 2017.

Tabla 5.Resultados estudio de amenazas cibernéticas que afectaron a Colombia en el año 2017

Ataques o Amenazas	Conclusiones
Phishing	En el año 2017 fueron las acciones menos habituales en comparación al 2016 Colombia se posicionó en el sexto lugar a nivel América Latina en cuanto al listado
	de países que han sido víctimas de este tipo de ataques en la región. Los campos de la manufactura y retails fueron los más afectados por este tipo de amenazas
Spam	Continúa siendo una de las principales amenazas online en el país ocupando el puesto 25 en el mundo, afectando principalmente a la industria de Retail (75%), seguida por la de transporte y servicios públicos (58.4%).
Malware	Para el año 2016, el país ocupaba el puesto número 37 y en el 2017 pasó al puesto 65. Los ataques en Colombia son 1 en 425 amenazas.
Criptojacking,	Colombia ha mejorado en la región ya que ocupa el quinto lugar en comparación con Argentina y Chile que ocupan el tercer y cuarto puesto respectivamente

Fuente: Resultados estudio de amenazas cibernéticas que afectaron a Colombia en el año 2017 [imagen]. Colombia es el sexto país en Latinoamérica con mayor número de Ciberataques.2018.p.4. [Consultado: 26 de Septiembre 2018]. Disponible en Internet: https://www.colombia.com/tecnologia/internet/colombia-es-el-sexto-pais-en-latinoamerica-con-mayor-numero-de-ciberataques-188870

Adalid, Compañía especializada en servicios forenses, legales y de seguridad de la información, expone algunas cifras relacionadas con el estado en que se encuentra el cibercrimen en Colombia a principios de año 2017:

[183] Colombia es el sexto país en Latinoamérica con mayor número de Ciberataques [en línea]. Colombia. Bogotá. (2 de Mayo de 2018).párr. 4. [Consultado: 26 de Septiembre 2018]. Disponible en Internet: https://www.colombia.com/tecnologia/internet/colombia-es-el-sexto-pais-en-latinoamerica-con-mayor-numero-de-ciberataques-188870

- Más de $1500 millones anuales pierden las empresas colombianas por fraudes electrónicos.
- Más de 8000 denuncias fueron recibidas por el Departamento de Delitos Informáticos de la Policía Nacional de Colombia en 2016.
- Las amenazas cibernéticas en el país crecen a un ritmo del 60% mientras que el presupuesto que invierten las empresas en seguridad aumentan al 10%.[184]

En el año 2016, los reportes de ataques cibernéticos en el sector empresarial crecieron del 5 al 28% y se estima que cada 7 de usuarios podrían ser víctimas de delitos en la red. [185]

A pesar de estas cifras desalentadoras, la Encuesta Anual de Seguridad de la información, documento publicado por la empresa servicios de aseguramiento EY [186] indicó que en Colombia el 78% de las empresas invirtieron menos de un US$1 millón anual en estrategias o políticas que permitan evitar ser víctimas de ataques informáticos.

Según el mismo reporte[187], para el año 2017, 64% de las organizaciones carecían de programas formales de inteligencia de amenazas. Además de esto, se encontró que el 59% de las empresas del país mantuvieron o redujeron los recursos destinados a estos servicios.

"Las empresas colombianas lo han ido entendiendo y se han hecho avances; sin embargo, la evolución de las técnicas del cibercrimen es acelerada y se deben hacer mayores esfuerzos económicos y técnicos para enfrentarlas y reducir su impacto"[188], indicó la vocera de EY Colombia, María Conchita Jaimes.

---

[184] Por qué su empresa debe invertir en seguridad informática? [en línea].Adalid.[consultado:1 de Octubre de 2018].Disponible en Internet: http://www.adalid.com/por-que-su-empresa-debe-invertir-en-seguridad-informatica/

[185] Ibid.,p.89.

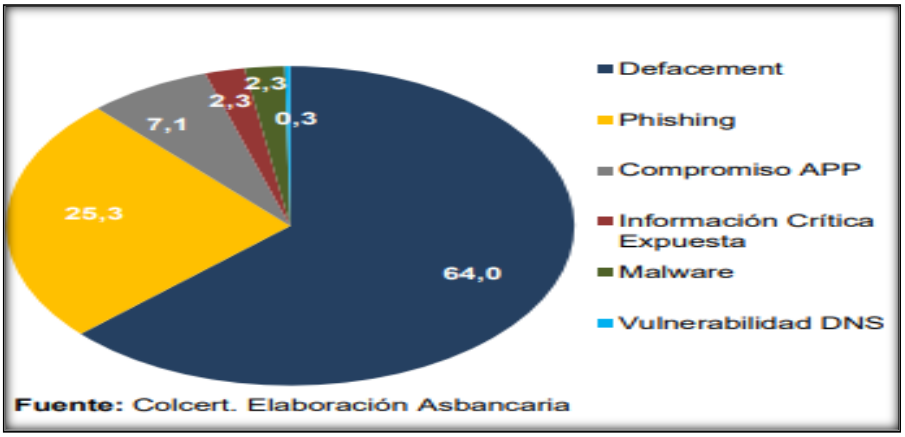
[186] Ibid.,p.89.

[187] Encuesta Anual de Seguridad de la información en: EY Colombia.2016. Citado por:
GUEVARA BENAVIDES, Lina María. Empresas colombianas deben invertir más en ciberseguridad [en línea].La República.p.2.[Consultado:25 de Septiembre de 2018].Disponible en Internet: https://www.larepublica.co/consumo/empresas-colombianas-deben-invertir-mas-en-ciberseguridad-2464836

[188] Las empresas colombianas escatiman en gastos y se rajan en ciberseguridad [en línea] En Revista Dinero. Enero, 2017,p.2.[Consultado 30 de Septiembre de 2018].Disponible en Internet: https://www.dinero.com/empresas/articulo/encuesta-anual-de-seguridad-de-la-informacion-de-la-firma-ey/241201

En informe presentado por el Centro Cibernético Policial[189] se plantea que el cibercrimen en Colombia presentó un aumentó 28,3% en 2017 frente a los resultados de 2016 y 446 empresas reportaron haber sido víctimas de este tipo de ataques. Según el mismo reporte, las amenazas cibernéticas más frecuentes en el país el año pasado fueron: ransomware, ataques a entidades estatales, la suplantación de correo corporativo, el carding (uso ilegitimo de las tarjetas de crédito, con el fin de obtener beneficios propios realizando fraude con ellas) y estafas por Internet.

Figura 16.Tipos de incidentes cibernéticos en Colombia en 2017

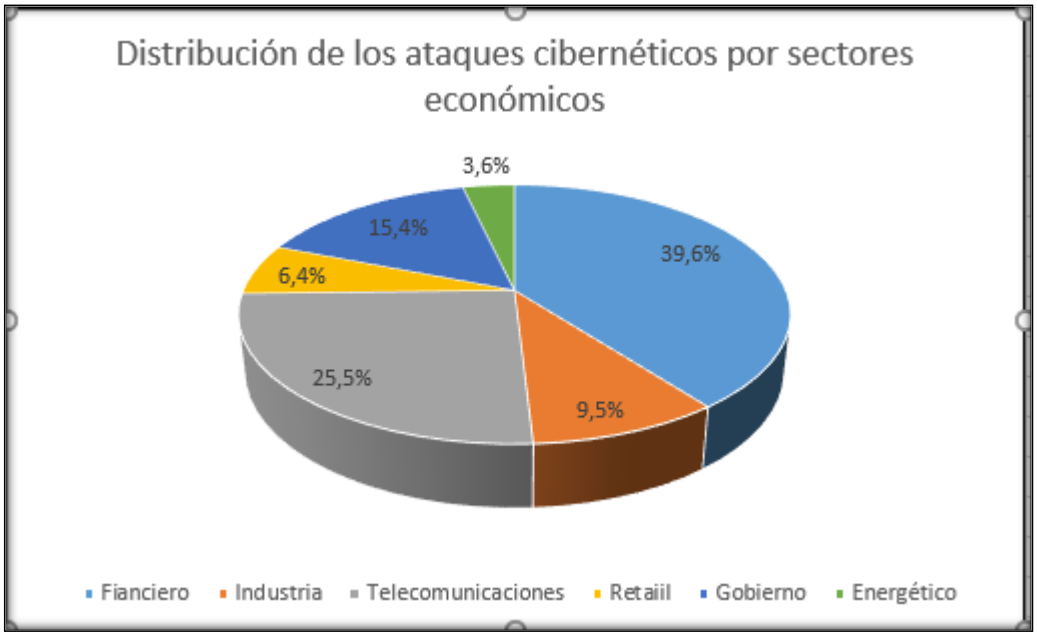


Fuente: Tipos de incidentes cibernéticos en Colombia en 2017 En Colsert-Grupo de Respuesta a Emergencias Cibernéticas de Colombia. Citado por Asobancaria. La gestión de la ciberseguridad: un asunto de supervivencia para las organizaciones [en línea].p.2 .[Consultado:25 de Septiembre de 2018].Disponible en Internet: http://www.asobancaria.com/wp-content/uploads/1133-C-23-04-2018.pdf

[189] Informe balance cibercrimen en Colombia 2017[en línea]. Centro Cibernético Policial. [Consultado:3 de Septiembre de 2018]. Disponible en Internet:https://caivirtual.policia.gov.co/sites/default/files/informe_cibercrimen_2017.pdf

En artículo publicado en el portal Actualícese, se define Defacement como “un término utilizado en informática para hacer referencia a la deformación o cambio producido de manera intencionada en una página web por parte de un atacante.”[190]

Figura 17.Distribución de los ataques cibernéticos en Colombia por sectores económicos



Fuente: MUÑOZ, Víctor Manuel. Distribución de los ataques cibernéticos en Colombia por sectores económicos. [imagen]. Sector financiero y de telecomunicaciones, los que más ataques cibernéticos reciben en Colombia.2018.p.2. [Consultado: 6 de Octubre de 2018]. Disponible en Internet: https://actualicese.com/actualidad/2018/10/04/sector-financiero-y-de-telecomunicaciones-los-que-mas-ataques-ciberneticos-reciben-en-colombia/

Abordando el tema de amenazas móviles en el país, Según publicación de RCN Radio realizada por Jules[191], parte el porcentaje de las amenazas que en todo el mundo se han detectado para equipos con sistema operativo Android están en

[190] Sector financiero y de telecomunicaciones, los que más ataques cibernéticos reciben en Colombia [en línea]. Actualicese. [Consultado: 6 de Octubre de 2017]. Disponible en Internet: https://actualicese.com/actualidad/2018/10/04/sector-financiero-y-de-telecomunicaciones-los-que-mas-ataques-ciberneticos-reciben-en-colombia/

[191] JULES,Javier. Cibercriminales también pueden robar los datos de celulares y tabletas a través de un mensaje [en línea].RCN Radio.(27 de Junio de 2017),párr.1. [Consultado: 1 de Octubre de 2017]. Disponible en Internet: https://www.rcnradio.com/mcontent/5b36d2435f0049e5d1302823/amp

Colombia. Esto para indicar que la información almacenada en dispositivos móviles, por lo menos los que trabajan sobre la plataforma anteriormente descrita, también puede ser robada por ciberdelincuentes.

Camilo Gutiérrez, Jefe del Laboratorio de Investigación de ESET en Latinoamérica, plantea "el Malware o los códigos maliciosos para afectar dispositivos móviles con sistema Android han ido creciendo en los últimos años, Colombia no es la excepción, estamos hablando que un 15 por ciento de códigos maliciosos del Malware lo detectamos en usuarios en Colombia".[192]

5.2. FALLAS DE SEGURIDAD QUE SE PRESENTAN EN SISTEMAS OPERATIVOS MÓVILES ANDROID Y IOS

5.2.1 Recomendaciones de seguridad para reducir amenazas existentes plataforma Android: Según publicación de TrendMicro[193], estudios indican que para el año 2019 el número de teléfonos móviles en el mundo llegarán a cerca de cinco mil millones. Este número parece bastante importante, no solo para a industria, sino para los criminales que están al acecho de estos equipos y sus métodos de ataques se adaptan y mejoran buscando obtener ganancias de este número importante de víctimas potenciales.

En el mismo escrito, TrendMicro [194]expone que los delincuentes siguen con su labor basada en identificar vulnerabilidades en seguridad en aplicaciones, sistemas operativos y software liberados para plataformas móviles tratando de sacar el mayor provecho de estas, antes de que los parches que solucionan dichas fallas sean liberados por fabricantes. La misma publicación plantea solo un ejemplo de amenazas para cada una de las plataformas que controlan el mercado de los dispositivos móviles en la actualidad: "ZNU (detectado por Trend Micro como AndroidOS_ZNIU), que tiene más de 300,000 detecciones en la plataforma de Android, puede plantar una puerta trasera y realizar robo de información. Por otra parte, iXintpwn / YJSNPI(detectado como TROJ_YJSNPI.A), demuestra que

[192] Ibid.,p.91.

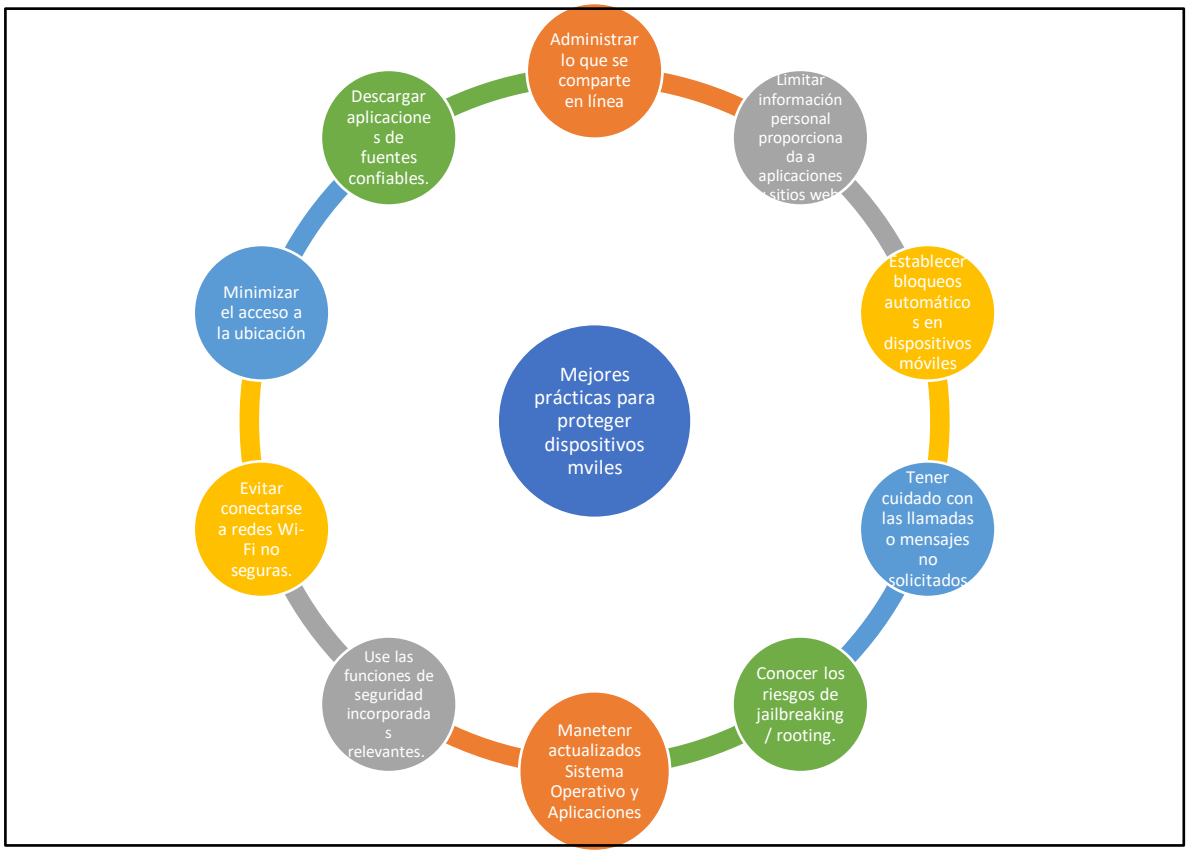
[193] Best Practices: Securing Your Mobile Device [en línea].Trend Micro. [Consultado: 24 de Septiembre de 2018]. Disponible en Internet: https://www.trendmicro.com/vinfo/us/security/news/mobile-safety/best-practices-securing-your-mobile-device

[194] Ibid.,p.92.

iOS no es del todo indestructible con su capacidad para bloquear dispositivos iOS".[195]

En la siguiente ilustración se muestran algunos puntos a tener en cuenta para proteger dispositivos móviles. Algunos de ellos son: evitar en lo posible conectarse a redes WIFI inseguras, deshabilitar la opción de geolocalización, y descargar aplicaciones de fuentes confiables entre otras prácticas recomendadas.

Figura 18.Recomendaciones para proteger dispositivos móviles



Fuente: SYED FARHAN, Alam Zaidi, et al. Recomendaciones para proteger dispositivos móviles. [imagen] Best Practices: Securing Your Mobile Device.2017.p.2.[Consultado: 27 de Septiembre de 2018]. Disponible en Internet: https://www.trendmicro.com/vinfo/us/security/news/mobile-safety/best-practices-securing-your-mobile-device

[195] Ibid.,p.92.

El trabajo monográfico ha mostrado a lo largo de su contenido que Android es la plataforma más flexible en el campo del mercado de los móviles. Su ventaja con respecto a la cantidad de usuarios que hacen uso de este tipo de dispositivos han convertido esta plataforma en un punto de convergencia de ataques cibercriminales.

Por tal razón es primordial que se tengan en cuenta algunas prácticas y medidas preventivas dirigidas a identificar y detener ataques orientados a afectar la seguridad implementada este tipo de móviles.

A continuación, se exponen algunas de las mejores prácticas recomendadas para proteger un equipo Android, así como los datos almacenados en el mismo. Algunos de ellos considerados sencillos, pero al fin y al cabo son más efectivos que llevar a procesos de seguridad complejos.

En primera instancia, Vaughan-Nichols[196] recomienda en su artículo publicado en ZDnet adquirir teléfonos inteligentes de proveedores o marcas que lanzan parches de Android rápidamente, así como tener en cuenta el respaldo que presten dichos proveedores a sus dispositivos. Para tener una lista de proveedores importantes expone Carlon, “primero debe considerar a LG, Motorola, HTC y Sony, todas las cuales lograron obtener sus primeras actualizaciones en menos de 100 días.”[197]

Otra de las recomendaciones que se plantean para buscar protección de dispositivos Android es hacer uso de redes virtuales. Este concepto aplica sobre todo cuando se requiere hacer conexiones a redes WIFI gratuitos. A pesar de que los puntos Wi-Fi públicos son considerados prácticos, estas redes generalmente son inseguras y están expuestas a ataques por parte hackers e intrusos ya que llevan cabo conexiones no cifradas.

---

[196] VAUGHAN-NICHOLS, Steven J [en línea].ZDNet.(1 de Marzo de 2018), párr. 3. [Consultado: 25 de Septiembre de 2018]. Disponible en Internet: https://www.zdnet.com/article/the-ten-best-ways-to-secure-your-android-phone/

[197]CARLON, Kris. Which Android manufacturer updates its phones the fastest?[en línea] Android Authority.(14 de Enero de 2017),párr.12.[Consultado:24 de Septiembre de 2018].Disponible en Internet: https://www.androidauthority.com/android-oem-update-speed-743073/

Lo recomendable en estos casos es usar VPN´s (Redes Públicas Virtuales), lo cual permite encriptar la conexión a Internet para protegerla y proteger la privacidad de la persona que accede la red.

Para Triggs[198] , otra de las consideraciones importante a la hora de proteger los dispositivos Android es instalar las actualizaciones del sistema operativo. Además, expone Triggs, que "desde que Google comenzó a proporcionar actualizaciones de seguridad mensuales para Android, la protección contra exploits maliciosos ha mejorado mucho y tiene sentido mantenerse al día con estos parches lo antes posible para reforzar la seguridad de Android."[199]

En el mismo escrito, Triggs[200] afirma que varias aplicaciones de Android hacen uso de autenticación de dos pasos: inicialmente requieren de la creación de una contraseña y demás de ello vincula la cuenta del usuario al número telefónico, o al correo electrónico del mismo. En el caso de que alguna persona trate de acceder a la cuenta desde el dispositivo o en su defecto solicite cambiar la contraseña, tendrá que llevar a cabo la segunda parte de la autenticación, lo que hace su acceso mucho más complejo. Estos tipos de autenticaciones son muy comunes en aplicaciones de la Banca.

Otra recomendación a tener en cuenta a la hora de proteger la información del móvil Android es la configuración de la pantalla de bloqueo del dispositivo. Este paso debe ser definido como uno de los primeros aspectos de seguridad a tener en cuenta después de haber configurado el equipo. Este puede ser del tipo PIN, patrón o contraseña de pantalla. Antes de apartarse de este tema es importante, si se hace uso de patrones de bloqueo, se recomienda limpiar la pantalla después de ingresarlo, ya que se pueden dejar marcas que pueden revelar dicho patrón.

Una de las prácticas más recomendadas, aunque parece obvia, es siempre descargar software o aplicaciones desde sitios confiables. Para el caso de Android, El App Store es el lugar indicado. Las tiendas de terceros y servicios de

---

[198] TRIGGS,Robert.Best Android security practices [en línea]. Android Authority.(30 de Junio de 2016),párr.2.[Consultado:26 de Septiembre de 2018].Disponible en Internet: https://www.androidauthority.com/best-android-security-practices-700393/

[199] Ibid.,p.95.

[200] Ibid.,p.95.

descarga no prestan atención a la hora de verificar la existencia de software malicioso en sus aplicaciones.

La configuración de cifrado de almacenamiento del teléfono, según plantea Wallen[201], es importante cuando los datos almacenados en el dispositivo sean considerados de alta confidencialidad. Se puede encriptar la información almacenada en el teléfono de manera que requiera una contraseña de cifrado para usarlo. Esto es una puerta de seguridad más fuerte que la contraseña estándar de pantalla de bloqueo, ya que los datos, al estar encriptados no son legibles al usuario, a menos que ingrese la contraseña definida para su descifrado.

Adicionalmente a las buenas prácticas de seguridad planteadas en la presente monografía, es recomendable instalar una aplicación anti-malware. Según Wallen[202], debido al incremento en los últimos años del número en este tipo de ataques es recomendable instalar y usar regularmente un software que se encargue, por ejemplo, de escanear aplicaciones después de ser instaladas, en búsqueda de software malicioso dentro de las mismas.

Otro de los consejos considerados sencillos y fáciles de llevar a cabo es que si no se está haciendo uso de Wi-Fi o Bluetooth o de la ubicación geográfica del dispositivo es recomendable mantenerlos desactivados. Además de ahorrar algo de vida útil de la batería este tipo de conexiones pueden usarse para atacar el equipo. Adicionalmente, es importante anotar que, para reducir las posibilidades de ataques a los dispositivos, una manera efectiva es solo mantener en el móvil las aplicaciones que realmente se utilizan.

Dentro de los riegos a los cuales se encuentran expuestos los dispositivos móviles, independiente de su plataforma, es el robo o extravío de equipos. Cuando se presentan estas situaciones, expresa Triggs[203], una de las opciones disponibles para mantener la seguridad de los datos almacenados en el dispositivo es borrar

[201] WALLEN,Jack. 10 things you can do to make Android more secure [en línea]. TechRepublic (17 de Junio de 2014),parr. 5.[Consultado:25 de Septiembre de 2018]. Disponible en Internet: https://www.techrepublic.com/blog/10-things/10-things-you-can-do-to-make-android-more-secure/

[202] Ibid.,p.96.

[203] TRIGGS, Op. cit., p. 95.

sus datos de forma remota. Afortunadamente, Google ofrece ese tipo de servicio de forma gratuita a todos sus clientes de Android.

Por último, pero no menos importantes, algunas recomendaciones adicionales que pueden ayudar a mantener la seguridad en los equipos Android son: llevar a cabo copias de seguridad de datos en línea, leer la lista de permisos para aplicaciones antes de llevar a cabo sus instalaciones, y elegir contraseñas con niveles de seguridad intermedios o avanzados.

5.2.2 Recomendaciones de seguridad para reducir amenazas existentes plataforma IOS: Muchos de los consejos o buenas prácticas para mitigar amenazas de ataques por parte de delincuentes a dispositivos móviles tratados para dispositivos Android se aplican a la plataforma IOS.

TendMicro[204] recomienda además de utilizar las funciones de seguridad integradas en iOS, y en aras de mejorar el nivel de seguridad de los dispositivos, hacer uso de aplicaciones antirrobo, como Buscar mi iPhone. TendMicro expone en su publicación que “esta aplicación puede ayudarlo a ubicar su teléfono, rastrear dónde está o dónde ha estado, y borrar datos de forma remota en caso de que no pueda recuperar el dispositivo”. [205]

Otra consideración importante planteada por Costello[206] indica que, si el dispositivo Apple tiene el escáner de huellas dactilares Touch ID de Apple debe hacer uso de esta característica. El hecho de escanear una huella digital o el rostro de un usuario para desbloquear un dispositivo maneja un nivel de seguridad mucho mayor que la definición de un código de acceso de cuatro dígitos el cual se puede olvidar o adivinar, en caso de tener un computador con tiempo suficiente.

[204] TREND MICRO. 7 Ways to Improve Security on Your iOS Device . [en línea].Trend Micro. [Consultado: 26 de Septiembre de 2018]. Disponible en Internet: https://www.trendmicro.com/vinfo/us/security/news/mobile-safety/7-ways-to-improve-security-on-ios-device

[205] Ibid.,p.97.

[206] COSTELLO,Sam. Do These 7 Things to Make Your iPhone More Secure [en línea].Lifewire.(28 de Agosto de 2018),párr.9.[Consultado: 26 de Septiembre de 2018].Disponible en Internet: https://www.lifewire.com/tips-to-improve-iphone-security-2000265

Además de realizar copias de seguridad, expone Costello[207] cuando estas se llevan a cabo en un dispositivo diferente al movil.es conveniente encriptarlas. Esto con el objetivo de que una persona, diferente al propietario de esta información pueda tener acceso a ella. Esto se hace en iTunes cuando se requiera sincronizar su iPhone o iPod Touch.

Una sugerencia considerada por algunos como arriesgada es la planteada por Painter[208], en la cual plantea la posibilidad, de que después de varios intentos para acceder a un IPhone el equipo borrará automáticamente todo su contenido, lo que hará el dispositivo inservible. En el caso de activar esta opción, explica Painter[209], se recomienda activar también la copia de seguridad automática de iCloud, de tal manera de que si se borran los datos del equipo (debido a un accidente o alguien que intente hackearlo) todo se mantendrá almacenado en la nube.

Adicionalmente, Painter[210] expone algunos inconvenientes presentados con Siri. Siri, el asistente personal disponible en dispositivos Apple, además de facilitar la vida de usuarios de la plataforma, pone a disposición de atacantes información privada almacenada en el IPhone. A pesar de que la herramienta solicita algún tipo de verificación antes de permitir acceso a contactos, fotos y alguna otra información personal, se han presentado casos en donde las personas han encontrado la forma de acceder a este tipo de información eludiendo las barreras de seguridad definidas por el sistema. La recomendación es desactivar esta característica disponible en este tipo de dispositivos.

Ritchie [211] expresa en su escrito que, si a un usuario le preocupa la privacidad y seguridad de su dispositivo Apple, debe encargase de desactivar el centro de notificaciones, y el centro de control desde la pantalla de bloqueo, así como las vistas previas para sus mensajes. Esto con el objeto de eliminar la posibilidad de que un intruso pueda deshabilitar su dispositivo o leer los mensajes del usuario.

---

[207] Ibid.,p.97.

[208] PAINTER,Lewis. iPhone security tips: How to protect your iPhone from hackers [en línea]. Macworld.(2 de Mayo de 2018),párr.20.[Consultado:26 de Septiembre de 2018].Disponible en Internet: https://www.macworld.co.uk/how-to/iphone/iphone-security-tips-3638233/

[209] Ibid.,p.98.

[210] Ibid.,p.98.

[211] RITCHIE,Rene. Six ways to increase your iPhone and iPad security in 2017 [en línea]. Imore. (4 de Enero de 2017),párr. 7.[Consuiltado:26 de Septiembre de 2018].Disponible en Internet: https://www.imore.com/6-ways-increase-iphone-ipad-security-privacy

Para evitar el uso de contraseñas consideradas débiles, y la creación de una buena cantidad de ellas por cada aplicación utilizada, surgieron los administradores de contraseñas. Acerca del uso de administradores de contraseñas, Ritchie expone que estos "almacenan todas sus contraseñas sólidas y únicas y le otorgan acceso con una sola contraseña maestra o su huella digital a través de Touch ID. Gracias a las extensiones de acción, incluso puede usarlas para rellenar contraseñas directamente en Safari y otras aplicaciones."[212]

Una recomendación adicional, brindada por Price[213] es desactivar la opción de autocompletar (Auto-Fill), el cual está asociada con la posibilidad que se tiene en dispositivos móviles de completar información personal del tipo apellidos, nombres, números de identificación, tarjetas de crédito entre otras. Esta característica fue inicialmente implementada pensado como un ahorro de tiempo en digitación, pero esta vez se analiza como un problema de seguridad ya que si esta información cae en manos no autorizadas se corre el riesgo de robo de identidad y otros delitos asociados a este. Nuevamente lo mejor, desde el punto seguridad, es deshabilitar esta característica en los dispositivos.

5.2.3 Aplicaciones de seguridad para dispositivos Android: En un principio, plantea Goldman[214], a la hora de ofrecer soluciones de seguridad en dispositivos móviles era necesario implementar una aplicación antivirus junto con una aplicación antirrobo por separado y en algunos casos bloqueadores de aplicaciones individuales.

La mayoría de las soluciones actuales de seguridad para Android ofrecen todas están funcionabilidades en una sola aplicación. Esta lista incluye en su mayoría soluciones de seguridad de base amplia de Android, junto con una aplicación antirrobo y administración de contraseñas de tres niveles entre otras.

[212] Ibid.,p.98.

[213] PRICE, Dan. 7 iOS Settings to Change If You Want Better Privacy in Safari [en línea].MakeUseOf.(27 de Junio de 2018), párr.5.[Consultado: 26 de Septiembre de 2018].Disponible en Internet: https://www.makeuseof.com/tag/change-ios-settings-privacy-safari/

[214] GOLDMAN,Jeff. Top 20 Android Security Apps [en línea]. eSecurityPlanet.(27 de Octubre de 2015).párr 1.[Consultado:1de Octubre de 2018]. Disponible en Internet: https://www.esecurityplanet.com/mobile-security/top-20-android-security-apps.html

A continuación, se muestra figura con una lista de aplicaciones separadas por categorías, desarrolladas en el campo de la seguridad de dispositivos Android. Es importante tener en cuenta descargar estas aplicaciones de una fuente confiable como Google Play Store.

Tabla 6.Listado de aplicaciones de seguridad - plataforma Android

Categorías	Aplicaciones	Descripción
Mensajería y correo Electrónico	Signal Private Messenger	Es una aplicación gratuita que utiliza encriptación de extremo a extremo para mantener los mensajes y chats de voz privados. También puede realizar llamadas de voz cifradas y no cifradas desde la aplicación.
	Wickr Me	Wickr Me también ofrece mensajes de texto, video e imágenes, así como también chat de voz cifrados de extremo a extremo.
	ProtonMal	Servicio de correo electrónico con sede en Suiza, requiere dos contraseñas, una para iniciar sesión en la cuenta y la otra para cifrar y descifrar los mensajes.
Navegadores y VPN	Navegador de privacidad de Ghostery	Ghostery ayuda a minimizar el acceso a sus datos por parte de los rastreadores de anuncios y otras herramientas. También le permite borrar rápidamente sus cookies y su caché, y puede elegir entre ocho motores de búsqueda diferentes.
	Avira Phantom VPN	Una red privada virtual, como Avira Phantom VPN o NordVPN, encripta su conexión y su ubicación para mantenerse fuera de control. Es clave al requerir el uso de redes WiFi para proteger la información almacenada en el dispositivo.
	Adblock Browser para Android de Eyeo GmbH	Se puede hacer uso Adblock Browser, cuando se requeire bloquear anuncios que no desee ver en un momento determinado, además de brindar la opción de escoger las aplicaciones que le gustaría apoyar.

Tabla 6. (Continuación)

Categorías	Aplicaciones	Descripción
Llamadas telefónicas	Silent Phone	En el caso de que un usuario requiera encriptar las llamadas realizadas en su equipo móvil, Silent Phone no solo encripta sus llamadas telefónicas, sino que también ofrece intercambio seguro de archivos y tiene una función de autodestrucción para mensajes de texto.
Archivos y aplicaciones	SpiderOakONE	El almacenamiento en la nube es una gran opción a la hora de mirar movilidad y disponibilidad de los archivos permanentemente. Al ser un servicio en línea, se debe lidiar a su susceptibilidad a accesos no permitidos. SpiderOakONE se promociona a sí mismo como una aplicación 100% sin conocimiento, lo que significa que solo puede leer sus datos.
	AppLock	AppLock permite mantener a los posibles espías del móvil lejanos del equipo bloqueando aplicaciones con una contraseña, PIN, patrón o huella digital. Este tipo de bloqueos proporciona una capa de seguridad adicional si su teléfono se pierde o es robado o alguien lo desbloquea

Fuente: MCLAUGHLIN, Molly. Listado de aplicaciones de seguridad - plataforma Android [imagen]. The Best Privacy and Security Apps for Android.2018.p.6. [Consultado: 1 de Octubre de 2018]. Disponible en Internet: https://www.lifewire.com/privacy-and-security-apps-for-android-4116583

Además de la anterior clasificación, Hill[215] propone una lista de las mejores aplicaciones de seguridad en Android, la mayoría de las cuales ofrecen aparate de una protección antivirus, una serie de otras herramientas que van desde el filtrado de contactos hasta el bloqueo o borrado remoto. La selección realizada por el autor se enuncia a continuación:

[215] Hill, Simon. The best security apps and antivirus protection for Android [en línea]. Digital Trends.(26 de Abril de 2018).párr.3.[Consultado:2 de Octubre de 2018].Disponible en Internet: https://www.digitaltrends.com/mobile/best-antivirus-protection-for-android/

Mejor antivirus en general: Trend Micro Mobile Security y Antivirus: Hill[216] indica que esta herramienta proporciona detección de malware del 99,9 por ciento en los últimos dos años de existencia. Dentro de las opciones ofrecidas por la aplicación se encuentran: protección contra sitios de phishing, un escáner de privacidad para Facebook y algunas herramientas ofrecidas para ahorrar batería y memoria.

Mejor protección contra malware: Avast Mobile Security. Además de ofrecer protección antivirus, Hill[217] indica que Avast Mobile Security analiza las aplicaciones instaladas en el móvil para proporcionar detalles acerca de lo que está haciendo y ofrece un escudo web que analiza las URL visitadas en busca de malware. ”Hay varias herramientas adicionales en el paquete que incluyen un bloqueador de llamadas para listas negras de problemas, un bloqueo de aplicaciones para proteger aplicaciones privadas con PIN y opciones de escaneo de Wi-Fi para mejorar la seguridad y la velocidad”[218], expone Hill.

Mejor conjunto de características: AVG. Una de las opciones software antivirus gratuito más importantes. AVG incluye “Antivirus, AntiMalware (Protección residente AVG), AVG Anti-Rootkit, Analizador de correos electrónicos AVG, Tecnología de Nube Protectora de AVG, Red de Protección de la Comunidad de AVG, AVG LinkScanner® Surf-Shield, Protección de Redes Sociales de AVG.”[219]

La mejor experiencia sin publicidad: Sophos Mobile Security. Según Shophos[220], esta aplicación protege los dispositivos Android sin afectar su rendimiento ni la duración de la batería. Alguna de sus características son expuestas en la página Web de Sophos: “identifica las aplicaciones maliciosas o no deseadas que podrían causar, por ejemplo, robos de datos, pérdida de datos y costes excesivos del uso de la red. Si el dispositivo se pierde o es objeto de un robo, el bloqueo o el borrado remotos protegen la información personal contra curiosos”[221].

---

[216] Ibid.,p.101.

[217] Ibid.,p.101.

[218] Ibid.p,.101.

[219] AVG AntiVirus 2018 [en línea].AVG Latinoamérica.[Consultado:2 de Octubre de 2018].Disponible en Internet: https://www.avg-la.com/avg-antivirus/

[220] Sophos Mobile Security para Android. [en línea].Sophos. [Consultado:2 de Octubre de 2018].Disponible en Internet: https://www.sophos.com/es-es/products/free-tools/sophos-mobile-security-free-edition.aspx

[221]Ibid.,p.102.

Mejor interfaz de usuario: Avira Antivirus Security 2018.Softonic[222], indica que la edición oficial 2018 del antivirus más importante de Avira se destaca no solo por las opciones de seguridad que ofrece, sino por su sencillo e intuitivo manejo. Esto es posible, expone Softonic en su artículo principalmente, "gracias al diseño de una interfaz amigable. fundamentalmente, gracias al diseño de una interfaz amigable y pensada para todos los públicos".[223]

El laboratorio de AV-TEST ha presentado un cuadro comparativo en el cual se analizan herramientas de seguridad teniendo en cuenta la protección, la usabilidad y las funciones adicionales que ofrecen 21 aplicaciones de seguridad y el mecanismo integrado en Android, Google Play Protect.

El laboratorio presentó dicho informe en Mayo de 2018, utilizando como plataforma base Android 6.0.1, obteniendo los siguientes resultados.

> En las categorías de protección y usabilidad, 12 aplicaciones consiguieron el máximo resultado de 13 puntos: Alibaba, Avast, AVG, Avira, Bitdefender, G Data, Kaspersky Lab, McAfee, PSafe, Symantec, Tencent y Trend Micro. Otras 3 aplicaciones obtuvieron la también muy buena puntuación de 12,5: BullGuard, F-Secure y Quick Heal. El resto de aplicaciones sumaron entre 12 y 9 puntos. El último de la lista fue Google Play Protect con solo 6 puntos."[224]

[222] Avira Free Antivirus. [en línea].Softonic. [Consultado:3 de Octubre de 2018].Disponible en Internet: https://avira-free-antivirus.softonic.com/

[223] Ibid.,p.103.

[224] Por si Google fracasa: examinamos 21 aplicaciones de seguridad para Android.[en línea].AV-Test. [Consultado:3 de Octubre de 2018].Disponible en Internet: https://www.av-test.org/es/noticias/por-si-google-fracasa-examinamos-21-aplicaciones-de-seguridad-para-android/.

Figura 19.Comparativo Aplicaciones de Seguridad Plataforma Android

21 apps para Android puestas a prueba
Google por sí solo no basta

AV-TEST

Proveedor	Producto	Certificado AV-TEST	Protección (max. 6 ptos)	Usabilidad (max. 6 ptos)	Funciones / Extras (max. 1 pto)	Puntuación total (max. 13 ptos)
Alibaba	Mobile Security - free		6,0	6,0	1,0	13,0
Avast	Mobile Security - free		6,0	6,0	1,0	13,0
AVG	AntiVirus FREE		6,0	6,0	1,0	13,0
Avira	Antivirus Security		6,0	6,0	1,0	13,0
Bitdefender	Mobile Security		6,0	6,0	1,0	13,0
G Data	Internet Security		6,0	6,0	1,0	13,0
Kaspersky Lab	Internet Security for Android		6,0	6,0	1,0	13,0
McAfee	Mobile Security		6,0	6,0	1,0	13,0
PSafe	dfndr security - free		6,0	6,0	1,0	13,0
Symantec	Norton Mobile Security		6,0	6,0	1,0	13,0
Tencent	WeSecure - free		6,0	6,0	1,0	13,0
Trend Micro	Mobile Security		6,0	6,0	1,0	13,0
BullGuard	Mobile Security		5,5	6,0	1,0	12,5
F-Secure	SAFE		6,0	5,5	1,0	12,5
Quick Heal	Mobile Security		5,5	6,0	1,0	12,5
AhnLab	V3 Mobile Security		6,0	5,0	1,0	12,0
Ikarus	mobile.security		5,0	5,5	1,0	11,5
Antiy	AVL - free		6,0	3,0	1,0	10,0
Cheetah Mobile	Security Master - free		6,0	3,0	1,0	10,0
Sophos	Mobile Security - free		6,0	3,0	1,0	10,0
NSHC	Droid X 3		2,0	6,0	1,0	9,0
Google	Play Protect	-	0,0	6,0	0,0	6,0

AV-TEST, mayo de 2018

www.av-test.org

Fuente: Comparativo Aplicaciones de Seguridad Plataforma Android [imagen]. Por si Google fracasa: examinamos 21 aplicaciones de seguridad para Android.2018.p.7. [Consultado: 2 de Octubre de 2018]. Disponible en Internet: https://www.av-test.org/es/noticias/por-si-google-fracasa-examinamos-21-aplicaciones-de-seguridad-para-android/

Tabla 7.Herramientas de seguridad disponibles en plataforma Android

Herramientas	Características
Trend Micro Mobile Security and Antivirus	Ofrece protección protección contra sitios de phishing, un escáner de privacidad para Facebook y algunas herramientas para ayudarlo a ahorrar batería y memoria. También hay una característica ordenada "Just-a-Phone" que elimina todos los procesos de fondo no esenciales.
Avast Mobile Security	Como una aplicación gratuita para la plataforma Android, Avast Mobile Security ofrece una impresionante gama de herramientas. Tiene protección antivirus, escanea tus aplicaciones para proporcionar detalles sobre lo que están haciendo, y tiene un escudo web que escanea las URL en busca de malware.
AVG	Ofrece un paquete completo de herramientas con AVG, que incluye un localizador de teléfono, bloqueo de aplicación, bloqueador de llamadas y fotocámara para ocultar esas instantáneas sensibles.
Sophos Mobile Security	Ofrece un escaneo robusto que cubre la instalación, las aplicaciones existentes y los medios de almacenamiento. También ofrece filtrado web, protección con contraseña para aplicaciones, bloqueo de spam, consejos de privacidad y seguridad, y algunas otras herramientas.
Avira Antivirus Security 2018	Puede confiar en la versión gratuita de Avira para proteger su teléfono inteligente o tableta Android. Tiene una huella ligera en términos de rendimiento y un diseño elegante y minimalista. Además de buscar malware o spyware, esta aplicación también cuenta con una amplia gama de herramientas antirrobo y recuperación y algunos otros extras.

Tabla 7. (Continuación)

Herramientas	Características
ESET Mobile Security & Antivirus	ESET ofrece protección básica para mantener al malware más peligroso alejado de tu smartphone Android y su mejor arma es su extensa base de datos de virus y malware.[225]

Fuente:HILL, Simon. Herramientas de seguridad disponibles en plataforma Android [imagen]. The best security apps and antivirus protection for Android.DigitalTrend.2018.p.13. [Consultado: 5 de Octubre de 2018]. Disponible en Internet: : https://www.digitaltrends.com/mobile/best-antivirus-protection-for-android/

5.2.4 Aplicaciones de seguridad para dispositivos IOS: A pesar de que contar con menos virus afectando la plataforma IOS, no está demás en contar con una capa adicional de seguridad. Savitsky describe en su artículo que entre los niveles de seguridad ofrecidos por los equipos IPhone a sus usuarios se encuentran "fuertes instancias de verificación de cada app que aparece en la App Store, restricciones de los programas que funcionan dentro de ese sistema operativo, backups automáticos de la información del dispositivo en la nube y otras. Todas estas funciones buscan hacer el sistema operativo más práctico y seguro para usar." [226]

Sin embargo, expone Savitsky[227], cuando los usuarios se enfrentan a tareas consideradas no convencionales, como la protección con clave para las fotos almacenadas en el dispositivo, hay necesidad de hacer uso de la App Store, donde se pueden encontrar desde antivirus hasta soluciones más sofisticadas de seguridad, algunas de ellas en forma gratuita. A continuación, se describen algunas aplicaciones que pueden proteger un iPhone y a su contenido.

[225] ANDRES,Ruben. Estos son los 7 mejores antivirus gratis para Android de 2018[en línea].En Computer Hoy.28 de Marzo de 2018.[Consultado:15 de Septiembre de 2018].Disponible en: https://computerhoy.com/listas/moviles/estos-son-7-mejores-antivirus-gratis-android-2018-78199

[226] SAVITSKY,Alex. Siete Aplicaciones De Seguridad Para Tu iPhone [en línea]. Kaspersky Labs.(21 de Abril de 2014),párr.1.[Consultado13 de Octubre de 2018].Disponible en Internet: https://latam.kaspersky.com/blog/siete-aplicaciones-de-seguridad-para-tu-iphone/2887/

[227] Ibid.,p.106.

Tabla 8.Herramientas de seguridad disponibles en plataforma IOS

Herramientas	Características
Find My iPhone	Dispositivo de seguimiento, bloqueo remoto y borrado de datos, modo perdido, entre otras características adicionales.
Avira Mobile Security	Escáner de proceso y aplicación, optimización de almacenamiento y batería, dispositivo de seguimiento.
Lookout	Permite rastrear el dispositivo, realizar copia de seguridad, transferencia de contactos entre otras funciones.
Wickr	La tienda de aplicaciones de Apple presenta a wickr como una herramienta con la cual el usuario "puede conectarse instantáneamente con sus amigos individualmente o en grupos, ahora con llamadas de voz, notas de voz completamente encriptadas, nuevas adiciones para el intercambio seguro de extremo a extremo de archivos, imágenes y videos." [228]
Prey Anti Theft	Control remoto, antirrobo, mensaje de alerta, protege hasta 3 dispositivos con una sola cuenta.

[228]Wickr Me – Private Messenger [en línea].Apple Store.[Consultado:3 de Octubre de 2018].Disponible en Internet: https://itunes.apple.com/us/app/wickr-me-private-messenger/id528962154?mt=8

Tabla 8. (Continuación)

Herramientas	Características
Kryptos	Aplicación de voz sobre IP (VoIP) para el iPhone para llamadas seguras, comunicaciones cifradas, ID individual única entre otras características.

Fuente: Herramientas de seguridad disponibles en plataforma IOS [imagen]. Top 12 Best and Free Security Apps for Your iOS Devices. Dr.fone.p.20.[Consultado:3 de Octubre de 2018].Disponible en Internet:**https://drfone.wondershare.com/iphone/iphone-security-apps.html#part2**

Para complementar el listado de herramientas ofrecido en la tabla anterior, Singh[229] expone las siguientes herramientas disponibles enfocados a brindar seguridad en los dispositivos móviles con sistema IOS:

mSecure Password Manager: Según se expone en la página de MSecure[230], esta herramienta se puede utilizar para generar contraseñas aleatorias, complejas y únicas para todos sus sitios. Además de ello, permite almacenar, compartir y administrar contraseñas e información confidencial.

Norton Mobile Security : En su artículo Singn[231] expresa que, Norton Mobile Security ofrece una protección efectiva para su iPhone y iPad contra robos y pérdidas. Adicionalmente Singh expresa que la herramienta "brinda la posibilidad de ubicar de forma remota el dispositivo IPhone desde cualquier lugar con una conexión a Internet o activar una alarma en el dispositivo perdido. También permite realizar copias de seguridad de contactos los cuales se pueden restaurar fácilmente en sus diferentes dispositivos móviles con sistemas IOS".[232]

[229] SINGH, Karanpreet. 15 Best Security Apps That You Must Have In your iPhone 2018[en línea].Techviral.(29 de Junio de 2018),párr.2.[Consultado:3 de Octubre de 2018]. Disponible en Internet: https://techviral.net/best-security-apps-iphone/

[230] mSecure 5 [en línea].Msecure.[Consultado:3 de Octubre de 2018]. Disponible en Internet: https://www.msecure.com/

[231] SINGH, Op.cit,.p.108.

[232] SINGH, Op.cit,.p.108.

Norton Snap: Según artículo publicado en Norton[233], Norton Snap es un analizador de código QR que protege a los dispositivos IPhone de las amenazas provenientes de códigos QR peligrosos, bloqueando los sitios web inseguros antes de que carguen en el dispositivo.

5.3 PRINCIPALES ERRORES QUE COMETEN LOS USUARIOS DE DISPOSITIVOS MÓVILES

5.3.1 Distribución del mercado de dispositivos móviles: En la disputa por el dominio del mercado de los dispositivos móviles y en aras de tomar ventaja en este aspecto, Gartner234 confirma en su estudio, que dos de los competidores Android y iOS se han alejado del resto en cuanto a usuarios conectados a través de sus equipos y la tecnología ofrecida. En su comunicado de prensa, Gartner235 plantea que, en el año 2017, las ventas de teléfonos inteligentes a los usuarios finales sumaron más de 1.500 millones de unidades, lo que representa un aumento del 2,7 por ciento con respecto al año 2016.

Por último, la investigación plantea que "si bien la participación de mercado de Apple se estabilizó en el cuarto trimestre de 2017 en comparación con el mismo trimestre de 2016, las ventas de iPhone cayeron un 5 por ciento" [236].

[233] Funciones de Norton Snap[en línea]Norton.[Consultado:4 de Octubre de 2018]. Disponible en Internet: https://support.norton.com/sp/es/mx/home/current/solutions/v64690996_EndUserProfile_es_mx

[234] VAN DER MEULEN, Rob y MCCALL, Thomas .Gartner Says Worldwide Sales of Smartphones Recorded First Ever Decline During the Fourth Quarter of 2017.[en línea].Gartner, Egham, UK.(22 de Febrero de 2018),párr.9. [Consultado: 26 de Abril de 2018]. Disponible en Internet: https://www.gartner.com/en/newsroom/press-releases/2018-02-22-gartner-says-worldwide-sales-of-smartphones-recorded-first-ever-decline-during-the-fourth-quarter-of-2017

[235] Ibid.,p.109.

[236] Ibid.,p.109.

Tabla 9.Ventas mundiales de teléfonos inteligentes a usuarios finales por sistema operativo en 2017 (miles de unidades)

Sistema Operativo	2017 Unidades	Participación en el mercado 2017 (%)	2016 Unidades	Participación en el mercado 2016 (%)
Android	1,320,118.1	85.9	1,268,562.7	84.8
IOS	214,924.4	14.0	216,064.0	14.4
Otro Sistemas Operativos	1,493.0	0.1	11,332.2	0.8
Total	1,536,535.5	100.0	1,495,959.0	100.0

Fuente: Gartner. Gartner Says Worldwide Sales of Smartphones Recorded First Ever Decline During the Fourth Quarter of 2017[en línea]. Egham, UK, 22 de Febrero de 2018. pg. 4.[Consultado: 6 de Mayo de 2018]. Disponible en Internet: https://www.gartner.com/en/newsroom/press-releases/2018-02-22-gartner-says-worldwide-sales-of-smartphones-recorded-first-ever-decline-during-the-fourth-quarter-of-2017

El portal de estadística Statista expone que "los teléfonos inteligentes, conocidos como teléfonos móviles con capacidades de procesamiento y conectividad más avanzadas que los teléfonos móviles normales, llegaron al mercado de consumidores a fines de los 90, pero solo ganaron popularidad con la introducción del iPhone de Apple en 2007"[237].

La aparición del IPhone, indica Statista[238] marcó un hito en el campo de industria de la telefonía móvil. Su interfaz de pantalla táctil y teclado virtual lo convirtieron en el pionero en ofrecer este tipo de características inexistentes para la época.Su

[237] STATISTA. Smartphones industry: Statistics & Facts[en línea].[Consultado:11 de Septiembre de 2018].Disponible en Internet: https://www.statista.com/topics/840/smartphones/

[238] Ibid.p.110.

primer equipo surgió en el mercado en Enero de 2007. El primer dispositivo inteligente con plataforma Android se introdujo en el mercado a fines de 2008.

El informe de Statista concluye que, desde aquella época esta industria ha estado evolucionando y creciendo constantemente tanto en manejo del mercado, como en modelos y proveedores." Se prevé que los envíos de teléfonos inteligentes en todo el mundo sumen aproximadamente 1.700 millones de unidades en 2020. Para 2021, se prevé que el 40 por ciento de la población mundial poseerá un teléfono inteligente." [239]

Si bien el mercado mundial de teléfonos inteligentes sigue estando bastante competitivo en términos de fabricantes que luchan por el dominio de los consumidores, parece que esta guerra por el dominio del mercado entre diferentes plataformas parece haber terminado.

Según un informe reciente publicado por Gartner[240], Android y iOS representan más del 99 por ciento de las ventas mundiales de teléfonos inteligentes, lo que hace que cualquier otra plataforma disponible sea irrelevante desde este punto de vista.

Haciendo un poco de historia, para el año 2010 los dispositivos Android e iOS controlaban, afirma Ritcher[241], menos del 40 por ciento de las ventas mundiales de teléfonos inteligentes. Para aquella época, los dispositivos con Sistemas Operativos Symbian y BlackBerry de Nokia representaban una parte importante de las ventas de teléfonos inteligentes.

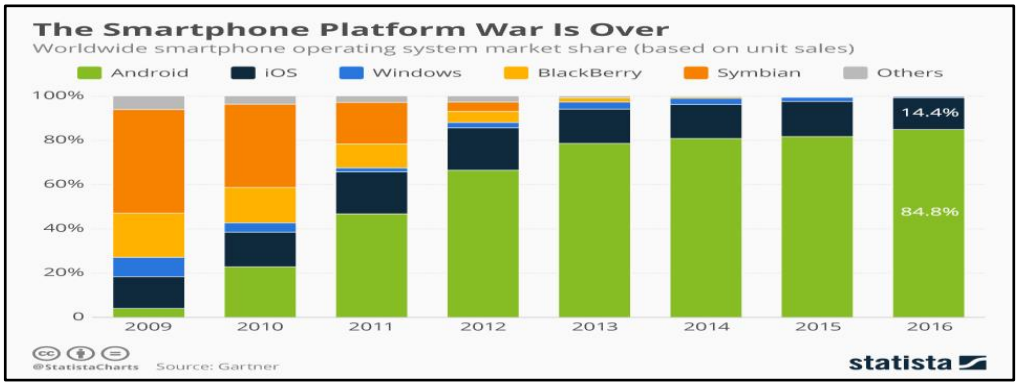
[239] Ibid.p.110.

[240]GOASDUFF, Laurence y FORNI Amy Ann. Gartner Says Worldwide Sales of Smartphones Grew 7 Percent in the Fourth Quarter of 2016.[en línea]. Gartner, Egham, U.K. (15 de Febrero de 2017).párr.11.[Consultado:12 de Septiembre de 2018].Disponible en Internet: https://www.gartner.com/en/newsroom/press-releases/2017-02-15-gartner-says-worldwide-sales-of-smartphones-grew-7-percent-in-the-fourth-quarter-of-2016

[241]RITCHER,Felix. The Smartphone Platform War Is Over [en línea].Statista.(20 de Febrero de 2017).párr.2.[Consultado:11 de Septiembre de 2018].Disponible en Internet: https://www.statista.com/chart/4112/smartphone-platform-market-share/

Además de lo anterior Ritcher[242] expresa que, teniendo claro que Symbian dejó de existir hace tiempo, y que BlackBerry comenzó a hacer la transición a dispositivos Android, Microsoft no ha dado por terminada su lucha con su sistema Windows 10 Mobile por el control parcial del mercado. Sin embargo, en la actualidad la posibilidad de que dicha plataforma controle, si quiera algún mercado importante dejado por sus inmediatos competidores es considerado improbable.

Figura 20.Distribución mercado Sistemas Operativos para Smartphone



Fuente: RITCHER,Felix. Distribución mercado Sistemas Operativos para Smartphone (Unidades vendidas) [imagen]. The Smartphone Platform War Is Over. Statista. 2017.pag. 2.[Consultado:11 de Septiembre de 2018].Disponible en Internet: https://www.statista.com/chart/4112/smartphone-platform-market-share/

Tomando como base las ventas realizadas en el año 2018, Gartner[243] expone que los usuarios de teléfonos inteligentes crecieron en el primer trimestre, con un aumento del 1.3 por ciento en comparación con el mismo periodo del año anterior. Continuando con el reporte de Gartner, este indica que “Las ventas en este periodo ascendieron a cerca de 384 millones de teléfonos inteligentes, lo que representa el 84 por ciento del total de teléfonos móviles vendidos”. [244]

[242] Ibid.,p.111.

[243]COSTELLO, Katie y HIPPOLD Sarah Cornelia. Gartner Says Worldwide Sales of Smartphones Returned to Growth in First Quarter of 2018[en línea]. Gartner ,Egham, U.K. (29 de Mayo de 2018).párr 1.[Consultado:14 de Septiembre de 2018].Disponible en Internet: https://www.gartner.com/newsroom/id/3876865

[244] Ibid.,p.112.

Figura 21.Ventas mundiales de Smartphones por Vendedor en Primer Cuarto de año en 2018 (Millones de Unidades)

Worldwide Smartphone Sales to End Users by Vendor in 1Q18 (Thousands of Units)				
Vendor	1Q18 Units	1Q18 Market Share (%)	1Q17 Units	1Q17 Market Share (%)
Samsung	78,564.8	20.5	78,776.2	20.8
Apple	54,058.9	14.1	51,992.5	13.7
Huawei	40,426.7	10.5	34,181.2	9.0
Xiaomi	28,498.2	7.4	12,707.3	3.4
OPPO	28,173.1	7.3	30,922.3	8.2
Others	153,782.1	40.1	169,921.1	44.9
Total	**383,503.9**	**100.0**	**378,500.6**	**100.0**

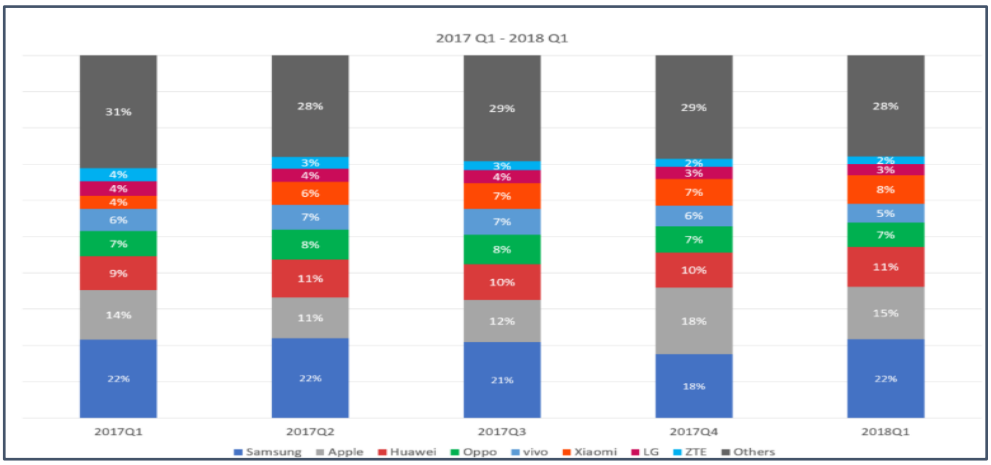
Fuente: COSTELLO, Katie y HIPPOLD Sarah Cornelia. Ventas mundiales de Smartphones por Vendedor en Primer Cuarto de año en 2018 (Millones de Unidades) [imagen]. Gartner Says Worldwide Sales of Smartphones Returned to Growth in First Quarter of 2018.Egham, UK. 2018.pag. 1.[Consultado:11 de Septiembre de 2018]. Disponible en Internet: https://www.gartner.com/newsroom/id/3876865

La grafica siguiente muestra comparativo de la distribución del mercado de dispositivos móviles por parte de los principales OEM´s (Fabricantes de Equipos Originales), tomando como base de análisis los años 2017 y 2018.

Algunos datos obtenidos del estudio realizado por la firma de investigación Counterpoint muestran que “los envíos de teléfonos inteligentes disminuyeron un 3% anual hasta llegar a 360 millones de unidades en el primer trimestre de 2018, la participación del mercado de teléfonos inteligentes cayó al 76% de todos los teléfonos móviles enviados en el trimestre, y las 10 principales marcas representaron el 76% de los volúmenes de teléfonos inteligentes en el primer trimestre de 2018.”[245]

[245] TEAM COUNTERPOINT. Global Smartphone Market Share: By Quarter [en línea].Countpoint.(16 de Mayo de 2018).párr 4.[Consultado:10 de Septiembre de 2018].Disponible en Internet: https://www.counterpointresearch.com/global-smartphone-share/

Figura 22.Distribución del mercado de dispositivos móviles por Fabricantes



Fuente: TEAM COUNTERPOINT. Distribución del mercado de dispositivos móviles por Fabricantes tomando como base segundos trimestres de los años 2017 y 2018 [imagen]. Global Smartphone Market Share: By Quarter. Counterpoint.2018.pag. 3.[Consultado:9 de Septiembre de 2018]. Disponible en Internet: https://www.counterpointresearch.com/global-smartphone-share/

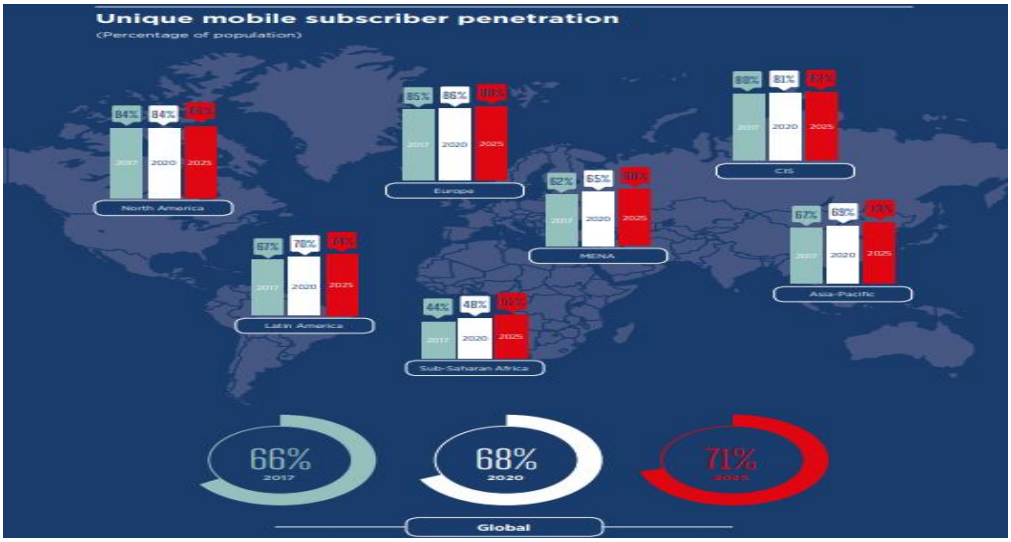
Distribución por países: Abordando el tema de distribución del mercado de telefonía móvil por países o regiones, GSMA[246] deja claro en su informe que, según datos obtenidos por la entidad, a finales de 2017 la tecnología móvil tuvo mejor alcance que cualquier otra tecnología para aquella época. Las cifras muestran que para el año 2017, el número de suscriptores móviles únicos han sobrepasado los 5 mil millones de usuarios.

Además de lo anterior, la entidad expone en su informe que "Entre 2017 y 2025, India y China agregarán más de 200 millones y 70 millones de nuevos suscriptores respectivamente, mientras que África Subsahariana, América Latina y tres otros principales países asiáticos (Pakistán, Indonesia y Bangladesh) generarán un total de más de 350 millones de nuevos suscriptores."[247]

[246] The Mobile Economy 2018. GSMA. [en línea].[Consultado:7 de Septiembre de 2018].Disponible en Internet: https://www.gsma.com/mobileeconomy/wp-content/uploads/2018/02/The-Mobile-Economy-Global-2018.pdf

[247] Ibid.,p.114.

Figura 23. Mercado Suscriptores móviles únicos finales 2017 distribuido por Países

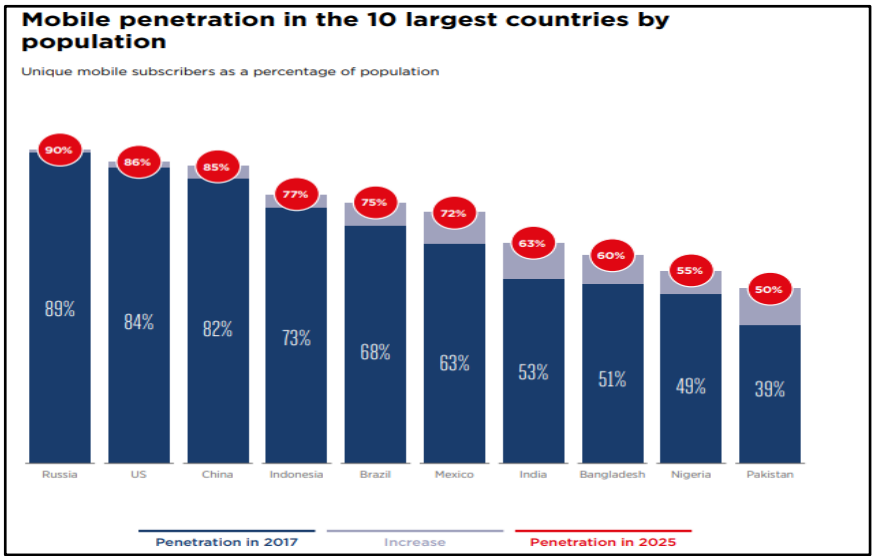


Fuente: GSMA. Mercado Suscriptores móviles únicos finales 2017 distribuido por Países [imagen]. The Mobile Economy 2018. p.13. [Consultado:9 de Septiembre de 2018]. Disponible en Internet:https://www.gsma.com/mobileeconomy/wp-content/uploads/2018/02/The-Mobile-Economy-Global-2018.pdf

Por último, el informe[248] indica que, entre los 10 más países más poblados del mundo, la brecha en cuanto a inclusión de tecnología móvil entre el suscriptor único más alto y más bajo será de alrededor de 40 puntos porcentuales en el año 2025. Los 10 países juntos representan casi el 60% del mercado global de suscriptores.

[248] Ibid.,p.114.

Figura 24, Inclusión tecnología móvil en los 10 países más grandes por población



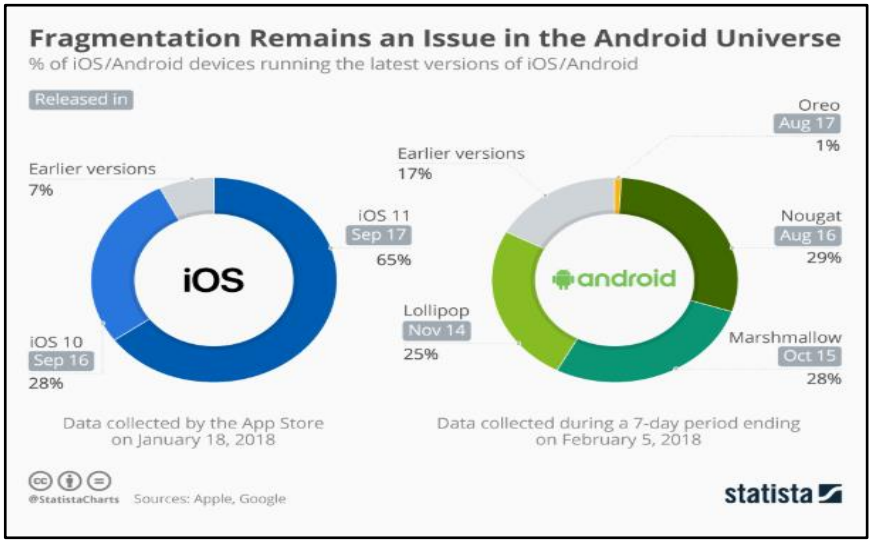
Fuente: GSMA. Inclusión tecnología móvil en los 10 países más grandes por población [imagen]. Mobile penetration in the 10 largest countries by population The Mobile Economy 2018. p.16. [Consultado:9 de Septiembre de 2018]. Disponible en Internet:https://www.gsma.com/mobileeconomy/wp-content/uploads/2018/02/The-Mobile-Economy-Global-2018.pdf

Por versión del sistema operativo: Como se muestra en la siguiente figura, Richter[249] expresa que, el 93 por ciento de los dispositivos con iOS ejecutan versión de iOS 11 o en su defecto IOS 10. La primera de ellas fue liberada en Septiembre de 2017. La segunda versión fue liberada en Septiembre de 2016. Por los lados de su competidor inmediato, la plataforma Android, su última versión de Android, Oreo, solo se encuentra instalada en el 1 por ciento de todos los dispositivos activos, mientras que 4 de cada 10 dispositivos funcionan en un sistema que tiene más de tres años.

Esto muestra un campo de acción para desarrolladores de IOS bastante unificado, mientras que la situación es completamente diferente para personas interesadas en llevar a cabo desarrollos sobre Android, quienes tienen que lidiar con un sistema altamente fragmentado.

[249] RITCHER,Felix. Fragmentation Remains an Issue in the Android Universe [en línea].Statista.(12 de Abril de 2018).párr. 3.[Consultado:12 de Septiembre de 2018].Disponible en Internet: https://www.statista.com/chart/5930/adoption-of-ios-and-android-versions/

Figura 25.Porcentaje de Dispositivos Android IOS ejecutando sus últimas versiones



Fuente: RITCHER,Felix. Porcentaje de Dispositivos Android IOS ejecutando sus últimas versiones[imagen]. % of IOS/Android devices running the latest versions of IOS/Android. Fragmentation Remains an Issue in the Android Universe.2018.p.2. [Consultado: 13 de Septiembre de 2018]. Disponible en Internet: https://www.statista.com/chart/5930/adoption-of-ios-and-android-versions/

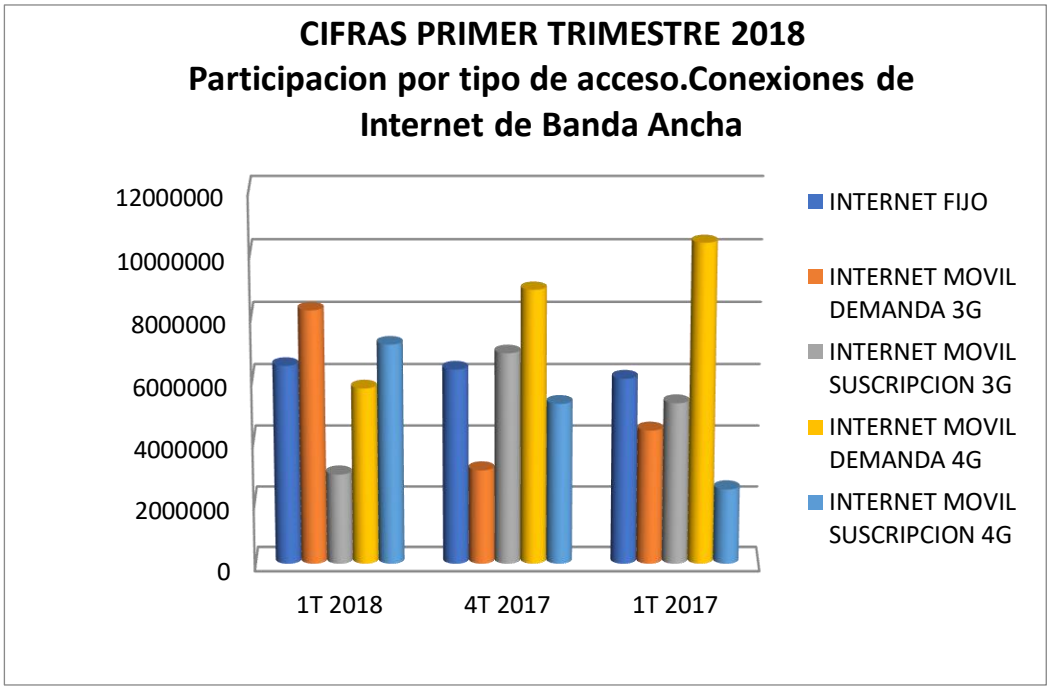
Estadísticas Participación en el mercado Colombia: Según informe publicado por el Ministerio de las Tecnologías de la Información y de la Comunicaciones," el total de líneas de telefonía celular habilitadas en el país llegó al cierre de 2017 a 62,2 millones, esto significa que por cada colombiano había 1,2 líneas en el país. La variación porcentual de abonados o usuarios en el servicio de telefonía móvil al término del tercer trimestre del 2017 fue del 1,73% en comparación con los datos obtenidos en el segundo trimestre del mismo año." [250]

Según el mismo informe del ministerio de las TIC´s, " la participación en el mercado de telefonía móvil en Colombia al cierre del año 2017,teniendo en cuenta

[250] MINISTERIO DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES - REPÚBLICA DE COLOMBIA. Boletín trimestral de las TICS, Cifras Tercer Trimestre de 2017[en línea].[Consultado:13 de Septiembre de 2018].Disponible en Internet: http://colombiatic.mintic.gov.co/602/articles-62299_archivo_pdf

el número de abonados que tienen los Proveedores de Redes y Servicios Móviles, estaba distribuida de la siguiente manera: Comunicación Celular S.A. COMCEL S.A con 47,90%; seguido de Colombia Telecomunicaciones S.A. E.S.P. con una participación del 23,25%; Colombia Móvil S.A. E.S.P., 18,34%; Virgin Mobile S.A.S., 4,54%, y los demás proveedores de telefonía móvil (5) con una participación del 5,98%".[251] Analizando los mismos datos para el primer trimestre del año 2018, los resultados obtenidos se muestran en la siguiente ilustración.

Figura 26.Participación en el mercado de Proveedores de Telefonía Móvil



Fuente: Ministerio de Tecnologías de la Información y las Comunicaciones - República de Colombia. Participación en el mercado de proveedores de Telefonía Móvil [imagen]. Boletín trimestral de las TICS Cifras primer trimestre de 2018. p.7. [Consultado: 12 de Septiembre de 2018]. Disponible en Internet: https://colombiatic.mintic.gov.co/679/articles-75854_presentacion_cifras.pdf

[251] Ibid.,p.117.

Futuro del mercado de dispositivos móviles: Según un nuevo pronóstico de International Data Corporation (IDC)[252] , se espera que los envíos mundiales de teléfonos inteligentes se incrementen levemente en 2017 con un crecimiento esperado de 3.0% respecto al año anterior. IDC además pronosticó que los envíos de teléfonos inteligentes llegarán a 1,53 mil millones de unidades en 2017, y eventualmente crecerán a 1,77 mil millones de unidades para el año 2021.

Desde la perspectiva de plataformas móviles, IDC[253] no espera muchos cambios a lo largo de los años estudiados respecto a la situación actual, ya que Google Android representa cerca del 85 por ciento de todos los envíos de teléfonos inteligentes, y Apple iOS se encarga del resto. En ese orden de ideas, las esperanzas para los teléfonos inteligentes basados en Microsoft por dominar parte importante de este mercado siguen siendo desalentadoras, dada la falta de soporte de los socios importantes.

Teniendo en cuenta las perspectivas provistas para un nuevo crecimiento de teléfonos inteligentes, según IDC[254], las Phablets se convertirán en la principal fuerza impulsora del mercado, debido a la gran variedad de dispositivos existentes en el mercado con funciones en los segmentos Premium y nivel básico. Este tipo de dispositivos tratan de conjugar en un mismo aparato la capacidad de comunicación y procesamiento de un Smartphone con el tamaño de las pantallas de las tabletas.

En el último estudio publicado por GSMA Mobile Economy, se plantean algunos aspectos a tener en cuenta en el futuro reciente en el campo de la telefonía móvil:

- La cantidad de suscriptores móviles únicos alcanzará 5.900 millones para 2025, equivalente al 71% de la población mundial.
- En 2019, 4G se convertirá en la tecnología de red móvil líder a nivel mundial por número de conexiones (más de 3.000 millones).
- El número de conexiones de Internet de las cosas (IoT) (celular y no celular) aumentará más de tres veces en todo el mundo entre 2017 y 2025, alcanzando los 25.000 millones.
- Mirando hacia 2025, las conexiones IoT celulares autorizadas llegar a 3,100 millones en todo el mundo, o 12% del total conexiones IoT.[255]

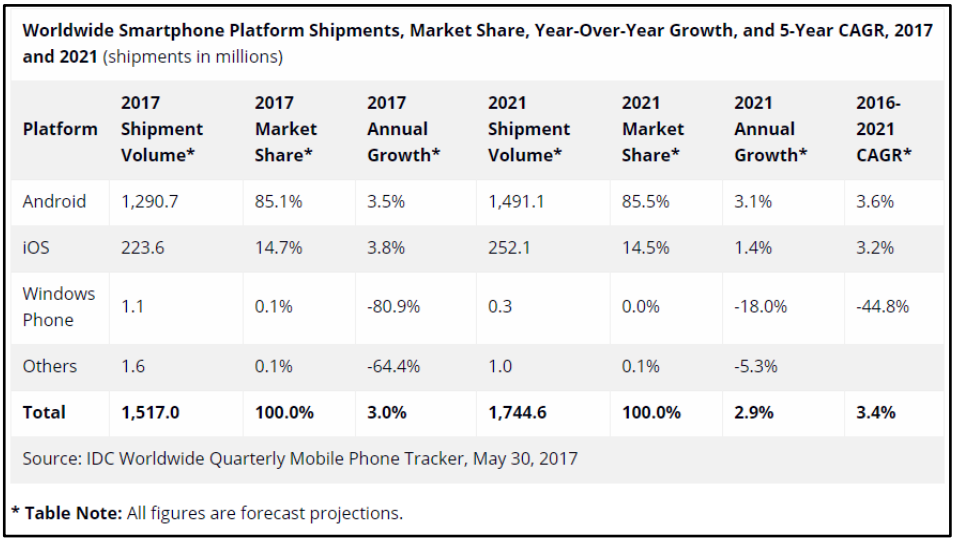
[252] IDC. Smartphone Volumes Expected to Rebound in 2017 with a Five-Year Growth Rate of 3.8%, Driving Annual Shipments to 1.53 Billion by 2021, According to IDC [en línea]. International Data Corporation (IDC).(1 de Marzo de 2017).párr.1.[Consultado:9 de Septiembre de 2018].Disponible en Internet: https://www.idc.com/getdoc.jsp?containerId=prUS42334717

[253] Ibid.,p.119.

[254] Ibid.,p.119.
}

[255] The Mobile Economy 2018.[en línea].GMS Association. [En línea].[Consultado:3 de Octubre de 2018].Disponible en Internet http://www.redestelecom.es/siteresources/files/843/44.pdf

Figura 27.Envíos Mundiales de Smartphones, Taza de Crecimiento Anual de Mercado - Años 2017 y 2021 (envíos en millones)



Worldwide Smartphone Platform Shipments, Market Share, Year-Over-Year Growth, and 5-Year CAGR, 2017 and 2021 (shipments in millions)

Platform	2017 Shipment Volume*	2017 Market Share*	2017 Annual Growth*	2021 Shipment Volume*	2021 Market Share*	2021 Annual Growth*	2016-2021 CAGR*
Android	1,290.7	85.1%	3.5%	1,491.1	85.5%	3.1%	3.6%
iOS	223.6	14.7%	3.8%	252.1	14.5%	1.4%	3.2%
Windows Phone	1.1	0.1%	-80.9%	0.3	0.0%	-18.0%	-44.8%
Others	1.6	0.1%	-64.4%	1.0	0.1%	-5.3%	
Total	**1,517.0**	**100.0%**	**3.0%**	**1,744.6**	**100.0%**	**2.9%**	**3.4%**

Source: IDC Worldwide Quarterly Mobile Phone Tracker, May 30, 2017

* **Table Note:** All figures are forecast projections.

Fuente: IDC. Envíos Mundiales de Smartphones, Taza de Crecimiento Anual de Mercado - Años 2017 y 2021 (envíos en millones) [imagen]. Worldwide Smartphone Platform Shipments, Market Share, and 5-Year CAGR, 2017 and 2021 (shipments in millions). Smartphone Volumes Expected to Rebound in 2017 with a Five-Year Growth Rate of 3.8%, Worldwide Smartphone Platform Shipments, Market Share, and 5-Year CAGR, 2017 and 2021 (shipments in millions) According to IDC.2017. p.4.[Consultado:11 de Septiembre de 2018]. Disponible en Internet: https://www.idc.com/url.do?url=/includes/pdf_download.jsp?containerId=prUS42334717&position=2

5.3.2 Errores comunes en el teléfono inteligente que lo exponen a riesgos de seguridad: Para un dispositivo que es considerado tan importante en la vida cotidiana y que almacena información confidencial de usuarios, muchas veces estos no son conscientes de los errores o riesgos a los que se exponen sus dispositivos móviles, unas veces por desconocimiento y en otras, a pesar de que se conocen se pasan por alto pensando que sus equipos no van a ser objeto de algún tipo de ataque. A continuación, se describen algunos de los errores comunes que cometen los usuarios que hacen uso de sus móviles y los riesgos a los que se exponen al no tener en cuenta medidas mínimas de seguridad.

En primera instancia, la instalación de aplicaciones de fuentes desconocidas, más conocido como carga lateral, expone Navarro[256], abre la posibilidad de que se infiltre software malicioso en nuestro teléfono. Este tipo de aplicaciones suelen parecer tentadoras a los usuarios debido que son gratuitas pero lo cierto es que permiten que malware disfrazado de aplicaciones legitimas infecten sus dispositivos. Lo recomendable para evitar este tipo de ataques es descargar software desde fuentes confiables y evitar el jailbreaking o cualquier otra solución que permita instalar aplicaciones desde fuentes diferentes a la App oficial.

En segunda instancia, el hecho de hacer clic en los enlaces desconocidos, puede traer consigo ataques de phishing, en los cuales se suplantan aplicaciones reales o actualizaciones que el usuario tiene instaladas, con el objeto de obtener contraseñas, números de identificación personales o cualquier otro tipo de información requerida por los atacantes para llevar a cabo su labor. Según expresa Navarro[257], este tipo de ataques también pude llevarse a cabo a través de correos electrónicos que provienen, en teoría, de entidades bancarias o entidades de comercio electrónico como PayPal. “Al hacer clic en los enlaces provistos por estos correos electrónicos falsos, a menudo se crean portales que intentarán robar sus datos e instalar malware para lanzar más ataques.”[258]

Continuando con la descripción de errores de seguridad a los cuales se exponen los dispositivos móviles se encuentra la definición de contraseñas débiles. Algunos de los inconvenientes encontrados en este tipo de contraseñas son: su longitud demasiado corta (mínimo se recomienda ocho caracteres), y su nivel de complejidad bajo (un ejemplo de este error es hacer uso de frecuencias de números o letras seguidas). Riesgos adicionales de seguridad asociados al uso indebido de contraseñas son: utilización de la misma clave para diferentes tipos de aplicaciones, escribirlas en medio físico o en algún lugar visible a otras personas y la ausencia de política de cambios permanentes de las mismas.

Otro de los puntos a tener en cual a la hora de definir parámetros de seguridad para evitar que la información almacenada en los equipos móviles esté expuesta a

[256] NAVARRO,Francis. Common security risks every smartphone user should know about [en línea].Kim Komando.(23 de Julio de 2017).párr. 4.[Consultado: 27 de Spetimbre de 2018].Disponible en Intenet: https://www.komando.com/tips/370318/common-security-risks-every-smartphone-user-should-know-about/all

[257] Ibid.,p.121.

[258] Ibid.,p.121.

ataques de intrusos es la activación del bloqueo del dispositivo. En este apartado existen diferentes formas de llevar a cabo esta labor, pero es recomendable la definición de claves o PIN lo suficientemente fuertes y, si es posible, hacer uso de bloqueo a través de huella dactilar, además de evitar el uso de patrones de bloqueo los cuales pueden ser pirateados fácilmente.

El robo de dispositivos es otro de los riegos los que se exponen estos equipos. Aparte de su valor comercial, entre los tipos de información que buscan los delincuentes en estos dispositivos, expone González[259] en su tesis, se encuentran: lista de contactos, registros de llamadas, historial del navegador, datos de configuración del dispositivo entre otros. Con el objeto de mitigar este tipo de amenazas, se recomienda, si el equipo lo permite, activar la característica que permite rastrear su localización y bloquearlo o borrarlo remotamente en caso de ser víctima de este tipo de ataques.

El no hacer uso de software antivirus, expone Mitroff,[260] convierte los equipos móviles en susceptibles de ser atacados por software malicioso (malware). Para los equipos con sistema Android, aplicaciones como Lookout, Avast o TrustGo son utilizadas para escanear y eliminar este tipo de software. Por su parte, en equipos con plataforma IOS, a pesar de que este tipo de ataques son menos comunes, Apple facilita a sus usuarios parches de seguridad cuando se detectan fallas en su sistema operativo que puedan afectar sus dispositivos frente este tipo de amenazas.

Hacer uso de redes públicas de Wi-Fi es, a pesar de ser una opción gratuita, una amenaza latente con la que deben lidiar los usuarios de los equipos móviles. Según platea Daniel “la información y los datos transmitidos a través de redes Wi-Fi públicas son visibles para cualquier persona en la red si saben cómo verla” [261]. La primera opción es, si no tiene otra opción diferente a conectarse a estas redes,

[259] GONZALEZ FERNANDEZ, Alfonso. Seguridad en Smartphone. Análisis de riesgos, de vulnerabilidades, y auditorias de dispositivos [en línea]Trabajo final para obtener el título de Master Interuniversitario de Seguridad en las Tecnologías de la Información y de las Comunicaciones (MISTIC). Universidad Abierta de Cataluña,2018,p.17. [Consultado: 26 de Septiembre de 2018]. Disponible en Internet: http://openaccess.uoc.edu/webapps/o2/bitstream/10609/72966/6/agonzalezfernandez3TFM0118Memoria.pdf

[260] MITROFF,Sarah. La seguridad es clave [diapositivas].CNet.3 de Marzo de 2016,diapositiva 5.[Consultado:26 de Septiembre de 2018].Disponible en Internet: https://www.cnet.com/es/imagenes/errores-seguridad-telefono/5/

[261] DANIEL, Jo. 10 Common Smartphone mistakes that expose you to security risks [en línea].Information Nigeria.(12 de Diciembre de 2016).párr 6. [Cosultado:27 de Septiembre de 2018].Disponible en Internet: http://www.informationng.com/2016/12/10-common-smartphone-mistakes-expose-security-risks.html

asegurase de hacer uso de una VPN, el cual expresa Daniel[262] es un método para conectarse a sitios web de forma segura. Ejemplos de este tipo de redes son: Droid VPN o TUNNEL BEAR VPN. La otra opción es hacer uso de una red de datos móviles.

Pasar por alto los procesos de actualizaciones, expresa Daniel[263], tanto de aplicaciones instaladas en el dispositivo como de software del sistema puede crear puertas traseras o puntos de acceso a los dispositivos poniendo en riegos la seguridad de la información almacenada.

El mismo autor[264] expresa que la gran mayoría de fabricantes de equipos móviles ponen a disposición de los usuarios actualizaciones de software para mejorar la funcionalidad de sus sistemas operativos y solucionar inconvenientes de seguridad identificados. Lo mismo ocurre con las aplicaciones de Android y IOS. La recomendación es acostumbrase a actualizar constantemente el software que se ejecuta en el equipo móvil.

Otro de los riegos a los que se enfrentan los usuarios de teléfonos móviles es la falta de verificación de aplicaciones instaladas en los equipos antes de llevarse a cabo dicho proceso. Con verificación se hace referencia a una pequeña investigación llevada a cabo desde la fuente de instalación de la aplicación elegida, incluyendo comentarios y calificaciones de usuarios anteriores a cerca de la misma, derechos solicitados para llevar cabo la instalación, tamaño de la misma entre otras características. En artículo de la revista Semana se expone “es muy recurrente que antes de descargar una aplicación los usuarios NO leen las condiciones que la misma aplicación informa que necesita para funcionar de la mejor manera. Casi todas las aplicaciones le informan si necesitan su correo o contraseñas, los permisos van hasta su ubicación diaria.”[265]

[262] Ibid.,p.122.

[263] Ibid.,p.122.

[264] Ibid.,p.122.

[265] ¿Cuánta información personal entrega cuando utiliza una aplicación?[en línea].En Revista Semana.30 de Enero de 2014.pág 3.[Consultado:26 de Septiembre de 2018].Disponible en Internet: https://www.semana.com/tecnologia/tips/articulo/cuanta-informacion-personal-entrega-cuando-utiliza-aplicacion/375589-3

Por último, FirstCounryBank[266] expresa en su artículo que, si bien Jailbreaking o Rootear son procedimientos utilizados para expandir las funcionalidades de dispositivos móviles, entre otras habilitar opciones por defectos deshabilitadas por el sistema, lo cierto es que estos procesos alteran la seguridad del sistema operativo exponiendo los datos personales almacenados en los equipos a ataques cibercriminales. Los delincuentes, indica FirstCounryBank "controlan la memoria del dispositivo y el uso de aplicaciones para recopilar información personal".[267]

[266] The Risks of "Jailbreaking" and "Rooting" Mobile Devices [en línea]. [Consultado:28 de Septiembre de 2018].Disponible en Internet: https://www.firstcountybank.com/sites/default/files/pdfs/Jailbroken%20and%20Rooted%20Devices%20Fraud%20Risks.pdf

[267] Ibid.,p.124.

6. CONCLUSIONES

Es una realidad que en los últimos años los desarrollos tecnológicos han cambiado la forma como llevar a cabo nuestras labores cotidianas. El ámbito de los dispositivos móviles no ha sido ajeno a este tipo de desarrollos. Debido al auge de los teléfonos inteligentes y del gran crecimiento en el uso de Smartphones estos se han convertido en blanco de ataques de diferentes tipos, con consecuencias que van desde el acceso remoto a equipos, robo de los mismos, acceso a información confidencial de usuarios entre otros. Tomando como base la presente monografía, se puede llegar a las siguientes conclusiones:

- A la hora de mirar las bondades de cada uno de los sistemas operativos para móviles estudiados en la presente monografía se puede afirmar que, en el caso de los sistemas Android, su costo al usuario final, así como el hecho de trabajar con plataforma abierta, además de no depender de un solo canal de distribución para sus aplicaciones lo convierten en una opción bastante llamativa, tanto para usuarios finales como para desarrolladores. La desventaja principal en este tipo de sistemas está asociada con los ataques de malware que pueden existir en aplicaciones disponible en su tienda Apple Store.

- Para el caso de los dispositivos móviles con sistema IOS, la característica que llama más la atención son los niveles de seguridad ofrecidos por la plataforma, que, aunque no pueden ser considerados invulnerables, si existe un proceso de revisión, cuando los desarrolladores desean publicar una aplicación en su tienda de Apple. Otra de las variables en las cuales este sistema encuentra buenas calificaciones son sus diseños e interfaces de usuarios. El costo de sus equipos juega en contra a la hora de compararlos con su competencia.

- Las características ofrecidas por cada una de las plataformas estudiadas en la monografía relacionadas con control total o más amplio de los equipos (jailbreaking, rooting), dejan abiertas puestas de seguridad accesible a los cibercriminales.

- Tareas tan comunes como deshabilitar característica Bluetooth en los Smartphones, el uso restringido de redes gratuitas (Wi-Fi), y la utilización de

programas antivirus confiables hacen que los riesgos de seguridad existentes en el ámbito de lo teléfonos móviles se reduzcan.

- Los dispositivos móviles requieren de dos tipos de protecciones orientadas a evitar diferentes tipos de amenazas que los asechan. Los riegos asociados con el primer tipo de protección (ciberseguridad) tienen que ver con amenazas asociadas a ataques de malware y vulnerabilidades en dispositivos, entre otros. En cuanto al segundo tipo de protección (física), los equipos están expuestos a daños de tipo físico, tales como humedad, exposición a temperaturas extremas, o al robo o extravío del dispositivo.

- Tomando como base estudios publicados en la Séptima Cumbre Latinoamericana de Analistas de Seguridad en realizados en el año 2017, se ´puede indicar que los fraudes financieros, el ransomware y los ataques móviles son las amenazas cibernéticas más comunes que se presentan en América Latina.

- En cuanto a fallas de seguridad identificadas en las dos plataformas estudiadas en la presente monografía, IOS presentó menos de la mitad de fallas identificadas comparadas con las halladas en la plataforma Android en el año 2017 (124 frente a 322 vulnerabilidades detectadas).

- En el ámbito local, las principales amenazas y ataques que afectaron a Colombia en el año 2017 fueron: phishing, spam, malware y criptojacking. Especialistas en aspectos de seguridad informática consideran que las empresas colombianas han ido entendiendo la importancia que se le debe brindar a este tema, sin embargo, debido a la rápida evolución de las técnicas del cibercrimen consideran prudente llevar a cabo mayores esfuerzos económicos y técnicos para enfrentarlas y reducir su impacto.

- Entre los errores más comunes que cometen los usuarios de dispositivos móviles se encuentran: la instalación de aplicaciones de fuentes desconocidas, hacer clic en enlaces desconocidos, definición de contraseñas débiles, no activación de bloqueo de dispositivos, no instalación de software antivirus reconocido y llevar a cabo labores de Jailbreaking o Rooting.

- A la hora de identificar puntos a tener en cuenta para proteger los dispositivos móviles contra ataques y amenazas de diferentes índoles, algunas de las buenas

prácticas o recomendaciones a tener en cuenta para mitigarlas son: mantener actualizados tanto el sistema operativo como sus aplicaciones, descarga de aplicaciones de fuentes confiables, y mantener en lo posible deshabilitada la opción de ubicación del equipo y evitar las conexiones a Wi-Fi inseguras.

- La gran mayoría de soluciones de seguridad en el mercado actual ofrecen aplicaciones antirrobos, administración de contraseñas, y bloqueadores de aplicaciones. Esto para dejar claro que las compañías no ofrecen soluciones que ataques una falla o vulnerabilidad específica, sino que apuntan a cubrir un gran objetivo definido como lo es brindar seguridad a los equipos móviles de sus clientes en diferentes escenarios a los que se enfrenten en la vida cotidiana.

- Tratando en tema de la distribución del mercado de los dispositivos móviles en lo que tiene que ver con los sistemas operativos dominantes, las estadísticas muestran que la mayor parte se encuentra distribuido entre las plataformas Android y IOS. Tomando como punto de comparación las ventas por fabricantes a nivel mundial los principales contendores en este mercado son Samsung y Apple.

7. BIBLIOGRAFIA

¿Cuánta información personal entrega cuando utiliza una aplicación?[en línea].En Revista Semana.30 de Enero de 2014.p.1-5.[Consultado:26 de Septiembre de 2018].Disponible en Internet: https://www.semana.com/tecnologia/tips/articulo/cuanta-informacion-personal-entrega-cuando-utiliza-aplicacion/375589-3

3 biggest security threats for Android users today [en línea]. Kim Komando.[Consultado:23 de Septiembre de 2018].Disponible en Internet: https://www.komando.com/tips/382348/3-biggest-security-threats-for-android-users-today

33 ataques por segundo: Kaspersky Lab registra un aumento del 59% en ataques de malware en América Latina [en línea]. Kaspersky Latinoamérica. [Consultado: 25 de abril de 2018]. Disponible en Internet: https://latam.kaspersky.com/about/press-releases/2017_33-attacks-per-second-increase-in-malware-attacks-in-latin-america

5 Major Benefits of Android App Development For Your Business [en línea]. Rishbash Software Blog.12 de Diciembre de 2017.[Consultado:26 de Agosto de 2018].Disponible en Internet: https://www.rishabhsoft.com/blog/5-advantages-of-android-app-development-for-your-business

5 mobile threats you should shut down in 2018 [en línea].Tektonika.[Consultado:21 de Septiembre de 2018].Disponible en Internet: https://www.tektonikamag.com/index.php/2018/05/04/5-mobile-threats-you-should-shut-down-in-2018/

A Whale of a Tale: HummingBad Returns [en línea].Checkpoint Blog. 23 de Enero de 2017.párr. 1.[Consultado:12 de Septiembre de 2018].Disponible en Internet: https://blog.checkpoint.com/2017/01/23/hummingbad-returns/

ACHIARI,Santiago. Ahora USSD Control está incluido en todos los productos de ESET [en línea]. ESET Latinoamérica.(25 de Marzo de 2013).[Consultado: 24 de Septiembre de 2018]. Disponible en Internet: http://www.somoseset.com/2013/03/25/ussd-control-incluido-productos-eset/

ALARCON,Jose Manuel. ¿Qué es la máquina virtual de Java o Java Virtual Machine? [en línea] Campus MPV. (23 de Octubre de 2017).[Consultado:23 de Agosto de 2018].Disponible en Internet: https://www.campusmvp.es/recursos/post/que-es-la-maquina-virtual-de-java-o-java-virtual-machine.aspx

Amenazas de seguridad móvil dirigidas a dispositivos Android [en línea]. Kaspesky Latinoamérica. Consultado: [1 de Septiembre de 2018]. Disponible en Internet: https://latam.kaspersky.com/resource-center/threats/mobile

ANDRES,Ruben. Estos son los 7 mejores antivirus gratis para Android de 2018[en línea].En Computer Hoy.28 de Marzo de 2018.[Consultado:15 de Septiembre de 2018].Disponible en: https://computerhoy.com/listas/moviles/estos-son-7-mejores-antivirus-gratis-android-2018-78199

Android OS Documentation[en línea].Read the Docs.[Consultado:7 de Abril de 2018[.Disponible en Internet: https://media.readthedocs.org/pdf/androidos/latest/androidos.pdf

Android Threats [en línea].Zonealarm. [Consultado:12 de Septiembre de 2018]. Disponible en Internet: https://www.zonealarm.com/mobile-security/android/threats/

Android through the years [en línea].Cnet.[Consultado: 2 de Septiembre de 2018]. Disponible en Internet: https://www.cnet.com/pictures/google-android-versions-history/

ARIAS, Ximena. Del 1 al 8: La evolución del sistema operativo IOS [en línea]. Revista Enter. (17 de Septiembre de 2014).[Consultado: 23 de Mayo de 2018]. Disponible en Internet: http://www.enter.co/especiales/vida-digital/del-1-al-8-la-evolucion-del-sistema-operativo-ios/

Ataque de arranque en frío (cold boot attack) [en línea]. Guías practicas [Consultado: 21 de Septiembre de 2018]. Disponible en Internet: http://www.guiaspracticas.com/recuperacion-de-datos/ataque-de-arranque-en-frio-cold-boot-attack

AVG AntiVirus 2018 [en línea].AVG Latinoamérica.[Consultado:2 de Octubre de 2018].Disponible en Internet: https://www.avg-la.com/avg-antivirus/

AZOKAN,Ajin. Android Architecture From a Developer's Perspective [en línea].ApkChef.(23 de Diciembre de 2016).[Consultado:3 de Mayo de 2018].Disponible en Internet: https://www.apkchef.net/2016/12/android-architecture.html

BACH, Michael. IPhone vs. Android: What are the pros and cons?[en línea].Quora.(27 de Febrero de 2016).[Consultado: 24 de Abril de 2018].Disponible en Internet: https://www.quora.com/IPhone-vs-Android-What-are-the-pros-and-cons

BAGCHI, Apeksha. The evolution of Android [en línea].Yaabot.(1 de Junio de 2017).[Consultado:14 de Octubre de 2018]. Disponible en Internet: https://www.yaabot.com/30831/the-evolution-of-android/

BANSAL,Gaurav. Android Runtime Improvements [en línea].MindOrks.(9 de Mayo de 2018).[Consultado: 1 de Octubre de 2018]. Disponible en Internet: https://medium.com/mindorks/android-runtime-improvements-e69bf7c1d10c

Best Practices: Securing Your Mobile Device [en línea].Trend Micro. [Consultado: 24 de Septiembre de 2018]. Disponible en Internet: https://www.trendmicro.com/vinfo/us/security/news/mobile-safety/best-practices-securing-your-mobile-device

BETANCUR JARAMILLO, Oscar y ERAZO HANRRYR, Sonia Elizabeth. Seguridad en dispositivos móviles Android [en línea]. Monografía presentada para optar el título de: Especialista en Seguridad Informática. Universidad Nacional Abierta y a Distancia – UNAD. Escuela de Ciencias Básicas, Tecnología e Ingeniería,2015. 109 p. [Consultado: 12 de Enero de 2018]. Disponible en Internet: https://stadium.unad.edu.co/preview/UNAD.php?url=/bitstream/10596/3614/1/59836994.pdf

BLANCCO TECHNOLOGY GROUP. Trend Report: Q2 2017 State of Mobile Device Performance and Health [en línea]. Blancco (Septiembre de 2017). [Consultado:11 de Septiembre de 2018].Disponible en Internet: https://download.blancco.com/download/en-rs-q2-2017-state-of-mobile-device-performance-report.pdf

BLAS,Erika. Arquitectura y Entorno de Desarrollo de Aplicaciones Móviles [en línea].Blog de Erika Blas. 26 de Mayo de 2014.[Consultado:19 de Marzo de 2018].Disponible en Internet: http://erykabp.blogspot.com/2014/05/arquitectura-y-entorno-de-desarrollo-de.html

CABALLERO, Alejandro. Seguridad en el desarrollo de aplicaciones móviles: los 5 mayores riesgos [en línea]. Blog seguridad desarrollo de aplicaciones moviles-mayores riesgos.(8 de Marzo de 2018).[Consultado:3 de Abril de 2018].Disponible en Internet: https://kingofapp.es/blog/seguridad-desarrollo-aplicaciones-moviles-mayores-riesgos/

CARLON, Kris. Which Android manufacturer updates its phones the fastest?[en línea] Android Authority.(14 de Enero de 2017).[Consultado:24 de Septiembre de 2018].Disponible en Internet: https://www.androidauthority.com/android-oem-update-speed-743073/

CASSAVOY, Lianne. What Does It Mean to Jailbreak an iPhone? [en línea].Lifewire.(12 de Mayo de 2018).[Consultado: 20 de Mayo de 2018].Disponible en Internet: https://www.lifewire.com/what-is-jailbreaking-an-iphone-577591

CHUNG, Ek. Evolution of Android Homescreen and Navigation [en línea].Google Design.(15 de Mayo de 2018).párr. 14.[Consultado:14 de Octubre de 2018]. Disponible en Internet: https://medium.com/google-design/evolution-of-android-homescreen-and-navigation-bad189d536f2

CLULEY, Graham. The latest iPhone lock screen bypass, and how to stop it [en línea].Integro (12 de Mayo de 2014).[Consultado:26 de Septiembre de 2018].Disponible en Internet: https://www.intego.com/mac-security-blog/iphone-lock-screen-bypass/

Cocoa Applicatuion Layer. Apple Developer.[Consultado 28 de Agosto de 2018]. Disponible en Internet: https://developer.apple.com/library/archive/documentation/MacOSX/Conceptual/OSX_Technology_Overview/CocoaApplicationLayer/CocoaApplicationLayer.html

Colombia es el sexto país en Latinoamérica con mayor número de Ciberataques [en línea]. Colombia. Bogotá. (2 de Mayo de 2018).párr. 4. [Consultado: 26 de Septiembre 2018]. Disponible en Internet: https://www.colombia.com/tecnologia/internet/colombia-es-el-sexto-pais-en-latinoamerica-con-mayor-numero-de-ciberataques-188870

Colombia es el tercer país de América Latina con más ciberataques [en línea]. En: el Tiempo.11 de Septiembre de 2017.[Consultado:26 de Septiembre de

2018].Disponible en Internet: https://www.eltiempo.com/tecnosfera/paises-latinoamericanos-en-ciberseguridad-129604

CONDE, Rita. Redes de telefonía celular ¿Qué significan 1G, 2G, 3G y 4G? [en línea]. About Español. (24 de abril de 2016). [Consultado: 1 de Septiembre de 2018]. Disponible en Internet: https://www.aboutespanol.com/redes-de-telefonia-celular-que-significan-1g-2g-3g-y-4g-580779

COSTELLO, Katie y HIPPOLD Sarah Cornelia. Gartner Says Worldwide Sales of Smartphones Returned to Growth in First Quarter of 2018[en línea]. Gartner ,Egham, U.K. (29 de Mayo de 2018).párr 1.[Consultado:14 de Septiembre de 2018].Disponible en Internet: https://www.gartner.com/newsroom/id/3876865

COSTELLO, Sam. Do These 7 Things to Make Your iPhone More Secure [en línea].Lifewire.(28 de Agosto de 2018).[Consultado: 26 de Septiembe de 2018].Disponible en Internet: https://www.lifewire.com/tips-to-improve-iphone-security-2000265

Cuál es el mejor sistema operativo para un smartphone?[en línea].Informática hoy.[Consultado: 3 de Septiembre de 2018].Disponible en Internet: https://www.informatica-hoy.com.ar/soluciones-moviles/Cual-es-el-mejor-sistema-operativo-para-un-smartphone.php

DANIEL, Jo. 10 Common Smartphone mistakes that expose you to security risks [en línea].Information Nigeria.(12 de Diciembre de 2016).[Cosultado:27 de Septiembre de 2018].Disponible en Internet: http://www.informationng.com/2016/12/10-common-smartphone-mistakes-expose-security-risks.html

DARMON,Luc. Protect Mobile In-Store Payments From Relay Attacks [en línea].Apparel Magazine.(12 de Septiembre de 2014).[Consultado:22 de

Septiembre de 2018].Disponible en Internet: https://apparelmag.com/protect-mobile-store-payments-relay-attacks

DAVI, Lucas Vincenzo. Code-Reuse Attacks and Defenses [en línea].Tesis para obtener el título de Doctorado en filosofía (PHD). Duisburgo, Alemania. Universidad Técnica de Darmstadt. Departamento de Ciencias

DCIT. Security assesment of mobile applications (iOS, Android)[en línea].[Consultado:20 de Marzo de 2018].Disponible en Internet: https://www.dcit.cz/en/security/mobile-applications-security

DE LOOPER,Christian. From Android 1.0 to Android 7.0, here's how the top mobile OS has evolved over the years [en línea]. Yahoo Finance .(4 de Septiembre de 2018).[Consultado:3 de Septiembre de 2018] . Disponible en Internet: https://finance.yahoo.com/news/android-1-0-android-9-192746756.html

EDMOND , Ramin Users are biggest impediment to Apple iOS security.[en línea]. SearchMobileComputing.(31 de julio de 2017) [Consultado: 1 de septiembre de 2018]. Disponible en Internet: https://searchmobilecomputing.techtarget.com/news/450423643/Users-are-biggest-impediment-to-Apple-iOS-security

Encuesta Anual de Seguridad de la información en: EY Colombia.2016. Citado por:

ESET Security Report Latinoamérica 2018 [en línea]. [Consultado: 27 de Septiembrre de 2018]. Disponible en Internet: https://www.welivesecurity.com/la-es/2018/06/19/eset-security-report-2018-el-estado-de-la-seguridad-de-la-informacion-en-las-empresas-de-la-region/

ESET Security Report Latinoamérica 2017 [en línea].ESET Latinoamérica.[Consultado: 27 de Septiembrre de 2018]. Disponible en Internet:

https://www.welivesecurity.com/wp-content/uploads/2017/04/eset-security-report-2017.pdf

Evolución de la red de comunicación móvil, del 1G al 5G [en línea].Universidad Internacional de Valencia.[Consultado el 1 de Septiembre de 2018]. Disponible en Internet: https://www.universidadviu.com/evolucion-la-red-comunicacion-movil-del-1g-al-5g/

Evolution of Android OS [en línea].Spinfold.[Consultado:1 de Septiembre de 2018]. Disponible en Internet: http://www.spinfold.com/evolution-of-android-os/

FERNANDEZ CASTRILLO, Alejandro. Medidas de protección frente ataques de denegación de servicio (DoS) [en línea]. Centro de Respuesta a incidentes de Seguridad e Industria CERTSI. España.(26 de Enero de 2018).[Consultado:11 de Septiembre de 2018].Disponible en Internet: https://www.certsi.es/blog/medidas-proteccion-frente-ataques-denegacion-servicio-dos

FLORES, Javier. ¿Qué es lo que más preocupa a quienes usan Smartphone Android? [en línea]. Revista Muy Interesante.[Consultado: 15 de Abril de 2018].Disponible en Internet: https://www.muyinteresante.es/curiosidades/preguntas-respuestas/ique-es-lo-que-mas-preocupa-a-quienes-usan-smartphones-android

Funciones de Norton Snap[en línea]Norton.[Consultado:4 de Octubre de 2018]. Disponible en Internet: https://support.norton.com/sp/es/mx/home/current/solutions/v64690996_EndUserProfile_es_mx

GIUSTO BILIĆ, Denise. Balance semestral de la seguridad móvil [en línea].Welivesecurity.(6 de Agosto de 2018).[Consultado:29 de Septiembre de 2018].Disponible en Internet: https://www.welivesecurity.com/la-es/2018/08/06/balance-semestral-seguridad-movil/

Global Cyber Attack Trends Report[en línea].Checkpoint Research.[Consultado:28 de Septiembre de 2018].Disponible en Internet: https://www.checkpoint.com/downloads/product-related/infographic/H2_2017_Global_Cyber_Attack_Trends_Report.pdf?mkt_tok=eyJpIjoiTW1FMlpXUTBaREZqWXpSbCIsInQiOiJTYzFzV1UxWVdTc2pOa24yeHh3aXZodEcwZ2czMnlOQnhHRlJcL3l6ZHI3YjRpUU9mbXpra1BtN3FjUnlNZzRGb3ByVDVWdzdhMythZjRWbThYQnk0dFFEQ1NyXC9JSWVcL1FzejZhcjRodzdlaE8zNExcL3FPeDlGSk5UMDRua2tGbTEifQ%3D%3D

GOASDUFF, Laurence y FORNI Amy Ann. Gartner Says Worldwide Sales of Smartphones Grew 7 Percent in the Fourth Quarter of 2016.[en línea]. Gartner, Egham, U.K. (15 de Febrero de 2017).[Consultado:12 de Septiembre de 2018].Disponible en Internet: https://www.gartner.com/en/newsroom/press-releases/2017-02-15-gartner-says-worldwide-sales-of-smartphones-grew-7-percent-in-the-fourth-quarter-of-2016

GOLDMAN,Jeff. Top 20 Android Security Apps [en línea]. eSecurityPlanet.(27 de Octubre de 2015).[Consultado:1de Octubre de 2018]. Disponible en Internet: https://www.esecurityplanet.com/mobile-security/top-20-android-security-apps.html

GONDI, Tilakkumar. IOS – Architecture [en línea]. Tilakgondi Page.(14 de Enero de 2015).[Consultado:13 de Octubre de 2018].Disponible en Internet: https://tilakgondi.wordpress.com/2015/01/14/ios-architecture/

GONZALEZ FERNANDEZ, Alfonso. Seguridad en Smartphone. Análisis de riesgos, de vulnerabilidades, y auditorias de dispositivos [en línea]Trabajo final para obtener el título de Master Interuniversitario de Seguridad en las Tecnologías de la Información y de las Comunicaciones (MISTIC). Universidad Abierta de Cataluña,2018,121 p. [Consultado: 26 de Septiembre de 2018]. Disponible en Internet:http://openaccess.uoc.edu/webapps/o2/bitstream/10609/72966/6/agonzalezfernandez3TFM0118Memoria.pdf

GORDON, Whitson. Everything You Need to Know About Rooting Your Android Phone [en línea]. Lifehacker.(9 de Abril de 2013).[Consultado:2 de Septiembre de

2018].Disponible en Internet: https://lifehacker.com/5789397/the-always-up-to-date-guide-to-rooting-any-android-phone

GUEVARA BENAVIDES, Lina María. Empresas colombianas deben invertir más en ciberseguridad [en línea].La República.p.2-4.[Consultado:25 de Septiembre de 2018].Disponible en Internet: https://www.larepublica.co/consumo/empresas-colombianas-deben-invertir-mas-en-ciberseguridad-2464836

Guía de Seguridad Informática. En Internet, el mejor sistema de seguridad eres tú ¡protégete! [en línea]. Blog Andalucía es digital.30 de noviembre de 2016. [Consultado: 1 de Septiembre de 2018].Disponible en Internet: https://www.blog.andaluciaesdigital.es/guia-de-seguridad-informatica/

Guía de Seguridad para usuarios de Smartphones. [en línea]. ESET Latinoamérica [Consultado: 20 de Abril de 1918]. Disponible en Internet: https://www.welivesecurity.com/wp-content/uploads/2014/01/documento_guia_de_seguridad_para_usuarios_de_smartphone_baj.pdf

Gustavo. Kaspersky Lab registra un alza de 60% en ataques cibernéticos en América Latina [en línea]. Kaspersky Lab Latinoamérica.(14 de Agosto de 2018).[Consultado:28 de Septiembre de 2018].Disponible en Internet: https://latam.kaspersky.com/blog/kaspersky-lab-registra-un-alza-de-60-en-ataques-ciberneticos-en-america-latina/13266/

GUTIERREZ, Javier J. Qué es un framework web [en línea].Universidad de Sevilla. España.[Consultado: 2 de Mayo de 2028]. Disponible en Internet: http://www.lsi.us.es/~javierj/investigacion_ficheros/Framework.pdf

HEIN, Buster. The evolution of iOS: From iPhone OS to iOS 11 [en línea].Cult of Mac.(24 de Mayo de 2017). [Consultado:2 de Septiembre de 2018].Disponible en Internet: https://www.cultofmac.com/488454/ios-evolution-iphone-os/

HEISLER, Yoni. The history and evolution of iOS, from the original iPhone to iOS 9 [en línea]. Brg.(12 de Febrero de 2016).[Cosultado:29 de Septiembre de 2018] Disponible en Internet: https://bgr.com/2016/02/12/ios-history-iphone-features-evolution/

HilI, Simon. The best security apps and antivirus protection for Android [en línea]. Digital Trends.(26 de Abril de 2018).[Consultado:2 de Octubre de 2018].Disponible en Internet: https://www.digitaltrends.com/mobile/best-antivirus-protection-for-android/

HILL,Simon. Android vs. iOS: Which smartphone platform is the best?[En línea].Digital Trends.(7 de Marzo de 2018).[Consultado:8 de Septiembre de 2018].Disponible en Internet: https://www.digitaltrends.com/mobile/android-vs-ios/

HOPPING, Clare. Android vs iOS: which mobile OS is right for you? [En línea]. ITPRO Analysis Business Insigth.(31 de Agosto de 2018).[Consultado:7 de Septiembre de 2018],Disponible en Internet: http://www.itpro.co.uk/mobile/30409/android-vs-ios-which-mobile-os-is-right-for-you

IDC. Smartphone Volumes Expected to Rebound in 2017 with a Five-Year Growth Rate of 3.8%, Driving Annual Shipments to 1.53 Billion by 2021, According to IDC [en línea]. International Data Corporation (IDC).(1 de Marzo de 2017).párr.1.[Consultado:9 de Septiembre de 2018].Disponible en Internet: https://www.idc.com/getdoc.jsp?containerId=prUS42334717

Informe balance cibercrimen en Colombia 2017[en línea]. Centro Cibernético Policial. [Consultado:3 de Septiembre de 2018]. Disponible en: https://caivirtual.policia.gov.co/sites/default/files/informe_cibercrimen_2017.pdf

Informe sobre amenazas para la seguridad en Internet [en línea]. Symantec. [Consultado; 20 de Abril de 2018]. Disponible en Internet: https://www.symantec.com/content/dam/symantec/mx/docs/reports/istr-23-executive-summary-mx.pdf

Informe Sobre las Amenazas para la Seguridad en Internet Volumen 23[en línea].Symantec.[Consultado:27 de Septiembre de 2018].Disponible en Internet: http://images.mktgassets.symantec.com/Web/Symantec/%7B3eb3b2d7-76de-484e-951f-e903d31ea889%7D_ISTR23-FINAL_ES.pdf

Internet Security Threat Report [en línea].Symantec. [Consultado:17 de Septiembre de 2018]. Disponible en Internet: https://www.symantec.com/content/dam/symantec/docs/reports/istr-23-2018-en.pdf

iOS Architecture [en línea].Intellipaat.[Consultado:28 de Agosto de 2018].Disponible en Internet: https://intellipaat.com/tutorial/ios-tutorial/ios-architecture/

ISMAIL, Nick. Common security vulnerabilities of mobile devices [en línea].InformationAge.(21 de Febrero de 2017).[Consultado:22 de Septiembre de 2018].Disponible en Internet: https://www.information-age.com/security-vulnerabilities-mobile-devices-123464616/

IT BUSINESS SOLUTIONS. ¿Cuáles son los vectores de ataque que usan los delincuentes informáticos?[en línea].[Consultado:13 de Septiembre de 2017].Disponible en Internet: https://www.itbusiness-solutions.com.mx/vectores-de-ataque-de-ciberdelincuentes

JR, Rafael. 5 mobile security threats you should take seriously in 2018 [en línea]. CSO.(13 de Diciembre de 2017).[Consultado:17 de Septiembre de 2018].Disponible en Internet: https://www.csoonline.com/article/3241727/mobile-security/5-mobile-security-threats-you-should-take-seriously-in-2018.html

JR,Raphael. Android versions: A living history from 1.0 to Pie [en línea].Computerworld.(7 de Agosto de 2018),párr.14.[Consultado:13 de Octubre de 2018]. Disponible en Internet: https://www.computerworld.com/article/3235946/android/android-versions-a-living-history-from-1-0-to-today.html?page=2

JULES,Javier. Cibercriminales también pueden robar los datos de celulares y tabletas a través de un mensaje [en línea].RCN Radio.(27 de Junio de 2017). [Consultado: 1 de Octubre de 2017]. Disponible en Internet: https://www.rcnradio.com/mcontent/5b36d2435f0049e5d1302823/amp

KALLIN Jakob y LOBO VALBUENA Irene. Excess XSS A comprehensive tutorial on cross-site scripting [en línea] Excess XSS. [Consultado: 23 de Septiembre de 2018]. Disponible en Internet: https://excess-xss.com/

Kaspersky Lab registra un alza de 60% en ataques cibernéticos en América Latina [en línea].Blog Kaspersky Lab Latinoamérica.14 de Agosto de 2018. [Consultado: 27 de Septiembre de 2018]. Disponible en Internet: https://latam.kaspersky.com/blog/kaspersky-lab-registra-un-alza-de-60-en-ataques-ciberneticos-en-america-latina/13266/

Kaspersky Lab: Brasil, México y Colombia lideran incidentes de secuestros digitales en América Latina [en línea] Kaspersky Lab Latinoamérica.(18 de Septiembre de 2017).[Consultado:27 de Septiembre de 2018].Disponible en Internet: https://latam.kaspersky.com/about/press-releases/2017_kaspersky-lab-incidents-of-digital-kidnappings-in-latin-america

KATARIYA,Jayanti. Apple Vs Android - A comparative study 2017[En línea] Mobile Apps Channel.27 de Febrero de 2017.[Consultado:12 ad Abril de 2018].Disponible en Internet: https://www.whatech.com/mobile-apps/blog/archive/267836-apple-vs-android-a-comparative-study-2017

KOVACS, Nadia. ¿Qué es Grayware, Adware y Madware?[en línea]. Norton Protection Blog. 7 de abril de 2016. Consultado: [20 de abril de 2018]. Disponible en Internet: https://community.norton.com/es/blogs/norton-protection-blog/%C2%BFqu%C3%A9-es-grayware-adware-y-madware

La Computación,2015.189 p. [Consultado: 23 de Septiembre de 2018]. Disponible en Internet: http://tuprints.ulb.tu-darmstadt.de/4622/7/Davi-PhD-Code-Reuse-Attacks-and-Defenses.pdf

LA PORTA,Liarna. Malicious profiles – one of the most serious threats to IPhones [en línea].Wandera.(14 de Abril de 2018).[Consultado: 3 de Octubre de 2018].Disponible en Internet: https://www.wandera.com/malicious-profiles-come/

Las empresas colombianas escatiman en gastos y se rajan en ciberseguridad [en línea] En Revista Dinero. Enero, 2017,p.2-5.[Consultado 30 de Septiembre de 2018].Disponible en Internet: https://www.dinero.com/empresas/articulo/encuesta-anual-de-seguridad-de-la-informacion-de-la-firma-ey/241201

LORD,Nat, Social Engineering Attacks: Common Techniques & How to Prevent an Attack [en línea].DigitalGuardian.(19 de Septiembre de 2018).[Consultado:21 de Septiembre de 2018].Disponible en Internet: https://digitalguardian.com/blog/social-engineering-attacks-common-techniques-how-prevent-attack

LVDAQIAN ,Darwin. Mobile Security Primer[en línea]. GitHub, Inc.(3 de Marzo de 2017), párr. 2.[Consultado: 24 de Marzo de 2018].Disponible en Internet: https://github.com/nowsecure/secure-mobile-development/blob/master/en/primer/mobile-security.md

LYN, La. Android through the years [diapositivas].Cnet.22 de Febrero de 2016, 15 diapositivas. [Consultado: 2 de Septiembre de 2018]. Disponible en Internet: https://www.cnet.com/pictures/google-android-versions-history/

MEDINA, Edgar. Cinco mitos y verdades sobre la batería de su celular [en línea]. En El Tiempo.(16 de Febrero de 2017)[Consultado: 23 de Agosto de 2018]. Disponible en Internet: https://www.eltiempo.com/tecnosfera/tutoriales-tecnologia/cinco-mitos-y-verdades-sobre-la-bateria-de-su-celular-59543

MENDOZA,Azury. ¿A qué se le conoce como vectores de ataque en ciberseguridad y cómo puedes eliminarlos de tus ambientes digitales? [en línea]. GB Advisors.(2 de Mayo de 2018).[Consultado:13 de Septiembre de 2018].Disponible en Internet: http://www.gb-advisors.com/es/vectores-de-ataque-en-ciberseguridad/

MITROFF,Sarah. La seguridad es clave [diapositivas].CNet.3 de Marzo de 2016, 8 diapositivas.[Consultado:26 de Septiembre de 2018].Disponible en Internet: https://www.cnet.com/es/imagenes/errores-seguridad-telefono/5/

Mobile security threats in Android [en línea]. TechAdvisory.[Consultado:23 de Septiembre de 2018].Disponible en Internet: https://www.techadvisory.org/2017/06/mobile-security-threats-in-android/

Mobility, performance and engagement How CIOs can contribute to business performance by shaping the employee experience [en línea]. The Economist Intelligence Unit.[Consultado:17 de Septiembre de 2018].Disponible en Internet: https://www.arubanetworks.com/pdf-viewer/?q=/assets/EIUStudy.pdf

MON KYWE,Su. Mobile Threat Blog [en línea]. Appthority.32 de Mayo de 2018, párr. 1. [Consultado: 12 de Octubre de 2018].Disponible en Internet: https://www.appthority.com/mobile-threat-center/blog/ios-update-11-4-security-details/

Monográfico de seguridad en dispositivos móviles [en línea]. Instituto Nacional de Tecnologías de la Comunicación. [Consultado:15 de Marzo de 2018]. Disponible en Internet: https://www.firma-e.com/wp-content/uploads/2013/03/monografico_seg_disp_moviles.pdf

MOREAU, Sean. The evolution of iOS [diapositivas].Computerworld.6 de Junio de 2018,13 diapositivas.[Consultado:23 de Mayo de 2018].Disponible en Internet: https://www.computerworld.com/article/2975868/apple-ios/the-evolution-of-ios.html#slide4

MORILLO POZO, Julian David. Introducción a los dispositivos móviles [en línea].Universidad Abierta de Cataluña [Consultado:2 de Septiembre de 2018].Disponible en Internet: https://www.exabyteinformatica.com/uoc/Informatica/Tecnologia_y_desarrollo_en_dispositivos_moviles/Tecnologia_y_desarrollo_en_dispositivos_moviles_(Modulo_2).pdf

mSecure 5 [en línea].Msecure.[Consultado:3 de Octubre de 2018]. Disponible en Internet: https://www.msecure.com/

NAVARRO,Francis. Common security risks every smartphone user should know about [en línea].Kim Komando.(23 de Julio de 2017).[Consultado: 27 de Spetimbre de 2018].Disponible en Intenet: https://www.komando.com/tips/370318/common-security-risks-every-smartphone-user-should-know-about/all

Operating Systems [en línea]. BBC.[Consultado en: 3 de Septiembre de 2018].Disponible en Internet: https://www.bbc.com/bitesize/guides/ztcdtfr/revision/1

OWASP Mobile Security Project [en línea]. OWASP. [Consultado: 27 de Octubre de 2018]. Disponible en Internet: https://www.owasp.org/index.php/OWASP_Mobile_Security_Project#tab=Top_10_Mobile_Risks

PACHECO SEBASTIAN, Exequiel Y PIAZZA ORLANDO Carlos Damián. Estudio y análisis de seguridad en dispositivos móviles. BYOD y su impacto en las organizaciones [en línea]. Tesis presentada para optar al título de Licenciatura en Sistemas. La Plata, Argentina. Universidad Nacional de la Plata. Facultad de Informática, 2016. 139 p. [Consultado; 16 de abril de 2018]. Disponible en Internet: http://sedici.unlp.edu.ar/bitstream/handle/10915/58591/Documento_completo.%20y%20Piazza%20Orlando,%20C.%20Estudio%20y%20an%C3%A1lisis%20de%20seguridad%20en%20dispositivos%20m%C3%B3viles.pdf-PDFA.pdf?sequence=4&isAllowed=y

PADHYA, Bhargavi y DESAI, Prasad. Comparison of Mobile Operating Systems [en línea]. En: International Journal of Innovative Research in Computer and Communication Engineering. Agosto, 2016.vol 4 no 8, p.1-3.[Consultado: 3 de Septiembre de 2018]. Disponible en Internet: http://www.ijircce.com/upload/2016/august/132_Comparison.pdf.ISSN: 2320-9798.E-ISSN: 2320-9801

PAGANINI, Pierluigi. WireLurker, Masque: Every Apple iOS App Could Be Compromised [en línea]. Infosec Institute. (14 de Septiembre de 2018).[Consultado:28 de Septiembre de 2018].Disponible en Internet: https://resources.infosecinstitute.com/wirelurker-masque-every-apple-ios-app-compromised/#gref

PAINTER,Lewis. iPhone security tips: How to protect your iPhone from hackers [en línea]. Macworld.(2 de Mayo de 2018).[Consultado:26 de Septiembre de 2018].Disponible en Internet: https://www.macworld.co.uk/how-to/iphone/iphone-security-tips-3638233/

PHILLIPS Cassie. Five Immediate Threats to Android Security for 2016 and How to Eliminate Them [en línea].Appknox Blog.2016.[Consultado:22 de Septiembre de 2018].Disponible en Internet: https://blog.appknox.com/five-immediate-threats-android-security-2016-eliminate/

Por qué su empresa debe invertir en seguridad informática? [en línea].Adalid.[consultado:1 de Octubre de 2018].Disponible en Internet: http://www.adalid.com/por-que-su-empresa-debe-invertir-en-seguridad-informatica/

Por si Google fracasa: examinamos 21 aplicaciones de seguridad para Android.[en línea].AV-Test. [Consultado:3 de Octubre de 2018].Disponible en Internet: https://www.av-test.org/es/noticias/por-si-google-fracasa-examinamos-21-aplicaciones-de-seguridad-para-android/

PRICE, Dan. 7 iOS Settings to Change If You Want Better Privacy in Safari [en línea].MakeUseOf.(27 de Junio de 2018).[Consultado: 26 de Septiembre de 2018].Disponible en Internet: https://www.makeuseof.com/tag/change-ios-settings-privacy-safari/

PRICE, Dan. How to Fix 5 Common iPhone & iPad Security Threats [en línea].MakeUseOf.(26 de Enero de 2016).[Consultado: 22 de Septiembre de 2018].Disponible en Internet: https://www.makeuseof.com/tag/fix-5-common-iphone-ipad-security-threats/

RAMNATH, Rajib y LOFFING, Cheyney. Beginning IOS Programming For Dummies[en línea].New Jesey. 2014,423 p.[Consylado:1 de Septiembre de 2014].Disponible en Internet: https://books.google.com.co/books?id=8tIsAwAAQBAJ&pg=PA14&lpg=PA14&dq=core+os+layer&source=bl&ots=DCjP-btpm_&sig=fBWxkvI98Bd5zfYU--zX_m7jJI8&hl=es&sa=X&ved=2ahUKEwiegKrntpXdAhVrs1kKHSi2DNk4ChDoATAGegQIBBAB#v=onepage&q=core%20os%20layer&f=false

Ransomware [en línea].Avast .[Consultado:30 de Septiembre de 2018].Disponible

en Internet: https://www.avast.com/es-es/c-ransomware

RAWAT, Inder. Advantages And Disadvantages Of Android Phones [en línea]. OneWorldNews.(23 de Febrero de 2017).[Consultado:30 de Septiembre de 2018].Disponible en Internet: http://www.oneworldnews.com/advantages-and-disadvantages-of-android-phones/

RAY,Jhon. Sam Teach Yourself IOS 8 Application development in 24 hours.[en línea] Indiana.USA: Pearson.2015,863 p.[Consultado:1 de Septiembre de 2018].Disponible en Internet: https://books.google.com.co/books?id=FS75BgAAQBAJ&pg=PA120&lpg=PA120&dq=Cocoa+Touch+Layer&source=bl&ots=SjAJJmydTc&sig=j9DEa8ZAY3Mx7y-2FlF_A9gqtBg&hl=es&sa=X&ved=2ahUKEwj_yNS6gJHdAhVJ2lMKHUgSDyw4ChDoATAGegQIBBAB#v=onepage&q=Cocoa%20Touch%20Layer&f=true

RITCHER,Felix. The Smartphone Platform War Is Over [en línea].Statista.(20 de Febrero de 2017).[Consultado:11 de Septiembre de 2018].Disponible en Internet: https://www.statista.com/chart/4112/smartphone-platform-market-share/

RITCHIE,Rene. Six ways to increase your iPhone and iPad security in 2017 [en línea]. Imore. (4 de Enero de 2017).[Consuiltado:26 de Septiembre de 2018].Disponible en Internet: https://www.imore.com/6-ways-increase-iphone-ipad-security-privacy

RODRIGUEZ MOLINA, Carlos. Evolución de Android desde su creación a Android 8.0 [en línea]. Tu experto Tecnología. (4 de Agosto de 2017). [Consultado: 13 de Mayo de 2018].Disponible en Internet: https://www.tuexperto.com/2017/08/04/evolucion-de-android-desde-su-creacion-a-android-8-o/

SAVITSKY,Alex. Siete Aplicaciones De Seguridad Para Tu iPhone [en línea]. Kaspersky Labs.(21 de Abril de 2014).[Consultado:13 de Octubre de 2018].Disponible en Internet: https://latam.kaspersky.com/blog/siete-aplicaciones-de-seguridad-para-tu-iphone/2887/

SAXENA,Sobhit. Evolution from iPhone OS 1 to iOS 10 – Journey of iOS [en línea]. Mobiloitte Technologies.(14 Septiembre de 2016).[Consulado: 2 de Mayo de 2018]. Disponible en Internet: https://www.mobiloitte.com/blog/evolution-iphone-os-1-ios-10-journey-ios/

Sector financiero y de telecomunicaciones, los que más ataques cibernéticos reciben en Colombia [en línea]. Actualicese. [Consultado: 6 de Octubre de 2017]. Disponible en Internet: https://actualicese.com/actualidad/2018/10/04/sector-financiero-y-de-telecomunicaciones-los-que-mas-ataques-ciberneticos-reciben-en-colombia/

Seguridad en los Dispositivos Móviles [en línea]. Centro de Estudios, Respuesta y Tratamiento de Incidentes de Seguridad en Brasil. [Consultado: 15 de Abril de 2018]. Disponible en Internet: https://cartilla.cert.br/fasciculos/dispositivos-moviles/fasciculo-dispositivos-moviles-slides.pdf

SICILIANO; Robert. What is a Backdoor Threat?[en línea] McAfee.(12 de Mayo de 2014).[Consultado: 24 de Septiembre de 2018*.Disponible en Internet: https://securingtomorrow.mcafee.com/consumer/identity-protection/backdoor-threat/

SINGH, Arpit. Top 15 Mobiles Phones Operating Systems 2018 [en línea].Digital SEO Guide.(6 de Julio de 2018).[Consultado:3 de Septiembre de 2019].Disponible en Internet https://www.digitalseoguide.com/technology/top-mobile-phones-operating-systems-os/#7_Blackberry_OS

Singh, Karanpreet. 15 Best Security Apps That You Must Have In your iPhone 2018[en línea].Techviral.(29 de Junio de 2018).[Consultado:3 de Octubre de 2018]. Disponible en Internet: https://techviral.net/best-security-apps-iphone/

SKVOR, Michael. Keeping your Android safe this year [en línea] Blog Avast. 24 de Enero de 2018. [Consultado:30 de Abril de 2018]. Disponible en Internet: https://blog.avast.com/keeping-your-android-safe-this-year

SMITH, Dave, The 13 most useful features in iOS 11 [en línea].Business Insider.(16 de Mayo de 2018).[Consultado: 2 de Septiembre de 2018].Disponible en Internet: https://www.businessinsider.com/apple-ios-11-best-features-2017-7

Software Library [en línea].Techopedia.[Consutado:25 de Agosto de 2018].Disponible en Internet: https://www.techopedia.com/definition/3828/software-library

Sophos Mobile Security para Android. [en línea].Sophos. [Consultado:2 de Octubre de 2018].Disponible en Internet: https://www.sophos.com/es-es/products/free-tools/sophos-mobile-security-free-edition.aspx

STATISTA. Smartphones industry: Statistics & Facts[en línea].[Consultado:11 de Septiembre de 2018].Disponible en Internet: https://www.statista.com/topics/840/smartphones/

STORM Darlene y DAVIDSON Michelle. Easy way to bypass passcode lock screens on iPhones, iPads running iOS 12 [en línea].(18 de Septiembre de 2018). [Consultado:10 de Octubre de 2018]. Disponible en Internet: https://www.computerworld.com/article/3041302/security/4-new-ways-to-bypass-passcode-lock-screen-on-iphones-ipads-running-ios-9.html

SYED FARHAN, Alam Zaidi, et al. A Survey on Security for Smartphone Device [en línea]. En (IJACSA) International Journal of Advanced Computer Science and Applications,2016, Vol. 7, No. 4, p.210-213.[Consultado:27 de Septiembre de 2018].Disponible en Internet: http://thesai.org/Downloads/Volume7No4/Paper_26-A_Survey_on_Security_for_Smartphone_Device.pdf

TEAM COUNTERPOINT. Global Smartphone Market Share: By Quarter [en línea].Countpoint.(16 de Mayo de 2018).[Consultado:10 de Septiembre de 2018].Disponible en Internet: https://www.counterpointresearch.com/global-smartphone-share/

The Mobile Economy 2018. GSMA Association [en línea].[Consultado:7 de Septiembre de 2018].Disponible en Internet: https://www.gsma.com/mobileeconomy/wp-content/uploads/2018/02/The-Mobile-Economy-Global-2018.pdf

The Mobile Economy 2018.[en línea].GSMA Association. [en línea]. [Consultado:3 de Octubre de 2018].Disponible en Internet http://www.redestelecom.es/siteresources/files/843/44.pdf

The Risks of “Jailbreaking” and “Rooting” Mobile Devices[en línea].[Consultado:28 de Septiembre de 2018].Disponible en Internet: https://www.firstcountybank.com/sites/default/files/pdfs/Jailbroken%20and%20Rooted%20Devices%20Fraud%20Risks.pdf

Threats to iOS Mobile Devices [en línea] Laccon Movile Security.[Consultado: 24 de Septiembre de 2018].(Agosto de 2014).Disponible en Internet: https://idency.com/wp-content/uploads/2014/08/Lacoon-White-Paper-iOS-Threats.pdf

TRAVIS,May. IOS, Android or Windows: what’s the best mobile operating system? [en línea]. The Whiz Cells.(17 de Febrero de 2017).párr.20.[Consultado:4 de Septiembre de 2018]. Disponible en: https://www.thewhizcells.com/ios-android-windows-whats-best-mobile-operating-system/

TREND MICRO. 7 Ways to Improve Security on Your iOS Device . [en línea].Trend Micro. [Consultado: 26 de Septiembre de 2018]. Disponible en Internet: https://www.trendmicro.com/vinfo/us/security/news/mobile-safety/7-ways-to-improve-security-on-ios-device

TRIGGS, Robert. Best Android security practices [en línea]. Android Authority.(30 de Junio de 2016).[Consultado:26 de Septiembre de 2018].Disponible en Internet: https://www.androidauthority.com/best-android-security-practices-700393/

TUTORIALPOINTS. Mobile Security - Attack Vectors[en línea].[Consultado:24 de Marzo de 2018].Disponible en Internet: https://www.tutorialspoint.com/mobile_security/mobile_security_attack_vectors.htm

UMAWING, Jovi. When three isn't a crowd: Man-in-the-Middle (MitM) attacks explained [en línea]. MalwareBytes Labs Bog.12 de Julio de 2018. [Consultado: 17 de Octubre de 2018].Disponible en Internet: https://blog.malwarebytes.com/101/2018/07/when-three-isnt-a-crowd-man-in-the-middle-mitm-attacks-explained/

VALERY,Yolanda. Qué es el virus HummingBad que afecta millones de teléfonos Android [en línea].BBC News.(6 de Julio de 2016).[Consultado: 23 de Septiembre de 2018]. Disponible en Internet: https://www.bbc.com/mundo/noticias-36726332

VAN ALLEN,Fox. The evolution of Apple iOS [diapositivas].Cnet.1 de Julio de 2017, 25 dispositivas .[Consultado: 25 de Mayo de 2018]. Disponible en Internet: https://www.cnet.com/pictures/the-evolution-of-apple-ios/8/

VAN DER MEULEN, Rob y MCCALL, Thomas .Gartner Says Worldwide Sales of Smartphones Recorded First Ever Decline During the Fourth Quarter of 2017.[en línea].Gartner, Egham, UK.(22 de Febrero de 2018). [Consultado: 26 de Abril de 2018]. Disponible en Internet: https://www.gartner.com/en/newsroom/press-

releases/2018-02-22-gartner-says-worldwide-sales-of-smartphones-recorded-first-ever-decline-during-the-fourth-quarter-of-2017

VANEGAS, Carlos Alberto. Android…. De que me hablan?[en línea]Revistas Udistrital.(Agosto de 2013) [Consultado:16 de Marzo de 2018].Disponible en Internet: http://revistas.udistrital.edu.co/ojs/index.php/vinculos/article/view/8022/9631%20una

VAUGHAN-NICHOLS, Steven J [en línea].ZDNet.(1 de Marzo de 2018). [Consultado: 25 de Septiembre de 2018]. Disponible en Internet: https://www.zdnet.com/article/the-ten-best-ways-to-secure-your-android-phone/

Ventajas e inconvenientes del sistema operativo iOS [en línea].Blog BeMovil.2 de Agosto de 2015.[Consultado: 11 de Septiembre de 2018].Disponible en Internet: https://www.bemovil.es/blog/ventajas-sistema-operativo-ios/

VISWANATHAN, Pryya. What Is a Mobile Device?[en línea].Lifewire.(13 de Mayo de 2018).[Consulado: 26 de Mayo de 2018].Disponible en Internet: https://www.lifewire.com/what-is-a-mobile-device-2373355.

VORA,Lopa. Evolution of mobile generation technology: 1G to 5G and review of upcoming wireless technology 5G [en línea]. En: International Journal of Modern Trends in Engineering and Research. Octubre de 2015, vol 2, no 10, p.1-5. [Consultado: 1 de Septiembre de 2018]. ISSN: 2349-9745. Disponible en Internet: https://pdfs.semanticscholar.org/4dfd/40cc3a386573ee861c5329ab4c6711210819.pdf.

WALLEN, Jack. 10 things you can do to make Android more secure [en línea]. TechRepublic (17 de Junio de 2014).[Consultado:25 de Septiembre de 2018]. Disponible en Internet: https://www.techrepublic.com/blog/10-things/10-things-you-can-do-to-make-android-more-secure/

Wickr Me – Private Messenger [en línea].Apple Store.[Consultado:3 de Octubre de 2018].Disponible en Internet: https://itunes.apple.com/us/app/wickr-me-private-messenger/id528962154?mt=8

WILLIAMS,Mat. Zero day vulnerabilities: how do you stop a threat you can't see coming? [en línea].Faraonics.(20 de Abril de 2017). [Consultado: 11 de Octubre de 2018].Disponible en Internet: https://www.faronics.com/news/blog/zero-day-vulnerabilities-stop-threat-cant-see-coming

XcodeGhost: qué es y cómo evitarlo. Fin de la invulnerabilidad de Apple [en línea].Panda Security.[Consultado:24 de Septiembre de 2018]. Disponible en Internet: https://www.pandasecurity.com/spain/mediacenter/noticias/xcodeghost-malware-apple/

ANEXOS

Anexo A Formato RAE

Fecha de Realización: 12/03/2019
Título: ESTADO DEL ARTE VULNERABILIDADES DE SEGURIDAD EN SISTEMAS OPERATIVOS MÓVILES ANDRIOID Y IOS
Autor: MUÑOZ CACERES, YAMIR ASMIRIO
Palabras Claves: Android, OIS, Jailbreak, rootear, malware, pishing, ingeniería social, Ataques XXS
Descripción: El auge de los dispositivos móviles en la actualidad hace que muchas personas los consideren parte fundamental de sus labores diarias, tanto a nivel personal como a nivel laboral. Sus funcionabilidades, sus portabilidad y facilidad de uso hacen de estos equipos hallan inundado el mercado de la tecnología en los últimos años. De la misma forma en que los usuarios de estas tecnologías se han incrementado exponencialmente, los riegos y amenazas a los que se encuentran expuestos estos equipos también se han incrementado en los últimos años. En monográfico de seguridad en dispositivos móviles se considera: ”Es evidente que los dispositivos móviles son cada vez más potentes y, de alguna forma, se parecen cada vez más a sus hermanos mayores -los ordenadores de sobremesa o los ordenadores portátiles- desde el punto de vista de las capacidades y funcionalidades que incorporan. Pero estas similitudes no terminan en sus capacidades o funcionalidades, sino que además están igualmente expuestos a amenazas similares”. Según ESET Latinoamérica, una visión que tiene los usuarios acerca de la necesidad de contar con una solución de seguridad en los nueve de cada diez usuarios afirmó que es cierto, pero solo el 20% cuenta con protección ante los códigos maliciosos o el robo del dispositivo. Según plantean Pacheco y Piaza ”la problemática de seguridad en dispositivos móviles se incrementa tanto por el desconocimiento de los inconvenientes de seguridad como las contramedidas o soluciones que se ofrecen por los fabricantes frente a estas amenazas”.

El trabajo de monografía está enfocado a desarrollar una investigación acerca de las vulnerabilidades o fallas identificadas en dispositivos móviles con sistemas operativos Android y IOS. Para llevar a cabo este objetivo, se tendrán en cuenta las siguientes actividades que nos ayudarán a desarrollar el objetivo inicialmente propuesto: realizar estudio acerca de las vulnerabilidades más comunes en los sistemas operativos móviles Android y IOS, determinar fallas de seguridad que se presentan en sistemas operativos móviles Android y IOS y la forma de mitigarlas e identificar los principales errores que cometen los usuarios de dispositivos móviles relacionados con aspectos de seguridad.

Como parte introductoria al presente trabajo, se abarcará el tema de conceptos y clasificación de dispositivos móviles. En este apartado se realiza una conceptualización de lo que es un dispositivo móvil, y sus principales características. A continuación, se aborda el tema de categorías de dispositivos móviles, teniendo en cuenta los estándares propuestos por T38 y DuPont Global Mobility Innovation Team. Además de ello, se plantea un comparativo entre las dos plataformas móviles más influyentes, teniendo en cuenta algunos parámetros en particular tales como: familia, desarrollador de la plataforma, tipo de licenciamiento que manejan, entre otros.

Las arquitecturas de los sistemas operativos móviles también son abordados en la monografía, Para el caso de Android, se describen elementos como: aplicaciones, framework de aplicaciones, librerías, y Run Time de Android. Por otro lado, haciendo referencia a los modelos IOS, su trabajo de arquitectura se basa en capas las cuales se pueden describir como: Core OS, capa de servicios principales, capa de media y Cocoa Touch Layer.

Seguidamente, se lleva a cabo una investigación acerca de cómo se comporta el mercado de teléfonos móviles en cuanto a la cantidad de usuarios que hacen uso de las principales plataformas. Esta información se plasma en una tabla en la cual se muestran las ventas mundiales de Smartphone por Sistema Operativo y cuya información fue consultada en página web de Gartner

Los riesgos, ataques y amenazas que están vinculadas con aplicaciones móviles

en las plataformas Android y IOS son tratados, con el objeto de brindar recomendaciones a cerca de procedimientos a llevar a cabo para mitigar este tipo de situaciones. En este aspecto, también son investigados los errores más frecuentes cometidos por los usuarios de Smartphones y sus posibles soluciones.

Adicionalmente a lo anterior, se llevar a cabo una consulta a cerca de herramientas que se enfocan en el tratamiento de aspectos se seguridad en dispositivos móviles. Se lleva a cabo una clasificación dependiendo de las plataformas sobre las cuales funcionan dichas herramientas. Finalmente se brindan algunas recomendaciones a la hora de hacer uso de Smartphones con el objeto de mitigar problemas de seguridad que se puedan presentar.

Fuentes:

¿Cuánta información personal entrega cuando utiliza una aplicación?[en línea].En Revista Semana.30 de Enero de 2014.p.1-5.[Consultado:26 de Septiembre de 2018].Disponible en Internet: https://www.semana.com/tecnologia/tips/articulo/cuanta-informacion-personal-entrega-cuando-utiliza-aplicacion/375589-3

3 biggest security threats for Android users today [en línea]. Kim Komando.[Consultado:23 de Septiembre de 2018].Disponible en Internet: https://www.komando.com/tips/382348/3-biggest-security-threats-for-android-users-today

33 ataques por segundo: Kaspersky Lab registra un aumento del 59% en ataques de malware en América Latina [en línea]. Kaspersky Latinoamérica. [Consultado: 25 de abril de 2018]. Disponible en Internet: https://latam.kaspersky.com/about/press-releases/2017_33-attacks-per-second-increase-in-malware-attacks-in-latin-america

5 Major Benefits of Android App Development For Your Business [en línea]. Rishbash Software Blog.12 de Diciembre de 2017.[Consultado:26 de Agosto de 2018].Disponible en Internet: https://www.rishabhsoft.com/blog/5-advantages-of-android-app-development-for-your-business

5 mobile threats you should shut down in 2018 [en línea].Tektonika.[Consultado:21 de Septiembre de 2018].Disponible en Internet: https://www.tektonikamag.com/index.php/2018/05/04/5-mobile-threats-you-should-shut-down-in-2018/

A Whale of a Tale: HummingBad Returns [en línea].Checkpoint Blog. 23 de Enero de 2017.párr. 1.[Consultado:12 de Septiembre de 2018].Disponible en Internet: https://blog.checkpoint.com/2017/01/23/hummingbad-returns/

ACHIARI,Santiago. Ahora USSD Control está incluido en todos los productos de ESET [en línea]. ESET Latinoamérica.(25 de Marzo de 2013).[Consultado: 24 de Septiembre de 2018]. Disponible en Internet: http://www.somoseset.com/2013/03/25/ussd-control-incluido-productos-eset/

ALARCON,Jose Manuel. ¿Qué es la máquina virtual de Java o Java Virtual Machine? [en línea] Campus MPV. (23 de Octubre de 2017).[Consultado:23 de Agosto de 2018].Disponible en Internet: https://www.campusmvp.es/recursos/post/que-es-la-maquina-virtual-de-java-o-java-virtual-machine.aspx

Amenazas de seguridad móvil dirigidas a dispositivos Android [en línea]. Kaspesky Latinoamérica. Consultado: [1 de Septiembre de 2018]. Disponible en Internet: https://latam.kaspersky.com/resource-center/threats/mobile

ANDRES,Ruben. Estos son los 7 mejores antivirus gratis para Android de 2018[en línea].En Computer Hoy.28 de Marzo de 2018.[Consultado:15 de Septiembre de 2018].Disponible en: https://computerhoy.com/listas/moviles/estos-son-7-mejores-antivirus-gratis-android-2018-78199

Android OS Documentation[en línea].Read the Docs.[Consultado:7 de Abril de 2018[.Disponible en Internet: https://media.readthedocs.org/pdf/androidos/latest/androidos.pdf

Android Threats [en línea].Zonealarm. [Consultado:12 de Septiembre de 2018]. Disponible en Internet: https://www.zonealarm.com/mobile-security/android/threats/

Android through the years [en línea].Cnet.[Consultado: 2 de Septiembre de 2018]. Disponible en Internet: https://www.cnet.com/pictures/google-android-versions-history/

ARIAS, Ximena. Del 1 al 8: La evolución del sistema operativo IOS [en línea]. Revista Enter. (17 de Septiembre de 2014).[Consultado: 23 de Mayo de 2018]. Disponible en Internet: http://www.enter.co/especiales/vida-digital/del-1-al-8-la-evolucion-del-sistema-operativo-ios/

Ataque de arranque en frío (cold boot attack) [en línea]. Guías practicas [Consultado: 21 de Septiembre de 2018]. Disponible en Internet: http://www.guiaspracticas.com/recuperacion-de-datos/ataque-de-arranque-en-frio-cold-boot-attack

AVG AntiVirus 2018 [en línea].AVG Latinoamérica.[Consultado:2 de Octubre de 2018].Disponible en Internet: https://www.avg-la.com/avg-antivirus/

AZOKAN,Ajin. Android Architecture From a Developer's Perspective [en línea].ApkChef.(23 de Diciembre de 2016).[Consultado:3 de Mayo de 2018].Disponible en Internet: https://www.apkchef.net/2016/12/android-architecture.html

BACH, Michael. IPhone vs. Android: What are the pros and cons?[en línea].Quora.(27 de Febrero de 2016).[Consultado: 24 de Abril de 2018].Disponible en Internet: https://www.quora.com/IPhone-vs-Android-What-are-the-pros-and-cons

BAGCHI, Apeksha. The evolution of Android [en línea].Yaabot.(1 de Junio de 2017).[Consultado:14 de Octubre de 2018]. Disponible en Internet: https://www.yaabot.com/30831/the-evolution-of-android/

BANSAL,Gaurav. Android Runtime Improvements [en línea].MindOrks.(9 de Mayo de 2018).[Consultado: 1 de Octubre de 2018]. Disponible en Internet: https://medium.com/mindorks/android-runtime-improvements-e69bf7c1d10c

Best Practices: Securing Your Mobile Device [en línea].Trend Micro. [Consultado: 24 de Septiembre de 2018]. Disponible en Internet: https://www.trendmicro.com/vinfo/us/security/news/mobile-safety/best-practices-securing-your-mobile-device

BETANCUR JARAMILLO, Oscar y ERAZO HANRRYR, Sonia Elizabeth. Seguridad en dispositivos móviles Android [en línea]. Monografía presentada para optar el título de: Especialista en Seguridad Informática. Universidad Nacional Abierta y a Distancia – UNAD. Escuela de Ciencias Básicas, Tecnología e Ingeniería,2015. 109 p. [Consultado: 12 de Enero de 2018]. Disponible en Internet: https://stadium.unad.edu.co/preview/UNAD.php?url=/bitstream/10596/3614/1/59836994.pdf

BLANCCO TECHNOLOGY GROUP. Trend Report: Q2 2017 State of Mobile Device Performance and Health [en línea]. Blancco (Septiembre de 2017). [Consultado:11 de Septiembre de 2018].Disponible en Internet: https://download.blancco.com/download/en-rs-q2-2017-state-of-mobile-device-performance-report.pdf

BLAS,Erika. Arquitectura y Entorno de Desarrollo de Aplicaciones Móviles [en

línea].Blog de Erika Blas. 26 de Mayo de 2014.[Consultado:19 de Marzo de 2018].Disponible en Internet: http://erykabp.blogspot.com/2014/05/arquitectura-y-entorno-de-desarrollo-de.html

CABALLERO, Alejandro. Seguridad en el desarrollo de aplicaciones móviles: los 5 mayores riesgos [en línea]. Blog seguridad desarrollo de aplicaciones moviles-mayores riesgos.(8 de Marzo de 2018).[Consultado:3 de Abril de 2018].Disponible en Internet: https://kingofapp.es/blog/seguridad-desarrollo-aplicaciones-moviles-mayores-riesgos/

CARLON, Kris. Which Android manufacturer updates its phones the fastest?[en línea] Android Authority.(14 de Enero de 2017).[Consultado:24 de Septiembre de 2018].Disponible en Internet: https://www.androidauthority.com/android-oem-update-speed-743073/

CASSAVOY, Lianne. What Does It Mean to Jailbreak an iPhone? [en línea].Lifewire.(12 de Mayo de 2018).[Consultado: 20 de Mayo de 2018].Disponible en Internet: https://www.lifewire.com/what-is-jailbreaking-an-iphone-577591

CHUNG, Ek. Evolution of Android Homescreen and Navigation [en línea].Google Design.(15 de Mayo de 2018).párr. 14.[Consultado:14 de Octubre de 2018]. Disponible en Internet: https://medium.com/google-design/evolution-of-android-homescreen-and-navigation-bad189d536f2

CLULEY, Graham. The latest iPhone lock screen bypass, and how to stop it [en línea].Integro (12 de Mayo de 2014).[Consultado:26 de Septiembre de 2018].Disponible en Internet: https://www.intego.com/mac-security-blog/iphone-lock-screen-bypass/

Cocoa Applicatuion Layer. Apple Developer.[Consultado 28 de Agosto de 2018]. Disponible en Internet: https://developer.apple.com/library/archive/documentation/MacOSX/Conceptual/O

SX_Technology_Overview/CocoaApplicationLayer/CocoaApplicationLayer.html

Colombia es el sexto país en Latinoamérica con mayor número de Ciberataques [en línea]. Colombia. Bogotá. (2 de Mayo de 2018).párr. 4. [Consultado: 26 de Septiembre 2018]. Disponible en Internet: https://www.colombia.com/tecnologia/internet/colombia-es-el-sexto-pais-en-latinoamerica-con-mayor-numero-de-ciberataques-188870

Colombia es el tercer país de América Latina con más ciberataques [en línea]. En: el Tiempo.11 de Septiembre de 2017.[Consultado:26 de Septiembre de 2018].Disponible en Internet: https://www.eltiempo.com/tecnosfera/paises-latinoamericanos-en-ciberseguridad-129604

CONDE, Rita. Redes de telefonía celular ¿Qué significan 1G, 2G, 3G y 4G? [en línea]. About Español. (24 de abril de 2016). [Consultado: 1 de Septiembre de 2018]. Disponible en Internet: https://www.aboutespanol.com/redes-de-telefonia-celular-que-significan-1g-2g-3g-y-4g-580779

COSTELLO, Katie y HIPPOLD Sarah Cornelia. Gartner Says Worldwide Sales of Smartphones Returned to Growth in First Quarter of 2018[en línea]. Gartner ,Egham, U.K. (29 de Mayo de 2018).párr 1.[Consultado:14 de Septiembre de 2018].Disponible en Internet: https://www.gartner.com/newsroom/id/3876865

COSTELLO, Sam. Do These 7 Things to Make Your iPhone More Secure [en línea].Lifewire.(28 de Agosto de 2018).[Consultado: 26 de Septiembe de 2018].Disponible en Internet: https://www.lifewire.com/tips-to-improve-iphone-security-2000265

Cuál es el mejor sistema operativo para un smartphone?[en línea].Informática hoy.[Consultado: 3 de Septiembre de 2018].Disponible en Internet: https://www.informatica-hoy.com.ar/soluciones-moviles/Cual-es-el-mejor-sistema-operativo-para-un-smartphone.php

DANIEL, Jo. 10 Common Smartphone mistakes that expose you to security risks [en línea].Information Nigeria.(12 de Diciembre de 2016).[Cosultado:27 de Septiembre de 2018].Disponible en Internet: http://www.informationng.com/2016/12/10-common-smartphone-mistakes-expose-security-risks.html

DARMON,Luc. Protect Mobile In-Store Payments From Relay Attacks [en línea].Apparel Magazine.(12 de Septiembre de 2014).[Consultado:22 de Septiembre de 2018].Disponible en Internet: https://apparelmag.com/protect-mobile-store-payments-relay-attacks

DAVI, Lucas Vincenzo. Code-Reuse Attacks and Defenses [en línea].Tesis para obtener el título de Doctorado en filosofía (PHD). Duisburgo, Alemania. Universidad Técnica de Darmstadt. Departamento de Ciencias

DCIT. Security assesment of mobile applications (iOS, Android)[en línea].[Consultado:20 de Marzo de 2018].Disponible en Internet: https://www.dcit.cz/en/security/mobile-applications-security

DE LOOPER,Christian. From Android 1.0 to Android 7.0, here's how the top mobile OS has evolved over the years [en línea]. Yahoo Finance .(4 de Septiembre de 2018).[Consultado:3 de Septiembre de 2018] . Disponible en Internet: https://finance.yahoo.com/news/android-1-0-android-9-192746756.html

EDMOND , Ramin Users are biggest impediment to Apple iOS security.[en línea]. SearchMobileComputing.(31 de julio de 2017) [Consultado: 1 de septiembre de 2018]. Disponible en Internet: https://searchmobilecomputing.techtarget.com/news/450423643/Users-are-biggest-impediment-to-Apple-iOS-security

Encuesta Anual de Seguridad de la información en: EY Colombia.2016. Citado por:

ESET Security Report Latinoamérica 2018 [en línea]. [Consultado: 27 de Septiembrre de 2018]. Disponible en Internet: https://www.welivesecurity.com/la-es/2018/06/19/eset-security-report-2018-el-estado-de-la-seguridad-de-la-informacion-en-las-empresas-de-la-region/

ESET Security Report Latinoamérica 2017 [en línea].ESET Latinoamérica.[Consultado: 27 de Septiembrre de 2018]. Disponible en Internet: https://www.welivesecurity.com/wp-content/uploads/2017/04/eset-security-report-2017.pdf

Evolución de la red de comunicación móvil, del 1G al 5G [en línea].Universidad Internacional de Valencia.[Consultado el 1 de Septiembre de 2018]. Disponible en Internet: https://www.universidadviu.com/evolucion-la-red-comunicacion-movil-del-1g-al-5g/

Evolution of Android OS [en línea].Spinfold.[Consultado:1 de Septiembre de 2018]. Disponible en Internet: http://www.spinfold.com/evolution-of-android-os/

FERNANDEZ CASTRILLO, Alejandro. Medidas de protección frente ataques de denegación de servicio (DoS) [en línea]. Centro de Respuesta a incidentes de Seguridad e Industria CERTSI. España.(26 de Enero de 2018).[Consultado:11 de Septiembre de 2018].Disponible en Internet: https://www.certsi.es/blog/medidas-proteccion-frente-ataques-denegacion-servicio-dos

FLORES, Javier. ¿Qué es lo que más preocupa a quienes usan Smartphone Android? [en línea]. Revista Muy Interesante.[Consultado: 15 de Abril de 2018].Disponible en Internet: https://www.muyinteresante.es/curiosidades/preguntas-respuestas/ique-es-lo-que-mas-preocupa-a-quienes-usan-smartphones-android

Funciones de Norton Snap[en línea]Norton.[Consultado:4 de Octubre de 2018].

Disponible en Internet: https://support.norton.com/sp/es/mx/home/current/solutions/v64690996_EndUserProfile_es_mx

GIUSTO BILIĆ, Denise. Balance semestral de la seguridad móvil [en línea].Welivesecurity.(6 de Agosto de 2018).[Consultado:29 de Septiembre de 2018].Disponible en Internet: https://www.welivesecurity.com/la-es/2018/08/06/balance-semestral-seguridad-movil/

Global Cyber Attack Trends Report[en línea].Checkpoint Research.[Consultado:28 de Septiembre de 2018].Disponible en Internet: https://www.checkpoint.com/downloads/product-related/infographic/H2_2017_Global_Cyber_Attack_Trends_Report.pdf?mkt_tok=eyJpIjoiTW1FMlpXUTBaREZqWXpSbCIsInQiOiJTYzFzV1UxWVdTc2pOa24yeHh3aXZodEcwZ2czMnlOQnhHRlJcL3l6ZHI3YjRpUU9mbXpra1BtN3FjUnlNZzRGb3ByVDVWdzdhMythZjRWbThYQnk0dFFEQ1NyXC9JSWVcL1FzejZhcjRodzdlaE8zNExcL3FPeDlGSk5UMDRua2tGbTEifQ%3D%3D

GOASDUFF, Laurence y FORNI Amy Ann. Gartner Says Worldwide Sales of Smartphones Grew 7 Percent in the Fourth Quarter of 2016.[en línea]. Gartner, Egham, U.K. (15 de Febrero de 2017).[Consultado:12 de Septiembre de 2018].Disponible en Internet: https://www.gartner.com/en/newsroom/press-releases/2017-02-15-gartner-says-worldwide-sales-of-smartphones-grew-7-percent-in-the-fourth-quarter-of-2016

GOLDMAN,Jeff. Top 20 Android Security Apps [en línea]. eSecurityPlanet.(27 de Octubre de 2015).[Consultado:1de Octubre de 2018]. Disponible en Internet: https://www.esecurityplanet.com/mobile-security/top-20-android-security-apps.html

GONDI, Tilakkumar. IOS – Architecture [en línea]. Tilakgondi Page.(14 de Enero de 2015).[Consultado:13 de Octubre de 2018].Disponible en Internet: https://tilakgondi.wordpress.com/2015/01/14/ios-architecture/

GONZALEZ FERNANDEZ, Alfonso. Seguridad en Smartphone. Análisis de riesgos, de vulnerabilidades, y auditorias de dispositivos [en línea]Trabajo final para obtener el título de Master Interuniversitario de Seguridad en las Tecnologías de la Información y de las Comunicaciones (MISTIC). Universidad Abierta de Cataluña,2018,121 p. [Consultado: 26 de Septiembre de 2018]. Disponible en Internet:http://openaccess.uoc.edu/webapps/o2/bitstream/10609/72966/6/agonzalezfernandez3TFM0118Memoria.pdf

GORDON, Whitson. Everything You Need to Know About Rooting Your Android Phone [en línea]. Lifehacker.(9 de Abril de 2013).[Consultado:2 de Septiembre de 2018].Disponible en Internet: https://lifehacker.com/5789397/the-always-up-to-date-guide-to-rooting-any-android-phone

GUEVARA BENAVIDES, Lina María. Empresas colombianas deben invertir más en ciberseguridad [en línea].La República.p.2-4.[Consultado:25 de Septiembre de 2018].Disponible en Internet: https://www.larepublica.co/consumo/empresas-colombianas-deben-invertir-mas-en-ciberseguridad-2464836

Guía de Seguridad Informática. En Internet, el mejor sistema de seguridad eres tú ¡protégete! [en línea]. Blog Andalucía es digital.30 de noviembre de 2016. [Consultado: 1 de Septiembre de 2018].Disponible en Internet: https://www.blog.andaluciaesdigital.es/guia-de-seguridad-informatica/

Guía de Seguridad para usuarios de Smartphones. [en línea]. ESET Latinoamérica [Consultado: 20 de Abril de 1918]. Disponible en Internet: https://www.welivesecurity.com/wp-content/uploads/2014/01/documento_guia_de_seguridad_para_usuarios_de_smartphone_baj.pdf

Gustavo. Kaspersky Lab registra un alza de 60% en ataques cibernéticos en América Latina [en línea]. Kaspersky Lab Latinoamérica.(14 de Agosto de 2018).[Consultado:28 de Septiembre de 2018].Disponible en Internet: https://latam.kaspersky.com/blog/kaspersky-lab-registra-un-alza-de-60-en-

ataques-ciberneticos-en-america-latina/13266/

GUTIERREZ, Javier J. Qué es un framework web [en línea].Universidad de Sevilla. España.[Consultado: 2 de Mayo de 2028]. Disponible en Internet: http://www.lsi.us.es/~javierj/investigacion_ficheros/Framework.pdf

HEIN, Buster. The evolution of iOS: From iPhone OS to iOS 11 [en línea].Cult of Mac.(24 de Mayo de 2017). [Consultado:2 de Septiembre de 2018].Disponible en Internet: https://www.cultofmac.com/488454/ios-evolution-iphone-os/

HEISLER, Yoni. The history and evolution of iOS, from the original iPhone to iOS 9 [en línea]. Brg.(12 de Febrero de 2016).[Cosultado:29 de Septiembre de 2018] Disponible en Internet: https://bgr.com/2016/02/12/ios-history-iphone-features-evolution/

HilI, Simon. The best security apps and antivirus protection for Android [en línea]. Digital Trends.(26 de Abril de 2018).[Consultado:2 de Octubre de 2018].Disponible en Internet: https://www.digitaltrends.com/mobile/best-antivirus-protection-for-android/

HILL,Simon. Android vs. iOS: Which smartphone platform is the best?[En línea].Digital Trends.(7 de Marzo de 2018).[Consultado:8 de Septiembre de 2018].Disponible en Internet: https://www.digitaltrends.com/mobile/android-vs-ios/

HOPPING, Clare. Android vs iOS: which mobile OS is right for you? [En línea]. ITPRO Analysis Business Insigth.(31 de Agosto de 2018).[Consultado:7 de Septiembre de 2018],Disponible en Internet: http://www.itpro.co.uk/mobile/30409/android-vs-ios-which-mobile-os-is-right-for-you

IDC. Smartphone Volumes Expected to Rebound in 2017 with a Five-Year Growth

Rate of 3.8%, Driving Annual Shipments to 1.53 Billion by 2021, According to IDC [en línea]. International Data Corporation (IDC).(1 de Marzo de 2017).párr.1.[Consultado:9 de Septiembre de 2018].Disponible en Internet: https://www.idc.com/getdoc.jsp?containerId=prUS42334717

Informe balance cibercrimen en Colombia 2017[en línea]. Centro Cibernético Policial. [Consultado:3 de Septiembre de 2018]. Disponible en: https://caivirtual.policia.gov.co/sites/default/files/informe_cibercrimen_2017.pdf

Informe sobre amenazas para la seguridad en Internet [en línea]. Symantec. [Consultado; 20 de Abril de 2018]. Disponible en Internet: https://www.symantec.com/content/dam/symantec/mx/docs/reports/istr-23-executive-summary-mx.pdf

Informe Sobre las Amenazas para la Seguridad en Internet Volumen 23[en línea].Symantec.[Consultado:27 de Septiembre de 2018].Disponible en Internet: http://images.mktgassets.symantec.com/Web/Symantec/%7B3eb3b2d7-76de-484e-951f-e903d31ea889%7D_ISTR23-FINAL_ES.pdf

Internet Security Threat Report [en línea].Symantec. [Consultado:17 de Septiembre de 2018]. Disponible en Internet: https://www.symantec.com/content/dam/symantec/docs/reports/istr-23-2018-en.pdf

iOS Architecture [en línea].Intellipaat.[Consultado:28 de Agosto de 2018].Disponible en Internet: https://intellipaat.com/tutorial/ios-tutorial/ios-architecture/

ISMAIL, Nick. Common security vulnerabilities of mobile devices [en línea].InformationAge.(21 de Febrero de 2017).[Consultado:22 de Septiembre de 2018].Disponible en Internet: https://www.information-age.com/security-vulnerabilities-mobile-devices-123464616/

IT BUSINESS SOLUTIONS. ¿Cuáles son los vectores de ataque que usan los delincuentes informáticos?[en línea].[Consultado:13 de Septiembre de 2017].Disponible en Internet: https://www.itbusiness-solutions.com.mx/vectores-de-ataque-de-ciberdelincuentes

JR, Rafael. 5 mobile security threats you should take seriously in 2018 [en línea]. CSO.(13 de Diciembre de 2017).[Consultado:17 de Septiembre de 2018].Disponible en Internet: https://www.csoonline.com/article/3241727/mobile-security/5-mobile-security-threats-you-should-take-seriously-in-2018.html

JR,Raphael. Android versions: A living history from 1.0 to Pie [en línea].Computerworld.(7 de Agosto de 2018),párr.14.[Consultado:13 de Octubre de 2018]. Disponible en Internet: https://www.computerworld.com/article/3235946/android/android-versions-a-living-history-from-1-0-to-today.html?page=2

JULES,Javier. Cibercriminales también pueden robar los datos de celulares y tabletas a través de un mensaje [en línea].RCN Radio.(27 de Junio de 2017). [Consultado: 1 de Octubre de 2017]. Disponible en Internet: https://www.rcnradio.com/mcontent/5b36d2435f0049e5d1302823/amp

KALLIN Jakob y LOBO VALBUENA Irene. Excess XSS A comprehensive tutorial on cross-site scripting [en línea] Excess XSS. [Consultado: 23 de Septiembre de 2018]. Disponible en Internet: https://excess-xss.com/

Kaspersky Lab registra un alza de 60% en ataques cibernéticos en América Latina [en línea].Blog Kaspersky Lab Latinoamérica.14 de Agosto de 2018. [Consultado: 27 de Septiembre de 2018]. Disponible en Internet: https://latam.kaspersky.com/blog/kaspersky-lab-registra-un-alza-de-60-en-ataques-ciberneticos-en-america-latina/13266/

Kaspersky Lab: Brasil, México y Colombia lideran incidentes de secuestros digitales en América Latina [en línea] Kaspersky Lab Latinoamérica.(18 de Septiembre de 2017).[Consultado:27 de Septiembre de 2018].Disponible en Internet: https://latam.kaspersky.com/about/press-releases/2017_kaspersky-lab-incidents-of-digital-kidnappings-in-latin-america

KATARIYA,Jayanti. Apple Vs Android - A comparative study 2017[En línea] Mobile Apps Channel.27 de Febrero de 2017.[Consultado:12 ad Abril de 2018].Disponible en Internet: https://www.whatech.com/mobile-apps/blog/archive/267836-apple-vs-android-a-comparative-study-2017

KOVACS, Nadia. ¿Qué es Grayware, Adware y Madware?[en línea]. Norton Protection Blog. 7 de abril de 2016. Consultado: [20 de abril de 2018]. Disponible en Internet: https://community.norton.com/es/blogs/norton-protection-blog/%C2%BFqu%C3%A9-es-grayware-adware-y-madware

La Computación,2015.189 p. [Consultado: 23 de Septiembre de 2018]. Disponible en Internet: http://tuprints.ulb.tu-darmstadt.de/4622/7/Davi-PhD-Code-Reuse-Attacks-and-Defenses.pdf

LA PORTA,Liarna. Malicious profiles – one of the most serious threats to IPhones [en línea].Wandera.(14 de Abril de 2018).[Consultado: 3 de Octubre de 2018].Disponible en Internet: https://www.wandera.com/malicious-profiles-come/

Las empresas colombianas escatiman en gastos y se rajan en ciberseguridad [en línea] En Revista Dinero. Enero, 2017,p.2-5.[Consultado 30 de Septiembre de 2018].Disponible en Internet: https://www.dinero.com/empresas/articulo/encuesta-anual-de-seguridad-de-la-informacion-de-la-firma-ey/241201

LORD,Nat, Social Engineering Attacks: Common Techniques & How to Prevent an

Attack [en línea].DigitalGuardian.(19 de Septiembre de 2018).[Consultado:21 de Septiembre de 2018].Disponible en Internet: https://digitalguardian.com/blog/social-engineering-attacks-common-techniques-how-prevent-attack

LVDAQIAN ,Darwin. Mobile Security Primer[en línea]. GitHub, Inc.(3 de Marzo de 2017), párr. 2.[Consultado: 24 de Marzo de 2018].Disponible en Internet: https://github.com/nowsecure/secure-mobile-development/blob/master/en/primer/mobile-security.md

LYN, La. Android through the years [diapositivas].Cnet.22 de Febrero de 2016, 15 diapositivas. [Consultado: 2 de Septiembre de 2018]. Disponible en Internet: https://www.cnet.com/pictures/google-android-versions-history/

MEDINA, Edgar. Cinco mitos y verdades sobre la batería de su celular [en línea]. En El Tiempo.(16 de Febrero de 2017)[Consultado: 23 de Agosto de 2018]. Disponible en Internet: https://www.eltiempo.com/tecnosfera/tutoriales - tecnologia/cinco-mitos-y-verdades-sobre-la-bateria-de-su-celular-59543

MENDOZA,Azury. ¿A qué se le conoce como vectores de ataque en ciberseguridad y cómo puedes eliminarlos de tus ambientes digitales? [en línea]. GB Advisors.(2 de Mayo de 2018).[Consultado:13 de Septiembre de 2018].Disponible en Internet: http://www.gb-advisors.com/es/vectores-de-ataque-en-ciberseguridad/

MITROFF,Sarah. La seguridad es clave [diapositivas].CNet.3 de Marzo de 2016, 8 diapositivas.[Consultado:26 de Septiembre de 2018].Disponible en Internet: https://www.cnet.com/es/imagenes/errores-seguridad-telefono/5/

Mobile security threats in Android [en línea]. TechAdvisory.[Consultado:23 de Septiembre de 2018].Disponible en Internet: https://www.techadvisory.org/2017/06/mobile-security-threats-in-android/

Mobility, performance and engagement How CIOs can contribute to business performance by shaping the employee experience [en línea]. The Economist Intelligence Unit.[Consultado:17 de Septiembre de 2018].Disponible en Internet: https://www.arubanetworks.com/pdf-viewer/?q=/assets/EIUStudy.pdf

MON KYWE,Su. Mobile Threat Blog [en línea]. Appthority.32 de Mayo de 2018, párr. 1. [Consultado: 12 de Octubre de 2018].Disponible en Internet: https://www.appthority.com/mobile-threat-center/blog/ios-update-11-4-security-details/

Monográfico de seguridad en dispositivos móviles [en línea]. Instituto Nacional de Tecnologías de la Comunicación. [Consultado:15 de Marzo de 2018]. Disponible en Internet: https://www.firma-e.com/wp-content/uploads/2013/03/monografico_seg_disp_moviles.pdf

MOREAU, Sean. The evolution of iOS [diapositivas].Computerworld.6 de Junio de 2018,13 diapositivas.[Consultado:23 de Mayo de 2018].Disponible en Internet: https://www.computerworld.com/article/2975868/apple-ios/the-evolution-of-ios.html#slide4

MORILLO POZO, Julian David. Introducción a los dispositivos móviles [en línea].Universidad Abierta de Cataluña [Consultado:2 de Septiembre de 2018].Disponible en Internet: https://www.exabyteinformatica.com/uoc/Informatica/Tecnologia_y_desarrollo_en_dispositivos_moviles/Tecnologia_y_desarrollo_en_dispositivos_moviles_(Modulo_2).pdf

mSecure 5 [en línea].Msecure.[Consultado:3 de Octubre de 2018]. Disponible en Internet: https://www.msecure.com/

NAVARRO,Francis. Common security risks every smartphone user should know about [en línea].Kim Komando.(23 de Julio de 2017).[Consultado: 27 de Spetimbre de 2018].Disponible en Intenet: https://www.komando.com/tips/370318/common-security-risks-every-smartphone-user-should-know-about/all

Operating Systems [en línea]. BBC.[Consultado en: 3 de Septiembre de 2018].Disponible en Internet: https://www.bbc.com/bitesize/guides/ztcdtfr/revision/1

OWASP Mobile Security Project [en línea]. OWASP. [Consultado: 27 de Octubre de 2018]. Disponible en Internet: https://www.owasp.org/index.php/OWASP_Mobile_Security_Project#tab=Top_10_Mobile_Risks

PACHECO SEBASTIAN, Exequiel Y PIAZZA ORLANDO Carlos Damián. Estudio y análisis de seguridad en dispositivos móviles. BYOD y su impacto en las organizaciones [en línea]. Tesis presentada para optar al título de Licenciatura en Sistemas. La Plata, Argentina. Universidad Nacional de la Plata. Facultad de Informática, 2016. 139 p. [Consultado; 16 de abril de 2018]. Disponible en Internet: http://sedici.unlp.edu.ar/bitstream/handle/10915/58591/Documento_completo.%20y%20Piazza%20Orlando,%20C.%20Estudio%20y%20an%C3%A1lisis%20de%20seguridad%20en%20dispositivos%20m%C3%B3viles.pdf-PDFA.pdf?sequence=4&isAllowed=y

PADHYA, Bhargavi y DESAI, Prasad. Comparison of Mobile Operating Systems [en línea]. En: International Journal of Innovative Research in Computer and Communication Engineering. Agosto, 2016.vol 4 no 8, p.1-3.[Consultado: 3 de Septiembre de 2018]. Disponible en Internet: http://www.ijircce.com/upload/2016/august/132_Comparison.pdf.ISSN: 2320-9798.E-ISSN: 2320-9801

PAGANINI, Pierluigi. WireLurker, Masque: Every Apple iOS App Could Be Compromised [en línea]. Infosec Institute. (14 de Septiembre de 2018).[Consultado:28 de Septiembre de 2018].Disponible en Internet: https://resources.infosecinstitute.com/wirelurker-masque-every-apple-ios-app-compromised/#gref

PAINTER,Lewis. iPhone security tips: How to protect your iPhone from hackers [en línea]. Macworld.(2 de Mayo de 2018).[Consultado:26 de Septiembre de 2018].Disponible en Internet: https://www.macworld.co.uk/how-to/iphone/iphone-security-tips-3638233/

PHILLIPS Cassie. Five Immediate Threats to Android Security for 2016 and How to Eliminate Them [en línea].Appknox Blog.2016.[Consultado:22 de Septiembre de 2018].Disponible en Internet: https://blog.appknox.com/five-immediate-threats-android-security-2016-eliminate/

Por qué su empresa debe invertir en seguridad informática? [en línea].Adalid.[consultado:1 de Octubre de 2018].Disponible en Internet: http://www.adalid.com/por-que-su-empresa-debe-invertir-en-seguridad-informatica/

Por si Google fracasa: examinamos 21 aplicaciones de seguridad para Android.[en línea].AV-Test. [Consultado:3 de Octubre de 2018].Disponible en Internet: https://www.av-test.org/es/noticias/por-si-google-fracasa-examinamos-21-aplicaciones-de-seguridad-para-android/

PRICE, Dan. 7 iOS Settings to Change If You Want Better Privacy in Safari [en línea].MakeUseOf.(27 de Junio de 2018).[Consultado: 26 de Septiembre de 2018].Disponible en Internet: https://www.makeuseof.com/tag/change-ios-settings-privacy-safari/

PRICE, Dan. How to Fix 5 Common iPhone & iPad Security Threats [en línea].MakeUseOf.(26 de Enero de 2016).[Consultado: 22 de Septiembre de 2018].Disponible en Internet: https://www.makeuseof.com/tag/fix-5-common-iphone-ipad-security-threats/

RAMNATH, Rajib y LOFFING, Cheyney. Beginning IOS Programming For Dummies[en línea].New Jesey. 2014,423 p.[Consylado:1 de Septiembre de 2014].Disponible en Internet:

https://books.google.com.co/books?id=8tIsAwAAQBAJ&pg=PA14&lpg=PA14&dq=core+os+layer&source=bl&ots=DCjP-btpm_&sig=fBWxkvI98Bd5zfYU--zX_m7jJI8&hl=es&sa=X&ved=2ahUKEwiegKrntpXdAhVrs1kKHSi2DNk4ChDoATAGegQIBBAB#v=onepage&q=core%20os%20layer&f=false

Ransomware [en línea].Avast .[Consultado:30 de Septiembre de 2018].Disponible en Internet: https://www.avast.com/es-es/c-ransomware

RAWAT, Inder. Advantages And Disadvantages Of Android Phones [en línea]. OneWorldNews.(23 de Febrero de 2017).[Consultado:30 de Septiembre de 2018].Disponible en Internet: http://www.oneworldnews.com/advantages-and-disadvantages-of-android-phones/

RAY,Jhon. Sam Teach Yourself IOS 8 Application development in 24 hours.[en línea] Indiana.USA: Pearson.2015,863 p.[Consultado:1 de Septiembre de 2018].Disponible en Internet: https://books.google.com.co/books?id=FS75BgAAQBAJ&pg=PA120&lpg=PA120&dq=Cocoa+Touch+Layer&source=bl&ots=SjAJJmydTc&sig=j9DEa8ZAY3Mx7y-2FlF_A9gqtBg&hl=es&sa=X&ved=2ahUKEwj_yNS6gJHdAhVJ2lMKHUgSDyw4ChDoATAGegQIBBAB#v=onepage&q=Cocoa%20Touch%20Layer&f=true

RITCHER,Felix. The Smartphone Platform War Is Over [en línea].Statista.(20 de Febrero de 2017).[Consultado:11 de Septiembre de 2018].Disponible en Internet: https://www.statista.com/chart/4112/smartphone-platform-market-share/

RITCHIE,Rene. Six ways to increase your iPhone and iPad security in 2017 [en línea]. Imore. (4 de Enero de 2017).[Consuiltado:26 de Septiembre de 2018].Disponible en Internet: https://www.imore.com/6-ways-increase-iphone-ipad-security-privacy

RODRIGUEZ MOLINA, Carlos. Evolución de Android desde su creación a Android

8.0 [en línea]. Tu experto Tecnología. (4 de Agosto de 2017). [Consultado: 13 de Mayo de 2018].Disponible en Internet: https://www.tuexperto.com/2017/08/04/evolucion-de-android-desde-su-creacion-a-android-8-o/

SAVITSKY,Alex. Siete Aplicaciones De Seguridad Para Tu iPhone [en línea]. Kaspersky Labs.(21 de Abril de 2014).[Consultado:13 de Octubre de 2018].Disponible en Internet: https://latam.kaspersky.com/blog/siete-aplicaciones-de-seguridad-para-tu-iphone/2887/

SAXENA,Sobhit. Evolution from iPhone OS 1 to iOS 10 – Journey of iOS [en línea]. Mobiloitte Technologies.(14 Septiembre de 2016).[Consulado: 2 de Mayo de 2018]. Disponible en Internet: https://www.mobiloitte.com/blog/evolution-iphone-os-1-ios-10-journey-ios/

Sector financiero y de telecomunicaciones, los que más ataques cibernéticos reciben en Colombia [en línea]. Actualicese. [Consultado: 6 de Octubre de 2017]. Disponible en Internet: https://actualicese.com/actualidad/2018/10/04/sector-financiero-y-de-telecomunicaciones-los-que-mas-ataques-ciberneticos-reciben-en-colombia/

Seguridad en los Dispositivos Móviles [en línea]. Centro de Estudios, Respuesta y Tratamiento de Incidentes de Seguridad en Brasil. [Consultado: 15 de Abril de 2018]. Disponible en Internet: https://cartilla.cert.br/fasciculos/dispositivos-moviles/fasciculo-dispositivos-moviles-slides.pdf

SICILIANO; Robert. What is a Backdoor Threat?[en línea] McAfee.(12 de Mayo de 2014).[Consultado: 24 de Septiembre de 2018*.Disponible en Internet: https://securingtomorrow.mcafee.com/consumer/identity-protection/backdoor-threat/

SINGH, Arpit. Top 15 Mobiles Phones Operating Systems 2018 [en línea].Digital

SEO Guide.(6 de Julio de 2018).[Consultado:3 de Septiembre de 2019].Disponible en Internet https://www.digitalseoguide.com/technology/top-mobile-phones-operating-systems-os/#7_Blackberry_OS

Singh, Karanpreet. 15 Best Security Apps That You Must Have In your iPhone 2018[en línea].Techviral.(29 de Junio de 2018).[Consultado:3 de Octubre de 2018]. Disponible en Internet: https://techviral.net/best-security-apps-iphone/

SKVOR, Michael. Keeping your Android safe this year [en línea] Blog Avast. 24 de Enero de 2018. [Consultado:30 de Abril de 2018]. Disponible en Internet: https://blog.avast.com/keeping-your-android-safe-this-year

SMITH, Dave, The 13 most useful features in iOS 11 [en línea].Business Insider.(16 de Mayo de 2018).[Consultado: 2 de Septiembre de 2018].Disponible en Internet: https://www.businessinsider.com/apple-ios-11-best-features-2017-7

Software Library [en línea].Techopedia.[Consutado:25 de Agosto de 2018].Disponible en Internet: https://www.techopedia.com/definition/3828/software-library

Sophos Mobile Security para Android. [en línea].Sophos. [Consultado:2 de Octubre de 2018].Disponible en Internet: https://www.sophos.com/es-es/products/free-tools/sophos-mobile-security-free-edition.aspx

STATISTA. Smartphones industry: Statistics & Facts[en línea].[Consultado:11 de Septiembre de 2018].Disponible en Internet: https://www.statista.com/topics/840/smartphones/

STORM Darlene y DAVIDSON Michelle. Easy way to bypass passcode lock screens on iPhones, iPads running iOS 12 [en línea].(18 de Septiembre de 2018).

[Consultado:10 de Octubre de 2018]. Disponible en Internet: https://www.computerworld.com/article/3041302/security/4-new-ways-to-bypass-passcode-lock-screen-on-iphones-ipads-running-ios-9.html

SYED FARHAN, Alam Zaidi, et al. A Survey on Security for Smartphone Device [en línea]. En (IJACSA) International Journal of Advanced Computer Science and Applications,2016, Vol. 7, No. 4, p.210-213.[Consultado:27 de Septiembre de 2018].Disponible en Internet: http://thesai.org/Downloads/Volume7No4/Paper_26-A_Survey_on_Security_for_Smartphone_Device.pdf

TEAM COUNTERPOINT. Global Smartphone Market Share: By Quarter [en línea].Countpoint.(16 de Mayo de 2018).[Consultado:10 de Septiembre de 2018].Disponible en Internet: https://www.counterpointresearch.com/global-smartphone-share/

The Mobile Economy 2018. GSMA Association [en línea].[Consultado:7 de Septiembre de 2018].Disponible en Internet: https://www.gsma.com/mobileeconomy/wp-content/uploads/2018/02/The-Mobile-Economy-Global-2018.pdf

The Mobile Economy 2018.[en línea].GSMA Association. [en línea]. [Consultado:3 de Octubre de 2018].Disponible en Internet http://www.redestelecom.es/siteresources/files/843/44.pdf

The Risks of “Jailbreaking” and “Rooting” Mobile Devices[en línea].[Consultado:28 de Septiembre de 2018].Disponible en Internet: https://www.firstcountybank.com/sites/default/files/pdfs/Jailbroken%20and%20Rooted%20Devices%20Fraud%20Risks.pdf

Threats to iOS Mobile Devices [en línea] Laccon Movile Security.[Consultado: 24 de Septiembre de 2018].(Agosto de 2014).Disponible en Internet: https://idency.com/wp-content/uploads/2014/08/Lacoon-White-Paper-iOS-

Threats.pdf

TRAVIS,May. IOS, Android or Windows: what's the best mobile operating system? [en línea]. The Whiz Cells.(17 de Febrero de 2017).párr.20.[Consultado:4 de Septiembre de 2018]. Disponible en: https://www.thewhizcells.com/ios-android-windows-whats-best-mobile-operating-system/

TREND MICRO. 7 Ways to Improve Security on Your iOS Device . [en línea].Trend Micro. [Consultado: 26 de Septiembre de 2018]. Disponible en Internet: https://www.trendmicro.com/vinfo/us/security/news/mobile-safety/7-ways-to-improve-security-on-ios-device

TRIGGS, Robert. Best Android security practices [en línea]. Android Authority.(30 de Junio de 2016).[Consultado:26 de Septiembre de 2018].Disponible en Internet: https://www.androidauthority.com/best-android-security-practices-700393/

TUTORIALPOINTS. Mobile Security - Attack Vectors[en línea].[Consultado:24 de Marzo de 2018].Disponible en Internet: https://www.tutorialspoint.com/mobile_security/mobile_security_attack_vectors.htm

UMAWING, Jovi. When three isn't a crowd: Man-in-the-Middle (MitM) attacks explained [en línea]. MalwareBytes Labs Bog.12 de Julio de 2018. [Consultado: 17 de Octubre de 2018].Disponible en Internet: https://blog.malwarebytes.com/101/2018/07/when-three-isnt-a-crowd-man-in-the-middle-mitm-attacks-explained/

VALERY,Yolanda. Qué es el virus HummingBad que afecta millones de teléfonos Android [en línea].BBC News.(6 de Julio de 2016).[Consultado: 23 de Septiembre de 2018]. Disponible en Internet: https://www.bbc.com/mundo/noticias-36726332

VAN ALLEN,Fox. The evolution of Apple iOS [diapositivas].Cnet.1 de Julio de 2017, 25 dispositivas .[Consultado: 25 de Mayo de 2018]. Disponible en Internet: https://www.cnet.com/pictures/the-evolution-of-apple-ios/8/

VAN DER MEULEN, Rob y MCCALL, Thomas .Gartner Says Worldwide Sales of Smartphones Recorded First Ever Decline During the Fourth Quarter of 2017.[en línea].Gartner, Egham, UK.(22 de Febrero de 2018). [Consultado: 26 de Abril de 2018]. Disponible en Internet: https://www.gartner.com/en/newsroom/press-releases/2018-02-22-gartner-says-worldwide-sales-of-smartphones-recorded-first-ever-decline-during-the-fourth-quarter-of-2017

VANEGAS, Carlos Alberto. Android…. De que me hablan?[en línea]Revistas Udistrital.(Agosto de 2013) [Consultado:16 de Marzo de 2018].Disponible en Internet: http://revistas.udistrital.edu.co/ojs/index.php/vinculos/article/view/8022/9631%20una

VAUGHAN-NICHOLS, Steven J [en línea].ZDNet.(1 de Marzo de 2018). [Consultado: 25 de Septiembre de 2018]. Disponible en Internet: https://www.zdnet.com/article/the-ten-best-ways-to-secure-your-android-phone/

Ventajas e inconvenientes del sistema operativo iOS [en línea].Blog BeMovil.2 de Agosto de 2015.[Consultado: 11 de Septiembre de 2018].Disponible en Internet: https://www.bemovil.es/blog/ventajas-sistema-operativo-ios/

VISWANATHAN, Pryya. What Is a Mobile Device?[en línea].Lifewire.(13 de Mayo de 2018).[Consulado: 26 de Mayo de 2018].Disponible en Internet: https://www.lifewire.com/what-is-a-mobile-device-2373355.

VORA,Lopa. Evolution of mobile generation technology: 1G to 5G and review of upcoming wireless technology 5G [en línea]. En: International Journal of Modern Trends in Engineering and Research. Octubre de 2015, vol 2, no 10, p.1-5.

[Consultado: 1 de Septiembre de 2018]. ISSN: 2349-9745. Disponible en Internet: https://pdfs.semanticscholar.org/4dfd/40cc3a386573ee861c5329ab4c6711210819.pdf.

WALLEN, Jack. 10 things you can do to make Android more secure [en línea]. TechRepublic (17 de Junio de 2014).[Consultado:25 de Septiembre de 2018]. Disponible en Internet: https://www.techrepublic.com/blog/10-things/10-things-you-can-do-to-make-android-more-secure/

Wickr Me – Private Messenger [en línea].Apple Store.[Consultado:3 de Octubre de 2018].Disponible en Internet: https://itunes.apple.com/us/app/wickr-me-private-messenger/id528962154?mt=8

WILLIAMS,Mat. Zero day vulnerabilities: how do you stop a threat you can't see coming? [en línea].Faraonics.(20 de Abril de 2017). [Consultado: 11 de Octubre de 2018].Disponible en Internet: https://www.faronics.com/news/blog/zero-day-vulnerabilities-stop-threat-cant-see-coming

XcodeGhost: qué es y cómo evitarlo. Fin de la invulnerabilidad de Apple [en línea].Panda Security.[Consultado:24 de Septiembre de 2018]. Disponible en Internet: https://www.pandasecurity.com/spain/mediacenter/noticias/xcodeghost-malware-apple/

Contenido del documento:

Lista de tablas

Introducción

Definición de problema

Antecedentes

- Formulación de problema
- Descripción de problema

Objetivos

- Objetivo general
- Objetivos específicos

Marco referencial

- Marco teórico
- Marco conceptual

Desarrollo de la investigación

Conclusiones

Bibliografía

Anexos

Metodología:

El tipo de investigación utilizada es documental.

Tomando como base este tipo de investigación se iniciará el proceso búsqueda de información acerca del tema seleccionado mediante fuentes bibliográficas confiables que permitan brindar una visión veraz de la situación analizada. La recopilación bibliográfica está basada en trabajos de investigación, artículos de revistas, periódicos, semanarios, documentos visuales, entre otras fuentes relacionadas con el tema de investigación.

La lectura, análisis y comprensión de la información obtenida garantizará tener un punto de vista claro e imparcial a cerca de los temas tratados en la monografía, involucrando en este proceso conceptos como el selección y clasificación de información obtenida, procesamiento de la misma y planteamiento de ideas siempre buscando brindar una visión real del problema y de los soluciones o recomendaciones planteadas a través del desarrollo de la monografía.

Conceptos nuevos: Run Time de Android, IOS layers (capas sistema operativo IOS),grayware, backsdoors, cold boot attacks , XcodeGhost, Jailbreaking, rooting.

Conclusiones:

Es una realidad que en los últimos años los desarrollos tecnológicos han cambiado la forma como llevar a cabo nuestras labores cotidianas. El ámbito de los dispositivos móviles no ha sido ajeno a este tipo de desarrollos. Debido al auge de los teléfonos inteligentes y del gran crecimiento en el uso de Smartphones estos se han convertido en blanco de ataques de diferentes tipos, con consecuencias que van desde el acceso remoto a equipos, robo de los mismos, acceso a información confidencial de usuarios entre otros. Tomando como base la presente monografía, se puede llegar a las siguientes conclusiones:

A la hora de mirar las bondades de cada uno de los sistemas operativos para móviles estudiados en la presente monografía se puede afirmar que, en el caso de los sistemas Android, su costo al usuario final, así como el hecho de trabajar con plataforma abierta, además de no depender de un solo canal de distribución para sus aplicaciones lo convierten en una opción bastante llamativa, tanto para usuarios finales como para desarrolladores. La desventaja principal en este tipo de sistemas está asociada con los ataques de malware que pueden existir en aplicaciones disponible en su tienda Apple Store.

Para el caso de los dispositivos móviles con sistema IOS, la característica que llama más la atención son los niveles de seguridad ofrecidos por la plataforma, que, aunque no pueden ser considerados invulnerables, si existe un proceso de revisión, cuando los desarrolladores desean publicar una aplicación en su tienda de Apple. Otra de las variables en las cuales este sistema encuentra buenas calificaciones son sus diseños e interfaces de usuarios. El costo de sus equipos juega en contra a la hora de compararlos con su competencia.

Las características ofrecidas por cada una de las plataformas estudiadas en la monografía relacionadas con control total o más amplio de los equipos (jailbreaking, rooting), dejan abiertas puestas de seguridad accesible a los cibercriminales.

Tareas tan comunes como deshabilitar característica Bluetooth en los Smartphones, el uso restringido de redes gratuitas (Wi-Fi), y la utilización de programas antivirus confiables hacen que los riesgos de seguridad existentes en el ámbito de lo teléfonos móviles se reduzcan.

Los dispositivos móviles requieren de dos tipos de protecciones orientadas a evitar

diferentes tipos de amenazas que los asechan. Los riegos asociados con el primer tipo de protección (ciberseguridad) tienen que ver con amenazas asociadas a ataques de malware y vulnerabilidades en dispositivos, entre otros. En cuanto al segundo tipo de protección (física), los equipos están expuestos a daños de tipo físico, tales como humedad, exposición a temperaturas extremas, o al robo o extravío del dispositivo.

Tomando como base estudios publicados en la Séptima Cumbre Latinoamericana de Analistas de Seguridad en realizados en el año 2017, se ´puede indicar que los fraudes financieros, el ransomware y los ataques móviles son las amenazas cibernéticas más comunes que se presentan en América Latina.

En cuanto a fallas de seguridad identificadas en las dos plataformas estudiadas en la presente monografía, IOS presentó menos de la mitad de fallas identificadas comparadas con las halladas en la plataforma Android en el año 2017 (124 frente a 322 vulnerabilidades detectadas).

En el ámbito local, las principales amenazas y ataques que afectaron a Colombia en el año 2017 fueron: phishing, spam, malware y criptojacking. Especialistas en aspectos de seguridad informática consideran que las empresas colombianas han ido entendiendo la importancia que se le debe brindar a este tema, sin embargo, debido a la rápida evolución de las técnicas del cibercrimen consideran prudente llevar a cabo mayores esfuerzos económicos y técnicos para enfrentarlas y reducir su impacto.

Entre los errores más comunes que cometen los usuarios de dispositivos móviles se encuentran: la instalación de aplicaciones de fuentes desconocidas, hacer clic en enlaces desconocidos, definición de contraseñas débiles, no activación de bloqueo de dispositivos, no instalación de software antivirus reconocido y llevar a cabo labores de Jailbreaking o Rooting.

A la hora de identificar puntos a tener en cuenta para proteger los dispositivos móviles contra ataques y amenazas de diferentes índoles, algunas de las buenas prácticas o recomendaciones a tener en cuenta para mitigarlas son: mantener actualizados tanto el sistema operativo como sus aplicaciones, descarga de aplicaciones de fuentes confiables, y mantener en lo posible deshabilitada la opción de ubicación del equipo y evitar las conexiones a Wi-Fi inseguras.

La gran mayoría de soluciones de seguridad en el mercado actual ofrecen aplicaciones antirrobos, administración de contraseñas, y bloqueadores de aplicaciones. Esto para dejar claro que las compañías no ofrecen soluciones que ataques una falla o vulnerabilidad específica, sino que apuntan a cubrir un gran objetivo definido como lo es brindar seguridad a los equipos móviles de sus clientes en diferentes escenarios a los que se enfrenten en la vida cotidiana.

Tratando en tema de la distribución del mercado de los dispositivos móviles en lo que tiene que ver con los sistemas operativos dominantes, las estadísticas muestran que la mayor parte se encuentra distribuido entre las plataformas Android y IOS. Tomando como punto de comparación las ventas por fabricantes a nivel mundial los principales contendores en este mercado son Samsung y Apple.

AUTOR: YAMIR ASMIRIO MUÑOZ CACERES