ANÁLISIS A LA SEGURIDAD EN APLICACIONES MÓVILES PARA SMARTPHONE SAMSUNG CON SISTEMA ANDROID 5.1

YESNIR ANTONIO REDONDO DANIEL

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA

ESCUELA DE CIENCIAS BÁSICAS E INGENIERÍA

ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA

RIOHACHA – LA GUAJIRA

2019

ANÁLISIS A LA SEGURIDAD EN APLICACIONES MÓVILES PARA SMARTPHONE SAMSUNG CON SISTEMA ANDROID 5.1

YESNIR ANTONIO REDONDO DANIEL

Monografía de grado para optar al título de especialista en seguridad informática

DIRECTOR

Martin Camilo Cancelado

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA

ESCUELA DE CIENCIAS BÁSICAS E INGENIERÍA

ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA

RIOHACHA – LA GUAJIRA

2019

NOTA DE ACEPTACION

_____

_____

_____

_____

_____

_____

_____

FIRMA DEL PRESIDENTE DEL JURADO

_____

FIRMA DEL JURADO

_____

FIRMA DEL JURADO

Riohacha, 11 de septiembre de 2019

DEDICATORIA

Dedico esta monografía a mis padres y hermanos
de quienes siempre he recibido un apoyo
incondicional, a mis amigos y compañeros
por el acompañamiento y la confianza,
gracias por creer que este logro, si era posible.

CONTENIDO

LISTA DE FIGURAS

pag.

INTRODUCCIÓN

La seguridad de la información se ha convertido en el pilar fundamental en todo el mundo, debido a la gran cantidad de amenazas que se presentan a diario, por ello es importante buscar siempre la manera de estar seguros, siendo necesario utilizar un gran número de herramientas tanto de hardware como de software que ayuden a minimizarlas.

Así como hay un aumento de dispositivos móviles en el mundo va creciendo el número de amenazas a estos y más al sistema operativo Android, el cual es el que domina el mercado mundial, por esta razón se elige en este estudio a la seguridad de sus aplicaciones móviles y más específicamente en su versión 5.1 Lollipop.

Se trata es de analizar la seguridad en las aplicaciones móviles en los teléfonos inteligentes de la marca Samsung que utilizan el sistema operativo Android 5.1, para dar a conocer los riesgos que pueden provocar la descarga de éstas y así mismo explorar algunos métodos preventivos que se deben tener ante la filtración de algún malware. Para ellos, se especifican inicialmente la estructura del Sistema Operativo Android (SOA) en su versión 5.1, los dispositivos Samsung que soportan dicha aplicación, los estándares de seguridad que maneja el SOA, para posteriormente mostrar las aplicaciones móviles más utilizadas y así determinar los niveles de seguridad. Una vez delimitado la temática de interés, se realiza la debida búsqueda de material bibliográfico para el análisis de la situación objeto de estudio y finalmente brindar una síntesis de aporte que vincule lo ya investigado por otros, la reflexión propia y el aporte que se requiere.

Es importante resaltar que el uso de los dispositivos móviles ha tenido un incremento en los últimos años, es por ello que se hace más atractivo para que los piratas informáticos realicen acciones que buscan vulnerar la seguridad de los mismos con el fin de conseguir algún tipo de información de los usuarios que le pueda servir para su lucro personal, esto se puede soportar en el estudio de Juniper

Networks, donde se argumenta que aunque “en 2010 el malware dirigido a Android constituía únicamente el 24 % de todas las amenazas de malware para dispositivos móviles, en la actualidad, estas amenazas suponen un 90 % de todo el malware destinado a dispositivos móviles”[1].

[1] Karpesky Seguridad para Android: cinco consejos fundamentales, Seguridad en Internet. 2017. Disponible en https://latam.kaspersky.com/resource-center/preemptive-safety/android-security-tips.

1. PLANTEAMIENTO DEL PROBLEMA

La necesidad de comunicación social ha puesto en marcha la promoción de aparatos con tecnologías móviles que permiten al ser humano mantenerse comunicado y realizar diversas operaciones donde se ahorra tiempo, dinero y agotamiento físico. Estas operaciones que por lo general suelen ser personales requieren que el equipo esté lo suficientemente protegido para evitar filtración de información o invasión por parte de malware entre otros códigos maliciosos que pueden colocar en riesgo la información que se maneja desde el dispositivo inteligente. En este estudio monográfico, se presenta interés de explorar el entorno móvil del sistema operativo Android 5.1 para celulares inteligentes de la marca Samsung, con la intención de analizar los niveles de seguridad de las aplicaciones que se ofrecen al usuario.

Con gran frecuencia las personas descargan aplicaciones sin conocer, los peligros, amenazas y vulnerabilidades de seguridad que se pueden presentar, no saben si por medio de estos puedan capturar la información que cada uno maneja en su dispositivo móvil como son, claves, información bancaria, información personal entre otros. Por ello se hace necesario brindar la información suficiente a la población para que a partir de ella puedan prevenir y protegerse de este tipo de situaciones originadas por terceros, por medio de las aplicaciones, aprovechando las vulnerabilidades de los sistemas operativos y el poco conocimiento en materia de seguridad informática de algunos usuarios.

Anteriormente los cibercriminales atacaban a los servidores que manejaban el gran flujo de información, pero esto con el pasar del tiempo ha dejado de ser interesante para ellos, debido a que cada día esto se hace más difícil, riesgoso y costoso, es por ello que han buscado otras formas de realizar sus ataques que le puedan ayudar al cumplimiento de sus objetivos, usando el eslabón más débil que se presenta en un sistema seguro, el usuario final, por ser la persona que menos conocimiento tiene sobre los mecanismos de protección ante el riesgo de un posible ataque.

Android, corresponde a ser una plataforma móvil libre, de mayor uso en la actualidad ya que posee software abierto legitimado bajo la licencia Apache para el uso de diversas aplicaciones y adicionalmente es de fácil manejo por la población. En este sentido, su libertad de uso puede provocar el fluido paso (en casos imperceptible) de amenazas que afectan la seguridad de la información privada del usuario del dispositivo móvil. Capobianco[2], expresa que los dispositivos móviles, son presentados al usuario listo con las aplicaciones que éste puede requerir utilizar, sin embargo, hoy es posible descargar aún más aplicaciones de las ya adheridas al equipo. Situación que lleva al usuario a preocuparse por los niveles de seguridad de la información que confía en estos aparatos. De esta manera, es posible preguntarse: ¿Cuáles son las aplicaciones móviles más utilizadas en los Smartphone Samsung con sistema operativo Android 5,1? ¿Qué características de software poseen y cuáles le son permitidas descargar? ¿Cómo son los niveles de seguridad de las aplicaciones móviles? ¿Cuáles son los parámetros de seguridad de las aplicaciones móviles con relación a su uso en los Smartphone Samsung? Para finalmente responder ¿Cuáles son los niveles de seguridad que se presentan en las aplicaciones móviles para Smartphone Samsung con Sistema Operativo Android 5,1?

[2] Capobianco, M; Stankevicius, A; Echaiz, J. Seguridad y privacidad en la plataforma Android. 2009

2. JUSTIFICACIÓN

En virtud del creciente uso de los dispositivos móviles creados y evolucionados en tecnologías para satisfacer las necesidades de comunicación de las personas y adicionalmente la gran cantidad de aplicaciones que ofrecen a los sistemas operativos de estos equipos, se mira con preocupación los niveles de seguridad a los que se enfrentan los usuarios al momento de descargar una determinada aplicación. En este sentido, se hace necesario teóricamente describir las aplicaciones móviles utilizadas bajo el sistema operativo Android en su versión 5,1 con la finalidad práctica de determinar cuáles son los parámetros de seguridad que contiene el equipo móvil ante la presencia de cierta aplicación, siendo potencialmente recomendada para su descarga o no. De esta manera, es posible sintetizar las aplicaciones que permiten los sistemas operativos de los dispositivos y los parámetros de seguridad.

En el contexto Colombiano, encontramos el Sistema Nacional de Ciencia, Tecnología e Innovación (SN-CTI) el cual, según lo señalado por Montenegro[3], respalda, a través de la Ley 1286 de 2009, que los procesos de generación de nuevo conocimiento, enfáticamente, respaldan acciones dinámicas y estructuradas, con el propósito de generar un mayor impacto en las comunidades, ubicando esta investigación en un aporte significativo al desarrollo científico de las diferentes regiones del país, debido al acelerado crecimiento que tiene el uso de los dispositivos móviles para resolver gran cantidad de situaciones humanas, simplificando el trabajo físico, entre otros. Su relevancia y pertinencia, se fundamenta en satisfacer los intereses personales y sociales de la población en general, dando a conocer lo que representa sumergirse en el avance tecnológico, sus alcances y riesgos adicionando la posibilidad de conocer mecanismos de protección de su información confidencial.

[3] Montenegro, L. Ciencia, tecnología e innovación en Colombia. 2014. Revista *UNIMAR*, 32(1), p. 11-13

La investigación monográfica se proyecta hacia la exploración de información aportada por otros estudios sobre la seguridad en aplicaciones móviles con SO Android y adicionalmente brindar un aporte novedoso que permita a la población colombiana y de otros entornos sociales conocer los escenarios bajo los cuales pone en riesgo la información personal manejada desde los dispositivos móviles para prevenir situaciones desagradables.

3. OBJETIVOS

3.1 OBJETIVO GENERAL

Analizar la seguridad de las aplicaciones móviles en los Smartphone Samsung con sistema operativo Android en su versión 5.1, para dar a conocer los riesgos que se pueden presentar al descargar algunas aplicaciones aprovechando las vulnerabilidades en su sistema.

3.2 OBJETIVOS ESPECÍFICOS

1. Describir la estructura del Sistema Operativo Android 5,1
2. Analizar las características de los Smartphone Samsung que soportan el uso del Sistema Operativo Android 5.1
3. Describir las aplicaciones móviles más utilizadas en los Smartphone Samsung con Sistema Operativo Android 5.1
4. Identificar los estándares de seguridad propuestos para el sistema operativo Android en su versión 5.1

4. MARCO CONCEPTUAL Y TEÓRICO

4.1 INVESTIGACIONES PREVIAS RELACIONADAS

En el contexto de este estudio, se encuentran investigaciones previas relacionadas que aportan fundamento contextualizado bajo la visión de diversos investigadores en diferentes partes del mundo. En este particular, se considera una investigación base fundamental, la mostrada por Montenegro la cual presenta los retos y compromisos que tiene el SN-CTI en la promoción de actividades académicas, científicas e investigativas relacionadas con los avances educativos para el desarrollo de la comunidad en general y "Al mismo tiempo, sostiene el hecho de establecer el conocimiento y su aplicación en los procesos de innovación, como un bien infinito, aplicable en los diversos contextos y maleable"[4], permitiendo la inversión económica que se le da a la educación y que en cierto plazo representa crecimiento económico para la población y/ o comunidad que lo aprovechará. En este sentido, su relación de aporte con este estudio radica en la importancia de fortalecer la comunidad científica colombiana en cuanto a los avances tecnológicos y al conocimiento de los mecanismos de comunicación más cercanos a la población quienes gozan de tecnologías móviles conscientemente desarrolladas para facilitar las diferentes operaciones personales que cada individuo debe realizar y es necesario que gocen del debido nivel de seguridad.

Seguidamente se presenta la investigación del Instituto Nacional de Tecnologías de la Comunicación (INTECO) en España, bajo la dirección de Pérez[5], correspondiente al informe anual generado en el año 2011 que comprende el análisis de 3655 entrevistas realizadas online (en PC) donde se realiza un diagnóstico de cómo se deben utilizar los dispositivos móviles y Smartphones por parte de los usuarios españoles de equipos con esta tecnología, en cuanto a las

[4] Ibíd., p. 11-13.
[5] Pérez, San José. Estudio sobre seguridad en dispositivos móviles y smartphones. 2011. Disponible en: https://www.red.es/redes/sites/redes/files/estudio_moviles_3c11.pdf

herramientas, usos y seguridad. Entre los análisis realizados se destaca la frecuencia de compartir información vía bluetooth, y establecer conexiones de internet y WiFi móvil. Destacan además que la frecuencia de uso que se le da al dispositivo móvil es para la lectura de correos electrónicos, descargar aplicaciones móviles y utilizar el servicio de localización geográfica para trasladarse a diversos lugares donde se desconoce el camino. En cuanto a las medidas de seguridad, el usuario utiliza clave de acceso al dispositivo móvil, bloqueo en inactividad y activación de bluetooth solo cuando va a utilizarlo. Las incidencias de seguridad indican extravío de contraseña, robo del equipo, virus o malware y fraudes telefónicos, encontrándose un 81.6% de personas que no han logrado demostrar algún suceso de los mencionados. La relación de aporte con lo que se espera de este estudio, es brindar innovación a los ciudadanos colombianos en el conocimiento de las tecnologías que manejan en función de canalizar actualizaciones en cuanto a seguridad tecnológica necesaria en virtud del creciente número de aplicaciones digitales para realizar transacciones bancarias, registro de datos personales, entre otras informaciones de nivel personal. El desarrollo de este tipo de estudios permite dar a conocer a las empresas en general el nivel de competencia que presentan los diferentes equipos y aplicaciones móviles en cuanto a los estándares de seguridad que representa cada uno de ellos para los usuarios.

Otro estudio de gran interés relacionado con ésta investigación corresponde al elaborado por González[6] titulado: *Seguridad en Dispositivos Android* presentado en las VI Jornada de Seguridad y Protección de Datos de Carácter Personal, en el destacan la importancia de estudiar el Sistema Android por ser el de mayor interés empresarial, se puede considerar susceptible de padecer diversas amenazas cibernéticas y la esencial relación con el estudio que aquí se presenta, es el poco análisis que se ha realizado sobre el riesgo de las aplicaciones que permite descargar Android.

[6] González, P. Seguridad en Dispositivos Android. 2014. Disponible en: https://lsi.vc.ehu.eus/pablogn/investig/JornadasSeguridad141112.pdf

También, Soroa[7] presenta el estudio en el cual abordan todos los contenidos y aspectos que son necesarios para la creación de la empresa de aplicaciones informáticas". considerando los diversos pasos para la creación y desarrollo de las aplicaciones móviles, lo que representa gran utilidad en esta investigación pues al analizar sus parámetros de diseño y creación es posible delimitar los posibles riesgos y las posibilidades de proteger la información que se maneje desde el dispositivo.

4.2 MARCO TEÓRICO

Es aquí donde se expresan los aspectos teóricos que fundamentan el estudio, partiendo de investigaciones realizadas por otros investigadores para el abordaje de asuntos relacionados.

Es importante realizar un recorrido por todas las versiones del sistema operativo para aplicaciones móviles como es el caso de Android, donde, según su página oficial, muestra al público todas sus versiones principales las cuales llevan nombres de dulces, estas son:

Apple Pie 1.0 (Tarta de Manzana), es la primera versión no utilizada de forma comercial y fue lanzada el 23 de septiembre 2008.

Banana Bread 1.1 (Pan de Banana), es una versión que buscaba corregir los errores presentados en la Apple Pie 1.0 que al igual que esta no fue de uso comercial y se lanzó el 9 de febrero de 2009.

Cupcake 1.5 (Magdalena), versión lanzada el 30 de abril del 2009, basada en el Kernel de Linux 2.6.27, incorpora la grabación y reproducción de videos, con capacidad para interactuar con programas de imágenes como es el Picasa y la

[7] Soroa, P. Estudio de viabilidad de una empresa de aplicaciones móviles. Proyecto Fin de Carrera. Universidad de Sevilla. España. 2014. p. 7.

plataforma de videos en línea YouTube, teclado con opción de autocompletar, Bluetooth y diferentes estilos de protector de pantalla.

Android 1.6 Donut, representó los primeros pasos del sistema, colocando la información del mundo en la palma de las manos del usuario y permitiendo a la empresa evolucionar. Basado en el Kernel de Linux 2.6.29, con fecha de lanzamiento del 15 de septiembre de 2009. En este se utiliza la búsqueda por voz.

Android 2.1 Eclair, su pantalla de alta densidad permitía mostrar fondos de pantalla que respondían al tocarlos, además de permitir los datos de navegación o recorrido físico de la persona en tiempo real, incluyendo el tráfico. Esta fue lanzada el 26 de octubre de 2009 y también es basada en el kernel de Linux 2.6.29 como es el caso de la versión 1.6 Donut.

Android 2.2 Froyo, da a conocer un sistema de teléfono ultrarrápido controlado por voz si se quería, además de permitir la conexión a internet en zonas WiFi. Fue lanzado el 20 de mayo del 2010, basado en el kernel de Linux 2.6.32

Android 2.3 Gingerbread, correspondía a una versión más sencilla pero rápida. Nuevo nivel en juegos y mayor duración de la batería, optimiza la categoría de aplicaciones gracias a su compatibilidad con NFC. Lanzado el 6 de diciembre de 2010, bajo el kernel de Linux 2.6.35.7

Android 3.0 Honeycomb, con las tablets en el mercado, presenta una interfaz sencilla que incluía grandes imágenes y navegación en pantalla fluida. Lanzado el 22 de febrero del 2011, con soporte de video chat usando Google Talk.

Android 4.0 Ice Cream Sandwich, permite personalizar la pantalla de inicio, establecer la cantidad de datos a utilizar y compartir información en cualquier momento. Lanzado el 19 de octubre de 2011, incorpora el reconocimiento facial y de voz del usuario.

Android 4.1 Jelly Bean, esta versión fue lanzada el 9 de julio del 2012, marca el inicio de la asistencia móvil personalizada con Google Now. Permitía la

interacción con las notificaciones y las diferentes cuentas del usuario, incluye nuevas lenguas distintas a las occidentales, además en esta Google Chrome se adapta como el navegador por defecto y se llega al final del soporte Flash Player.

Android 4.4 KitKat, versión lanzada el 31 de octubre de 2013 ejecuta acciones por voz, al decir “Ok Google” se inicia una búsqueda, envían mensaje de texto y también se puede escuchar música, además de presentar un nuevo diseño de contenido.

Android 5.0 Lollipop, lanzada el 25 de junio de 2014, llega a teléfonos, tablet, televisores, relojes, autos, incorporando Material Design con diseño atractivo y respuesta táctil rápida.

Android 6.0 Marshmallow, lanzada el 28 de mayo de 2015, aquí se tienen accesos directos sencillos y respuestas inteligentes, además que los nuevos permisos de las aplicaciones permiten tener un mayor control de la información.

Como se instala en dispositivos móviles y estáticos de diversas empresas desarrolladoras de equipos digitales. En lo cual es posible que se consideren las tablets, celulares inteligentes de distintas marcas, pero en el desarrollo de este estudio, el tema principal es el Smartphone Samsung, con sistema operativo Android en su versión 5.1.

4.2.1 Dispositivo Móvil

El término móvil, es utilizado desde diferentes ciencias para indicar movimiento de traslado de un lugar a otro de una cosa, incluso para indicar los movimientos del cuerpo humano. Cuando se hace referencia a un dispositivo móvil, señala Tardáguila[8], que se puede definir como aquellos micro-ordenadores que son lo suficientemente ligeros como para ser transportados por una persona, y que

[8] Tardáguila, C. Dispositivos móviles y multimedia. MOSAIC tecnología y comunicación multimedia. 2009. p. 4.

disponen de la capacidad de batería suficiente como para poder funcionar de forma autónoma. Este autor, establece una aclaratoria importante sobre no darle el calificativo de dispositivo móvil a un computador portátil, porque evidentemente no se definen de la misma forma.

Adicionalmente Morillo[9] indica que su definición se da en cuatro características que lo diferencian de otros dispositivos, como son:

1. Movilidad.
2. Tamaño reducido.
3. Comunicación inalámbrica.
4. Interacción con las personas.

Es de saber, que cada dispositivo móvil esta enriquecido de componentes estructurales que corresponden al hardware y de sistema que representan el software del equipo que es necesario describir, pues no todos contienen las mismas capacidades para el uso de ciertas aplicaciones. Esto implica una ampliación detallada de características que identifican a los dispositivos móviles y a las que Morillo (s/f) incorpora su capacidad de procesamiento, conexión a la red, memoria RAM, tarjetas MicroSD, flash, su uso en general es personal.

4.2.2 Tipos de Dispositivos Móviles

La necesidad de comunicación ha existido en todas las épocas que ha vivido la humanidad, el medio utilizado para que se de éste proceso ha evolucionado en correspondencia con los descubrimientos científicos que ha alcanzado la inteligencia humana. Posterior al surgimiento de los ordenadores que resolvieron grandes situaciones de cálculos y problemáticas organizacionales de manos de

[9]Morillo, J. (s/f). Introducción a los dispositivos móviles. Universidad Oberta de Catalunya. p.7. Disponible en: https://www.exabyteinformatica.com/uoc/Informatica/Tecnologia.pdf

profesionales que se desenvuelven en diversos ambientes laborales, surgen equipos de menor tamaño que facilitan el transporte de gran cantidad de información y alta capacidad de comunicación que son llamados dispositivos móviles y que Morillo[10] (s/f) lo muestra más ampliamente distinguiéndolos como: teléfonos móviles, organizadores y asistentes personales digitales, web-enabled phones, two-way pagers, Smartphones, handheld PC, tablet PC, tablets, libros electrónicos, pero Tardáguila[11] lo divide en tres clases.

1. Teléfonos.
2. PDAs, organizadores electrónicos u ordenadores de mano (Asistente Personal Digital).
3. Consolas.

Estos equipos han sido perfeccionados en el tiempo, pues inicialmente sólo permitían la realización de llamadas y envío de mensajes, en la actualidad su utilidad se ha vuelto casi imprescindible para las personas en el manejo de situaciones sociales propias de la vida cotidiana como mostrar su localización, realizar operaciones bancarias, hacer uso de la red para enviar correos electrónicos, realizar dinámicas comunicacionales mediante redes sociales, jugar, entre otras cosas. En este estudio se centra el interés por los dispositivos móviles que cuentan con el sistema operativo Android, es decir "a los teléfonos inteligentes (o "smartphones") que están desplazando a los teléfonos móviles convencionales, y a las tabletas (o "tablets") que compiten en prestaciones con los ordenadores portátiles"[12]. cuyo sistema operativo permite la descarga de aplicaciones conforme a la conveniencia o necesidad del usuario del equipo. Se observa con interés, el desplazamiento que van teniendo los ordenadores y laptop visto que sus potenciales acciones, van siendo incorporadas a estos dispositivos móviles cada

[10] Ibíd., p. 11.
[11] Tardáguila. Op., cit. p. 5.
[12] Gobierno de Navarra (s/f). Acércate a las TIC. Uso de dispositivos móviles (teléfonos móviles, "smartphones", "ebooks", GPS y "tablets"). p. 1. Disponible en: https://www.navarra.es/NR/rdonlyres/48F9746B-080C-4DEA-BD95-A5B6E01797E1/315641/7Usodedispositivosmoviles.pdf

vez más rápido; es por ello que hay que prestar atención a la posibilidad de presencia de algún malware y/o delincuentes cibernéticos, que busquen a través de las descargas de aplicaciones, acceder al equipo para manejar información confidencial y ocasionar daños al usuario, por ello la importancia de analizar la seguridad de las aplicaciones móviles en los sistemas operativos Android.

Trasladando el interés exclusivamente a los teléfonos inteligentes también llamados *Smartphones*, es posible indicar que sus características funcionales difieren de los convencionales básicamente en su amplio uso y su forma física es más sofisticada pues en la mayoría de los diseños sus teclados pasan a ser virtuales incluso permitiendo al usuario seleccionar el tipo de letra con que desea escribir, además de contar con una pantalla más amplia. Con relación al software de éstos equipos, se señala que, "Los teléfonos inteligentes tienen preinstalado su propio sistema operativo, acompañado de un conjunto básico de aplicaciones de uso común. El sistema operativo determina el aspecto de la pantalla, el entorno de trabajo y el manejo del aparato. El propietario o propietaria podrá configurar el dispositivo a su gusto y añadir nuevos programas, gratuitos o de pago"[13].

Cada marca de teléfono inteligente está asociada a un sistema operativo específico. Los que se encuentran actualmente más utilizados en el mercado son:

1. ***Sistema operativo iOS***, instalado en los dispositivos fabricados por ***Apple***, empresa que además cuenta con una tienda virtual de aplicaciones (*apps*)
2. ***Sistema operativo Android***, instalado habitualmente en los ***Smartphone***, es un sistema de código abierto asociado con ***Google*** y dispone de su tienda *on line* ***Google play*** para descargar aplicaciones (*apps*)
3. ***Sistema operativo Windows 8***, instalado en algunos Smartphone es de propiedad de la empresa ***Microsoft***, corresponde a lo esperado de la

[13] Ibíd., p. 7.

Redmond, sin embargo, es algo cuestionado por su falta de aplicaciones, que son necesarias para los usuarios.

4. El ***sistema operativo Firefox***, desarrollado por Mozilla Corporation, gratuito y de código abierto basado en ***HTML5,*** núcleo Linux, sus aplicaciones tienen comunicación con el dispositivo móvil mediante ***JavaScript*** y ***Open Web APIs***.

Ahora bien, de los sistemas operativos mencionados, Android es el de mayor interés en este estudio, por ser el más utilizado y por ende el de mayor riesgo a ataques. El estudio presentado por la empresa Deloitte donde encuestaron a 41 países y 49.000 entrevistadores, representando el 70% de la población mundial reportan que en Colombia se tomaron en cuenta 1000 personas de las cuales el 96% aseguran ser propietarios de equipos inteligentes, y ante la pregunta sobre *¿Cuáles de los siguientes dispositivos posee o tiene a su disposición*? manifestaron para el Teléfono Inteligente (Phablet) en el año 2015 un 32% y en 2016 un 40%; para el Teléfono Inteligente Normal en 2015 un 71% y en 2016 un 65%; el Teléfono Básico en 2015 un 12% y 2016 el 8%. Con relación a las tendencias de marcas móviles utilizadas predominó en ese estudio Samsung con un 34% en 2015 y un 39% en 2016, siguiéndole Huawei con un 15% en 2015 y 17% en 2016, otros con el 5% en 2015 y 11% en 2016, también en igual medida la Apple y Motorola con 10% para ambos años, quedando con los menores porcentajes Nokia, Alcatel, Sony, LG, Avvio, HTC. Como se observa en este estudio, predomina el uso de Samsung y Huawei, dispositivos móviles que usualmente se conoce que contienen sistemas operativos Android de manera que se muestra la importancia, relevancia y pertinencia del análisis a la seguridad de las aplicaciones móviles que con frecuencia se descargan e instalan en estos equipos[14].

[14] Deloitte. Consumo móvil en Colombia. Los móviles prueban ser indispensables en un mundo "siempre" conectado. 2017. Disponible en: https://www2.deloitte.com/content/dam/Deloitte/co/Documents/technology-media-telecommunications/Consumo%20movil(VF1).pdf

4.2.3 Estructura del Sistema Operativo Android

Para el análisis de la seguridad, es esencial en primera instancia identificar lo que es el SOA el cual desde su aparición en el mercado de los dispositivos móviles ha alcanzado una considerable evolución. Así pues, Molina[15], señala que Android es un sistema operativo para dispositivos móviles como teléfonos inteligentes y tabletas basado en el núcleo Linux. Es desarrollado por la Open Handset Allianse, la cual es liderada por Google, usando diversos conjuntos de herramientas de software de código abierto para dispositivos móviles.

Este SOA, brinda una plataforma que permite a los creadores de diversas aplicaciones móviles la posibilidad de ofrecerlas bajo descarga conforme al gusto del operador del dispositivo. Es de saber que esta tecnología va evolucionando a medida que los investigadores que diseñan las aplicaciones van evolucionando en los requerimientos para el desarrollo de la misma. De esta manera, se encuentran versiones cada día más actualizadas. Es de saber que, a diferencia de otros sistemas operativos, Android no necesariamente está asociada a una marca de teléfono en específico. Su sistema muy utilizado lo hace atractivo a la presencia de ataques a las aplicaciones de uso personal y confidencial, señala Basualdo;

> "Android es la plataforma que más sufre el malware con el 92% del total, debido en parte a las distintas versiones que circulan del sistema operativo. Según Google, el 3 de junio de 2013 solo el 4% de los usuarios de Android poseen la versión más reciente del sistema que esta inmune a las vulnerabilidades que explotan alrededor del 77% del malware para Android"[16].

[15] Molina, Y. Sistema operativo android: características y funcionalidad para dispositivos móviles. Programa Ingeniería de Sistemas y Computación. 2012. p. 37. Disponible en: http://repositorio.utp.edu.co/dspace/bitstream/handle/11059.

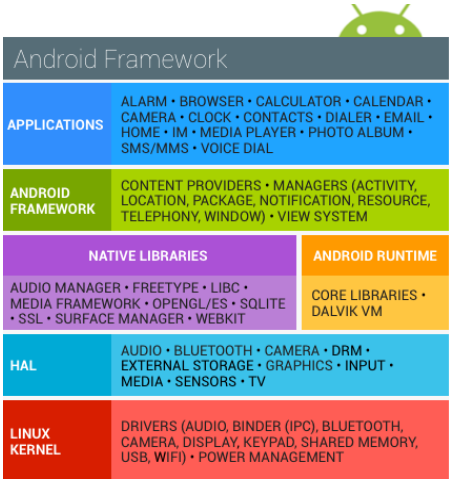
[16] Basualdo, A. El malware para los dispositivos móviles ha crecido un 600%, Android es el mayor objetivo. 2013. Disponible en: http://googlelizados.com/malware-dispositivos-moviles-crecido-600-ciento-Android-mayor-objetivo

Con la evolución de los dispositivos móviles, ha aumentado el riesgo a la información que en ellos se maneja, en la mayoría de los casos porque el usuario desconoce la forma como proteger la información al momento de hacer uso de aplicaciones desconocidas. Betancourt y Eraso[17] expresan que la mayor parte de los virus troyanos llegan vía mensajes SMS; medio que representa el 48% de las agresiones, le siguen con 29% las aplicaciones falsas y el 19% se origina en malware espía. También las conexiones inalámbricas, bluetooth ponen en riesgo la seguridad de los equipos con tecnología Android, es por ello que el usuario requiere conocer los riesgos que corre y aprender un poco sobre la manera de protegerse.

El sistema operativo Android al igual que Windows, distribuciones de Linux, etc. Está dividido por capas que componen su arquitectura. Cada una asume su responsabilidad y confía que la siguiente posee la seguridad adecuada. “Con la excepción de una pequeña cantidad de código del sistema operativo Android que se ejecuta como raíz, todo el código que está sobre el Kernel de Linux está restringido por Application Sandbox”[18].

[17] Betancur, J, Oscar; Eraso H, Sonia. Seguridad en dispositivos móviles Android. Monografía (Especialista en seguridad informática). Universidad Nacional Abierta Y A Distancia – UNAD. 2015. p. 14. Disponible en http://stadium.unad.edu.co/preview/UNAD.php?url=/bitstream/10596/3614/1/59836994.pdf.
[18] Android Open Source Project. Seguridad. 2018. Disponible en, https://source.android.com/security/

Figura 1. Pila de software Android



Fuente: Android Open Source Project. Pila de software Android. Seguridad [Consultado 15 de septiembre de 2018]. Disponible en: https://source.android.com/security/

Como se puede evidenciar en la figura las capas del sistema operativo Android, se muestran en una fila que va de abajo hacia arriba, que es necesario describir;

Kernel de Linux, proporciona el power management y los drivers para el audio, Binder, el bluetooth, la cámara, display, keypad, entre otros.

HAL, realiza el proceso de acceso y abstracción del hardware.

Native Libraries y Android Runtime, posee las librerías que ayudan a la seguridad de las comunicaciones, en la web, la máquina virtual de Dalvick

Android Framework, brinda acceso a las diferentes funcionalidades e información que se encuentra en el dispositivo.

Aplications, son las distintas aplicaciones del sistema operativo Android, como son; alarma, calculadora, calendario, cámara, reloj, álbum de fotos, grabador de vos, entre otros.

El SOA posee características específicas descritas por Basterra et al, a saber:

1. Logo que lo identifica.
2. Código abierto.
3. Núcleo basado en el Kernel de Linux.
4. Adaptable a muchas pantallas y resoluciones.
5. Utiliza SQLite para el almacenamiento de datos.
6. Ofrece diferentes formas de mensajería.
7. Navegador web basado en WebKit incluido.
8. Soporte de Java y muchos formatos multimedia.
9. Soporte de HTML, HTML5, Adobe Flash Player, etc.
10. Incluye un emulador de dispositivos, herramientas para depuración de memorias y análisis del rendimiento del software.
11. Catálogo de aplicaciones gratuitas o pagas en el que pueden ser descargadas e instaladas (Google Play).
12. Bluetooth
13. Google Talk desde su versión HoneyComb, para realizar video llamadas.
14. Multitarea real de aplicaciones.

Señala García[19] que Android es un sistema operativo móvil basado en Linux, desarrollado inicialmente por Android Inc. En 2003 y comprada por Google en 2005. y expresa además sobre el nombre que, aunque es el mismo de la empresa, su razón se debe "a la novela de Philip K. Dick *¿Sueñan los androides con ovejas eléctricas*? que posteriormente fue adaptada al cine como Blade Runner"[20]. Con respecto a las características mencionadas anteriormente, cada una de ellas tiene su descripción particular, a saber:

1. El logo que lo identifica, fue diseñado por Irina Blok que tras proponer múltiples diseños que hacían la idea de un robot, la empresa seleccionó el que ella consideró más sencillo.

[19] García, Modesto. La historia del logo de Android. 2012. Disponible en, http://www.brandemia.org/la-historia-del-logo-de-android
[20] Ibid., p. 2.

2. Código Abierto, es llamado simplemente OS (por ´Open Source´), y su diferencia del cerrado es la licencia. Expresa Armendáriz[21], que al tener la licencia de código abierto permite explícitamente: - utilizar el programa para cualquier propósito y sin limitaciones; – estudiar cómo funciona; -redistribuir copias (no se paga por la licencia); - modificar el programa.

3. Núcleo basado en el Kernel de Linux, creado aproximadamente en 1991 por Linus Torvalds, lo define Esteve expresando que:

   > "El núcleo (en inglés Kernel) del sistema GNU/Linux (al que habitualmente denominaremos Linux) [Vasb], es el corazón del sistema: se encarga de arrancarlo y, una vez este es ya utilizable por las aplicaciones y los usuarios, se encarga de gestionar los recursos de la máquina, en forma de gestión de la memoria, del sistema de ficheros, de las operaciones de entrada/salida y de los procesos y su intercomunicación"[22].

4. Adaptable a muchas pantallas y resoluciones, con relación a la compatibilidad que presenta Android con diversas pantallas, en tamaños por categorías como son pequeña, normal grande y extra grande.

5. Utiliza el sistema de administración de almacenamiento de datos SQLite: El departamento de la computación e IA All rights reserved describe a SQLite como un "gestor de base de datos relacional y es de código abierto, cumple con los estándares, y es extremadamente ligero. Además, guarda toda la base de datos en un único fichero"[23]. Es de saber que SQLite permite crear bases de datos totalmente independientes en cada una de las aplicaciones.

---

[21] Armendáriz, Luis. Sobre El código Abierto (Open Source). 2006. p. 2. Disponible en, https://guimi.net/descarga/tec-docs/Sobre_el_OS.pdf

[22] Esteve, José. El Núcleo Linux. 2011. Disponible en http://openaccess.uoc.edu/webapps/o2/bitstream/10609/61265/1/Administraci%C3%B3n%20avanzada%20del%20sistema%20operativo%20GNU_Linux_M%C3%B3dulo1_El%20n%C3%BAcleo%20Linux.pdf. p.5

[23] IA All rights reserved. copyright © 2012-13 Dept ciencia de la computación. 2013. p. 5

6. Ofrece diferentes formas de mensajería: la mensajería nacional propia de la línea telefónica, las aplicaciones de mensajería vía online: el conocido y popular ***WhatsApp*** fundada en 2009 y comprada por la empresa Facebook en 2014, la misma tiene a ***Messenger***, otra es ***Line*** que permite llamadas, envío de multimedia y contiene variedad de stickers, ***We chat*** aplicación China popular en Asia, ***Signal*** app dotada de la mejor seguridad al igual que ***WIRE***, también ***Viber***, ***Hangouts***, ***Threema***, ***Skype*** y ***Telegram*** desarrollada en 2013.

7. Navegador web basado en WebKit incluido. Los navegadores web son aplicaciones de software que representan el punto de partida que abre paso al recorrido virtual de una serie de servicios que son de gran utilidad tanto para el entretenimiento como para simplificar acciones físicas para resolver situaciones propias de la vida cotidiana. RUA (2015) expresa que "un navegador web es una aplicación que permite el acceso a internet, interpreta la información de archivos etiquetados en HTML y los presenta en pantalla según las directrices de presentación codificadas"[24] esta información realizada en una hoja de estilo CSS (Cascading Style Sheet) pasa por un WebKit que "es un motor renderizado de código abierto para navegadores web, desarrollado por Apple sobre la base del motor de renderizado de KHTML del navegador Konqueror"[25] este permite gestionar con los servidores web las solicitudes de descarga y manejo de las páginas web.

8. Soporte de Java y muchos formatos multimedia, corresponde a una plataforma independiente que permite ejecutar aplicaciones programadas en otro sistema, permite además extender las funcionalidades de los navegadores.

[24] Rua. Navegadores. Biblioteca universitaria. 2015. p. 4. Disponible en, https://rua.ua.es/dspace/bitstream/10045/46501/3/ci2_basico_2014-15_Navegadores.pdf.
[25] Ibid., p.9

9. Soporte de HTML, HTML5, Adobe Flash Player, etc., permite la incorporación de programas que facilitan la lectura de documentos en diversos formatos desde la web o mediante la descarga del respectivo programa de Adobe entre otros.

10. Incluye un emulador de dispositivos, que es una herramienta para la depuración de memorias y analizar el rendimiento de las memorias. Esto permite la instalación de aplicaciones para tenerlas visibles en pantalla.

11. Catálogo de aplicaciones tanto gratuitas como pagas que pueden ser descargadas e instaladas, Android cuenta con Google Play Store para mostrar todas las aplicaciones gratis y las que requieren pago, dando facilidad al usuario de seleccionar las que le sean de su gusto y necesidad.

12. Bluetooth, dispositivo industrial para redes inalámbricas transmisor de radiofrecuencia en la banda ISM de los 2.4 GHz, lo que facilita las comunicaciones entre equipos sin necesidad del uso de cables, incluso sin necesidad de internet.

13. Google Talk desde su versión de HoneyComb, para realizar video llamadas, en la medida que se actualizan las versiones de los dispositivos Android, va evolucionando GTalk y desde esa nueva versión se puede mantener una buena comunicación en sonido e imagen al instante a través de Gmail.

14. Multitarea real de aplicaciones, que permite el uso de diversas aplicaciones a la vez desde el mismo dispositivo móvil.

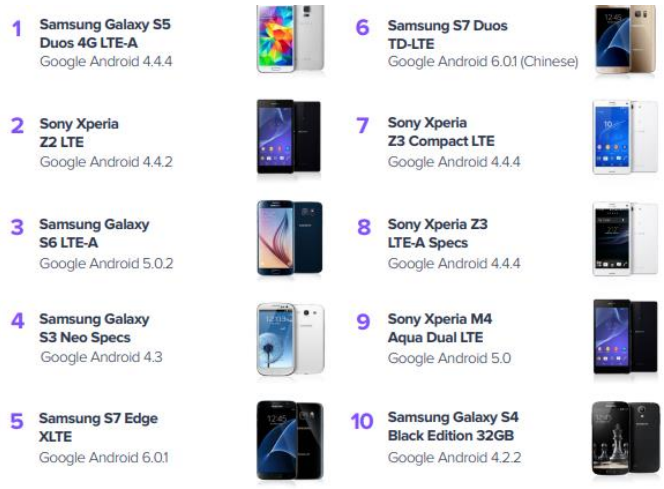
En general, la estructura del sistema operativo Android contiene todas las condiciones necesarias para disfrutar de un dispositivo móvil que proporcione seguridad y confiabilidad en la información que se maneje y a medida que va

pasando el tiempo la empresa va incorporando acciones propias que requiere la proyección de nuevas versiones.

4.2.4 Características de los dispositivos móviles Samsung con sistema operativo Android

Para realizar un análisis es importante tener en cuenta cuáles son los Smartphone más usados. Para ello es importante revisar el informe revelado por Avast, para el primer trimestre del año 2017, donde Samsung es la empresa que sigue dominando el mercado, ya que tiene a 6 de los 10 Smartphone más populares del mercado, correspondiente al 60%, como se evidencia en la siguiente figura

Figura 2. Los dispositivos más populares: Primer trimestre de 2017



Fuente: Informe de rendimiento y tendencias de Avast sobre aplicaciones para Android [Consultado el 10 de octubre de 2018]. Disponible en: http://files.avast.com/files/marketing/materials/es_avast_android_app_report.pdf

4.2.4.1 Samsung

Samsung, hace referencia a un grupo de empresas multinacionales ubicadas en Seúl, Corea del Sur, que cuenta con muchas filiales encargadas de negocios de diversos tipos: electrónica, biotecnología, aseguradoras, construcción, finanzas, tecnología, entre otras, fundado el 01 de marzo 1938 por el empresario Lee Byung-chul para la importación y exportación de diversos productos y luego se incorpora a otro tipo de negocios, siendo en 1990 que se da a conocer de manera internacional con productos electrónicos (electrodomésticos, teléfonos, móviles y semiconductores) llegando a ser Samsung Electronics la empresa más importante bajo su cargo, representando su ingreso el 17% del producto interno bruto nacional.

4.2.4.2 modelos de Smartphone Samsung

Samsung presenta múltiples modelos de Smartphone entre ellos están los que se exhiben en su página oficial: https://www.samsung.com/ y se detallan a continuación:

Samsung Galaxy On 7

Figura 3. Samsung Galaxy On 7

Fuente: Especificaciones: Disponible en https://www.kimovil.com/es/listado-moviles-por-sistema-operativo/android-5-1-1-lollipop

Descripción

1. Marca: Samsung
2. Otros Nombres: SM-G600FY, G600FY, SM-G6000, G6000
3. Presentación: Octubre 2015
4. Relacionados: Predecesor: Samsung Galaxy On5

Diseño y Pantalla

1. Estructura:
    - Tamaño:77.5 mm x 151.8 mm x 8.2 mm
    - Relación de Aspecto: 16:9
    - Peso: 172 g
    - Superficie útil: 70%
    - Materiales: Plastico
    - Colores: Oro, Blanco
    - Origami: Imagen
2. Pantalla:
    - Diagonal: 5.5”
    - Tipo: LCD IPS
    - Resolución: 720 x 1280 px (HD)
    - Densidad: media densidad, 267 Pixeles por pulgada diferenciables a menos de 40 cm. de distancia

- Otras: Capacitiva Multi-Touch

Potencia y Hardware

1. Procesador
    - Modelo: Qualcomm Snapdragon 410 MSM8916v2
    - CPU: ARM Cortex-A53
    - Tipo: Quad-Core
    - Frecuencia de reloj: 1.4 GHz
    - 64 Bits: Si
2. Graficos
    - GPU: Qualcomm Adreno 306
3. RAM
    - RAM: 1.5 GB
    - Tipo: --
4. Antutu

    Puntuación: 21.500 Rendimiento mejor que el 25% de los dispositivos
5. Almacenamiento:
    - Capacidad: 16 GB (Capacidad con el sistema operativo, depende del fabricante y ROM: 9-15 GB)
    - Aproximadamente: 2909 Canciones, 6400 Fotos y 228 Videos
    - Ampliable SD: Si. SD en Slot independiente
6. Seguridad:
    - Huella Dactilar: No

7. Sensores:
    - Huella Dactilar: No
    - Acelerómetro: Si
    - Luz Ambiental: Si
    - Proximidad: Si
8. Otras
    - LED de notificaciones
    - Refrigeración: No

Cámara

1. Trasera:
    - Resolución: 13 Mpx
    - Tipo: CMOS
    - Apertura: f/2.1
    - Flash: LED
    - Estabilización optica: No
    - Video Slow Motion: No. 30.0 fps
    - Caracteristicas: Autoenfoque, disparo continuo o ráfaga, estabilizador de imagen digital, zoom digital, compensación de exposición, detección de rostro, geoetiquetado, HDR, ajuste ISO, fotos panoramicas, modo de escena, enfoque tactil, ajuste de balance de blancos.
2. Selfie:
    - Resolución: 5 Mpx

Conectividad.

1. Compatibilidad de redes por país: Colombia
2. Cobertura:
    - 4G: 1 de 2 B7 (2600)
    - 3G: todas (2), B2 (1900), B5 (850)
    - 2G: todas (2), B2 (1900), B5 (850)
3. Por infraestructura
    - Claro: 4G todas (1), 3G todas (2), 2G todas (2)
    - Movistar: 4G 0 de 1, 3G todas (1), 2G todas (2)
    - TigoUNE: 4G 1 de 2, 3G todas (1), 2G todas (2)
    - Avantel: 4G 0 de 1, 3G todas (1), 2G no disponible
    - ETB: 4G 0 de 1, 3G todas (1), 2G todas (1)
4. Bandas
    - 4G: B1 (2100), B7 (2600), B38 (TDD 2600), B39 (TDD 1900), B40 (TDD 2300) B41 (TDD 2500)
    - 3G: B1 (2100), B2 (1900), B5 (850), B8 (900), B34 (TD 2000) B39 (TD 1900+)
    - 2G: CDMA BC0 (800), B2 (1900), B3 (1800), B5 (850), B8 (900)
5. Tarjeta SIM
    - Tipo: Dual SIM Dual Standby (Micro SIM + Micro SIM). Las tarjetas SIM (MiniSIM) pueden cortarse a MicroSIM, las MicroSIM a NanoSIM, tambien una SIM a NanoSIM (no recomendado)
6. WiFi
    - Estandares: 802.11b, 802.11g, 802.11n

- Otras: Punto acceso Wi-Fi

7. Bluetooth
    - Versión: Bluetooth 4.1
    - Perfiles: A2 DP (Distribución de audio avanzada)
8. Navegación:
    - Soporta: A-GPS, Beidou, GLONASS, GPS
9. USB:
    - Carga: Si
    - Almacen masivo: Si
10. SAR:
    - Medición Europea: 0.384 W/Kg en cabeza, 0,536 W/Kg en cuerpo. La Unión Europea fija como límite 2 W/Kg promediados en 10 gramos de tejido
    - Medición Americana: 0.793 W/Kg en cabeza, 0.904 W/Kg en cuerpo. La FCC fija como límite 1,6 W/Kg medidos en un volumen de 1 gramo de tejido.
11. Otras:
    - Audio Jack: Si
    - Radio FM: Si
    - Computer Sync: Si
    - OTA Sync: Si
    - Compartir Internet: Si

Bateria

1. Bateria:

    - Capacidad: 3000 mAh
    - Tipo: Li-Ion
    - Otras: Baterias Extraibles

Software

1. Sistema Operativo:

    - Android 5.0 Lollipop. Tambien se tienen otros telefonos con sistema operativo Android 5.1.1 Lollipop

4.2.5 Aplicaciones Móviles utilizadas En Los Equipos Con Sistema Operativo Android

Las aplicaciones móviles que contienen los Smartphone Samsung con sistema operativo Android 5.1, ya pasan a representar una necesidad en la vida cotidiana de las personas, pues permite la simplificación de múltiples actividades a través del uso de ellas. Estas en su totalidad son ofrecidas a los usuarios de los móviles por medio de la tienda oficial de Android y creada por Google, llamada Google Play.

En el mundo millones de usuarios utilizan estos dispositivos inteligentes, es decir que hay una gran cantidad de personas, empresas que trabajan y lo manejan para realizar distintas tareas, esto le genera mucho interés a los delincuentes cibernéticos que buscan la manera de sacar provecho, aprovechando el descuido y poco conocimiento de estos usuarios. Por ello es importante crear conciencia en el uso responsable de este tipo de tecnología.

A diario se instalan en los distintos dispositivos móviles aplicaciones de distintos lugares de la red, ya sea de la tienda de cada sistema operativo o desde los orígenes desconocidos, también se visitan páginas que pueden representar

algún riesgo de infección por medio de algún malware o virus, todo esto representa un gran riesgo para los usuarios y el tipo de información que manejan en su Smartphone.

la descarga e instalación de aplicaciones sin importar cuál sea el sitio usado, en muchos casos por desconocimiento o porque piensan que no tendrán ningún inconveniente si las usan en su dispositivo móvil, desconocen que detrás de algunas aplicaciones más que su uso, tienen otro tipo de intenciones, las cuales pueden ser, capturar información relevante la cual maneja cada uno en su celular inteligente, ya sea de alguna organización en caso de que sea uno corporativo o personal. otros piensan que por instalar las aplicaciones desde la tienda no presentan ningún problema de seguridad.

4.2.5.1 Que es una aplicación móvil

También conocidos como App, son programas diseñados para ser utilizados en dispositivos móviles, las cuales vienen instaladas de fábrica y otras son las que el usuario instala de acuerdo a su necesidad o gusto.

4.2.5.2 Tipos de aplicaciones

Los tipos de aplicaciones móviles son 3, llamadas así; App Nativas, App Hibridas y App Web.

App Nativas

Son desarrolladas para el uso exclusivo de cada sistema operativo móvil, en el caso del sistema operativo Android, estas aplicaciones se encuentran en las tiendas de Google Play o Play Store

App Web

Este tipo de aplicaciones son las que se adaptan a cualquier sistema operativo móvil, lo cual es una ventaja por ser multiplataforma y esto a su vez implica que su desarrollo sea más económico

App web nativas

También llamadas híbridas, porque involucra a las 2 descritas anteriormente.

El dispositivo móvil con sistema Android podrá realizar 2 tipos de descarga para la instalación de aplicaciones, como son:

- Orígenes desconocidos
- Tienda de Google play Store

Teniendo en cuenta los distintos medios utilizados para la descarga e instalación de aplicaciones en los Smartphone, es necesario listar o destacar las aplicaciones que son más recurrentes y usadas por los usuarios de estos teléfonos inteligentes con sistema operativo Android.

Figura 4. Las 50 aplicaciones para Android más instaladas

Fuente: Informe de rendimiento y tendencias de Avast sobre aplicaciones para Android [Consultado el 10 de octubre de 2018]. Disponible en: http://files.avast.com/files/marketing/materials/es_avast_android_app_report.pdf

En el informe elaborado por la empresa de seguridad Avast entre los meses de enero y marzo del año 2017 estas fueron las aplicaciones más descargadas desde la tienda de Google Play Store, según datos de más de 3 millones de usuarios en Android, donde se evidencia un gran dominio de las App de redes sociales, como son Facebook, WhatsApp, Instagram, Twitter entre otros. Dentro de los navegadores se destaca Google Chrome, en cuento a las herramientas de oficina las que lidera ese top 50 es Microsoft Word.

Por otro lado, las aplicaciones además permiten mantener el equipo personalizado, incluso algunas permiten parámetros de bloqueo del Smartphone. Entre las principales aplicaciones ofrecidas en la tienda Google Play y que han sido de mayor uso en 2018, se encuentran:

Amazon Alexa

Aplicación que permite configurar cualquier dispositivo compatible con Alexa, además de brindar al usuario la oportunidad de ver noticias, escuchar música y realizar planificaciones. Su logo se presenta como se muestra a continuación:

Amazon Go

Permite realizar compras en una tienda y luego de salir de ella te permite recibir en el Smartphone la factura de la compra.

Firefox: el navegador seguro

Su nuevo motor Quantum, permite una navegación más ágil con optimo rediseño de interfaz que ofrece una vista más atractiva, llevando el sello de seguridad Firefox.

Google Home

Permite configurar e interactuar con diversos dispositivos, ya sea con el asistente Google Home o Google Chromecast. Permite apagar y encender

dispositivos que estén conectados, además de enviar información a donde se quiera.

Google Keep: notas y listas

Permite organizar las actividades del día del usuario, predeterminando listas de acciones a realizar y notas sobre asuntos pendientes.

Google podcast

Es una aplicación que ocupa poco espacio en el dispositivo móvil, sencilla y eficiente que permite escuchar, organizar, hacer seguimiento y descubrir nuevos contenidos. Requiere 4.1 y versiones posteriores.

Microsoft Edge

Junto a Microsoft Launcher, su navegador web Edge hace posible una integración perfecta con los usuarios de Windows 10, ofreciendo una navegación rápida y segura. Requiere 4.4 y versiones posteriores.

Netflix

Corresponde a un servicio de streaming, su uso esta restringido a dispositivos libres de root o modificados. Su servicio tiene alta popularidad pues es la aplicación favorita de los amantes del cine y las series. Su requerimiento varia dependiendo del dispositivo.

YouTube Music

Ofrece un universo musical, listas de reproducción, discos, sugerencias conforme al gusto del usuario. Su requerimiento varia dependiendo del dispositivo.

Juegos

Con relación a los juegos destacados de 2018, se tienen que los de mayor atracción, se corresponden con versiones de SOA de 6.0 y posteriores (Armello, Dragon Ball Legends, Florence, Layton la villa misteriosa HD, Q12 trivia, Reings

Juego de Tronos, The Room: old sins), sin embargo se localizan los juegos: Great race: Route 66, Novice heroes, Ability draft, supercross pro, entre otros.

Como las ya mencionadas, muchisimas aplicaciones ofrece la tienda oficial Google Play que el usuario podra descargar de forma gratuita o pagando, dependiendo de su requerimiento personal en miras de poder solventar diversas situaciones desde su smartphone samsung con sistema operativo android 5.1.

A pesar de que existen variedad de aplicaciones que permiten contar con un smartphone protegido, el sistema operativo Android continua siendo amenazado, sobretodo para aquellos equipos que no es posible actualizarles el sistema y este hecho los ubica en estado de vulnerabilidad.

Recientemente, la empresa de seguridad china 360 reseña sobre la nueva amenaza que tiene android conocida como *Fakedebuggerd* la cual utiliza técnicas de "rootkit para mantenerse en el sistema y el usuario no pueda conseguir eliminarlo"[26]. La intención básica de éste es robar información del smartphone, haciendo el equipo vulnerable.

Es de saber, que el vector de infección que provoca la intromisión engañosa de este malware, se ubica en la descarga de ciertas aplicaciones que los delincuentes han modificado y que además se presentan como aplicaciones de linternas o calendarios que el usiuario no ha descargado en ningun momento y se les hace imposible eliminarlas, dado que los equipos no cuentan con actualizaciones importantes de sistema que permitan combatir este agente de infección digital.

Fakedebuggerd se interesa por "las llamadas recibidas, enviadas, SMS, informacion de la tarjeta SIM como el IMEI"[27] entre otros datos importantes del

[26] Albors Joseph. Conoce a Fakedebuggerd, la nueva amenaza para Android. En línea 15 de diciembre de 2014 disponible en: https://www.welivesecurity.com/la-es/2014/12/15/nueva-amenaza-android-fakedebuggerd/
[27] Ibid., p. 2

smarthphone. A pesar de su potencial amenaza, es posible evitar verse afectado si se siguen las siguientes recomendaciones:

1. Evitar descargar aplicaciones de sitios de terceros o desarrolladores que no tengan una reputación contrastada
2. No pulsar sobre enlaces recibidos por mensajería, SMS, correos, etc, si se desconoce a donde van dirigidos
3. Contar con una solución de seguridad en el dispositivo que permita detectar estas amenazas

En general, es importante estar atento a las descargas de aplicaciones ya que en cualquier descuido, el usuario sin querer podría estar provocando una fuerte infección en su smarthphone, generando problemas de seguridad y hasta perdida de sus datos.

Existen distintos tipos de usuario entre los que utilizan los Smartphone, por todas las ventajas que estos ofrecen en comparación con los celulares de antes, teniendo en cuenta que pueden tener usuarios en todos los niveles de conocimiento sobre el manejo de este potente dispositivo, se hace importante tener claridad sobre cuáles son los problemas de seguridad que se pueden presentar, si no se tiene el cuidado y el conocimiento necesario sobre los riesgos a los que pueden estar expuestos.

4.2.5.3. Descarga e instalación desde orígenes desconocidos

Es una opción para descargar e instalar aplicaciones por fuera de la tienda de Google, es usada desde los inicios del sistema operativo Android en su versión 1.0, donde para poder realizar este tipo de operación lo único que se debe hacer es ingresar a los ajustes del Smartphone y activar la opción de orígenes desconocidos, en la parte de bloqueo de seguridad.

Como se mencionaba esta opción es usada desde el inicio del sistema operativo y que aún está disponible para la versión Android 5.1 Lollipop

4.2.5.4 Tienda de Google Play Store

Desde ésta tienda, es posible encontrar las aplicaciones necesarias conforme a las características y necesidades del usuario, ya sean gratis o privadas por las cuales es necesario pagar un costo de instalación y uso.

Es importante mencionar que las aplicaciones fraudulentas no solo se encuentran por medio de la descarga en sitios desconocidos, ya que en las tiendas de Google y Apple también se filtran o ingresan este tipo de aplicaciones que pueden quizás contener código malicioso el cual genera un gran riesgo de infección.

Los investigadores de Eset Latinoamérica realizan un estudio, donde reconocen que en la tienda de Google Play hay ciertas aplicaciones que ofrecen distintas funciones para el usuario, como por ejemplo una para detectar archivos dañinos para el equipo, pero estas lo que hacían era mostrarle al usuario publicidad no deseada, en fin hay un total de 35 aplicaciones falsas, las cuales fueron detectadas y sacadas de dicha tienda[28].

Esta compañía indica, que este tipo de herramientas imitan las funciones básicas de seguridad, lo que origina que estas, aunque contengan código malicioso se detecten como legítimas, esto origina un gran riesgo para los usuarios.

Según un informe de Avast, las aplicaciones falsas, están infectando los dispositivos con sistema operativo Android con Spyware. Cuando se realiza la búsqueda de una aplicación en particular, salen otras distribuciones parecidas, las

[28] Tenotosfera. Advierten sobre falsas apps de ciberseguridad en Google Play. El tiempo. En línea, 20 de abril de 2018, disponible en: https://www.eltiempo.com/tecnosfera/apps/falsas-aplicaciones-de-ciberseguridad-en-google-play-207582

cuales dicen brindar las mismas funciones, características e incluso mejores que las originales.

Según los informes de Avast la aplicación Sex Game que ya no está disponible en la tienda de google Play store, desde el año 2016, pero que la pueden encontrar en páginas de terceros, tiene un spyware llamado Triout que puede[29]:

- Grabar y robar tus llamadas telefónicas
- Robar tus mensajes de texto
- Robar tus fotos y videos
- Ver y registrar tu ubicación

Pero no solo las aplicaciones falsas están generando inseguridad en los dispositivos móviles con sistema operativo Android, también se encuentran otro tipo de aplicaciones en las tiendas oficiales en este caso de Google Play Store que contienen malware, estas en algunos casos vienen ocultas como un actualización como es el caso de "Block Puzzle Jewel, My Blocks, Block Puzzles, Block Puzzles Free, My Puzzles"[30] que en un determinado tiempo solicita que se realice esa operación, engañando al usuario, porque en ella viene el código malicioso oculto. Es por ello que la tienda decidió sacar de su base de datos de aplicaciones nativas este tipo de juegos.

Los creadores de este tipo de código malicioso lo que hacen es aprovechar, que para los usuarios es normal que se solicite alguna actualización, esto no genera ningún tipo de sospecha, teniendo en cuenta que es algo normal y que pasa frecuentemente con las aplicaciones que están instaladas en el dispositivo inteligente, desconociendo su verdadero motivo.

[29] Avast Security News Team. App falsa infecta tu Android con spyware. Avast. En línea. 26 de agosto de 2018, disponible en: https://blog.avast.com/es/app-falsa-infecta-tu-android-con-spyware?utm_campaign=socialposts_es&utm_source=facebook&utm_medium=social
[30] Nohova Alena. Las apps de puzles abren la puerta al malware. Avast. En línea. 17 de octubre de 2018, disponible en: https://blog.avast.com/es/las-apps-de-puzles-abren-la-puerta-al-malware

4.2.6 Seguridad en el sistema operativo Android 5.1

Teniendo en cuenta el dominio que ha tenido el sistema operativo para dispositivos móviles Android, este se convierte en una gran posibilidad del aumento de los riesgos de amenaza para los dispositivos móviles que lo utilizan y por ende para sus usuarios. Por esta razón lo más recomendable para los usuarios que requieran realizar una descarga e instalación de aplicaciones es que lo realice por medio de la tienda de Google Play Store que, aunque en esta también se han encontrado aplicaciones infectadas y maliciosas es muchísimo más confiable que las realizadas por medio de orígenes desconocidos, enlaces y páginas de descarga.

Es importante que cada usuario conozca las medidas de seguridad que se pueden utilizar en el sistema operativo Android en su versión 5.1, para ello se realizará un recorrido con el fin de explicar las ventajas de su uso, para lo cual se iniciara por la conexión a una red por medio de WiFi.

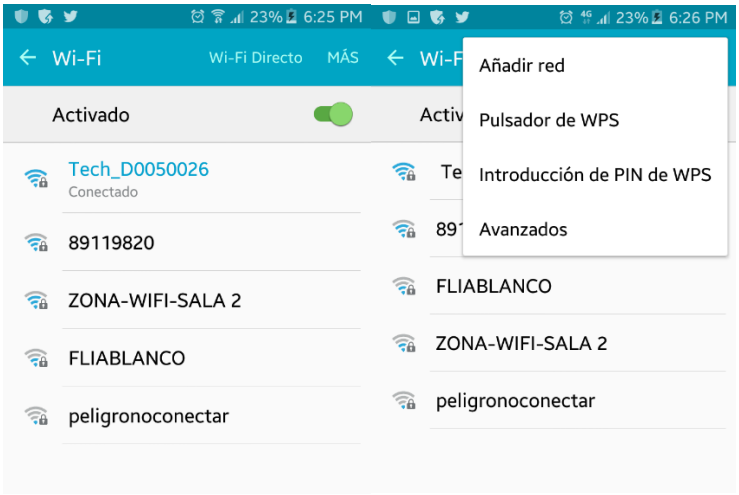
Para poder acceder a la red de internet es importante mencionar que se realiza por medio de una red WiFi o datos móviles.

4.2.6.1 Conexión WiFi

Es importante tener claro a qué tipo de redes WiFi se puede conectar, por lo que se recomienda, no utilizar aquellas que están emitiendo señal pública y que no conocen, ya que puede algún usuario en espera de la conexión, capturar la información que se maneja a través de ella.

Por otra parte es importante mencionar que cuando las redes son seguras, es decir tienen contraseña, no solo se puede acceder por medio de la autenticación, ya que el sistema operativo Android 5.1 tiene habilitada la opción de conexión mediante WPS, que le permitirá conectarse si el Router también posee esa opción, la cual no es recomendable, por que al momento de habilitarlo, terceros puedan aprovechar esa vulnerabilidad que es generada al ingresar y así poder utilizar ciertos conocimientos en caso de que los tenga y hacerse cargo de la red y la información que viaja a través de ella.

Figura 5. Conexión WiFi



Fuente: El autor

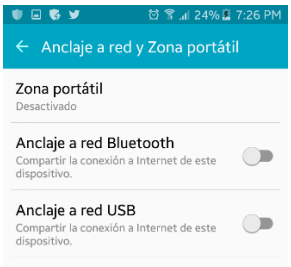
4.2.6.2 Desactivar conexiones que no se estén utilizando en el momento

Esta opción es muy importante para el ahorro de batería, ya que es posible desactivar opciones como WiFi, ubicación, Bluetooth, linterna, rotación de pantalla, entre otras, pero además es importante que la conexión por Bluetooth esté desactivada cuando no se está usando por seguridad, ya que existen dispositivos que no necesitan la aprobación en doble vía para conectarse a un dispositivo que lo utilice, lo cual genera un gran riesgo a la seguridad y representaría una gran amenaza

4.2.6.3 Anclaje de red y zona portátil

Esta es una de las bondades ofrecidas por el sistema operativo en mención ya que por medio de esta se pueden realizar más funciones como, compartir los datos con otros dispositivos móviles, portátiles y computadores de escritorio, por medio de 3 opciones, como son:

Figura 6. Anclaje de red y zona portátil



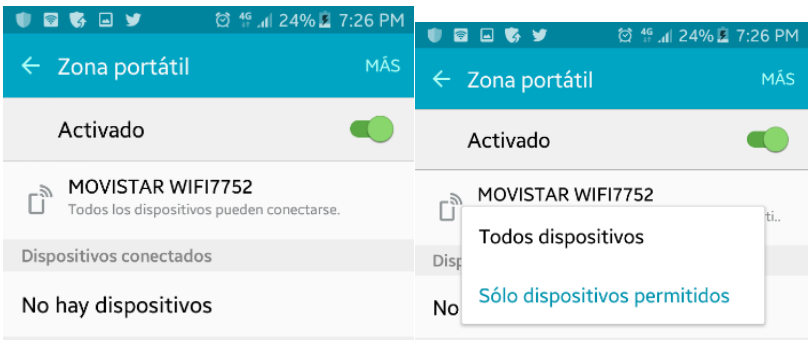
Fuente: el autor

Zona portátil

Se activa para compartir los datos en este caso del Smartphone a un dispositivo móvil, computador, PDA, entre otros por medio de la red WiFi, pero es necesario activar los mecanismos de seguridad que esta misma ofrece, para lo cual es necesario administrar los dispositivos limitando cuales serían los permitidos en nuestra red, por lo cual se debe ingresar en la opción más que se encuentra en la esquina superior derecha, escoger la opción dispositivos permitidos y luego añadir, para lo cual solicitará, el nombre del dispositivo a conectar y su dirección MAC.

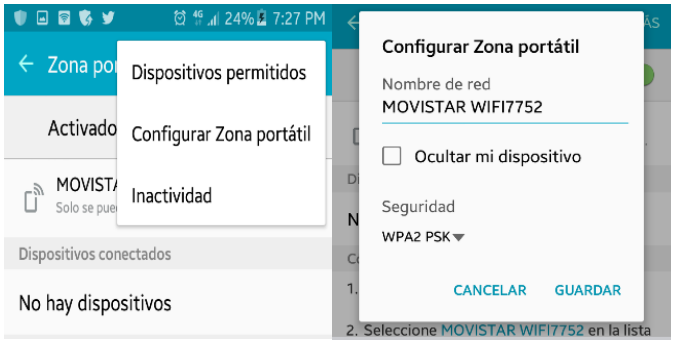
Otra opción desde la habilitación de la zona portátil es que una vez se tenga el acceso por medio de la contraseña a la cual se recomienda que, para aumentar su complejidad, su robustez es necesario realizar una combinación de números, símbolos y letras mayúsculas y minúsculas con una extensión mínima de 8 caracteres, luego del ingreso se habilita la opción ocultar mi dispositivo

Figura 7. Zona portátil



Fuente: el autor

Figura 8. Configuración de la zona portátil



Fuente el autor

Anclaje a red por Bluetooth:

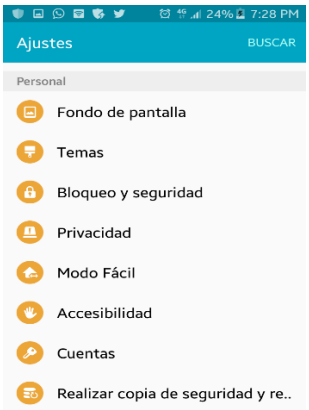
Es una opción que no es tan confiable cuando hay dispositivos cerca que pueden ingresar o compartir recursos sin la aceptación en ambos lados.

Anclaje a red por USB

En esta opción solo es necesario conectar al computador o dispositivo al que se le quiera compartir los datos de internet por medio de cable USB, lo cual limita el acceso a la red.

4.2.6.4 Bloqueo y seguridad

Figura 9. Ajustes Smartphone Samsung



Fuente: el autor

Se administran un gran número de opciones para la seguridad del dispositivo móvil, entre las que se pueden destacar

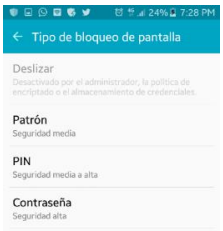
- Bloqueo de pantalla, es importante para mantener la seguridad de los datos, ya que el dispositivo podría caer en manos de personas que pueden utilizar la información que se maneja en este para su beneficio, para lo cual se encuentran 3 opciones:
  - ✓ Patrón de Bloqueo, ofrece una seguridad media
  - ✓ PIN, ofrece una seguridad media alta
  - ✓ Contraseña, Ofrece seguridad alta

Figura 10. Bloqueo y seguridad

Fuente: el autor

Cuando se ingresa al tipo de bloquedo mostrará 3 opciones como son Patrón, PIN y contraseña, como se evidencia el la figura numero 11

Figura 11. Tipos de bloqueo de pantalla



Fuente: el autor

4.2.6.5 Seguridad

Ofrece protección al sistema, informa si existen amenazas de malware o si se realizaron algunos cambios en el sistema, además de la activación de la protección KNOX

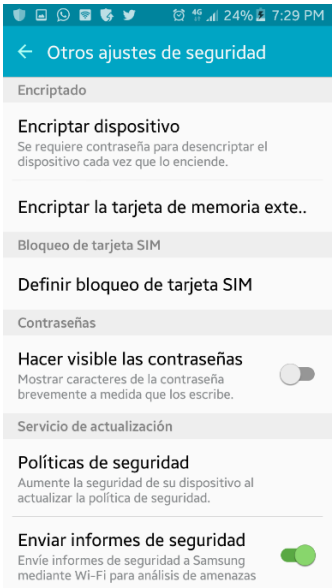
4.2.6.6 Orígenes desconocidos

Es importante tener claro que para esta opción lo mejor es mantenerla desactivada, para que no se instalen aplicaciones desde otras ubicaciones distintas a la tienda de Google Play Store,

4.2.6.7 Otros ajustes de seguridad

Encriptar dispositivo; allí se encuentra la opción para cifrar con una contraseña el dispositivo cuando se enciende, además, que se puede realizar el mismo cifrado a la memoria externa

Figura 12. Otros ajustes



Fuente: el autor

Hacer visibles contraseñas, es una opción que se debe mantener deshabilitada, ya que existe la posibilidad de tener instalado en el dispositivo móvil un programa que capture los movimientos de la pantalla, con el cual los delincuentes cibernéticos pueden conseguir la información, lo que facilitaría el descifrado de alguna contraseña, al siempre estar visible el último carácter digitado.

4.2.6.8 Políticas de seguridad

Esta se debe desarrollar con mucho análisis, teniendo en cuenta todos los factores a tener en cuenta cuando se realiza la implementación de los mecanismos que deben brindar la seguridad que requiere el dispositivo móvil.

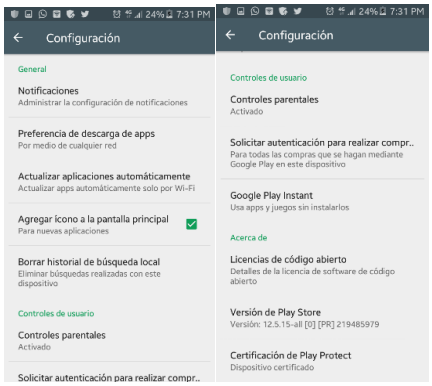
4.2.6.9 Acceso a datos de uso

Realizar copias de seguridad: es una medida importante ante la pérdida o robo de información, con la cual se pueden crear respaldos en la nube y en un computador para obtener un respaldo físico de forma local.

4.2.6.10 Configuraciones en la tienda Google Play Store

Además de las configuraciones anteriores también, es necesario administrar las de la tienda de Google Play Store, que es desde donde se recomienda realizar la descarga e instalación de las aplicaciones para los dispositivos móviles con sistema operativo Android 5.1, con el fin de aumentar la seguridad.

Figura 13. Configuración de Google Play Store

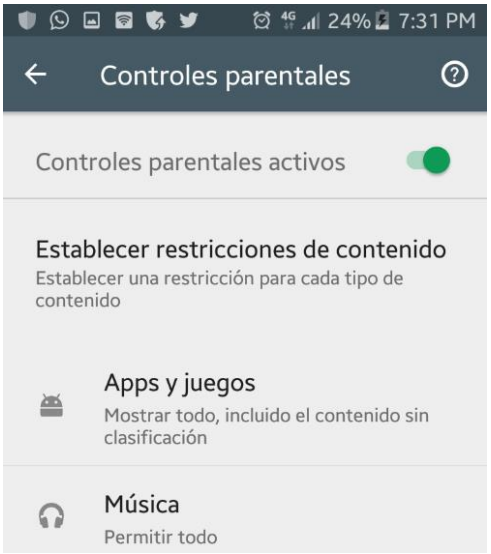


Fuente: el autor

- Notificaciones, es necesario habilitar la opción que permita recibir las notificaciones cuando existan actualizaciones de las aplicaciones instaladas en el dispositivo móvil inteligente
- Habilitar la opción, para que no se realicen actualizaciones automáticas, es importante que se conozcan y se decida cuales actualizaciones desee aplicar
- Activar los controles parentales, para controlar lo que hacen y qué aplicaciones pueden descargar e instalar los menores de edad.
- Habilitar el requerimiento de contraseñas cuando se realicen las descargas.
- Activar La autenticación cuando se requiera instalar alguna aplicación de pago
- además de estas opciones también en necesario tener en cuenta
- No rootear el dispositivo móvil
- revisar los permisos que requiere cada aplicación cuando se instala

Es importante la activación de los controles parentales, ya que estos ayudan a que se controle lo que realizan los menores de edad en la red de internet.

Figura 14. Controles parentales



Fuente. El autor

4.2.6.11 Uso de software antivirus para dispositivos móviles

Esta es una medida de protección muy importante, ya que con él se pueden detectar amenazas de Spyware, Malware, Adware y Ransomware las cuales puede rechazar automáticamente, buscando mantener protegido al dispositivo inteligente.

Es importante que el antivirus que se utilice en el Smartphone Samsung, este actualizado y siempre tener instalada su última versión, ya que, así como los ciberdelincuentes siempre están explorando nuevas formas de ataque, los programas de protección contra este tipo de amenazas siempre están buscando proteger y crear barreras de protección para que estas no penetren y vulneren nuestra seguridad.

5. ASPECTOS METODOLÓGICOS

Los aspectos metodológicos en la investigación, hacen referencia directa a los pasos que se siguen para el buen desarrollo de la misma. En este sentido, como se está presentando una monografía, donde lo esencial es la selección de un tema, su delimitación y analisis para alcanzar la profundización deseada con respecto al tema.

En este estudio, se centro el interés en analizar las aplicaciones moviles para Smartphone Samsung con sistema operativo Android 5.1 con la finalidad de dar a conocer los riesgos que representan algunas que vienen acompañadas de codigos maliciosos y aprovechan la vulnerabilidad del sistema.

Para ello, ha sido necesaria la revisión documental de información, tanto digital como impresa, para analizar los pormenores del estudio en miras de dar repuesta a cada uno de los objetivos que se plantean, a saber:

Para la descripción de la estructura del sistema operativo android 5.1, se localizó información documental explicativa de lo que es el sistema, sus características y detalles, considerando la anotación de citas relevantes para referenciar en el documento que aquí se presenta.

La descripción de aplicaciones móviles mas utilizadas en el equipo seleccionado invitó a la revisión documental descriptiva de las caracteristicas de ciertas aplicaciones y de la empresa encargada de su comercialización, la finalidad de la misma, asociada a los requerimientos del usuario, entre otros detalles que requieren de un proceso riguroso de lecturas donde se profundiza al respecto de las codificaciones implicitas en ellas.

Adicionalmente el requerimiento de identificación de los estandares de seguridad del SOA 5.1, vinculados a las aplicaciones cuando éstas son instaladas en los equipos, aportan una reacción que bien puede ser positiva o negativa dependiendo de las previsiones que se hayan tomado. De manera que la revisión de

documentos que describen estas situaciones ha sido esencial en el desarrollo de esta investigación monografica.

Una vez organizada la documentación, realizadas las lecturas y delimitadas las citas, se redacta el documento que expresa en definitiva el estudio exhaustivo realizado para el analisis de la seguridad en el Smartphone identificado.

6. CONCLUSIONES

Después de realizar el análisis al sistema operativo móvil Android 5.1, para Smartphone Samsung, se pudieron comprobar ciertas fallas de seguridad que se deben ir corrigiendo en cada actualización del SOA, ya que con ellas se busca ir eliminando los errores que se presentan en versiones anteriores, de acuerdo a las experiencias obtenidas

Teniendo en cuenta que la población que maneja estos celulares inteligentes, es necesario que todas las personas conozcan las medidas mínimas de seguridad, para ello es necesario dar a conocer las posibles consecuencias que debe tener cada usuario si no le presta la atención necesaria a la seguridad del Smatphone Samsung que también es suya.

Después de abordar todos los objetivos de esta monografía de grado, es importante que el eslabón más débil de la cadena de seguridad, es decir el usuario final, no debe pensar que no tendrán problemas de seguridad si no son precavidos en cuanto a las páginas que visitan, las aplicaciones que descargan e instalan y que siempre es necesario estar prevenidos ante cualquier tipo de ataque que pueda vulnerar la seguridad del Smartphone Samsung con sistema operativo Android 5.1

Es necesario buscar la manera de mantener actualizado el sistema SOA, debido a que los fallos presentados en versiones como en la que se abordó en el recorrido de esta monografía son corregidas en las nuevas que lanzan al mercado.

7. RECOMENDACIONES

Aunque existen pruebas de que hay y se pueden filtrar aplicaciones sospechosas, que contienen código malicioso en la tienda de Google Play Store, lo más recomendable es que las descargas e instalaciones de sus aplicaciones se realicen por medio de esta.

Mantener desactivado la instalación desde sitios desconocidos, esto ayudará para que no lleguen a los Smartphone aplicaciones que se desconocen

Mantener con contraseña los ajustes del su Smartphone Samsung para que sin su consentimiento no se habilite la opción de las descargas de sitios desconocidos

Es importante que siempre se verifique que aplicación móvil se va a instalar sin importar desde donde se realice su descarga.

Buscar buenos antivirus para su Smartphone Samsung, para que ayude a bloquear las entradas de aplicaciones maliciosas

REFERENCIAS BIBLIOGRÁFICAS

Albors Joseph. Conoce a Fakedebuggerd, la nueva amenaza para Android. En línea 15 de diciembre de 2014 disponible en: https://www.welivesecurity.com/la-es/2014/12/15/nueva-amenaza-android-fakedebuggerd/

Armendáriz, Luis. Sobre El código Abierto (Open Source). 2006. Disponible en, https://guimi.net/descarga/tec-docs/Sobre_el_OS.pdf

Avast. (2017). Informe de rendimiento y tendencias de Avast sobre aplicaciones para Android. Disponible en: http://files.avast.com/files/marketing/materials/es_avast_android_app_report.pdf

Basualdo, A (2015). El malware para los dispositivos móviles ha crecido un 600%, Android es el mayor objetivo. [Consulta: 08 de octubre 2017]. Disponible en: http://googlelizados.com/malware-dispositivos-moviles-crecido-600-ciento-Android-mayor-objetivo.

Betancur, J, Oscar; Eraso H, Sonia. Seguridad en dispositivos móviles Android. 2015 monografía (Especialista en seguridad informática). Universidad Nacional Abierta Y A Distancia – UNAD. Disponible en http://stadium.unad.edu.co/preview/UNAD.php?url=/bitstream/10596/3614/1/59836994.pdf.

Capobianco, M; Stankevicius, A; Echaiz, J. (2009). Seguridad y privacidad en la plataforma Android.

Colorado, A, Pedro; Torres, B, Inírida. Análisis De Seguridad De Aplicaciones Móviles Nativas Para El Sistema Operativo Android Versión Jelly Bean 4.1.2 En Dispositivos Móviles Smartphone. Villavicencio, 2015, 247p. Trabajo de grado (Especialista en seguridad informática). Universidad Nacional Abierta Y A Distancia – UNAD. Disponible en http://repository.unad.edu.co/handle/10596/3412.

Deloitte (2017). Consumo móvil en Colombia. Los móviles prueban ser indispensables en un mundo “siempre” conectado. [Consulta: 08 de octubre 2017]. Disponible en: https://www2.deloitte.com/content/dam/Deloitte/co/Documents/technology-media-telecommunications/Consumo%20movil(VF1).pdf

Drake, J. (2014), Android Hacker's Handbook. Wiley Publishing. Disponible en http://www.wiley.com/WileyCDA/WileyTitle/productCd-111860864X.html.

ESET. (2017). Guía de seguridad para Usuarios de Smartphones. Disponible en https://www.welivesecurity.com/wp-content/uploads/2014/01/documento_guia_de_seguridad_para_usuarios_de_smartphone_baj.pdf.

Esteve, José. El Núcleo Linux. 2011. Disponible en http://openaccess.uoc.edu/webapps/o2/bitstream/10609/61265/1/Administraci%C3%B3n%20avanzada%20del%20sistema%20operativo%20GNU_Linux_M%C3%B3dulo1_El%20n%C3%BAcleo%20Linux.pdf. p.5

Gobierno de Navarra (s/f). Acércate a las TIC. Uso de dispositivos móviles (teléfonos móviles, “smartphones”, “ebooks”, GPS y “tablets”). [Consulta: 08 de octubre 2017]. Disponible en: https://www.navarra.es/NR/rdonlyres/48F9746B-080C-4DEA-BD95-A5B6E01797E1/315641/7Usodedispositivosmoviles.pdf

González, P. (2014). Seguridad en Dispositivos Android. [Consulta: 29 de septiembre 2017]. Disponible en: https://lsi.vc.ehu.eus/pablogn/investig/JornadasSeguridad141112.pdf

Karpesky (2017). Seguridad para Android: cinco consejos fundamentales, Seguridad en Internet. [En línea]. Disponible en https://latam.kaspersky.com/resource-center/preemptive-safety/android-security-tips.

Londoño, A, Darly; Hurtado, R, Juan. Esquema de seguridad para protección de

dispositivos móviles con el sistema operativo Android. Medellín, 2014, 53p. Trabajo de grado (Especialista en seguridad informática). Universidad De San Buenaventura. Disponible en http://bibliotecadigital.usb.edu.co/bitstream/10819/2283/1/Esquema_Seguridad_Dispositivos_Londono_2014.pdf.

Molina, Y; Sandoval, J; Toledo, S. (2012). Sistema operativo Android: características y funcionalidad para dispositivos móviles. Programa Ingeniería de Sistemas y Computación. [Consulta: 06 de octubre 2017]. Disponible en: http://repositorio.utp.edu.co/dspace/bitstream/handle/11059.

Montenegro, L. (2014). Ciencia, tecnología e innovación en Colombia. Revista *UNIMAR*, 32(1), 11-13.

Morillo, J. (s/f). Introducción a los dispositivos móviles. Universidad Oberta de Catalunya. [Consulta: 09 de octubre 2017]. Disponible en: https://www.exabyteinformatica.com/uoc/Informatica/Tecnologia.pdf

OWASP Mobile Security Project. (2014). Disponible en https://www.owasp.org/index.php/OWASP_Mobile_Security_Project.

Pérez, M, Enrique. Estudio de Soluciones de Seguridad para Apps Móviles en Sanidad. Valladolid, 2016, 108p. Trabajo de grado (Ingeniería de Tecnologías Especificas de Telecomunicación). Universidad de Valladolid.

Pérez, P; García, L; Álvarez, E; Rodríguez, S; Gutiérrez, C. (2012). Estudio sobre Seguridad en Dispositivos Móviles y Smartphones. Informe Anual 2011 (8ª Oleada). España: Instituto Nacional de Tecnologías de la Comunicación (INTECO), 2012, 32

Rua. Navegadores. Biblioteca universitaria. 2015. Disponible en, https://rua.ua.es/dspace/bitstream/10045/46501/3/ci2_basico_2014-15_Navegadores.pdf.p.4

Soroa, P. (2014). Estudio de viabilidad de una empresa de aplicaciones móviles. Proyecto Fin de Carrera. Universidad de Sevilla. España.

Tardáguila, C. (2009). Dispositivos móviles y multimedia. MOSAIC tecnología y comunicación multimedia.

UPEL (2008) Manual de Trabajos de Grado de Especialización y Maestría y Tesis Doctorales. Fondo editorial de la Universidad Pedagógica Experimental Libertador.

ANEXOS

Anexo (1) RESUMEN ANALÍTICO DE EDUCACIÓN - RAE

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA UNAD ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA

FECHA			Noviembre de 2017				
TITULO			ANÁLISIS A LA SEGURIDAD EN APLICACIONES MÓVILES PARA SMARTPHONE SAMSUNG CON SISTEMA ANDROID 5.1				
AUTOR			Yesnir Antonio Redondo Daniel				
EDICION			Universidad Nacional Abierta y a Distancia UNAD				
DIRECTIR (ES)/ ASESOR(ES)			Martin Camilo Cancelado				
AÑO ELABORACIÓN			5 de diciembre de 2018				
DESCRIPCIÓN			Trabajo de grado para optar al título de especialista en seguridad informática. Se busca realizar un Análisis A La Seguridad En Aplicaciones Móviles Para Smartphone Samsung Con Sistema Android 5.1, con el fin de conocer las vulnerabilidades que pueden aprovechar los ciberdelincuentes para sustraer información de los usuarios, además de brindarle la información para que cada uno conozca los riesgos y amenazas existentes y que en cualquier momento pueden ser víctimas de algún ataque que busca vulnerar su seguridad, capturando datos e información privada.				
PAGINAS	**66**	**TABLAS**	**0**	**FIGURAS**	**20**	**ANEXOS**	**5**
CONTENIDO							
PALABRAS CLAVES							

Dispositivo móvil, Sistema operativo, Android, Aplicaciones móviles, Seguridad, Samsung.

FORMULACIÓN DEL PROBLEMA

La necesidad de comunicación social ha puesto en marcha la promoción de aparatos con tecnologías móviles que permiten al ser humano mantenerse comunicado y realizar diversas operaciones donde se ahorra tiempo, dinero y agotamiento físico. Estas operaciones que por lo general suelen ser personales requieren que el equipo esté lo suficientemente protegido para evitar filtración de información o invasión por parte de malware entre otros códigos maliciosos que pueden colocar en riesgo la información que se maneja desde el dispositivo inteligente. En este estudio monográfico, se presenta interés de explorar el entorno móvil Android con la intención de analizar los niveles de seguridad de las aplicaciones móviles que se ofrecen al usuario.

Con gran frecuencia las personas descargan aplicaciones sin conocer, los peligros, amenazas y vulnerabilidades de seguridad que se pueden presentar, no saben si por medio de estos puedan capturar la información que cada uno maneja en su dispositivo móvil como son, claves, información bancaria, información personal entre otros. Por ello se hace necesario brindar la información suficiente a la población para que a partir de ella puedan prevenir y protegerse de este tipo de situaciones originadas por terceros, por medio de las aplicaciones, aprovechando las vulnerabilidades de los sistemas operativos.

Androide, corresponde a ser una plataforma móvil libre, de mayor uso en la actualidad ya que posee software abierto legitimado bajo la licencia Apache para el uso de diversas aplicaciones y adicionalmente es de fácil manejo por la población. En este sentido, su libertad de uso puede provocar el fluido paso (en casos imperceptible) de amenazas que afectan la seguridad de la información privada del usuario del dispositivo móvil. Capobianco, et al (2009) expresa que los dispositivos móviles, son presentados al usuario listo con las aplicaciones que éste puede requerir utilizar, sin embargo, hoy es posible descargar aún más aplicaciones de las ya adheridas al equipo. Situación que lleva al usuario a preocuparse por los niveles de seguridad de la información que confía en estos

aparatos. De esta manera, es posible preguntarse: ¿Cuáles son las aplicaciones móviles más utilizadas en los dispositivos modernos? ¿Qué características de software poseen los diferentes dispositivos móviles y cuáles le son permitidas descargar? ¿Cómo son los niveles de seguridad de las aplicaciones móviles? ¿Cuáles son los parámetros de seguridad de las aplicaciones móviles con relación a su uso en determinado equipo? Para finalmente responder ¿Cuáles son los niveles de seguridad en las aplicaciones móviles con Sistema Operativo Android?

CONTENIDO

La importancia de esta monografía de grado se basa en el papel fundamental que juega un dispositivo móvil con sistema operativo Android 5.1 Lillipop como es el caso de los Smartphone de la marca Samsung. Debido a su gran crecimiento y uso en los últimos años, algo que quieren o han aprovechado los ciberdelincuentes, que han optado por atacar el eslabón más débil que es el usuario, con el fin de obtener la información que necesitan o requieren. Todo esto originó que la seguridad de la información se haya convertido en el pilar fundamental en todo el mundo, debido a la gran cantidad de amenazas que se presentan a diario, así pues, es importante buscar siempre la manera de estar seguros, para ello es necesario utilizar un gran número de herramientas tanto de hardware como de software que ayuden a minimizar y mitigar el riesgo de ser atacados, pero esto no es suficiente si no se crea conciencia en cuanto a las medidas de seguridad que deben tener en cuenta las comunidades que utilizan estos dispositivos inteligentes.

En este estudio se centra el interés en analizar la seguridad de la información que corresponde a los sistemas tecnológicos configurados para desarrollarse en dispositivos móviles, donde se han incrementado considerablemente las amenazas gracias al gran número de datos confidenciales que se pueden manejar ahí, aún más al Sistema Operativo Android (SOA) que domina actualmente el mercado mundial. Por esta razón, se delimita al análisis de la seguridad de las aplicaciones móviles de la versión 5.1 Lollipop.

Así como hay un aumento de dispositivos móviles en el mundo va creciendo el número de amenazas a estos y más al sistema operativo Android, el cual es el que domina el mercado mundial, por esta razón se elige en este estudio a la

seguridad de sus aplicaciones móviles y más específicamente en su versión 5.1 Lollipop.

Analizar la seguridad en las aplicaciones móviles en los teléfonos inteligentes llevo a considerar la selección de una marca específica: Samsung con SOA 5.1 con la finalidad de dar a conocer los riesgos que pueden provocar la descarga de éstas y así mismo explorar algunos métodos preventivos que se deben tener ante la filtración de algún malware. Para ellos, se especifican inicialmente la estructura del Sistema Operativo Android (SOA) en su versión 5.1, los dispositivos Samsung que soportan dicha aplicación, los estándares de seguridad que maneja el SOA, para posteriormente mostrar las aplicaciones móviles más utilizadas y así mostrar los niveles de seguridad. Una vez delimitada la temática de interés, se realizó la debida búsqueda de material bibliográfico para el análisis de la situación objeto de estudio y finalmente brindar una síntesis de aporte que vincule lo ya investigado por otros, la reflexión propia y el aporte que se requiere.

Es importante resaltar que el uso de los dispositivos móviles ha tenido un incremento en los últimos años, es por ello que se hace más atractivo para que los piratas informáticos realicen acciones que buscan vulnerar la seguridad de los mismos con el fin de conseguir algún tipo de información de los usuarios que le pueda servir para su lucro personal, esto se puede soportar en el estudio de Juniper Networks, donde se argumenta que aunque “en 2010 el malware dirigido a Android constituía únicamente el 24 % de todas las amenazas de malware para dispositivos móviles, en la actualidad, estas amenazas suponen un 90 % de todo el malware destinado a dispositivos móviles” . Cifra realmente alarmante pues se espera que con la evolución en las actualizaciones de los SOA se involucre una plataforma móvil con mayor seguridad para la información que manejan los usuarios.

METODOLOGIA DE INVESTIGACION

Se trata de un estudio monográfico donde a través de una revisión documental exhaustiva de artículos científicos relacionados con el tema, se realizan las respectivas lecturas y se analiza la información para luego aportar un punto de vista que sea de utilidad para la comunidad académica-social lectora. Estos documentos son consultados a través de la red de internet.

CONCLUSIONES

Después de realizar el análisis al sistema operativo móvil Android 5.1, para Smartphone Samsung, se pudieron comprobar ciertas fallas de seguridad que se deben ir corrigiendo en cada actualización del SOA, ya que con ellas se busca ir eliminando los errores que se presentan en versiones anteriores, de acuerdo a las experiencias obtenidas

Teniendo en cuenta que la población que maneja estos celulares inteligentes es necesario que todas las personas conozcan las medidas mínimas de seguridad, para ello es necesario dar a conocer las posibles consecuencias que debe tener cada usuario si no le presta la atención necesaria a la seguridad del Smartphone Samsung que también es suya.

Después de abordar todos los objetivos de esta monografía de grado, es importante que el eslabón más débil de la cadena de seguridad, es decir el usuario final, no debe pensar que no tendrán problemas de seguridad si no son precavidos en cuanto a las páginas que visitan, las aplicaciones que descargan e instalan y que siempre es necesario estar prevenidos ante cualquier tipo de ataque que pueda vulnerar la seguridad de nuestro Smartphone Samsung con sistema operativo Android 5.1

Es necesario buscar la manera de mantener actualizado el sistema SOA, debido a que los fallos presentados en versiones como en la que hemos abordado en el recorrido de esta monografía son corregidas en las nuevas versiones del sistema.

RECOMENDACIONES

Aunque existen pruebas de que hay y se pueden filtrar aplicaciones sospechosas, que contienen código malicioso en la tienda de Google Play Store, lo más recomendable es que las descargas e instalaciones de sus aplicaciones se realicen por medio de esta.

Mantener desactivado la instalación desde sitios desconocidos, esto ayudará para que no lleguen a nuestro Smartphone aplicaciones que no conocemos

Mantener con contraseña los ajustes del su Smartphone Samsung para que sin su consentimiento no se habilite la opción de las descargas de sitios desconocidos

Es importante que siempre se verifique que aplicación móvil se va a instalar sin importar desde donde se realice su descarga.

Buscar buenos antivirus para su Smartphone Samsung, para que ayude a bloquear las entradas de aplicaciones maliciosas

FUENTES BIBLIOGRAFICAS

Albors Joseph. Conoce a Fakedebuggerd, la nueva amenaza para Android. En línea 15 de diciembre de 2014 disponible en: https://www.welivesecurity.com/la-es/2014/12/15/nueva-amenaza-android-fakedebuggerd/

Armendáriz, Luis. Sobre El código Abierto (Open Source). 2006. Disponible en, https://guimi.net/descarga/tec-docs/Sobre_el_OS.pdf

Avast. (2017). Informe de rendimiento y tendencias de Avast sobre aplicaciones para Android. Disponible en: http://files.avast.com/files/marketing/materials/es_avast_android_app_report.pdf

Basualdo, A (2015). El malware para los dispositivos móviles ha crecido un 600%, Android es el mayor objetivo. [Consulta: 08 de octubre 2017]. Disponible en: http://googlelizados.com/malware-dispositivos-moviles-crecido-600-ciento-Android-mayor-objetivo.

Betancur, J, Oscar; Eraso H, Sonia. Seguridad en dispositivos móviles Android. 2015 monografía (Especialista en seguridad informática). Universidad Nacional Abierta Y A Distancia – UNAD. Disponible en

http://stadium.unad.edu.co/preview/UNAD.php?url=/bitstream/10596/3614/1/59836994.pdf.

Capobianco, M; Stankevicius, A; Echaiz, J. (2009). Seguridad y privacidad en la plataforma Android.

Colorado, A, Pedro; Torres, B, Inírida. Análisis De Seguridad De Aplicaciones Móviles Nativas Para El Sistema Operativo Android Versión Jelly Bean 4.1.2 En Dispositivos Móviles Smartphone. Villavicencio, 2015, 247p. Trabajo de grado (Especialista en seguridad informática). Universidad Nacional Abierta Y A Distancia – UNAD. Disponible en http://repository.unad.edu.co/handle/10596/3412.

Deloitte (2017). Consumo móvil en Colombia. Los móviles prueban ser indispensables en un mundo “siempre” conectado. [Consulta: 08 de octubre 2017]. Disponible en: https://www2.deloitte.com/content/dam/Deloitte/co/Documents/technology-media-telecommunications/Consumo%20movil(VF1).pdf

Drake, J. (2014), Android Hacker's Handbook. Wiley Publishing. Disponible en http://www.wiley.com/WileyCDA/WileyTitle/productCd-111860864X.html.

ESET. (2017). Guía de seguridad para Usuarios de Smartphones. Disponible en https://www.welivesecurity.com/wp-content/uploads/2014/01/documento_guia_de_seguridad_para_usuarios_de_smartphone_baj.pdf.

Esteve, José. El Núcleo Linux. 2011. Disponible en http://openaccess.uoc.edu/webapps/o2/bitstream/10609/61265/1/Administraci%C3%B3n%20avanzada%20del%20sistema%20operativo%20GNU_Linux_M%C3%B3dulo1_El%20n%C3%BAcleo%20Linux.pdf. p.5

Gobierno de Navarra (s/f). Acércate a las TIC. Uso de dispositivos móviles (teléfonos móviles, “smartphones”, “ebooks”, GPS y “tablets”). [Consulta: 08 de

octubre 2017]. Disponible en: https://www.navarra.es/NR/rdonlyres/48F9746B-080C-4DEA-BD95-A5B6E01797E1/315641/7Usodedispositivosmoviles.pdf

González, P. (2014). Seguridad en Dispositivos Android. [Consulta: 29 de septiembre 2017]. Disponible en: https://lsi.vc.ehu.eus/pablogn/investig/JornadasSeguridad141112.pdf

Karpesky (2017). Seguridad para Android: cinco consejos fundamentales, Seguridad en Internet. [En línea]. Disponible en https://latam.kaspersky.com/resource-center/preemptive-safety/android-security-tips.

Londoño, A, Darly; Hurtado, R, Juan. Esquema de seguridad para protección de dispositivos móviles con el sistema operativo Android. Medellín, 2014, 53p. Trabajo de grado (Especialista en seguridad informática). Universidad De San Buenaventura. Disponible en http://bibliotecadigital.usb.edu.co/bitstream/10819/2283/1/Esquema_Seguridad_Dispositivos_Londono_2014.pdf.

Molina, Y; Sandoval, J; Toledo, S. (2012). Sistema operativo Android: características y funcionalidad para dispositivos móviles. Programa Ingeniería de Sistemas y Computación. [Consulta: 06 de octubre 2017]. Disponible en: http://repositorio.utp.edu.co/dspace/bitstream/handle/11059.

Montenegro, L. (2014). Ciencia, tecnología e innovación en Colombia. Revista *UNIMAR*, 32(1), 11-13.

Morillo, J. (s/f). Introducción a los dispositivos móviles. Universidad Oberta de Catalunya. [Consulta: 09 de octubre 2017]. Disponible en: https://www.exabyteinformatica.com/uoc/Informatica/Tecnologia.pdf

OWASP Mobile Security Project. (2014). Disponible en https://www.owasp.org/index.php/OWASP_Mobile_Security_Project.

Pérez, M, Enrique. Estudio de Soluciones de Seguridad para Apps Móviles en Sanidad. Valladolid, 2016, 108p. Trabajo de grado (Ingeniería de Tecnologías Especificas de Telecomunicación). Universidad de Valladolid.

Pérez, P; García, L; Álvarez, E; Rodríguez, S; Gutiérrez, C. (2012). Estudio sobre Seguridad en Dispositivos Móviles y Smartphones. Informe Anual 2011 (8ª Oleada). España: Instituto Nacional de Tecnologías de la Comunicación (INTECO), 2012, 32

Rua. Navegadores. Biblioteca universitaria. 2015. Disponible en, https://rua.ua.es/dspace/bitstream/10045/46501/3/ci2_basico_2014-15_Navegadores.pdf.p.4

Soroa, P. (2014). Estudio de viabilidad de una empresa de aplicaciones móviles. Proyecto Fin de Carrera. Universidad de Sevilla. España.

Tardáguila, C. (2009). Dispositivos móviles y multimedia. MOSAIC tecnología y comunicación multimedia.

UPEL (2008) Manual de Trabajos de Grado de Especialización y Maestría y Tesis Doctorales. Fondo editorial de la Universidad Pedagógica Experimental Libertador.