Buenas prácticas para mitigar los riesgos de Malware en Smartphones con sistema operativo Android.

OSCAR FERNANDO TABARES GUTIÉRREZ

INGENIERIA EN SISTEMAS

DIRECTOR: GABRIEL TABORDA

INSTITUTO TECNOLÓGICO METROPOLITANO

2016

RESUMEN

Uno de los avances tecnológicos más notables de comienzos del siglo XXI son los Smartphones, aumentando su uso año tras año, creciendo un 5,7% a nivel mundial, llegando a los 399,5 millones de unidades vendidas en el cuarto trimestre del 2015, según datos publicados anualmente por la revista Dealer World (2016). Estos dispositivos son preferidos por los usuarios al poseer conexión a internet las 24 horas del día, teniendo la posibilidad de realizar transacciones tanto bancarias como comerciales, además de intercambio de información personal a través de mensajería instantánea, correo electrónico o redes sociales. Exponiéndose así a riesgos de robo de información, no solo usando técnicas como phishing para engañar a los usuarios sino también gusanos, troyanos, spyware, Adware, entre otros.

El malware, también conocido como badware, es una clase de software que tiene como propósito dañar el hardware o software de una computadora o infiltrarse sin la autorización del propietario. Un software es considerado malware, dependiendo de los efectos que cause en una computadora, los cuales pueden ser: generar imposibilidad de abrir ciertos programas, aparición de avisos o mensajes en pantalla, problemas al arrancar el ordenador, robo de información, entre otros. Algunos ejemplos de estos tipos de malware son: virus, gusanos, troyanos, rootKits, scareware, spyware, Adware, etc.

Por lo anterior, esta investigación tiene como objetivo orientar a las personas y entidades que usan las aplicaciones ofrecidas por el sistema operativo Android en sus Smartphones, teniendo la posibilidad de conocer los tipos de malware, las características principales de estos y lo vulnerables que pueden ser desde el momento en que se conectan a la red de internet. De esta manera, se pretende prevenir daños o robo de información que los Malwares causan en los dispositivos móviles, dependiendo de la característica de estos.

Palabras clave: Malwares, Smartphone, Sistema operativo Android, virus.

RECONOCIMIENTOS

Agradecimiento muy especial al profesor y asesor Gabriel Taborda.

A mí familia y seres queridos, por su constante apoyo.

ACRÓNIMOS

HTC: High Tech Computer Corporation.

API: Application Programming Interface.

GUI: Graphical User Interface.

SSL: Secure Sockets Layer.

SDK: Software Development Kit.

HTTP: HyperText Transfer Protocol.

SO: Sistema Operativo.

VPN: Virtual Private Network.

TABLA DE CONTENIDO

LISTA DE TABLAS

LISTA DE FIGURAS

1. INTRODUCCIÓN

Los Smartphones se han vuelto cada vez más indispensables para las personas, manejando información de mayor interés, confiando las actividades y laborales cotidianas a estos. Haciendo de él una herramienta cada vez más indispensable, pero con una mayor posibilidad de ser víctimas de los tipos de software maliciosos que hoy se encuentran en la red de internet.

En cuanto al sistema operativo Android, está basado en código Linux, por lo tanto es de código abierto. La propiedad más importante de este, es que permite que los fabricantes realicen modificaciones para adaptarlos al hardware que producen y ponerlos en el mercado, esto es más rentable para ellos, que crear un nuevo sistema operativo desde cero y comercializarlo. La gran aceptación de Android ha provocado que los maleantes informáticos centren su atención hacia este.

Por su parte, los malware, es todo aquel software malicioso conocido comúnmente por ejemplo como gusanos, troyanos, que pueden causar diferentes tipos de daños a ordenadores, redes, dispositivos móviles y datos. Las consecuencias de los daños causados puede variar en función del tipo específico de malware y el tipo de dispositivo infectado, en algunos casos los resultados de una infección de malware puede ser imperceptible para el usuario, en otras ocasiones pueden ser muy graves.

Por lo anterior, esta investigación tiene como objetivos:

Objetivo General

Identificar buenas prácticas para mitigar el riesgo de malware en dispositivos móviles con sistema operativo Android.

Objetivos Específicos

- Caracterizar el funcionamiento y las variantes de Malware que representan riesgo para los Smartphones con sistemas operativos Android.

- Proponer una clasificación de los malware para sistema operativo Android de acuerdo a su afectación y las propiedades de seguridad de la información: confidencialidad, integridad, disponibilidad y/o autenticidad.

- Identificar los malware que representan más riesgo en la actualidad para los usuarios que utilizan Smartphones con sistema operativo Android, basado en los más recientes estudios de seguridad informática

- Proponer buenas prácticas para mitigar el riesgo de Malware en Smartphones con sistema operativo Android a partir de los potenciales riesgos identificados.

De esta manera, se pueda prevenir daños o robo de información que los Malwares causan en los dispositivos móviles, dependiendo de la característica de estos.

En los siguientes capítulos, se hará un tratamiento de los conceptos de los Smartphones, su historia, la evolución de los diseños de los dispositivos móviles, los diferentes sistemas operativos que funcionan en la actualidad para estos dispositivos y las ventas de Smartphones. De igual manera, se hablará del sistema operativo Android, su historia, la participación de este en el mercado, las versiones de este sistema operativo, arquitectura y una de sus principales características como lo es la Play Store.

Además, se explica los Malwares y su evolución, el crecimiento de los Malwares para Smartphones con sistema operativo Android, la categorización de los Malwares, la clasificación de estos y los que representan más riesgo para los Smartphones con el sistema

operativo Android. De igual modo, se describen los Anti-malware o antivirus, los tipos de antivirus, el funcionamiento de estos y antivirus que son utilizados para los dispositivos con sistema operativo Android.

Al final, como resultado, se propone buenas prácticas para mitigar el riesgo de Malware en Smartphones con sistema operativo Android a partir de los potenciales riesgos identificados.

De igual manera, se desarrolla el trabajo en el marco del semillero de investigación en seguridad en sistema informático (SISSI) del Instituto Tecnológico Metropolitano (ITM), bajo la línea de investigación en seguridad de dispositivos móviles, con el propósito de obtener la mayor información posible sobre los malware en Smartphones con sistema operativo Android y evidenciar los riesgos que se exponen los usuarios con estos dispositivos.

2. MARCO CONCEPTUAL: Smartphones y Android

2.1 Smartphones.

Los Smartphones permiten la instalación de aplicaciones para mejorar la experiencia de acuerdo a la necesidad de cada persona, por ende se le asigna el nombre de "inteligente", y en vista a que el dispositivo cuenta principalmente con acceso a internet, admite una gran cantidad de funciones personalizables, como lo son: correo electrónico e instantáneo, transacciones electrónicas, entre otras funciones. Por esta razón, las aplicaciones fomentan el desarrollo de nuevos sistemas operativos más livianos y ágiles, capaces de implementarlas en cada Smartphone con facilidad.

2.1.1 Historia de los Smartphones

Para muchos, se considera al Simon de IBM como el primer Smartphone (Teléfono inteligente), cuyo prototipo hizo aparición en 1992 y su venta empezó en 1994. Su éxito fue muy limitado y se dejó de comercializar en febrero de 1995. La idea principal de un teléfono inteligente, era que pudiera tener las funciones de un Personal Digital Assistant (PDA, por sus singlas en inglés), con las capacidades telefónicas para poder mandar y recibir SMS (Short Message Service), y una pantalla táctil. (Pastor, 2014)

2.1.2 Evolución en el diseño de los teléfonos móviles. (IDG, 2012)

En los años 90, al inicio de la telefonía móvil, se apostó por la miniaturización de los dispositivos móviles, pero eso cambió rápidamente con el aumento de ventas de los Smartphones. Ahora el mercado está enfocado a la maximización de la pantalla y, a la vez, a la reducción del volumen del aparato, principalmente el espesor.

Los ejemplos de estos primeros teléfonos: Nokia 8210/8850, Ericsson T68/T28/T18s, Sony CDM-Z7, Motorola StarTAC/V50, Samsung Z500/D500.

Ya para los años 1996 y 2002, los teléfonos móviles cumplían con unas funciones básicas; realizaban llamadas de voz y enviaban SMS. Pero en los mercados europeos desde 2001 se comenzaba a establecer un cambio de concepción de lo que era un teléfono móvil, el lanzamiento del Nokia 7650 (el primer modelo de la marca con cámara integrada) supuso un cambio en el mercado. Pero para aquella época, la gente no necesitaba una pantalla muy grande, solo lo suficiente para escribir SMS, leer registros de llamadas y manejar contactos entre otras funcionalidades.

Por ejemplo: Ericsson R380, Motorola Accompli, BlackBerry 6230/7230, HTCs con SO Windows Mobile.

El 23 de Octubre de 2007 se estrenaba el modelo Samsung G800, mismo año del lanzamiento del iPhone, donde la competencia con un producto de grandes dimensiones continuaba, al igual que otros modelos como el Samsung F480 y Pixon. Los pocos Smartphones que por aquella época se comercializaban fueron ganando terreno, al ofrecer más funcionalidades y servicios. Fue a partir de la proliferación de las cámaras fotográficas cuando los teléfonos móviles se vieron obligados a crecer y dejar espacio para la tecnología de cámara digital. Con la mejora de estas se empezó a apostar por ópticas y resoluciones cada vez más especiales integradas en los móviles, y junto a ello la implementación de pantallas de teléfono más amplias, con el fin de mejorar la visualización a la hora de realizar y revisar las fotografías en la pantalla del teléfono.

En los Smartphones actuales, la pantalla es lo que prima y condiciona el tamaño general del teléfono móvil, y las compañías están decididas además en adelgazar el perfil y aligerar los cuerpos de los dispositivos para que el gran tamaño se haga menos perceptible. Son cada vez más los que buscan un producto todo en uno; para comunicarse, para trabajar, y para divertirse. Se hace inviable el volver a pequeños dispositivos donde solo se podía comunicar por SMS o voz.

Por ejemplo: Samsung Galaxy Note7, iPhone 7, LG G4, Lenovo Moto Z, Sony Xperia Z3, entre otros.

2.1.3 Sistemas operativos para móviles.

Un sistema operativo es un programa o conjunto de programas que gestionan los recursos de hardware y provee servicios a los programas de aplicación, ejecutándose en modo privilegiado respecto de los demás, siendo los sistemas operativos móviles más sencillos y orientan más a la conectividad inalámbrica, los formatos multimedia y las diferentes maneras de introducir información en ellos. (Tapia, 2013)

Entre los más conocidos se encuentran:

- **Android**: es un sistema operativo móvil basado en el kernel de Linux, con una interfaz de programación Java, diseñado para ser utilizado en dispositivos móviles como teléfonos inteligentes, tabletas, Google TV y otros. Desarrollado por la Open Handset Alliance la cual es liderada por Google. (Tapia, 2013)

- **iOS**: anteriormente denominado iPhone OS es un sistema operativo móvil de Apple. Originalmente desarrollado para el iPhone, para luego ser usado en dispositivos como el iPod Touch, iPad y el Apple TV. Apple, Inc. no permite la instalación de iOS en hardware de terceros. (Tapia, 2013)

- **Windows Phone**: al principio llamado Windows Mobile, es un sistema operativo móvil desarrollado por Microsoft, diseñado para su uso en teléfonos inteligentes. Windows Phone hace parte de los sistemas operativos con interfaz natural de usuario, se basa en el núcleo del sistema operativo Windows CE y posee un conjunto de aplicaciones básicas que utilizan las APIs de Microsoft Windows. (Tapia, 2013)

- **BlackBerry OS**: anteriormente conocida como Research In Motion (RIM), es el sistema operativo móvil de código cerrado desarrollado por BlackBerry que permite la función de multitarea y tiene soporte para diferentes métodos de entrada adoptados por RIM para su uso en computadoras de mano, particularmente la trackwheel, trackball, touchpad y pantallas táctiles. (Molina, 2015)

- **FireFox OS**: El Firefox OS ha sido desarrollado por Mozilla Corporation con apoyo de empresas como Telefónica. Este sistema operativo está basado en Linux, al igual que Android, y usa la tecnología de Mozilla, Gecko. De igual manera, se basa en estándares abiertos como por ejemplo HML5, CSS3 y JavaScript. Este sistema operativo fue concebido para funcionar de manera realmente abierta, a diferencia del SO de Android, donde Google controla ciertos aspectos del sistema. (Molina, 2015)

2.1.4 Ventas de Smartphones.

Según datos publicados por la firma internacional de investigación y análisis IDC (2016), durante el segundo trimestre del 2016, se vendieron 343,3 millones de Smartphones en el mundo, una cantidad que está un 0,3% por encima del mismo periodo de 2015. (Tabla 1).

Top Five Smartphone Vendors, Shipments, Market Share, and Year-Over-Year Growth, Q2 2016 Preliminary Data (Units in Millions)					
Vendor	**2Q16 Shipment Volumes**	**2Q16 Market Share**	**2Q15 Shipment Volumes**	**2Q15 Market Share**	**Year-Over-Year Change**
Samsung	77.0	22.4%	73.0	21.3%	5.5%
Apple	40.4	11.8%	47.5	13.9%	-15.0%
Huawei	32.1	9.4%	29.6	8.6%	8.4%
OPPO	22.6	6.6%	9.6	2.8%	136.6%
vivo	16.4	4.8%	9.1	2.7%	80.2%
Others	154.8	45.1%	173.6	50.7%	-10.8%
Total	**343.3**	**100.0%**	**342.4**	**100.0%**	**0.3%**
Source: IDC Worldwide Quarterly Mobile Phone Tracker, July 28, 2016					

Tabla 1: Ventas de Smartphones. (IDC, 2016).

2.2 Android

Esta plataforma, cada día manejan más volumen de información y de mayor interés. Esta información es lo que convierte el mercado de los dispositivos móviles en un blanco para los cibercriminales, teniendo los mismos peligros que un computador convencional. (Jakobsson & Ramzan, 2008)

En los últimos años, principalmente en el último lustro, los dispositivos móviles se han desarrollado de una manera más acelerada que en otros momentos de la historia. Gracias a estos adelantos, los dispositivos móviles pueden realizar prácticamente cualquier tarea requerida por el portador, teniendo la posibilidad de optimizar su trabajo en todos los ambientes, tanto laborales, como sociales. (Salazar & Gordillo, 2012)

Los dispositivos móviles han estado en constante evolución. El desarrollo de su hardware y software ha permitido que se lleven actividades más complejas que realizar una llamada o enviar un mensaje de texto. (Rueda & Rico, 2014)

Android, es el sistema operativo más utilizado en los dispositivos móviles, con un 343.3% del mercado en el 2016, según informe publicado por la consultora IDC (International Data Corporation). Esto le da el primer puesto también en la mayor cantidad de malware creados para este sistema operativo, aumentando la producción de estos cada año.

2.2.1 Historia de Android

El pionero en el desarrollo de Android es Andy Rubin quien trabajó en firmas como Apple, WebTv y Danger Inc. En la última desarrolló un sistema operativo para móviles llamado DangerOS. Después de dejar esta empresa y lleno de muchas ideas en el 2003 formó un equipo con ingenieros amigos de empresas pasadas, la compañía se denominó Android Inc. Rubin se dedicó a buscar compañías inversionistas, exponiendo los beneficios de la plataforma basada en Linux que estaba desarrollando su equipo. Una de estas empresas fue Google quien compró Android en el año 2005, lo que presuponía la intención de Google de adentrarse en el mundo de los dispositivos móviles. Desde entonces han ocurrido diferentes

acontecimientos que han logrado convertir a Android la plataforma para dispositivos móviles más popular.

En el año 2007 se estableció el Open HandSet Alliance, un consorcio de distintas empresas de software y hardware, incluyendo Google, cuyo principal objetivo es: "acelerar la innovación en los dispositivos móviles y ofrecer a los consumidores una rica, barata y mejor experiencia móvil".

El Android Open Source Project (AOSP) es el grupo encargado de desarrollar y mantener las compatibilidades de las distintas versiones de Android.

El sistema operativo Android está basado en el núcleo Linux. Fue diseñado principalmente para dispositivos móviles con pantalla táctil, como teléfonos inteligentes, tablets o tabléfonos; hoy en día, también se usa para relojes inteligentes, televisores y automóviles. El primer móvil con el sistema operativo de Android fue el HTC Dream y se vendió en octubre del 2008 y a partir de ese momento ha tenido un crecimiento importante, llegando hoy en día a ser la líder en teléfonos inteligentes. Como consecuencia, en la actualidad, es una de las plataformas para la que más códigos maliciosos están apareciendo, explotando ciertas características presentes en la arquitectura del sistema y sus repositorios de aplicaciones. (ESET Latinoamérica, 2013)

2.2.2 Participación de Android en el mercado.

Según los datos entregados por la consultora Gartner (2016), el dominio de Android es evidente, en el que cuatro de cada cinco terminales comprados durante también el segundo trimestre 2016 tienen el sistema operativo de Android con un 86,2%; un 12,9% de iPhone (iOS); 0,6% Windows Phone y un 0,1% para BlackBerry. La gran popularidad que tiene Android lo hace el sistema operativo más interesante para los atacantes, lo cual lo vuelve el sistema operativo más vulnerable ante la gran cantidad de malware que existen en la internet, y el riesgo es aún mayor cuando no se toman precauciones, o también es muy

frecuente que se presente por falta de conocimiento sobre ellos. En la siguiente imagen se puede observar la gran acogida del sistema operativo Android. (Tabla 2)

Worldwide Smartphone Sales to End Users by Operating System in 2Q16 (Thousands of Units)

Operating System	2Q16 Units	2Q16 Market Share (%)	2Q15 Units	2Q15 Market Share (%)
Android	296,912.8	86.2	271,647.0	82.2
iOS	44,395.0	12.9	48,085.5	14.6
Windows	1,971.0	0.6	8,198.2	2.5
Blackberry	400.4	0.1	1,153.2	0.3
Others	680.6	0.2	1,229.0	0.4
Total	**344,359.7**	**100.0**	**330,312.9**	**100.0**

Source: Gartner (August 2016)

Tabla 2: SO Vs Smartphones. (Gartner, 2016).

2.2.3 Versiones del SO Android. (Android, 2016)

Desde su primera versión comercial en septiembre de 2008, han salido considerables actualizaciones. Estás actualizaciones, normalmente corrigen fallos de programas o agregan nuevas funcionalidades.

A continuación se exponen las actualizaciones más sobresalientes de este sistema operativo:

Apple Pie. (Versión 1.0)

Fecha de Lanzamientos: 23 de septiembre de 2008

Principales Características:

- Google Search, permite a los usuarios buscar en internet, en aplicaciones del teléfono móvil, en contactos, en calendario, etc.
- Mensajería instantánea con Google Talk.
- Mensajería instantánea, mensajes de texto y MMS.
- Android Market Programa con un mercado para la descarga y actualización de aplicaciones.
- Navegador Web para visualizar páginas webs en full HTML y XHTML.
- Fondo de escritorio y widgets de la pantalla de inicio.
- Reproductor de vídeo YouTube.
- Soporte para Wi-Fi y Bluetooth.

Banana Bread. (Versión 1.1)

Fecha de Lanzamientos: 09 de febrero de 2009

Principales Características:

- Pantalla en llamada más larga por defecto cuando están en uso el manos libres, además la habilidad de mostrar/esconder el marcador.
- Posibilidad de guardar archivos adjuntos en los mensajes.
- Añadido soporte para marquesina en diseños de sistemas.

Cupcake. (Versión 1.5)

Fecha de Lanzamientos: 27 de abril de 2009

Principales Características:

- Grabación y reproducción en formatos MPEG-4 y 3GP.
- Auto-sincronización y soporte para Bluetooth estéreo añadido (perfiles A2DP y AVRCP).
- Características de Copiar y pegar agregadas al navegador web.
- Fotos de los usuarios son mostradas para favoritos en los contactos.
- Marcas de fecha/hora mostradas para eventos en registro de llamadas y acceso con un toque a la tarjeta de un contacto desde un evento del registro de llamadas.

- Pantallas de transiciones animadas.
- Agregada opción de auto-rotación.
- Agregada la animación de inicio por defecto actual.
- Habilidad de subir vídeos a YouTube.
- Habilidad de subir fotos a Picasa.

Donut. (Versión 1.6)

Fecha de Lanzamientos: 15 de septiembre de 2009

Principales Características:

- Búsqueda facilitada y habilidad para ver capturas de las aplicaciones en el Android Market(Google Play).
- Galería, cámara y videocámara con mejor integración, con rápido acceso a la cámara.
- La galería ahora permite a los usuarios seleccionar varias fotos para eliminarlas.
- Actualización soporte a tecnología para CDMA/EVDO, 802.1x, VPNs y un motor text-to-speech.
- Soporte para resoluciones de pantalla WVGA.
- Mejoras de velocidad en búsqueda y aplicaciones de cámara.
- Framework de gestos y una nueva herramienta de desarrollo GestureBuilder.

Eclain. (Versión 2.1)

Fecha de Lanzamientos: 26 de octubre de 2009

Principales Características:

- Nuevas características para la cámara, incluyendo soporte de flash, zoom digital, modo escena, balance de blancos, efecto de colores y enfoque macro.
- Mejorada velocidad en el teclado virtual, con diccionario inteligente que aprende el uso de palabras e incluye nombres de contactos como sugerencias.
- Renovada interfaz de usuario del navegador con imágenes en miniatura de marcador, zoom de toque-doble y soporte para HTML5.

- Vista agenda del calendario mejorada, que muestra el estado asistiendo a cada invitado, y la capacidad de invitar a nuevos invitados a los eventos.
- Optimización en velocidad de hardware y GUI renovada.
- Soporte para más tamaños de pantalla y resoluciones, con mejor ratio de contraste.
- Mejorado Google Maps 3.1.2.
- Clase MotionEvent mejorada para rastrear eventos multi-touch.31
- Adición de fondos de pantalla animados, permitiendo la animación de imágenes de fondo de la pantalla inicio para mostrar movimiento.

Froyo. (Versión 2.2)

Fecha de Lanzamientos: 20 de mayo de 2010

Principales Características:

- Funcionalidad de anclaje de red por USB y Wi-Fi hotspot
- Agregada opción para deshabilitar acceso de datos sobre red móvil
- Actualizada la aplicación Market con características de grupo y actualizaciones automáticas35
- Cambio rápido entre múltiples lenguajes de teclado y diccionario
- Discado por voz e intercambio de contactos por Bluetooth
- Soporte para docks Bluetooh-habilitado para autos y de escritorio
- Soporte para contraseñas numéricas y alfanuméricas
- Soporte para subida de archivos en la aplicación del navegador37
- Soporte para instalación de aplicaciones en la memoria expandible
- Soporte para Adobe Flash38
- Soporte para pantallas de alto número de PPI (320 ppi), como 4" 720p39
- Galería permite a los usuarios ver pilas de imágenes mediante un gesto de zoom

Gingerbread. (Versión 2.3)

Fecha de Lanzamientos: 06 de diciembre de 2010

Principales Características:

- Mejoras en el sistema.49
- Mejoras en el rendimiento por red del Nexus S 4G.
- Arreglado una falla de Bluetooth en el Samsung Galaxy S.
- Mejoras a la aplicación de correo electrónico.
- Animación de sombras al deslizar por listas.
- Mejoras al software de la cámara.
- Mejorada la eficiencia de la batería.

Honeycomb. (Versión 3.2)

Fecha de Lanzamientos: 22 de febrero de 2011

Principales Características:

- Refinamiento a la interfaz de usuario.
- Conectividad para accesorios USB.
- Lista expandida de aplicaciones recientes.
- Widgets redimensionables en la pantalla de inicio.
- Soporte para teclados externos y dispositivos punteros.
- Soporte para joysticks y gamepads.
- Soporte para reproducción de audio FLAC58 59
- Bloqueo de Wi-Fi de alto rendimiento, manteniendo conexiones Wi-Fi de alto rendimiento cuando la pantalla del dispositivo está apagada.
- Soporte para proxy HTTP para cada punto de acceso Wi-Fi conectado.

Ice Cream Sandwich. (Versión 4.0)

Fecha de Lanzamientos: 18 de octubre de 2011

Principales Características:

- Numerosas optimizaciones y corrección de errores.
- Mejoras en gráficos, bases de datos, corrección ortográfica y funcionalidades Bluetooth.

- Nueva API para los desarrolladores, incluyendo una API de actividad social en el proveedor de contactos.
- Mejoras en el calendario.
- Nuevas aplicaciones de la cámara en mejora de la estabilidad en los videos y resolución QVGA.
- Mejoras de accesibilidad tales como la mejora de acceso al contenido para lectores de pantalla.

Jelly Bean. (Versión 4.1)

Fecha de Lanzamientos: 09 de julio de 2012

Principales Características: es la versión que más actualizaciones tiene, ya que el enfoque primario de mejorar la funcionalidad y el rendimiento de la interfaz de usuario:

- Arreglos de seguridad en la depuración USB.
- Arreglos de seguridad en los accesos directos de las apps.
- Solución en la conexión automática WI-FI.
- Ajustes en MMS, Email/Exchange, Calendario, Contactos, DSP, IPv6 y VPN.
- Solución del atasco en la pantalla de activación.
- Arreglo del LED en las llamadas perdidas.
- Arreglo del gráfico de uso de datos.
- Arreglos en VoIP.
- Corrección para conformidad de la FCC.
- Nueva Interfaz del marcador.
- Corrección de subtítulos.

Kitkat. (Versión 4.4)

Fecha de Lanzamientos: 31 de octubre de 2013

Principales Características:

- Las horas del reloj ya no se muestran con números en negrita, tanto minutos como horas son finos.
- Transparencias en la barra de estado y barra de navegación.

- Introducción del modo inmersivo en el que tanto la barra de estado como la barra de navegación se ocultan en determinadas aplicaciones para una visualización a pantalla completa.
- Optimización y rendimiento en dispositivos de especificaciones técnicas comedidas, así como la implementación de zRAM.
- Posibilidad de impresión mediante WiFi.
- WebViews basadas en el motor de Chromium.
- Nuevo marco de transiciones y efectos visuales.
- Implementación de manera opcional y para desarrolladores de la máquina virtual ART.
- Desactivado el acceso a las estadísticas de batería a aplicaciones de terceros.
- Los monitores de actividad de red y señal desplazados al menú de ajustes rápidos.

Lollipop. (Versión 5.0)

Fecha de Lanzamientos: 12 de noviembre de 2014

Principales Características:

- Vectoriales dibujables, que escala sin perder definición.
- Soporte para vistas previas de impresión.
- Pantalla de bloqueo refrescada y ya no soporta widgets.
- Bandeja de notificación refrescada y configuraciones rápidas desplegable.
- Project Volta, para las mejoras de la vida de la batería.
- Las búsquedas se pueden realizar dentro de la configuración del sistema para un acceso más rápido a los ajustes particulares.
- Pantalla de bloqueo proporciona accesos directos a aplicaciones y configuraciones de notificación.
- Los inicios de sesión de usuarios y múltiples cuentas de usuario están disponibles en más dispositivos, como los teléfonos.
- Entrada y salida de audio a través de dispositivos USB.

- Las aplicaciones de terceros recuperan la capacidad de leer y modificar los datos ubicados en cualquier lugar del almacenamiento externo, como en tarjetas SD.
- Fijación de pantalla de una de aplicación para la actividad restringida de usuario.
- Aplicaciones utilizadas recientemente se recuerdan incluso después de reiniciar el dispositivo.
- WebViews reciben actualizaciones de forma independiente a través de Google Play por razones de seguridad, en lugar de depender de actualizaciones del vendedor de todo el sistema
- La adición de 15 nuevos idiomas: Vasco, bengalí, birmano, chino (Hong Kong), gallego, islandés, kannada, Kirguistán, Macedonia, Malayo, marathi, nepalí, singalés, tamil y telugu
- Tap and Go permite a los usuarios migrar rápidamente a un nuevo dispositivo Android, el uso de NFC y Bluetooth para transferir Detalles de la cuenta Google, ajustes de configuración de datos del usuario y las aplicaciones instaladas.

Mashmallow. (Versión 6.0)

Fecha de Lanzamientos: 05 de octubre de 2015

Principales Características: Ahora Android realizará restauraciones y copias de seguridad de datos completas y automáticas de nuestras aplicaciones tras cambiar de dispositivo o tras restablecerlo de fábrica para continuar con todos nuestros datos y partidas.

- Direct Share: una forma de compartir contenido más simplificada
- "Doze": nuevo sistema que intentará minimizar los wakelocks cuando el dispositivo no se está usando de forma activa
- Soporte oficial para tarjetas SD y USB
- Compatibilidad con lápices bluetooth
- Pantalla de bloqueo mejorada
- Controles de volumen simplificados
- Mejoras en el modo silencio y modo prioridad
- Opción experimental para modificar partes de la IU del sistema

- Direct Links: podemos vincular cada una de nuestras aplicaciones con direcciones URL, para que determinados enlaces siempre se abran con sus respectivas aplicaciones
- Explorador de archivos nativo
- Mejoras en el apartado de memoria RAM
- Mejoras en la selección de texto
- Soporte de Hots

Nougat. (Versión 7.0)

Fecha de Lanzamientos: 15 de junio de 2016

Principales Características:

- Se mejora las animaciones
- Se incorpora la opción de multiventana de forma nativa.
- Es posible arrastrar contenido de una aplicación a otra.
- Mejoras en el uso de la batería.
- Se incorporan nuevos emojis (Emoticonos)
- Nuevo centro de notificaciones. (Se pueden cambiar directamente los iconos que se deseen ver al deslizar los dedos hacia abajo).
- Las notificaciones entrantes se pueden programar para que no aparezcan de forma continua o evitarlas por un lapso de tiempo.

Nombre Versión	Fecha de lanzamiento	Número de versión
Apple Pie	23 de septiembre de 2008	1
Banana Bread	9 de febrero de 2009	1.1
Cupcake	30 de abril de 2009	1.5
Donut	15 de septiembre de 2009	1.6
Eclair	26 de octubre de 2009	2.0 al 2.1
Froyo	20 de mayo de 2010	2.2 al 2.2.3
Gingerbread	6 de diciembre de 2010	2.3 al 2.3.7
Honeycomb	22 de febrero de 2011	3.0 al 3.2.4
Ice Cream Sandwich	12 de octubre de 2011	4.0 al 4.0.4
Jelly Bean	30 de julio de 2012	4.1 al 4.3
KitKat	31 de octubre de 2013	4.4 al 4.4.4
Lollipop	03 de noviembre de 2014	5.0 al 5.1.1
Marshmallow	5 de octubre de 2015	6.0 al 6.0.1
Nougat	22 de agosto de 2016	7

Tabla 3: Versiones del SO Android. (Android, 2016)

2.2.4 Arquitectura Android.

Android es una plataforma para dispositivos móviles que contiene una pila de software donde se incluye un sistema operativo, middleware y aplicaciones básicas para el usuario.
En las siguientes líneas se dará una visión global por capas de cuál es la arquitectura empleada en Android. (Cancela & Ostos, 2012) (Figura 1)

- Aplicaciones: este nivel contiene, tanto las incluidas por defecto de Android como aquellas que el usuario vaya añadiendo posteriormente, ya sean de terceras empresas o de su propio desarrollo. Todas estas aplicaciones utilizan los servicios, las API y librerías de los niveles anteriores.

- Framework de Aplicaciones: representa fundamentalmente el conjunto de herramientas de desarrollo de cualquier aplicación. Toda aplicación que se desarrolle para Android, ya sean las propias del dispositivo, las desarrolladas por Google o terceras compañías, o incluso las que el propio usuario cree, utilizan el mismo conjunto de API y el mismo "framework", representado por este nivel.

Entre las API más importantes ubicadas aquí, se pueden encontrar las siguientes:

- Activity Manager: conjunto de API que gestiona el ciclo de vida de las aplicaciones en Android.

- Window Manager: gestiona las ventanas de las aplicaciones y utiliza la librería Surface Manager.

- Telephone Manager: incluye todas las API vinculadas a las funcionalidades propias del teléfono (llamadas, mensajes, etc.).

- Content Provider: permite a cualquier aplicación compartir sus datos con las demás aplicaciones de Android. Por ejemplo, gracias a esta API la información de contactos, agenda, mensajes, etc. será accesible para otras aplicaciones.

- View System: proporciona un gran número de elementos para poder construir interfaces de usuario (GUI), como listas, mosaicos, botones, "check-boxes", tamaño de ventanas, control de las interfaces mediante teclado, etc. Incluye también algunas vistas estándar para las funcionalidades más frecuentes.

- Location Manager: posibilita a las aplicaciones la obtención de información de localización y posicionamiento.

- Notification Manager: mediante el cual las aplicaciones, usando un mismo formato, comunican al usuario eventos que ocurran durante su ejecución: una llamada entrante, un mensaje recibido, conexión Wi-Fi disponible, ubicación en un punto determinado, etc. Si llevan asociada alguna acción, en

Android denominada Intent, (por ejemplo, atender una llamada recibida) ésta se activa mediante un simple clic.

- XMPP Service: colección de API para utilizar este protocolo de intercambio de mensajes basado en XML.

- Librerías: las aplicaciones Android están escritas en lenguaje Java y son traducidas a bytecodes; aquel tipo de instrucción que la máquina virtual de Java espera recibir, para posteriormente ser compilada a lenguaje de máquina, mediante un compilador JIT a la hora de su ejecución. Android tiene su propia máquina virtual interpretadora de bytecodes llamada Dalvik, en la que simplemente interviene al final como receptor de un archivo ejecutable producto de una recopilación de los archivos .Class de Java. Y de esta manera ser flexible ante el diseño de hardware de un dispositivo móvil. Además JVM no es de licencia GPL, así que Google decidió generar su propia herramienta.

  Entre las librerías más importantes ubicadas aquí, se pueden encontrar las siguientes:

  - Librería libc: incluye todas las cabeceras y funciones según el estándar del lenguaje C. Todas las demás librerías se definen en este lenguaje.

  - Librería Surface Manager: es la encargada de componer los diferentes elementos de navegación de pantalla. Gestiona también las ventanas pertenecientes a las distintas aplicaciones activas en cada momento.

  - OpenGL/SL y SGL: representan las librerías gráficas y, por tanto, sustentan la capacidad gráfica de Android. OpenGL/SL maneja gráficos en 3D y permite utilizar, en caso de que esté disponible en el propio dispositivo móvil, el hardware encargado de proporcionar gráficos 3D. Por otro lado,

SGL proporciona gráficos en 2D, por lo que será la librería más habitualmente utilizada por la mayoría de las aplicaciones. Una característica importante de la capacidad gráfica de Android es que es posible desarrollar aplicaciones que combinen gráficos en 3D y 2D.

- Librería Media Libraries: proporciona todos los codecs necesarios para el contenido multimedia soportado en Android (vídeo, audio, imágenes estáticas y animadas, etc.)

- FreeType: permite trabajar de forma rápida y sencilla con distintos tipos de fuentes.

- Librería SSL: posibilita la utilización de dicho protocolo para establecer comunicaciones seguras.

- Librería SQLite: creación y gestión de bases de datos relacionales.

- Librería WebKit: proporciona un motor para las aplicaciones de tipo navegador y forma el núcleo del actual navegador incluido por defecto en la plataforma Android.

- Tiempo de ejecución de Android: al nivel que las librerías de Android, se sitúa el entorno de ejecución. Éste lo constituyen las Core Librareis, que son librerías con multitud de clases Java y la máquina vistual Dalvik.

- Núcleo Linux: Android utiliza el núcleo de Linux 2.6 como una capa de abstracción para el hardware disponible en los dispositivos móviles. Esta capa contiene los drivers necesarios para que cualquier componente hardware pueda ser utilizado mediante las llamadas correspondientes. Siempre que un fabricante incluye un nuevo elemento de hardware, lo primero que se debe realizar para que pueda ser

utilizado desde Android es crear las librerías de control o drivers necesarios dentro de este kernel de Linux integrado en el propio Android.

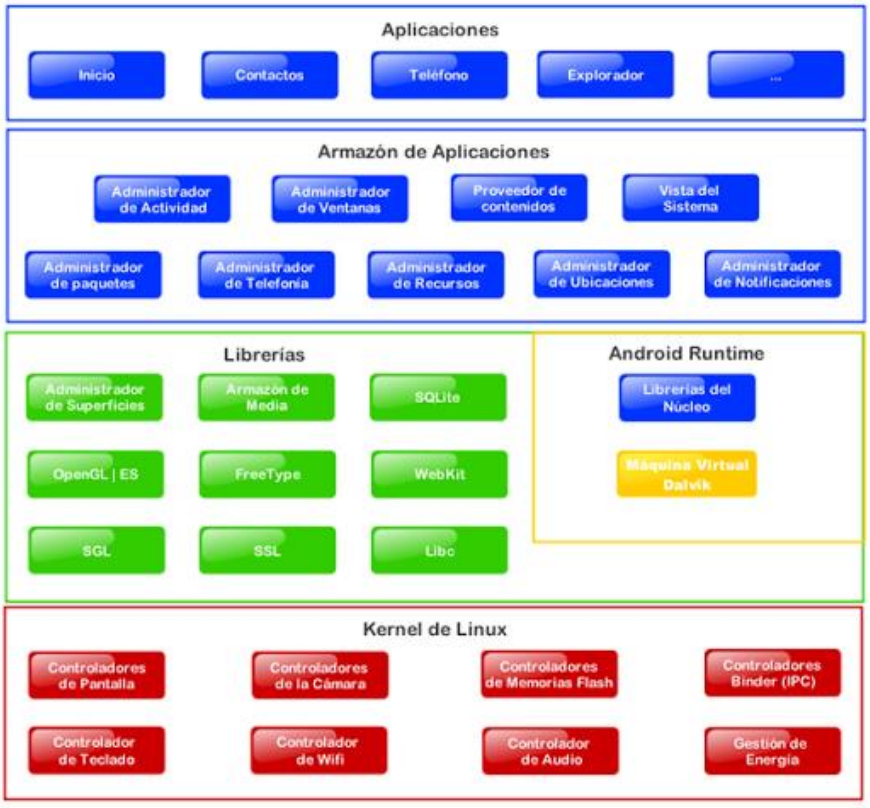


Figura 1: Arquitectura Android. (Cancela & Ostos, 2010)

2.2.5 Play Store.

Es una plataforma de distribución digital con aplicaciones móviles, desarrollada y operada por Google lanzada en el 2008, en la que se integra contenido como: aplicaciones, juegos, libros, películas y música para los sistemas operativos Android, disponible al momento de acceder a la web. Anteriormente se conocía como Android Market, fue cambiada en marzo de 2012 al nombre que en la actualidad lleva debido a la fusión entre Android Market + Google Music. Esta plataforma permite navegar y descargar aplicaciones desarrolladas mediante Android SDK (Software Development Kit), creada para aplicaciones Android, incluye un conjunto de herramientas de desarrollo. Las aplicaciones se pueden conseguir de forma gratuita o pagando, dependiendo del desarrollador.

De acuerdo al informe entregado por la consultora SensorTower Inc.(2016), en el que entrega el top 5 de las principales categorías de descargas internacionales en la Google play, en el que se puede observar cómo ha aumentado con referencia al mismo periodo del año anterior. (Figura 2)

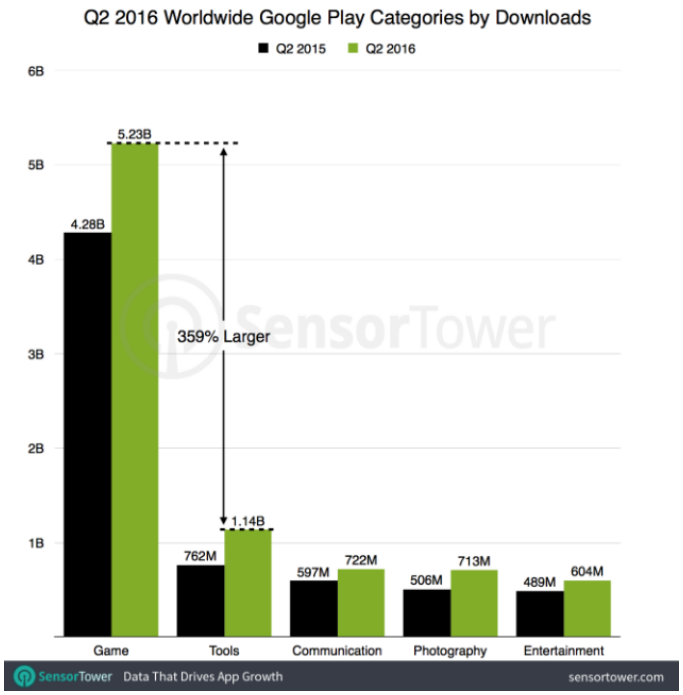


Figure 2: Store Intelligence Q2 2016 Data Digest. (Nelson, 2016).

3. MALWARES Y ANTIVIRUS

3.1 Malwares.

Los malware, son aplicaciones diseñadas para infiltrar un sistema de computadora con la intención de dañar sin el conocimiento y el consentimiento del usuario (Prowse, 2011). En pocas palabras, es un programa de computadora utilizado para llevar a cabo acciones maliciosas. El término de malware es una fusión en inglés de las palabras "malicious + software", software malicioso. El objetivo final de la mayoría de los cibercriminales es instalar malware en las computadoras o dispositivos móviles. Una vez instalados, estos atacantes pueden obtener potencialmente el control completo sobre ellos. Mucha gente tiene la idea errónea de que el malware solo es un problema que se presenta solo en las computadoras Windows, el malware puede infectar a cualquier dispositivo informático, incluyendo teléfonos inteligentes y tables. (OUCH!, 2014)

Aunque los malware generan la mayor cantidad de pérdidas económicas, no siempre es la causa principal, también el desconocimiento de las características o propósitos de estos, pueden jugar un papel importante a la hora de saber cómo defenderse de los virus. Uno de los ejemplos más claros de la falta de conocimiento sobre los malware en el internet, sucedió en la Administración de Desarrollo Económico (EDA), del Departamento de Comercio de los Estados Unidos, donde recibieron en diciembre del 2011 del departamento de Seguridad Nacional una notificación que les indicaba una posibilidad de infección de malware en sus sistemas. La paranoia y la falta de información adicional hicieron el resto: ante la posibilidad de un ciber-ataque proveniente de una nación enemiga, la agencia ordenó la destrucción física del hardware; Ordenadores libres de malware y completamente funcionales, impresoras, cámaras, teclado. Las órdenes dadas por la agencia, conllevaron a los siguientes gastos: consultoría de un contratista de seguridad informático, un alquiler temporal de infraestructura mientras se llevaba a cabo la investigación y el proceso de destrucción de los hadwares y softwares. Esto demandó más de 2,7 millones de dólares. (Pardo, 2013)

La catástrofe se atribuye a una mala interpretación y falta de conocimientos, debido a que en un comienzo se advirtió a la EDA que más de la mitad de sus sistemas estaban infectados, cuando no se sabían con certeza cuántos de ellos presentaban esta problemática.

3.1.1 Evolución de los malware (ESET, 2014)

La historia del malware se remonta a 1986, año en el que apareció el primer virus para plataformas IBM PC utilizando mecanismos de ocultamiento. El entonces llamado Pakistani Brain, infectó el sector de arranque de los discos floppy, lo que le permitió propagarse en cuestión de semanas. A su vez, hacia finales de los 80, surge el Gusano Morris, malware conocido como el primer gusano que se propagó en miles o quizás decenas de miles de minicomputadoras y estaciones de trabajo como VMS, BSD y SunOS.

En la década del 90, aparece Michelangelo; virus que infectaba el sector de arranque de los disquetes floppy y el sector MBR de los discos rígidos. En 1994 se detectó el primer malware de tipo ransomware, llamado OneHalf, y aunque no pedía rescate ni había un código de desactivación, cifraba la primera serie de sectores del disco rígido. Si se usaba FDISK/MBR, el sector MBR infectado se reemplazaba por uno vacío y el sistema ya no era capaz de arrancar. Ya para el año de 1997 comenzó a surgir la tendencia de abandonar el malware auto-propagante por los troyanos. El furor por el robo de credenciales de las cuentas de AOL adoptó diferentes formas que presagiaron el fenómeno de phishing que viene dominando el siglo XXI.

En el 2000 llegó un gusano para correo electrónico, que atacó a millones de PC´s Windows. También fue conocido como ILOVEYOU, llegaba como un archivo adjunto que se hacía pasar por una carta de amor, y era capaz de acceder al sistema operativo, al almacenamiento secundario, al sistema y a los datos de usuario de la víctima.

Ya hacia 2005 sale CommWarrior, el primer *malware* para teléfonos móviles capaz de propagarse mediante mensajes MMS Y Bluetooth atacaba la línea de teléfonos inteligentes Symbian Series 60. Aunque tuvo poco impacto, sus implicaciones para los expertos en antivirus fueron enormes.

En 2008, apareció Conficker, el código malicioso que convertía a los equipos infectados en parte de una botnet, haciendo que se ejecutarán automáticamente, de esta manera, lograba controlar todos los ordenadores y servidores infectados de forma remota. Esta amenaza se propagó por mucho tiempo y afectó a miles de usuarios mientras que sus algoritmos variables impedían su rastreo, esto constituyó un indicador para los desarrollos futuros.

En 2010 apareció un gusano llamado Stuxnet, marcando una nueva era del malware moderno. Este atacaba los sistemas de control industrial y se utilizó contra instalaciones nucleares iraníes. Ya para el 2012, apareció Medre, malware que robaba información extrayendo documentos de AutoCAD. El equipo de ESET lo descubrió y analizó, llegando a la conclusión de que se había desarrollado para robar planos de empresas privadas, especialmente de Perú.

Los códigos maliciosos han evolucionado con el paso del tiempo y las amenazas han llegado a ser cada vez más sofisticadas. En la actualidad, las amenazas que más se detectan son los Troyanos, así como también diferentes tipos de Ransonware; aquellos malware que restringen el acceso a determinadas partes o archivos del sistema infectado, pidiendo rescate a cambio de quitar esta restricción.

También, nos encontramos con amenazas como Hesperbot, troyano avanzado que atacó a usuarios bancarios mediante campañas de estilo phishing, imitando a organizaciones confiables. Así cuando los atacantes lograban que sus víctimas ejecutaran el malware, obtenían las credenciales de inicio de sesión. Al mismo tiempo, apareció Windigo, que en 2014 tomó el control de 25.000 servidores Unix en todo el mundo y envió millones de mensajes de spam diarios con el fin de secuestrar servidores, infectar los equipos y robar información.

Hoy en día, las amenazas, no sólo llegan a ser más masivas que en sus inicios sino que también sus metodologías de propagación e infección son más elaboradas, buscando como principal objetivo el beneficio económico para el cibercriminal.

3.1.2 Crecimiento de los malware para Smartphone con SO Android.

La incidencia de amenazas para Android sobre el total de detección de malware para este sistema operativo ocurridas en Latinoamérica: México (23%), Perú (14%) y Brasil (13%), encabezan la lista de países, correspondiente al primer trimestre de 2016. (Giusto, 2016) (Figura 3)

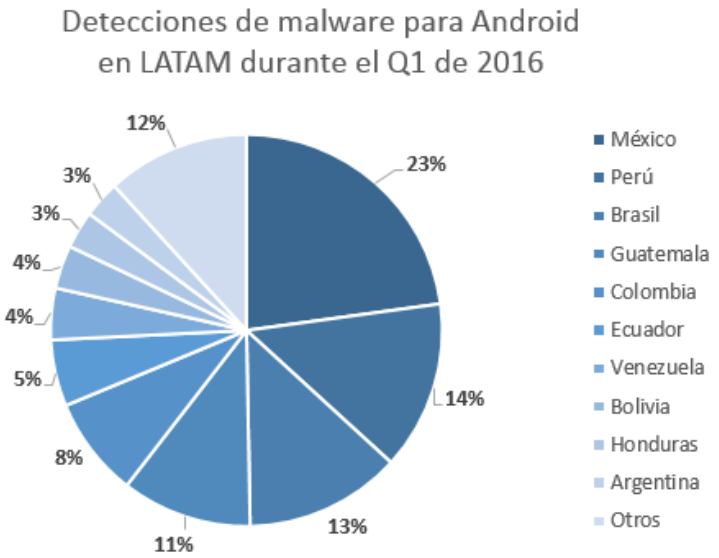


Figura 3: La incidencia de amenazas para Android. (Giusto, 2016).

Los ciberatacantes siguen perfeccionando las técnicas para engañar a los usuarios, de acuerdo a estadísticas publicadas por la revista electrónica SecureList(2016), en el primer trimestre del 2016 "Kaspersky Lab" detectó 2´045.323 de paquetes de instalación de Malwares, 11 veces más que el trimestre anterior y 1,2 veces más que el trimestre antepasado. Cómo se muestra en la siguiente imagen. (Figura 4)

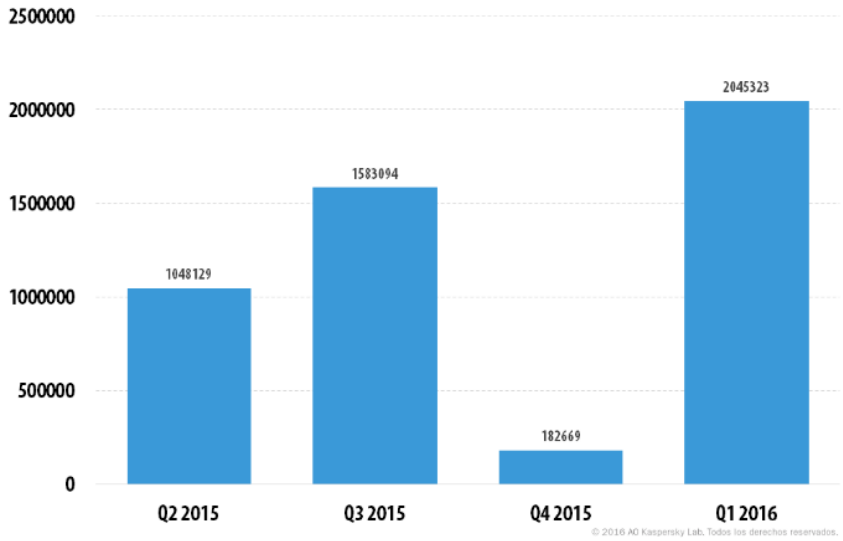


Figura 4: Número de nuevas amenazas móviles. (SecureList, 2016).

Se destacan para el primer trimestre del 2016, las aplicaciones publicitarias potencialmente indeseables (Adware), el porcentaje de este, ha aumentado en 13% en comparación con el cuarto trimestre del 2015 y alcanza el 42.7%, como se puede observar en el gráfico siguiente: (Figura 5)

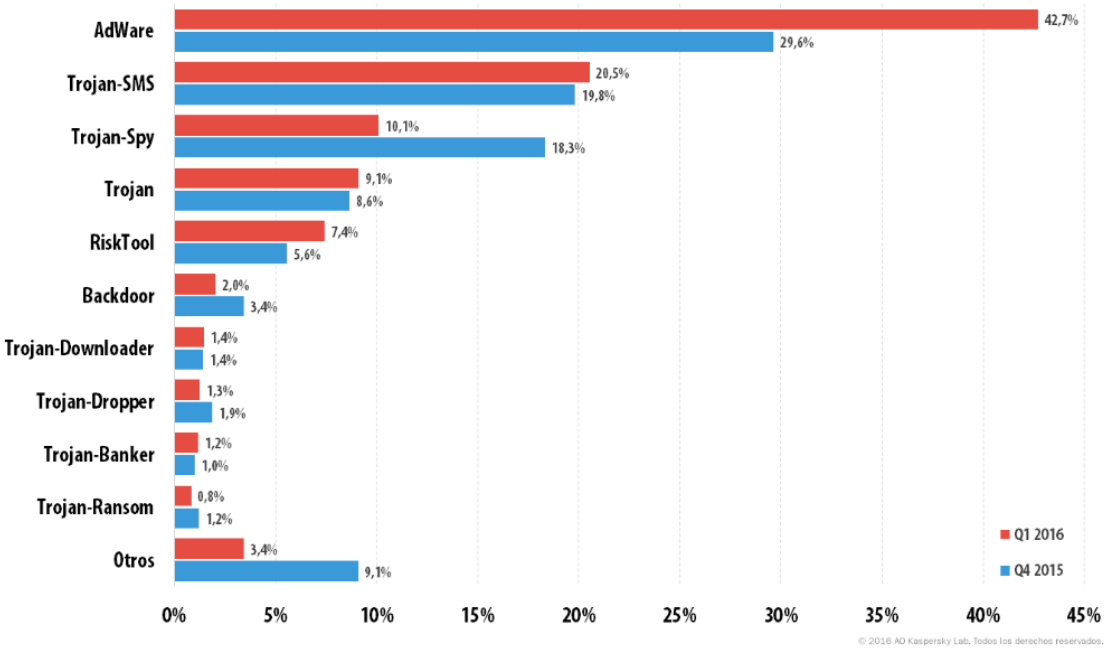


Figura 5: Distribución por tipos de los Malware móviles detectados. (SecureList, 2016).

De igual manera, se observa un crecimiento para los Trojan-SMS, y considerando que este es el trimestre consecutivo de la propagación de los malware de este tipo detectados. En el cuarto trimestre del 2015, el porcentaje de Trojan-SMS en el flujo general de las amenazas móviles aumentó considerablemente, del 6,2% al 19,8%, mientras que en el primes trimestre del 2016 aumentó 0,7%, alcanzando el 20,5%.

Se menciona en el artículo una clasificación de los 20 malwares para móviles, en los que cada vez más, se observa el aumento de troyanos que utilizan la publicidad como el principal medio de obtención de ingresos. Su fin es mostrar al usuario la mayor cantidad de publicidad posible de diversas maneras, entre ellas se destaca la instalación de nuevos programas de publicidad. Estos troyanos pueden usar los derechos de súper usuario para ocultarse en el directorio del sistema, desde donde será más difícil eliminarlos. (Tabla 4)

	Nombre	% de usuarios atacados*
1	DangerousObject.Multi.Generic	73,7
2	Backdoor.AndroidOS.Ztorg.c	11,3
3	Trojan.AndroidOS.Iop.c	8,9
4	Trojan.AndroidOS.Ztorg.a	8,7
5	Trojan-Ransom.AndroidOS.Fusob.pac	6,2
6	Trojan-Dropper.AndroidOS.Agent.ar	4,6
7	Trojan-ClickerAndroidOS.Gopl.a	4,5
8	Backdoor.AndroidOS.Ztorg.b	4,3
9	Trojan.AndroidOS.Iop.m	3,7
10	Trojan.AndroidOS.Agent.ej	3,7
11	Trojan.AndroidOS.Iop.q	3,5
12	Trojan.AndroidOS.Ztorg.i	3,3
13	Trojan.AndroidOS.Muetan.b	3,1
14	Trojan.AndroidOS.Agent.gm	3,1
15	Trojan-SMS.AndroidOS.Podec.a	3,1
16	Trojan-Downloader.AndroidOS.Leech.a	3,0
17	Trojan-Dropper.AndroidOS.Guerrilla.b	2,8
18	Exploit.AndroidOS.Lotoor.be	2,8
19	Backdoor.AndroidOS.Ztorg.a	2,8
20	Backdoor.AndroidOS.Triada.d	2,4

* Porcentaje de usuarios únicos atacados por este programa malicioso, del total de los usuarios atacados del antivirus móvil de Kaspersky Lab.

Tabla 4: TOP 20 de programas maliciosos móviles. (SecureList, 2016).

El primer lugar, lo ocupa DangerousObject.Multi.Generic (73,7%), es el malware detectado mediante el uso de tecnologías en la nube. Está tecnología se activa cuando en las bases de datos de los antivirus no existe ni firmas, ni heurísticas que detecten el programa malicioso.

3.1.3 Categorización de los Malwares para Smartphones con SO Android.

De acuerdo con Kaspersky Labs, las amenazas para los Smartphones incrementaron un 6.1% durante el año 2011, llevándose la peor parte, los que poseen sistema operativo Android, encontrando 5 principales tipos de malware (Baquía, 2012), los cuales son: (Figura 6)

- Andr/PJApps-C. Una aplicación de este tipo suele ser una App que ha sido modificada empleando una herramienta disponible públicamente en Internet. Generalmente se trata de aplicaciones de pago que han sido alteradas. No necesariamente son siempre maliciosas, pero es probable que realicen acciones ilegales, como mostrar publicidad sin autorización del usuario. (63,4%)

- Andr/BBridge-A. También conocido como BaseBridge, este malware utiliza un exploit de escalada de privilegios para, precisamente eso, incrementar sus privilegios e instalar aplicaciones maliciosas adicionales en los dispositivos Android. De igual manera, emplea HTTP para comunicarse con un servidor central y filtrar información potencialmente identificable. además, es capaz de enviar y leer mensajes SMS, lo que puede repercutir en un gasto para el propietario del dispositivo móvil. De hecho, es capaz de escanear los mensajes SMS entrantes y eliminar automáticamente las advertencias de que al usuario se le esté cobrando por utilizar servicios de tarificación premium. (8,8%)

- Andr/Generic-S. Son una variedad de familias de aplicaciones maliciosas que incluyen desde exploits de escalada de privilegios a programas adware agresivos, como por ejemplo, las variantes del malware Plankton para Android. (6,1%)

- Andr/BatteryD-A. Se presenta falsamente como una aplicación para ahorrar batería en un dispositivo Android. Pero lo que realmente hace es enviar información potencialmente identificable a un servidor mediante HTTP, y mostrar anuncios en el teléfono. (4,0%)

- Andr/ DrSheep-A. Un equivalente para Android de la herramienta Firesheep para ordenadores de sobremesa. Permite a los hackers piratear o secuestrar sesiones de Twitter, Facebook y LinkedIn en un entorno de red inalámbrica. (2,6%)

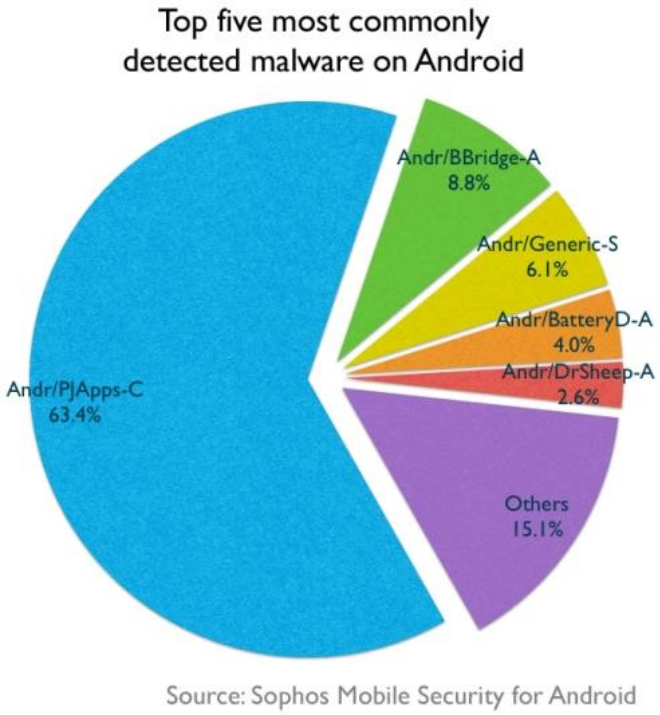


Figura 6: Cinco principales códigos maliciosos para Android. (Teijeira, 2012).

"El volumen de malware que hemos descubierto pone de manifiesto que la seguridad móvil es un problema real y creciente, sobre todo en Android", afirma Graham Cluley, Consultor Senior de Seguridad de Sophos. "Los delincuentes están creando malware más específico para diferentes plataformas, y los usuarios de Smartphones deben conocer que la seguridad ya no se limita a los PCs, ya que tanto los móviles como las tabletas también están en riesgo, sobre todo, si no están lo suficientemente protegidos".

Además, de acuerdo con Kaspersky Labs (2016), se deben categorizar los Malwares en función de su actividad en los ordenadores de los usuarios. El sistema de categorizar utilizado por Kaspersky también lo emplean otros proveedores de antivirus como base para sus categorizaciones de virus informáticos.

El sistema de categorización de Kaspersky asigna a cada objeto detectado una descripción clara y una ubicación específica en el "árbol de categorización" que aparece en la Figura 7 a continuación.

- Los tipos de comportamiento que plantean la menor amenaza se muestran en el área inferior del diagrama.
- Los tipos de comportamiento que plantean una amenaza mayor se muestran en el área superior del diagrama.

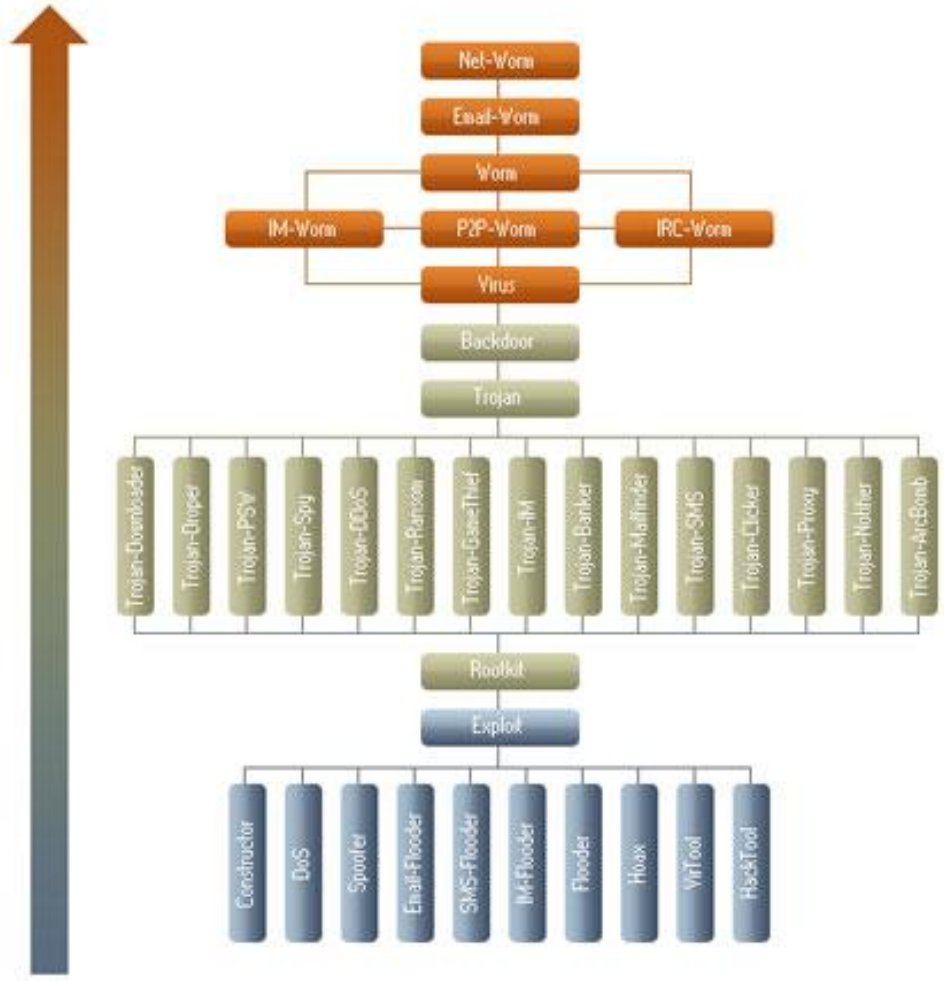


Figura 7: Árbol de clasificaciones de Malwares. (Kaspersky Labs, 2016).

Estas reglas solo se aplican al malware y no están relacionadas con adware, riskware u otros objetos detectados mediante la defensa proactiva (prefijo PDM) o el analizador exhaustivo (prefijo HEUR).

Los programas de malware individual a menudo incluyen varias funciones y rutinas de propagación maliciosas. Sin reglas de clasificación adicionales, este comportamiento puede llevar a confusiones.

Por ejemplo, un programa malicioso específico puede tener capacidad para propagarse a través de un archivo adjunto a un correo electrónico y también como archivos a través de

redes P2P. El programa de igual manera puede tener capacidad para recopilar direcciones de correo electrónico de un ordenador infectado sin el consentimiento del usuario. Con esta variedad de funciones, el programa puede clasificarse correctamente como Email-Worm, P2P-Worm o Trojan-Mailfinder. Para evitar la confusión, Kaspersky aplica un conjunto de reglas que permiten categorizar de forma segura un programa malicioso en función de su comportamiento específico, independientemente de las funciones del programa:

- El árbol de clasificación muestra que a cada comportamiento se ha asignado su propio nivel de amenaza.

- En el árbol de clasificación, los comportamientos que plantean un riesgo mayor se sitúan en un nivel superior en la clasificación con respecto a los comportamientos que representan un riesgo menor.

- La regla para la elección del comportamiento que ocupa un nivel superior en la clasificación solo se aplica a troyanos, virus y gusanos. No se aplica a las herramientas maliciosas

Actualmente, ningún antivirus cuenta con un mecanismo para detectar y clasificar totalmente efectivo y no es posible para las compañías crear antivirus que abarquen las miles de muestras que reciben a diario. “Se sabe que la mayoría de esas muestras son variaciones de malware que ya se tiene identificado y que pocos son completamente nuevos. La clasificación del malware actualmente es el foco de muchas investigaciones. Con el desarrollo de la tecnología, el desarrollo del malware también ha debido innovarse y hoy en día existen diversas técnicas anti-análisis” (Rivera, 2014), las cuales son:

- Cifrado; (carga útil cifrada)
- El polimorfismo; (carga útil encriptada, variando claves)
- El metamorfismo; (Instrucciones diferentes, misma funcionalidad)
- La ofuscación; (preservar la semántica)

Inicialmente, los programadores desarrollaban códigos maliciosos para poner a prueba sus conocimientos en cómputo y era común propagarlos a través de dispositivos de almacenamiento como diskettes o CD-ROM. Generalmente, estos códigos informáticos infectaban los sectores de arranque o renombraban algún archivo válido del sistema para evitar su adecuado funcionamiento. El malware de aquella época requería de la intervención del usuario para infectar el equipo. Hoy en día, estas técnicas de infección y de propagación son obsoletas. El malware de esta generación es capaz de auto-replicarse, aprovechando alguna vulnerabilidad o simplemente con incrustar código a través de alguna aplicación, Sumando de igual manera que los intereses de los atacantes también han cambiado: ahora se enfocan el desarrollo de sus códigos para robar información sensible, modificar registros DNS (Domain Name Services), explotar vulnerabilidades, usurpar sitios Web, etc. Siempre buscando con ello algún beneficio económico. (Fuentes, 2008)

Por ende, si se conocen las amenazas a las que se exponen los dueños de Smartphones, no solos aquellos en los que tienen el sistema operativo Android, sino también los demás sistemas operativos utilizados en móviles, se evitará que se propaguen tan rápidamente los malware por estos dispositivos, al momento en el que se conectan a la red de internet o ejecutan un software malicioso.

3.1.4 Clasificación de los Malwares.

De acuerdo a la publicación de la revista electrónica Kaspersky Lab Daily (2013). Presentan una clasificación de los malware más comunes, para contar con la mayor información posible, de igual manera indican que es difícil distinguir entre los diferentes tipos de malware que hay:

Los virus informáticos son un tipo de código auto-replicante que se instala sin el consentimiento del usuario. Se pueden diferenciar según aquello que infectan, los métodos que utilizan para seleccionar al objeto y las técnicas de ataque. Puedes verlos en forma de adjuntos en los correos electrónicos o como enlaces maliciosos que se descargan por Internet (e infectan el sistema operativo de múltiples formas). Hoy en día, los virus ya no son tan frecuentes porque los cibercriminales quieren tener mayor control sobre la

distribución de los malware; de lo contrario, nuevos tipos de virus caerían rápidamente en manos de los productores de antivirus.

- **Worm**: los gusanos informáticos, o "worms", son una sub-clasificación de los virus, ya que también son programas auto-replicantes. Lo que los diferencian de los virus es que no infectan a archivos existentes sino que se instalan directamente en las computadoras y se quedan allí "reposando" hasta que llega el momento adecuado para penetrar en otros sistemas a través, por ejemplo, de redes vulnerables. Como los virus, también los worms infectan, por ejemplo vía mail, por mensajes instantáneos o compartiendo archivos. Algunos gusanos informáticos son ellos mismos archivos, mientras otros solo residen en la memoria del equipo.

- **Troyanos**: son todo lo contrario de los virus y de los worms. Los Troyanos parecen programas legítimos pero están diseñados para atacar. El nombre Troyano deriva del caballo de Troya de la Grecia antigua; se "disfrazan" de programas útiles para el usuario, pero tienen funciones destructivas. Como los Troyanos no son auto-replicantes, como los wormsn, no se difunden solos, aunque llegan a un gran número de usuarios a través de Internet. Existen varios tipos, como los Troyanos Backdoor (que quieren tomar el control remoto de los ordenadores de las víctimas) y los Troyanos Downloader (que instalan códigos maliciosos).

- **Ransomware**: Está exclusivamente diseñado para extorsionar dinero a sus víctimas. Puede aparecer en forma de pop up, enlace de phishing o web maliciosa, y una vez que se hace clic en él, impulsa una vulnerabilidad en el sistema del usuario. Para tomar dinero de sus víctimas lo que hace es extorsionarlos diciéndoles que tienen un software pirateado, que han visto videos ilegales, de forma que reaccionen rápidamente ante el aviso que se despliega y paguen rápidamente una fianza.

- **Rootkit**: son una parte especial de los malware, ya que están diseñados específicamente para ni el usuario ni el software de protección se enteren de la

existencia del malware en el sistema. Algunos incluso se activan antes de que arranque el sistema operativo (éste rootkit se llama Bootkit). Algunos programas antivirus muy sofisticados consiguen detectar los Rootkit y eliminarlos.

- **Backdoor** (RAT): conocidos en inglés como "Remote Administration Tools", son aplicaciones a través de las cuales los administradores de sistemas y los cibercriminales pueden acceder al sistema sin que el usuario se entere. Dependiendo de las funcionalidades de los backdoor, los hacker pueden instalar y lanzar otros programas, enviar keylogger, descargar o borrar archivos, encender los micrófonos o la cámara del dispositivo, registrar la actividad de la computadora y enviarla al cibercriminal.

- **Downloader**: son piezas de códigos que toman archivos ejecutables o cualquier otro archivo del sistema para llevar a cabo algunas tareas específicas desde el servidor del cibercriminal. Una vez que el usuario haya descargado los downloader desde un adjunto de un correo o de una imagen, los delincuentes envían instrucciones para descargar otros malware en el equipo.

Ahora bien, la compañía de seguridad informática Eset (2016), clasifica además los siguientes Malwares:

- **Adware** propagación de mensajes publicitarios. mostrando ventanas emergentes durante la navegación en Internet. Los mensajes publicitarios permiten a los desarrolladores de programas gratuitos obtener ingresos ofreciendo funcionalidades del programa que se encuentran disponibles solo en la versión comercial. En la mayoría de los casos la instalación de adware se encuentra dentro de los lineamientos legales; existen muchos programas de publicidad legítima.

- **Rogue**: programas que simulan ser una aplicación anti-malware (o de seguridad), ocasionando los efectos contrarios a esta, instala códigos maliciosos. Por lo general,

se trata de ataques que muestran en la pantalla del usuario advertencias llamativas respecto a la existencia de infecciones en su equipo. Los objetivos varían desde instalar códigos maliciosos en el equipo para obtener información confidencial o dinero a través del ataque.

- **Spyware:** programa que con ayuda de Internet, recolecta piezas de información sensible del usuario sin su conocimiento. Algunos de estos programas buscan información tal como la referente a aplicaciones instaladas y al historial de sitios web visitados. Otros programas del tipo spyware son creados con un objetivo mucho más peligroso, recolectando información financiera o personal para el robo de identidad.

- **Botnet**: son cualquier grupo de dispositivos infectados y controlados por un atacante de forma remota, al principio solo infectaban a PC's, sin embargo, ya también han aparecido para los Smartphone. Son llamados "bots" o "zombie", crea un botnet a través de un malware que infecta a una gran cantidad de máquinas. Es decir, es una gran red de ordenadores o dispositivos móviles infectados con una variedad de malware. (Muena, 2014)

De esta manera se puede aportar una clasificación, teniendo en cuenta las estadísticas de ataques de Malwares para sistemas operativos Android y las categorizaciones indicadas en este trabajo, los Malwares más presentes en estos ataques son:

1. Adware.
2. Troyanos.
3. Spyware.
4. Fakeapps.

A continuación se detalla más cada uno de ellos y como pueden afectar a los Smartphones con sistema operativo Android.

3.1.5 Malware que representan más riesgos para Smartphone con sistema operativo Android.

De acuerdo a las clasificación planteada en la publicación de la revista electrónica Rootear (2014), los porcentajes expuestos en Giusto (2016), Kaspersky Labs (2016) y Teijeira (2012). Definiendo lo que es cada malware para Android, validando también los Fakeapps que se encuentran en la Play Store de Google, los cuales son:

- **Aplicaciones funcionales con Adware:**

Estas aplicaciones infectadas, no solo tratan de confundir al usuario, sino que re-empaquetan la aplicación original con algunas variaciones en el código, haciendo mediante el Adware, que automáticamente muestra publicidad web al usuario durante la instalación o mientras usa la aplicación, generando lucro a sus autores.

Las réplicas exactas de aplicaciones legítimas, son Adware, las cuales no contienen la funcionalidad del software original que intentan suplantar. Son las Fakeapps (Aplicaciones falsas; por su traducción al español). En ellas, el fabricante es inventado o el título remite a algo importante de la aplicación. Suelen tener características a las que no corresponden a los de las aplicaciones legítimas y sirven para liberar el Adware en el Smartphone.

Desafortunadamente, este tipo de infecciones a veces no son detectadas por los antivirus. Incluso requieren menos permisos que las aplicaciones originales. Basta con que no sean lo que prometen para que se las pueda considerar como fakeapps.

- **Troyanos**:

Son aquellos malware que roban los datos de los usuarios, suplantan las apps bancarias, phishing. Hay algunos que hasta intentan infectar el pc de escritorio a través del teléfono y viceversa cuando se conectan entre sí, aunque son los más difíciles de ver en Play Store. Sin importar las características o comportamientos de estos troyanos conocidos, lo que buscan es robar la información personal, que luego terceros podrían sacar provecho de ella; como perder el dinero en cuentas.

“En cuanto a los ataques de ingeniería social, estas actúan mediante anuncios publicitarios que pretenden ser legítimos, al reportar una infección y que recomiendan "hacer click" en un botón para eliminarla. Posteriormente, una advertencia emergente de Android pide al usuario eliminar el virus, se realiza un supuesto análisis y envía información del virus, a la vez que obtiene contraseñas e información de tarjetas bancarias y después solicita que instale la aplicación.” (Informador.mx, 2014)

- **Aplicaciones Espías (Spyware):**

Se crearon con el fin de monitorizar las actividades de los usuarios, pensadas para usuarios que deseen directamente espiar o infectar a alguien con un troyano. No se ocultan como las demás clases de Malwares, y su utilización la dejan a criterio de los usuarios. Normalmente son retiradas de la Play Store.

- **Replicas falsas de aplicaciones legítimas (Fakeapps):**

Este tipo de malware intenta confundir al usuario. Lo que busca es conseguir descargas y lucrarse con publicidad, o infectar al usuario por otros medios. Suelen ser oportunistas y suelen ir acompañados de una coletilla, como por ejemplo “free”, “tips”, “tricks” o “wallpapers” por poner algunos ejemplos. Mientras que las guías legítimas o las aplicaciones de personalización suelen dejar bien claro lo que es en la imagen y descripción de la apps, otros malware no se molestan en hacer una distinción, sino que se aprovechan de la confusión del usuario para infectarlo.

Un ejemplo claro de lo anterior, es el caso de buscar una aplicación en la Play Store, en la que sale la aplicación de la siguiente manera. (Ver Figura 8)

Figura 8: Imagen de fakeapps. (Google Play, 2013).

El cliente de WhatsApp es totalmente falso (LHLH Mobile Soft). En cambio la aplicación legítima es la que se puede observar en la Figura 9.

Figura 9: Imagen Original de la App. (Google Play, 2014).

Actualmente Google es mucho más exigente en el control de las aplicaciones que publica en su plataforma, pero aun así es posible encontrar Malwares con esta descripción.

Además este tipo de malware, busca estafar al usuario invitándolos a pagar por servicios que no pagaría normalmente. Esto incluye suscripciones a servicios de mensajes premium. Esto significa que elude la confirmación por PIN de Google Play "respondiendo" automáticamente por el usuario, de forma que el propio programa lee el mensaje de confirmación y "responde" por el usuario. Así, queda suscrito de forma transparente sin confirmación explícita, y se le comienza a cobrar por mensajes recibidos.

3.1.6 Modo de instalación del malware.

En todo aplicativo creado para Android se obtendrá un paquete de instalación en el que se almacena un archivo comprimido con formato .APK (Android Applicacion Package). Dentro encontraremos los siguientes componentes:

- Archivo Android Manifest: se encuentran todas las características principales que tendrá nuestra aplicación al ejecutarse en un dispositivo móvil. Como los son los

bloques que posee la aplicación, los permisos, la versión del aplicativo, de igual manera las versiones previas soportadas, las dimensiones de la pantalla, etc.

- Archivo classes.dex: es el fichero compilado preparado para ejecutarse en la Máquina Virtual Dalvik, y el que más modifican los ciberdelincuentes para realizar sus ataques.

- La carpeta Resources: se encontran todos los archivos externos que se usan para construir los proyecto, como por ejemplo: iconos, audio, archivos planos de texto, los archivos .xml de diseño, etc.

- Librerías nativas: es el archivo .APK que contiene aquellas librerías de las cuales depende todas las aplicaciones.

- Carpeta META-INF: en esta se guarda archivos que corresponden a las Firmas Digitales de la aplicación. Con esta especificación puedes indicar el creador y dueño de la aplicación, además se indica el ID del desarrollador para ser reconocido y autenticado en procesos de comercialización. Google es muy riguroso con este último tema.

En el trabajo realizado por Y. Zhou and X. Jiang (2012). Se expone algunas de las formas como se instalan estos softwares maliciosos:

- Repackaging: es la técnica más utilizada para la instalación de los Malwares. Ya que todos tienen acceso a Play Store; tienda de aplicaciones de Google. Cualquiera puede descargar una aplicación inicialmente benigna, una vez descargado el programa, se puede aplicar técnicas de ingeniería inversa para poder desensamblar el programa, agregar el código malicioso sin quitar la funcionalidad principal de la aplicación original, finalmente se ensambla el programa nuevamente y se coloca en el mercado de aplicaciones. Posteriormente, usuarios inocentes descargan esta aplicación infectada, convirtiéndose en víctimas. Para evitar esta situación, Google

ha aumentado las normas y los requisitos para subir contenido en su plataforma. Aproximadamente el 86% de las muestras obtenidas en el estudio, se observa este tipo de técnica.

- Update Attack: en este caso, no se alberga completamente el malware en la aplicación, es en el momento en el que se ejecuta la actualización de la aplicación. Este tipo de instalación es muy difícil de detectar.

- Drive-by Download: se inducen a los usuarios a realizar "descargas" que son presentadas como beneficiosas para sus dispositivos, pero cuya verdadera finalidad es introducir en sus sistemas operativos, rutinas maliciosas. Un ejemplo de esta técnica, es cuando sale un mensaje que dice: "Su teléfono está en peligro, repararlo ahora!", si se da clic en la imagen, se acepta el mensaje y lo que se está haciendo es descargando un malware.

3.2 Anti-Malware o Antivirus

Un antivirus es un programa, cuya finalidad es prevenir y evitar la infección de virus informáticos, impidiendo de igual manera la propagación de estos. Tiene capacidad para detectar y eliminar los virus, restaurar los archivos afectados por la infección. Teniendo tres componentes principales. (Mosquera & Restrepo, 2011)

- Vacuna o monitor antivirus: programa que actúa en tiempo real, analizando los archivos del dispositivo que son abiertos o los programas que se ejecutan. Esta función es importante, ya que si un archivo infectado ha conseguido alojarse en el sistema y por cualquier motivo no se ha verificado, el antivirus avisa del peligro cuando se intente ejecutar.

- Motor de detección: programa cuya función es realizar el escaneo constante de los archivos, directorios o unidades que se seleccionen del dispositivo. Trabaja analizando los archivos en los que busca la existencia de códigos maliciosos y que

el programa reconoce por comparación si están registrados en la lista de definiciones.

- Desinfectador: programa que una vez localizado el objeto infectado en el dispositivo, desactiva su estructura y procede a eliminarlo, reparando sus efectos en el sistema, aunque muchas veces no es posible, todo depende del tipo de virus y los efectos producidos.

Para que el antivirus sea productivo y efectivo hay que configurarlo cuidadosamente de tal forma que aprovechemos todas las cualidades que ellos poseen. Hay que saber cuáles son sus fortalezas y debilidades y tenerlas en cuenta a la hora de enfrentar a los virus.

Un antivirus es una solución para minimizar los riesgos, aunque nunca será una solución definitiva, lo principal es mantenerlo actualizado. Para mantener el sistema estable y seguro el antivirus debe estar siempre actualizado. Siempre es importante tomar medidas preventivas y estar constantemente leyendo sobre los nuevos virus y tecnologías en el mercado.

3.2.1 Funcionamiento de los Antivirus. (Domínguez, 2015)

Un antivirus compara el código de cada archivo con una base de datos de los códigos (también conocidos como firmas o vacunas) de los virus conocidos, por lo que es importante actualizarla periódicamente a fin de evitar que un virus nuevo no sea detectado. También se les ha agregado funciones avanzadas, como la búsqueda de comportamientos típicos de virus (técnica conocida como Heurística) o la verificación contra virus en redes de computadores.

Comúnmente, un antivirus tiene un componente que se carga en memoria y permanece en ella para verificar todos los archivos abiertos, creados, modificados y ejecutados en tiempo real. Es muy común que tengan componentes que revisen los adjuntos de los correos electrónicos salientes y entrantes, así como los script

Algunos ejemplos de antivirus en el mercado son:

- Bitdefender Antivirus.
- Norton Security.
- AvastPro Antivirus.
- Kaspersky Antivirus, entre otros.

3.2.2 Tipos de antivirus. (Enciclopedia de Clasificaciones, 2016)

ANTIVIRUS HEURISTICOS: Los heurísticos analizan el código de cada archivo con métodos genéricos y detectan virus nuevos que todavía no se han incluido en la base de datos de virus de estos programas. Ejemplos:

- Nod32 2.51.30
- Vba32 3.11.0
- VirIT 6.1.9
- AVG 7.1.405 Professional
- AVG 7.1.405 freeware

ANTISPYWARE: Los Spywares o Programas Espía, son aplicaciones que se dedican a recopilar información del sistema en el que se encuentran instaladas para luego enviarla a través de Internet, generalmente a alguna empresa de publicidad. Todas estas acciones se enmascaran tras confusas autorizaciones al instalar programas de terceros, por lo que rara vez el usuario es consciente de ello, por ejemplo:

- Ad-aware SE Personal
- Spybot S&D
- A-squared Free:
- CWShredder de Intermute / Trend Micro:
- SpywareBlaster:
- SpywareGuard
- SpySweeper

- Windows Defender

ANTISPAM: Spam, es la palabra que se utiliza para calificar el correo no solicitado enviado por Internet. La mayor razón para ser indeseable es que la mayoría de las personas conectadas a la Internet no goza de una conexión que no les cueste, y adicionalmente reciben un cobro por uso del buzón. Por lo tanto el envío indiscriminado de este tipo de correo ocasiona costos al lector. Contrario al 'correo basura' o Junk Mail que recibimos en nuestros buzones ordinarios (físicos, en papel), el recibo de correo por la red le cuesta a un buen número de personas, tanto en la conexión como en el uso de la red misma. El correo físico no tiene ningún costo para quien lo recibe.

Tipos más comunes de Antispam:

- Spam: enviado a través del correo electrónico.
- Spim: específico para aplicaciones de tipo Mensajería Instantánea (MSN Messenger, Yahoo Messenger, etc).
- Spit: spam sobre telefonía IP. La telefonía IP consiste en la utilización de Internet como medio de transmisión para realizar llamadas telefónicas.
- Spam SMS: spam destinado a enviarse a dispositivos móviles mediante SMS (Short Message Service).
- Anti-Phishing: Existen varias técnicas diferentes para combatir el phishing, incluyendo la legislación y la creación de tecnologías específicas que tienen como objetivo evitarlo.

FIREWALL: Un cortafuegos (o firewall en inglés), es un elemento de hardware o software utilizado en una red de computadoras para controlar las comunicaciones, permitiéndolas o prohibiéndolas según las políticas de red que haya definido la organización responsable de la red.

ANTIPOP-UPS: tiene como finalidad impedir que se ejecuten las ventanas pop-ups o emergentes, aquellas ventanas que surgen repentinamente sin que el usuario lo haya decidido, mientras navega por Internet.

3.2.3 Los antivirus para dispositivos móviles más recomendados.

De acuerdo a las investigaciones realizadas por el AV-TEST The Independent IT-Security Institute (2016), se brinda los antivirus más eficaces a la hora de detectar un malware en los dispositivos móviles con SO android: (Tabla 5)

Tabla 5: El mejor software antivirus para Android. (Av-Test, 2016).

Para la investigación realizada por Av-Test, se tuvieron en cuenta los siguientes parámetros para la evaluación de cada antivirus:

Resultado Protección:

- Detección de malware más reciente para Android en tiempo real.
- Detección de malware actual para Android descubierto en las últimas 4 semanas.

Resultado Utilidad:

- Pruebas de funcionamiento: Las aplicaciones no influyen en la carga de la batería.
- Pruebas de funcionamiento: Las aplicaciones no ralentizan el uso del aparato durante su uso normal.
- Pruebas de funcionamiento: Las aplicaciones solo generan poco tráfico.
- Falsas alarmas durante la instalación y el uso de una aplicación desde Google Play Store.
- Falsas alarmas durante la instalación y el uso de una aplicación desde app stores de terceros.

De igual manera, la página de Android Básico (2016), expone su lista de los mejores antivirus para Android gratuitos, en los que considera como parámetros para evaluar los antivirus: base de datos de Malware, interfaz amigable a los usuarios, diferentes opciones de seguridad, antispam, gestor de aplicaciones y optimización del sistema operativo. (Tabla 6)

Antivirus	Ventajas
Eset Mobile Security	Interfaz muy sencilla de utilizar y bastante clara. Dispone de una base de datos de malware y virus muy extensa.
NQ Mobile Security	Interfaz amigable y Dispone de miles de opciones de seguridad, antispam, gestor de aplicaciones y optimización del sistema Android.
Avast! Mobile Security & Antivirus	Dispone de filtros de SMS y llamadas, opción de bloqueo y rastreo GPS.
AVG Antivirus	Analiza aplicaciones, configuraciones, medios y todo tipo de archivos que tenga el terminal.
Lookout Seguridad y antivirus	Análisis completo de las aplicaciones antes de la descarga.
360 Security	Limpia el terminal de archivos viejos, aplicaciones y aquellos que pudieran estar corruptos. Monitorea el uso de datos, bloquear SMS, llamadas y un perfecto economizador de la batería.
Norton Antivirus y Seguridad	Elimina del móvil o tablet el malwares antes de que se metan en los dispositivos mediante un análisis de forma automática y periódica de las aplicaciones.

CM Security	Comprueba mediante una foto quién ha intentado desbloquear el terminal. Además se tiene la posibilidad de bloquear aplicaciones.
Bitdefender Antivirus Free	Se ha integrado de forma ligera en los móviles, también es sencillo de utilizar y hará un trabajo excelente con los virus.
Kaspersky	Es creada por una de las compañías que más confianza dan en este terreno de los antivirus.

Tabla 6: Antivirus para Android. (Android Básico, 2016)

Ya sea por su nivel de protección, detección de Malwares en tiempo real o usabilidad, se debe tener siempre muy presente que los antivirus no son la forma más efectiva de evitar que el dispositivo se contagie con un Malware, siempre es importante la prevención y el auto-cuidado por la gran cantidad de malware que salen diariamente.

4. METODOLOGÍA

Para la realización de la investigación y del trabajo de grado, se usaron las siguientes fases, en las que se busca la planeación detallada y más sencilla, logrando de esta manera abarcar toda la investigación:

FASE 1: se realizó un estado del arte en el área de seguridad informática para dispositivos móviles con sistema operativo Android, centrándose en los códigos maliciosos o malware, como es comúnmente conocido. Por consiguiente, se llevó a cabo la metodología cualitativa, debido a que los resultados obtenidos se enfocaron en las diferentes características de los malware. Ésta metodología se realizó en tres etapas principales: planificación, realización y documentación, a su vez, estas se componen también de otros procedimientos que se basaron en aplicar seis procesos (Serna & Serna, 2013):

1. Se definieron las preguntas de investigación:
   ¿Qué Son los Malware para dispositivos móviles?
   ¿Cómo atacan a los Smartphones con SO Android?
   ¿Cuándo se es más vulnerable al ataque de un malware?
   ¿Por qué los Malwares atacan a los Smartphones con SO Android?

2. Se definió el proceso de búsqueda:
   Se investigó a través de:
   Buscadores: Google Académico.

   Revistas: ENTER.CO, PCWorld.COM.MX, fayerwayer.com, xataka.com, wayerless.com, kaspersky.es, bbc.com, gdatasoftware.co.uk, welivesecurity.com (ESET), lookout.com, elevenpaths.com, av-test.org, owasp.org, entre otros.

   Bases de datos universitarios:
   Engineering Village, Institute of Education Scienses (ERIC), IEEE

De igual manera se desarrolló en el marco del semillero de investigación en seguridad en sistema informático (SISSI) del Instituto Tecnológico Metropolitano (ITM), bajo la línea de investigación en seguridad de dispositivos móviles, con el propósito de obtener la mayor información posible sobre los malware en Smartphones con sistema operativo Android y evidenciar los riesgos que se exponen los usuarios con estos dispositivos

3. Se definió como criterios de inclusión y exclusión de cada documento encontrado al tomar como palabras claves: Malware y Android, además, se tomaron los documentos con las estadísticas y cifras a partir del 2005, años en el que apareció CommWarrior, malware para móviles capaz de propagarse mediante mensajes msm y Bluetooth.
4. Se definió la valoración de calidad de cada documento, hallando y actualizando la mayor información posible encontrada del año 2016.

FASE 2: Se seleccionaron las fuentes obtenidas en la investigación en donde estén las descripciones de los malware que más riesgos representan para los Smartphones con sistemas operativos Android, todo esto se hizo teniendo en cuenta los siguientes pasos (Instituto Tecnológico de Monterrey, 2012):

1. Se identificaron y se comprendieron las ideas principales: Malware y Android
2. Se sintetizó el argumento central de cada sección a través de la supresión y generalización de ideas principales.
3. Se elaboraron fichas de trabajo de cada sección revisada con estrategias de síntesis y paráfrasis.

Ahora bien, teniendo en cuenta los anteriores pasos, se dividió en dos partes para el desarrollo del tema, teniendo en cuenta la selección de las fuentes obtenidas en la investigación, y como ejemplo de lo que está contenido en este trabajo, los cuales son:

- **Marco Conceptual: Smartphone y Android**

  En este punto se abarca la historia, evolución de los Smartphones, clases sistemas operativos para dispositivos móviles y ventas de estos. Del mismo modo se trata el tema de Android, su historia, participación en el mercado, versiones y arquitectura de este sistema operativo y se explica una de las principales funciones de Android, como lo es la Play Store.

- **Malware y Antivirus.**

  Siendo uno de los temas menos conocidos por los usuarios, se explica en que consiste los Malwares, la evolución de estos virus, el aumento de Malwares para los Smartphone con sistema operativo Android, la categorizaciones de los Malwares para los dispositivos móviles con este sistema operativo y las diferentes clasificación de los Malwares. Por la clasificación y categorizaciones anteriormente nombrados, se nombran los Malwares que más riesgo representan para los Smartphones con sistema operativo Android y el modo como se instala los virus. Al igual que se expone el tema de los Anti-malware o antivirus, funcionamientos, tipos y los antivirus más recomendados para dispositivos móviles.

FASE 3: Se clasificaron los malware para Smartphones con sistemas operativos Android por sus características, con la intención de identificar buenas prácticas para la protección y prevención ante el contagio de Malwares.

Se propone la clasificación de los Malwares de acuerdo a las diferentes categorizaciones de los Malwares para los dispositivos móviles con este sistema operativo propuestas por el estudio realizado por Banquia (2012) y Kaspersky Labs (2016) y las diferentes clasificación de los Malwares propuestas por Kaspersky Lab Daily (2013), Eset (2016) y Muena (2014) en sus investigaciones, esto se expone en los siguientes puntos del trabajo:

- Categorización de los Malwares para smartphones con SO Android
- Clasificación de los Malwares.

Por lo anterior, se propone la organización de la siguiente manera, teniendo en cuenta el porcentaje de ataques y tipos de Malware. A continuación, se muestra un ejemplo de lo realizado en este trabajo:

1. **Adware.**

   El objetivo de este virus es mostrar banners publicitarios, reorientando así las consultas de búsqueda de anuncios de las páginas web publicitarias etc. Además, recopilan datos acerca de las actividades de los usuarios en Internet. (Kaspersky, 2016).

2. **Troyanos.**

   Son códigos maliciosos que, a diferencia de los virus y gusanos, no puede reproducirse por sí mismo e infectar archivos. Comunmente se encuentra en forma de archivo ejecutable (.exe, .com) y no contiene ningún elemento más, a excepción del propio código del troyano. Por esta razón la única solución consiste en eliminarlo. (Eset, 2016)

3. **Spyware.**

   Es un programa que se vale de Internet para recolectar piezas de información sensible del usuario sin su consentimiento. Algunos de estos softwares, buscan información tal como la referente a aplicaciones instaladas y al historial de sitios web visitados. Otros programas del tipo spyware son creados con un objetivo mucho más peligroso, como lo es la recolección de información financiera o personal para el robo de identidad. (Eset, 2016)

4. **Fakeapps**

   Son apps que no contienen la funcionalidad del software original que intentan suplantar. El fabricante es inventado o remite a alguna parte del título del juego. Es importante destacar que en ocasiones, ni siquiera son cazados como malware por ningún motor antivirus, a veces incluso, requieren menos permisos que las originales, o no contienen un sistema de profesionalización del malware. (Elevenpaths, 2014

FASE 4: Luego de realizar un estado del arte sobre los malwares en Smartphones con sistema operativo Android, se brindan algunas de las buenas prácticas encontradas para mitigar el riesgo de estos virus en el sistema operativo Android, los cuales son:

- Revisa periódicamente tus cuentas, nunca está de más revisar tus cuentas bancarias de forma periódica, para estar al tanto de cualquier irregularidad en tus transacciones online.
- Descargar Software de sitios confiables, cuando se necesita un programa, se suele descargarlo de Internet, pero pocas veces se repara los sitios desde donde realizamos la descarga. Lo mejor es descargar todos los programas de la página oficial de cada uno de los creadores o desde la Play Store, para evitar el contagio de las clases de Malwares.
- No hacer clic en ventanas emergentes que le indican que su equipo está infectado con un virus. Los antivirus no funcionan de esa manera. Esas "fakeapps" instalan software malicioso en su Smartphone sin que usted se percate.
- Tener mucho cuidado con los archivos adjuntos del correo electrónico. No todos los archivos son dañinos, pero es conveniente proceder a eliminar el correo electrónico o identificarlo como spam si no reconoce al remitente. Nunca descargue ni abra el archivo adjunto. Y si el archivo es de un remitente conocido, no está de más examinarlo con el antivirus.
- Utilice contraseñas para todo y verificar que sean claves fuertes. No utilice la misma contraseña para todos los sitios ni contraseñas fáciles de adivinar. Utilice contraseñas seguras que tengan al menos ocho caracteres donde se incluya letra mayúscula, números y caracteres alternativos. Se recomienda cambiar las contraseñas con frecuencia.
- Revise sus cuentas bancarias y reportes de endeudamiento de manera periódica. Debe convertirse en un hábito obligatorio el de hacer seguimiento en busca de signos de fraude o cargos que no haya hecho en los últimos días.
- Refuerza la seguridad de tu ordenador, el sentido común y la prudencia es tan indispensable como mantener tu equipo protegido con un buen antivirus que

bloquee este tipo de ataques. Además, siempre debes tener actualizado tu sistema operativo y navegadores web.

- Verifica la fuente de información de tus correos entrantes, los banco nunca le pedirán que le envíen las claves o datos personales por correo. Nunca responda a este tipo de preguntas y si tienes una mínima duda, llama directamente a su banco para aclararlo.
- Tener sumo cuidado con el tipo de información que comparte en redes sociales. Todo el mundo utiliza Facebook, suben fotos, se tengan conversaciones, juegue en línea y se adjunten todo tipo de aplicaciones a esta red. Al hacerlo, pone en riesgo su privacidad. Hay empresas que exploran estos sitios y obtienen datos personales. Recogen información sobre usted y su organización de los sitios de registros públicos. Por tanto, hay que tener muy claro que información se comparte y en qué lugar y con qué finalidad.
- No utilice puntos de acceso Wi-Fi públicos sin utilizar una conexión VPN. Una VPN cifrará sus comunicaciones hacia y desde internet para que cualquiera que pueda estar escuchándole a escondidas no pueda robar la información.
- Cuando se realizan descargas desde internet o de la Play Store Google, se debe verificar los permisos que le estamos otorgando a la aplicación, ya que muchas veces el robo de información viene de esos permisos que le damos a los aplicativos que instalamos. Antes de instalar una aplicación, así sea desde la Play Store Google, se debe revisar bien los permisos que se le den antes de instalarse.
- Instalar un antivirus del tipo móvil, hay muchas opciones que se encuentran disponibles, unas más ligeras y otras mucho más potentes, puede ser de pago o gratuito, todo depende de lo que se está buscando para elegir alguna de estas opciones, pero es muy importante instalar una de las opciones de antivirus para nuestro Android.
- El sentido común y las buenas prácticas de navegación en la web y al descarga archivos, es fundamental para evitar ser víctima de los ataques de ciberdelincuentes. No descargar archivos desde sitios que no se conozcan, abrir correos electrónicos de

personas desconocidas con archivos adjuntos no solicitados, entre otras acciones, ya que pueden contar con algún tipo de malware, que será dañino para los equipos.

En la sección de Resultados y Discusiones, se encuentran los ejemplos de las buenas prácticas para mitigar el riesgo de estos virus en el sistema operativo Android con la referencia a los tipos de Malwares que le pueden implementar para evitar contagios a estos dispositivos.

5. RESULTADOS Y DISCUSIÓN.

Las siguientes son algunas de las buenas prácticas que se pueden considerar a la hora de mitigar el riesgo de malware en Smarthphone con sistema operativo Android.

Teniendo en cuenta la clasificación de los Malwares que representan más riesgos para los Smartphones con sistema operativo Android, expuestos en este trabajo, se realiza una tabla en la que se exponen las buenas prácticas y para que Malware se pueden implementar, y así evitando el contagio de estos.

Tabla 7: Buenas prácticas para mitigar el riesgo de Malware.

Buenas prácticas para mitigar el riesgo de Malware	T*	S*	F*	A*
El sentido común y las buenas prácticas de navegación en la web y al descarga archivos, es fundamental para evitar ser víctima de los ataques de ciberdelincuentes. No descargar archivos desde sitios que no se conozcan, abrir correos electrónicos de personas desconocidas con archivos adjuntos no solicitados, entre otras acciones, ya que pueden contar con algún tipo de malware, que será dañino para los equipos.	●	●	●	●
No hacer clic en ventanas emergentes que le indican que su equipo está infectado con un virus. Los antivirus no funcionan de esa manera. Esas “fakeapps” instalan software malicioso en su Smartphone sin que usted se percate.			●	
Instalar un antivirus del tipo móvil, hay muchas opciones que se encuentran disponibles, unas más ligeras y otras mucho más potentes, puede ser de pago o gratuito, todo depende de lo que se está buscando para elegir alguna de estas opciones, pero es muy importante instalar una de las opciones de antivirus para nuestro Android.	●	●	●	●
Cuando se realizan descargas desde internet o de la Play Store		●	●	●

Google, se debe verificar los permisos que le estamos otorgando a la aplicación, ya que muchas veces el robo de información viene de esos permisos que le damos a los aplicativos que instalamos. Antes de instalar una aplicación, así sea desde la Play Store Google, se debe revisar bien los permisos que se le den antes de instalarse.				
Tener mucho cuidado con los archivos adjuntos del correo electrónico. No todos los archivos son dañinos, pero es conveniente proceder a eliminar el correo electrónico o identificarlo como spam si no reconoce al remitente. Nunca descargue ni abra el archivo adjunto. Y si el archivo es de un remitente conocido, no está de más examinarlo con el antivirus.		●	●	
No utilice puntos de acceso Wi-Fi públicos sin utilizar una conexión VPN. Una VPN cifrará sus comunicaciones hacia y desde internet para que cualquiera que pueda estar escuchándole a escondidas no pueda robar la información.	●	●		
Utilice contraseñas para todo y verificar que sean claves fuertes. No utilice la misma contraseña para todos los sitios ni contraseñas fáciles de adivinar. Utilice contraseñas seguras que tengan al menos ocho caracteres donde se incluya letra mayúscula, números y caracteres alternativos. Se recomienda cambiar las contraseñas con frecuencia.	●	●		
Revise sus cuentas bancarias y reportes de endeudamiento de manera periódica. Debe convertirse en un hábito obligatorio el de hacer seguimiento en busca de signos de fraude o cargos que no haya hecho en los últimos días.	●			
Tener sumo cuidado con el tipo de información que comparte en redes sociales. Todo el mundo utiliza Facebook, suben fotos, se tengan conversaciones, juegue en línea y se adjunten todo tipo de aplicaciones a esta red. Al hacerlo, pone en riesgo su privacidad. Hay empresas que exploran estos sitios y obtienen datos personales.		●		

Recogen información sobre usted y su organización de los sitios de registros públicos. Por tanto, hay que tener muy claro que información se comparte y en qué lugar y con qué finalidad.				
Verifica la fuente de información de tus correos entrantes, los banco nunca le pedirán que le envíen las claves o datos personales por correo. Nunca responda a este tipo de preguntas y si tienes una mínima duda, llama directamente a su banco para aclararlo.	●			
Refuerza la seguridad de tu ordenador, el sentido común y la prudencia es tan indispensable como mantener tu equipo protegido con un buen antivirus que bloquee este tipo de ataques. Además, siempre debes tener actualizado tu sistema operativo y navegadores web.	●			
Descargar Software de sitios confiables, cuando se necesita un programa, se suele descargarlo de Internet, pero pocas veces se repara los sitios desde donde realizamos la descarga. Lo mejor es descargar todos los programas de la página oficial de cada uno de los creadores o desde la Play Store.	●	●	●	●
Revisa periódicamente tus cuentas, nunca está de más revisar tus cuentas bancarias de forma periódica, para estar al tanto de cualquier irregularidad en tus transacciones online.		●		●

*T: Troyano *S: Spyware *F: Fakeapps *A: Adware

6. CONCLUSIONES, RECOMENDACIONES Y TRABAJO FUTURO

Conclusiones.

Se es consciente del riesgo que se corre al tener un Smartphone conectado constantemente a la web, en la que a pesar de los controles que se realizan por parte de las herramientas especializadas (Antivirus) contra la gran cantidad de Malware, es tan fácil caer en las trampas de los ciber-delincuentes con sus Ataques. El auto cuidado juega un papel tan importante a la hora de cuidar nuestra información personal y lo demás que hay allí almacenado. Por ende, es sumamente importante tener en cuenta hábitos cotidianos de las medidas de seguridad al ingresar en la web, expuestas en este trabajo, y asimismo mitigar el riesgo de ser víctimas de los Malware.

Al caracterizar el funcionamiento que tiene cada uno de los Malware que afectan los Smartphone con SO Android, se cuenta además con la posibilidad de mitigar el contagio conociendo la forma en la que estos atacan a los dispositivos móviles.

Android es el sistema operativo para móviles más utilizado en la actualidad, y como tal está en la mira de todos los ciber-ataques. A causa de esto es el masivo crecimiento de los Malware desarrollados para esta plataforma. Los atacantes se aprovechan generalmente de las fallas del sistema, y en el modelo de seguridad “orientado a permisos”, no provee una protección efectiva, por el mal manejo de los permisos que existe y la libertad que propone Google para las descargas de aplicaciones de tiendas, ya que Google no tiene control sobre los mismos y es utilizado como foco de propagación de malware.

Las empresas de seguridad están evolucionando, aunque lentamente ante esta situación, pero ya existen aplicaciones con buen desempeño frente a estos Malwares. Para poder protegerse adecuadamente de todos estos virus, lo mejor es conocer las características de

cada uno de ellos. La otra opción, naturalmente, es elegir un antivirus fuerte, capaz de defendernos de todos los posibles ataques.

Recomendaciones.

Es necesario mantenerse informado de los Malware que salen y se actualizan constantemente, y de igual manera conocer cuáles son las principal herramientas que permiten brindar una pequeña protección de este problema que a nivel mundial afecta a todos los usuarios de los Smartphones y los demás dispositivos que se conectan a la web.

Trabajos Futuros.

Una visión más amplia de todos los dispositivos que pueden ser contagiados de Malwares, con el objetivo de identificar buenas prácticas para la protección y prevención ante el contagio de todos los dispositivos.

REFERENCIAS

International Data Corporation (IDC). (2016). "Worldwide Smartphone Volumes Relatively Flat in Q2 2016 Marking the Second Straight Quarter Without Growth, According to IDC. Obtenido de: http://www.idc.com/getdoc.jsp?containerId=prUS41636516

Gartner, Inc. (2016). Gartner Says Five of Top 10 Worldwide Mobile Phone Vendors Increased Sales in Second Quarter of 2016". Obtenido de: http://www.gartner.com/newsroom/id/3415117

Cancela, L., & Ostos, S. (2012). Android. Obtenido de: https://sites.google.com/site/swcuc3m/home/android

Pardo, L. (2013). La infección de malware que costó casi tres millones de dólares. Obtenido de http://www.neoteo.com/la-infeccion-de-malware-que-costo-tres-millones

Rueda, J. S., & Rico, D. (2014). Análisis forense digital en dispositivos móviles.

Eset. (2012). Guía de seguridad para usuarios de smartphone.

Jakobsson, M., & Ramzan, Z. (2008). Crimeware. Understanding New attacks and Defenses. Boston: Pearson Education Inc.

Pastor, J. (2014). Y el primer smartphone de la historia fue. Obtenido de http://www.xatakamovil.com/movil-y-sociedad/y-el-primer-smartphone-de-la-historia-fue

Salazar, D., & Gordillo, A. (2012). Seguridad en Dispositivos Móviles. Obtenido de: http://acmor.org.mx/cuamweb/reportescongreso/2012/Fisico-mate/120.pdf

Puerto, K. (2015). ¿Quién es el líder del mercado de smartphones?. Obtenido de http://www.xataka.com/moviles/quien-es-el-lider-del-mercado-de-smartphones

ESET Latinoamérica. (2013). Malware en dispositivos móviles. Obtenido de www.eset-la.com.

Prowse, D. L. (2011). CompTIA Security+. Pearson Education, Indianapolis, IN, 2nd ededition.

OUCH!. (2014). ¿Qué es el malware?. Obtenido de http://www.securingthehuman.org.

Baquía. (2012). Malware para Android: conoce los cinco tipos más frecuentes. Obtenido de http://www.baquia.com/tecnologia-y-negocios/entry/emprendedores/2012-06-21-malware-para-android-conoce-los-cinco-tipos-mas-frecuentes

Kaspersky Labs. (2016). “Clasificación de Malwares”. Obtenido de: http://www.kaspersky.es/internet-security-center/threats/malware-classifications.

Eset. (2016). “Definición de virus, códigos maliciosos y ataques remotos”. Obtenido de: http://soporte.eset-la.com/kb186/?locale=es_ES

Rivera, R. (2014). Análisis de caraterísticas estáticas de ficheros ejecutables para clasificación de malware. Facultad de Informática, Universidad Politénica de Madrid. Madrid, España. pp. 17-19.

Fuentes, L. (2008). Malwares, una amenaza de internet. Universidad Nacional Autónoma de Mexico. España. Revista Digital Universitaria. Volumen 9. Número 4.

Brereton, P., & Kitchenham, B., & Budgen, D., & Turner, M., & Khalil, M. (2007). Lessons from applying the systematic literatura review process within the software engineering domain. Journal of Systems and Software. Vol. 80. pp. 571-583.

Kitchenham, B. (2003). Procedures for Undertaking Systematic Literature Reviews. Joint Technical Report. Computer Science Department, Keele University. Keele, UK. pp. 35-37.

Kitchenham, B., & Budgen, D., & Turner, M., & Bailey, J., & Linkman, S. (2009). Systematic literature reviews in software engineering: A systematic literatura review. Information and Software Technology. Vol. 51. pp. 7-15.

Instituto Tecnológico y de Estudios Superiores de Monterrey, Universidad Virtual. (2012). Buscar y seleccionar fuentes: los pasos de una buena revisión bibliográfica. Obtenido de http://sitios.ruv.itesm.mx/portales/crea/buscar/que/6_lospasos.htm

Zhou, Y. and Jiang, X. (2012).“Dissecting android malware: Characterization and evolution.”. Department of Computer Science Nort Carolina State University.

Kaspersky Lab Daily. (2013). Clasificacion de Malwares. Obtenido de https://blog.kaspersky.com.mx/clasificacion-de-malwares/1608.

D.Giusto. (2016). “Malware móvil en Latinoamérica: la realidad para iOS y Android”.Obtenido de: http://www.welivesecurity.com/la-es/2016/05/20/malware-movil-en-latinoamerica-ios-android/

Gostev, A. & Unuchek, R & Garnaeva, M. & Makrushin, D. &Ivanov A. (2016). “Desarrollo de las amenazas informáticas en el primer trimestrede 2016”. Obtenido de: https://securelist.lat/analysis/informes-trimestrales-sobre-malware/83079/it-threat-evolution-in-q1-2016/

Teijeira, P. (2016). “Sophos expone los cinco principales códigos maliciosos para Android”. Obtenido de: https://pabloteijeira.wordpress.com/2012/06/20/sophos-expone-los-cinco-principales-codigos-maliciosos-para-android/

Agudelo, S. (2014). “Descubre qué clase de malware puede infectar tu Android”. Obtenido de: http://rootear.com/android/tipos-aplicaciones-falsas

De los Santos, S. (2014). “El negocio de las “FakeApps” y el malware en google play (I): introducción”. Obtenido de: http://blog.elevenpaths.com/2014/02/el-negocio-de-las-fakeapps-y-el-malware.html

INFORMADOR.MX. (2014). "Antivirus falsos y publicidad engañosa, principales ataques en Android". Obtenido de: http://www.informador.com.mx/tecnologia/2014/560039/6/antivirus-falsos-y-publicidad-enganosa-principales-ataques-en-android.htm

SensorTower Inc. (2016). "Store Intelligence Q2 2016 Data Digest". Obtenido de: https://sensortower.com/blog/q2-2016-data-digest

IDG. (2012). "Opinión e Historia De la miniaturización del Motorola V50 a la maximización del HTC Sensation XL". Obtenido de: http://alexistechblog.com/2012/04/19/opinion-e-historia-de-la-miniaturizacion-del-motorola-v50-a-la-maximizacion-del-htc-sensation-xl/

Tapia, M. (2013). ESTUDIO Y DESARROLLO DE APLICACIONES PARA DISPOSITIVOS MÓVILES ANDROID. Facultad de Ingeniería en ciencias aplicadas, Universidad técnica del Norte. Ibarra, Ecuador. pp. 02-20.

Welivesecurity**.** (2014). "Infografía: 28 años de historia del malware". Obtenido de: http://www.welivesecurity.com/la-es/2014/11/04/infografia-historia-malware/

Molina, M. (2015). "Sistemas operativos móviles: ¿Cuál es el mejor?". Obtenido de: http://www.giztab.com/sistemas-operativos-moviles-cual-es-el-mejor/

Mosquea, A. and Resterpo, A (2011). Guía de referencias: los antivirus y sus tendencias futuras. Facultad de Ingeniería de sistemas y computación, Universidad tecnológica de Pereira. Pereira, Colombia. pp. 27-28.

Dominguez, A. (2015). “Seguridad y Confianza digital”. Obtenido de: http://recursos.crfptic.es:9080/jspui/bitstream/recursos/949/2/Bloque%201.%20Introducci%C3%B3n%20y%20navegaci%C3%B3n%20segura.pdf

Enciclopedia de Clasificaciones. (2016).”Tipos de antivirus de computadora.” Obtenido de:http://www.tiposde.org/informatica/626-tipos-de-antivirus-de-computadora/

Android Básico. (2016). “Antivirus para Android.” Obtenida de: http://androidbasico.com/mejores-antivirus-para-android-gratis.html

Cancela, L, and Ostos, S. (2010). Arquitectura Android. [Figura 1]. Recuperado de: https://sites.google.com/site/swcuc3m/home/android/generalidades/2-2-arquitectura-de-android

Nelson, R. (2016). Sensor Tower's Q2 2016 Data Digest: U.S. App Revenue Grows 55% Year-Over-Year. [Figura 2]. Recuperado de: https://sensortower.com/blog/q2-2016-data-digest

Giusto, D. (2016). Malware móvil en Latinoamérica: la realidad para iOS y Android. [Figura 3]. Recuperado de: http://www.welivesecurity.com/la-es/2016/05/20/malware-movil-en-latinoamerica-ios-android/

SecureList. (2016). Desarrollo de las amenazas informáticas en el primer trimestre de 2016. [Figura 4]. Recuperado de: https://securelist.lat/analysis/informes-trimestrales-sobre-malware/83079/it-threat-evolution-in-q1-2016/

SecureList. (2016). Desarrollo de las amenazas informáticas en el primer trimestre de 2016. [Figura 5]. Recuperado de: https://securelist.lat/analysis/informes-trimestrales-sobre-malware/83079/it-threat-evolution-in-q1-2016/

Teijeira, P. (2012). Sophos expone los cinco principales códigos maliciosos para Android. [Figura 6]. Recuperado de: https://pabloteijeira.wordpress.com/2012/06/20/sophos-expone-los-cinco-principales-codigos-maliciosos-para-android/

Kaspersky Labs. (2016). Árbol de clasificaciones de los Malwares [Figura 7]. Recuperado de: http://www.kaspersky.es/internet-security-center/threats/malware-classifications.

Google Play. (2013). Imagen de fakeapps. [Figura 8]. Recuperado de: https://play.google.com

Google Play. (2014). Imagen Original de la App. [Figura 9]. Recuperado de: https://play.google.com

IDC. (2016). Worldwide Smartphone Volumes Relatively Flat in Q2 2016 Marking the Second Straight Quarter without Growth, According to IDC. [Tabla 1]. Recuperado de: http://www.idc.com/getdoc.jsp?containerId=prUS41636516

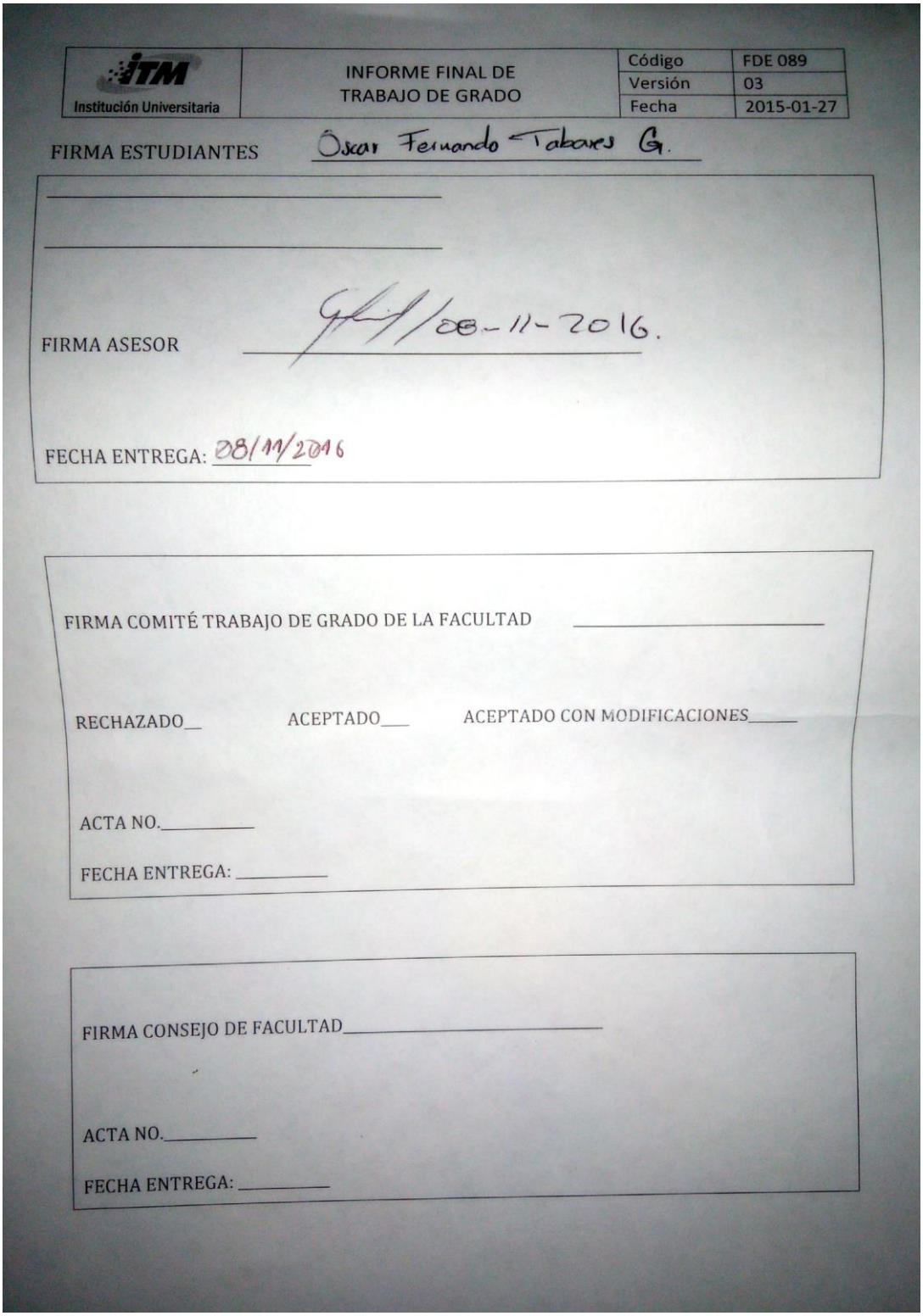
Gartner. (2016). Gartner Says Five of Top 10 Worldwide Mobile Phone Vendors Increased Sales in Second Quarter of 2016. [Tabla 2]. Recuperado de: http://www.gartner.com/newsroom/id/3415117

Android (2016). Versiones del SO Android [Tabla 3]. Recuperado de: https://www.android.com/intl/es_es/history

SecureList. (2016). Desarrollo de las amenazas informáticas en el primer trimestre de 2016. [Tabla 4]. Recuperado de: https://securelist.lat/analysis/informes-trimestrales-sobre-malware/83079/it-threat-evolution-in-q1-2016/

Av-Test. (2016). El mejor software antivirus para Android. [Tabla 5]. Recuperado de: https://www.av-test.org/es/antivirus/moviles/.

Android Básico. (2016). Antivirus para Android. [Tabla 6]. Recuperado de: http://androidbasico.com/mejores-antivirus-para-android-gratis.html



Institución Universitaria | INFORME FINAL DE TRABAJO DE GRADO | Código: FDE 089 | Versión: 03 | Fecha: 2015-01-27

FIRMA ESTUDIANTES Oscar Fernando Tabares G.

FIRMA ASESOR 08-11-2016.

FECHA ENTREGA: 08/11/2016

FIRMA COMITÉ TRABAJO DE GRADO DE LA FACULTAD _____

RECHAZADO__ ACEPTADO___ ACEPTADO CON MODIFICACIONES_____

ACTA NO._____

FECHA ENTREGA: _____

FIRMA CONSEJO DE FACULTAD_____

ACTA NO._____

FECHA ENTREGA: _____