UNIVERSIDAD AUTÓNOMA DEL ESTADO DE MÉXICO

CENTRO UNIVERSITARIO UAEM TEXCOCO

"ANÁLISIS DE LA VULNERABILIDAD EN LAS APLICACIONES *ANDROID* DE LOS DISPOSITIVOS MÓVILES"

T E S I S

QUE PARA OBTENER EL TÍTULO DE LICENCIADO
EN INFORMÁTICA ADMINISTRATIVA

PRESENTAN

JOVITA JANET TAPIA RUÍZ

MICHAEL GARCÍA FLORES

DIRECTOR

M en C. JUAN MANUEL MUÑOZ ARAUJO

REVISORES

M. en. C. YEDID ERANDINI NIÑO MEMBRILLO

I. en C. E. FERNANDO ROBLES GIL

TEXCOCO, ESTADO DE MÉXICO MARZO 2016

Texcoco, México; a 15 de Febrero de 2016

M. en. C.E. VIRIDIANA BANDA ARZATE
SUBDIRECTORA ACADÉMICA DEL
CENTRO UNIVERSITARIO UAEM TEXCOCO
PRESENTE.

AT´N. L. en D. MARCO RODRIGO LÓPEZ GONZÁLEZ
RESPONSABLE DEL DEPARTAMENTO DE TITULACIÓN

Con base en las revisiones efectuadas al trabajo escrito titulado "**ANÁLISIS DE LA VULNERABILIDAD EN LAS APLICACIONES ANDROID DE LOS DISPOSITIVOS MÓVILES**" que para obtener el título de Licenciado en **Informática Administrativa**, presentan los sustentantes **Jovita Janet Tapia Ruíz** y **Michael García Flores**, con número de cuenta **0623331** y **0621382** respectivamente, se concluye que cumplen con los requisitos teórico – metodológicos necesarios para su aprobación, pudiendo continuar con la etapa de digitalización del trabajo escrito.

ATENTAMENTE

Revisor. M. en. C. YEDID ERANDINI NIÑO MEMBRILLO

Revisor. I. en C. E. FERNANDO ROBLES GIL

Director. M. en C. JUAN MANUEL MUÑOZ ARAUJO

TITULACION
RECIBIDO
Por
Texcoco, Méx., a 15 de 2 del 16

c.c.p. Jovita Janet Tapia Ruíz y Michael García Flores
c.c.p. M. en C. Juan Manuel Muñoz Araujo. Director de Tesis
c.c.p. L. en D. Marco Rodrigo López González. Responsable del Departamento de Titulación

Agradecimientos

A Dios, creador y dador de vida, por protegerme durante todo mi camino y darme fuerzas para superar obstáculos y dificultades a lo largo de toda mi vida.

A mi Padre Germán, que en paz descansas, por ser mi fuente de inspiración para salir adelante, por tus sabios consejos y por todo ese amor que siempre me has tenido.

A Mary, mi Amor incondicional, por tu entrega y por la paciencia que me has tenido durante estos años, por insistirme siempre para la realización de este proyecto.

A mi asesor de Tesis, M. Juan Manuel, por el tiempo dedicado en la elaboración de este proyecto de Tesis

A la Universidad Autónoma del Estado de México, en especial al Centro Universitario UAEM Texcoco, por haberme dado la oportunidad de formar parte de esta gran familia universitaria.

A mi amiga y compañera de Tesis, Janet, por tu paciencia y entrega, que por coincidencias del destino hizo posible que juntos culmináramos con este proyecto.

A Mi madre querida, Hortencia, por tu confianza y apoyo que sin duda alguna me has brindado, por tu el amor y cariño que me tienes, y por creer en mí.

A mis hermanos César, Alba, Germaín, Magda, Marco y Adriana, por confiar en mí y porque siempre están conmigo cuando más los necesito.

A Mi tío Ing. Mardonio, por el apoyo incondicional que me has brindado, por ser un padre para mí y por todos tus sabios consejos.

A mis revisores de Tesis M. Yedid Erandini e Ing. Fernando, por su empeño y colaboración en la revisión de este proyecto de Tesis.

A mis estimados amigos de la Universidad, en especial a Adrían por ser un gran amigo y por creer siempre en mí, un agradecimiento sincero también a tus padres.

A todas aquellas personas que colaboraron conmigo en la realización y culminación de este proyecto de Tesis.

"Todo logro empieza con la decisión de intentarlo"

Dedicatorias

Quiero dedicar esta Tesis a mis Padres queridos, Germán y Hortencia, que gracias a ustedes soy una persona íntegra, que con sus esfuerzos hicieron posible que yo culminara una carrera universitaria y que ahora gracias a sus sacrificios por fin le doy fin a este paso de mi vida profesional sellándola con la titulación.

Así mismo dedico esta Tesis a mi compañera de vida, María de Jesús, porque siempre has sido fundamental en mi vida profesional y amorosa, gracias a ti he logrado un paso más.

También dedico esta Tesis a mi tío Mardonio, por ese gran interés y esa insistencia para que yo lograra este objetivo, de culminar de esta forma mi carrera profesional.

Una dedicatoria especial a mis hermanos César, Alba, Germain, Magda, Marco y Adriana, por creer siempre en mí y por los ánimos que siempre me han demostrado.

Dedico esta tesis a mis sobrinos Vanesa, Julio, Adael, Anahí, Julián y Christofer, por ser parte de mi familia y espero les sirva este esfuerzo como ejemplo e inspiración para que ustedes inicien una carrera profesional en un futuro.

Con cariño Michael.

Agradecimientos

A mis padres, por el esfuerzo y apoyo que me han brindado durante toda mi vida y por darme esta gran herencia que es concluir una licenciatura; simplemente gracias por todo, los Amo

A mi hermano, por ser mi gran ejemplo a seguir, por tu apoyo y consejos que siempre me brindas en todas mis decisiones, Gracias por estar siempre conmigo.

A mi gran amor HCSY, por estar conmigo en todo momento y por el apoyo que me has brindado durante esta etapa de titulación, Gracias por formar parte de mi vida

A mi director y revisores de tesis, por el tiempo y apoyo en la revisión de este proyecto de titulación, Gracias

Dedicatorias

Dedico esta tesis a mis padres,

Porque me impulsaron para estudiar una licenciatura, porque creyeron en mí, por el gran esfuerzo económico que hicieron para sacarme adelante, por apoyarme en todo momento, por darme ejemplos de superación y entrega, porque en gran parte gracias a ustedes, hoy puedo ver alcanzada mi meta. Va por ustedes, por lo que valen, porque admiro su fortaleza y por lo que han hecho de mí.

Gracias mamá.

Gracias papá.

Con cariño Janet.

ÍNDICE

ÍNDICE DE ILUSTRACIONES

ÍNDICE DE TABLAS

INTRODUCCIÓN

Los dispositivos móviles constituyen el principal medio de comunicación que hoy en día utilizamos, cada vez se emplean en un mayor número de entornos diferentes, desde el acceso a datos corporativos con un alto grado de confidencialidad hasta el ocio personal, pasando por multitud de aplicaciones de uso habitual, como el acceso a las redes sociales y a la navegación por Internet que mejoran la experiencia del usuario.

Es tal la importancia que han adquirido los Dispositivos Móviles que parece que fuera imposible el desarrollo de cualquier actividad sin la utilización de los mismos. Se han hecho imprescindibles tanto en el ámbito de las comunicaciones personales como en el entorno empresarial; así lo demuestra el dato, bastante significativo, que en el primer semestre de 2015, existen en el mundo más de 7300 millones de líneas móviles activas (Rivero, 2015), superando considerablemente a la población (la población mundial es de 7250 millones de personas).

En el marco tecnológico Actualmente existen varios sistemas operativos que dan soporte a los múltiples dispositivos móviles o también llamados *Smartphone*, como lo son iOS, Windows Phone y *Android*, esta última es considerada en el mundo de la tecnología como uno de los sistemas operativos más utilizados.

Textualmente, "*Android* es un sistema operativo, inicialmente diseñado para teléfonos móviles. En la actualidad este sistema operativo no sólo se instala en móviles, sino también en múltiples dispositivos, como *Tablet*as, GPS, televisores, discos duros multimedia, mini ordenadores entre otros, incluso se ha instalado en microondas y lavadoras.

Este sistema está basado en Linux, que es un núcleo de sistema operativo libre, gratuito y multiplataforma, permite programar aplicaciones empleando una variación de Java llamada *Dalvik*, y proporciona todas las interfaces necesarias para desarrollar fácilmente aplicaciones que acceden a las funciones del teléfono (como el GPS, llamadas, agenda etcétera) utilizando el lenguaje de programación Java" (Clodo Aldo Robledo Sacristán, 2012)

Los dispositivos móviles tienen características únicas que les permiten entrar en una clasificación de gamas, como los son alta, media y baja respectivamente, estas características son definidas por los fabricantes, que a su vez desarrollan nuevas tecnologías que implementan en los diferentes modelos que producen.

Los equipos móviles están expuestos a ser blanco fácil para los creadores de programas maliciosos, una tendencia que se ve reflejada cotidianamente. Desafortunadamente estos sistemas son vulnerables a riesgos derivados por fallas en la seguridad, ataques de *malware* o por virus los cuales son adquiridos a través de diferentes medios como las comunicaciones inalámbricas, estas constituyen la base de la conexión de los dispositivos móviles que son soportadas por distintas tecnologías de comunicación como Wi-Fi (Wireless Fidelity) que permite el acceso a Internet sin consumir ancho de banda; GSM (Global System for Mobile communications) que es un sistema estándar libre de regalías, el cual ha tenido diferentes evoluciones en sus generaciones como lo son 2G, 3G y 4G para el acceso a Internet, llamadas telefónicas, tráfico de mensajes SMS y videollamadas; *Bluetooth* para conexiones entre dispositivos móviles o con otros dispositivos fijos y NFC (Near Field Comunication), utilizada para comunicaciones de corta distancia y con aplicaciones para pagos a través del móvil.

Lamentablemente, todas estas tecnologías presentan pautas de vulnerabilidades y riesgos de seguridad. Por ello, este proyecto de investigación tiene el mayor interés de proporcionar al usuario las medidas necesarias de protección adecuadas para eliminar, o al menos reducir, el nivel de riesgo de encontrar algún tipo de amenaza por ello se realizó un análisis detallado de las principales vulnerabilidades a los que los usuarios están expuestos, mediante la aplicación de una encuesta basada principalmente en los errores más comunes que se tienen al hacer uso de algún medio de comunicación inalámbrica.

PLANTEAMIENTO DEL PROBLEMA

La problemática radica en que los usuarios de los dispositivos móviles del sistema operativo *Android*, son altamente susceptibles a la introducción de aplicaciones móviles dañinas y al robo de su información personal, esto representado por medio de algún tipo de virus, vulnerabilidad del sistema o ataques cibernéticos, ya que en este medio tecnológico es muy usual enviar y recibir información de manera instantánea por medio de algún medio de comunicación, cómo lo es el acceso a internet, este inconveniente es a causa de la falta de conocimiento o por el simple hecho del nulo interés por parte del usuario

JUSTIFICACIÓN

Los dispositivos móviles disponen de crecientes alicientes para ser atacados por los cibercriminales. Su uso está generalizado y en continua expansión, contienen una gran cantidad de información personal y confidencial, y tienen la capacidad para realizar prácticamente todo tipo de transacciones.

El tema de investigación que se presenta surge de la necesidad por orientar y recomendar a los usuarios, de las distintas formas de inseguridad o vulnerabilidad en las que pueden estar expuestos sus dispositivos móviles al hacer uso de la tecnología móvil. Ya que por conocimiento propio los usuarios generalmente desconocen el problema de seguridad de sus equipos móviles.

Un aspecto interesante en lo referente a la seguridad en estos dispositivos móviles son los canales de comunicación, pues las amenazas suelen provenir de algún medio como: SMS, *Bluetooth*, WiFi, navegadores Web, aplicaciones, correos electrónicos o desde algún medio de almacenamiento, hecho lamentable que pudiera propiciar la difusión de un código malicioso orientado a la plataforma móvil. Esta amenaza podría permitir a los hackers borrar dispositivos, instalar programas maliciosos, acceder a datos y hasta controlar aplicaciones de los dispositivos móviles.

OBJETIVOS

OBJETIVO GENERAL

Analizar medidas de seguridad para la prevención y reducción de la vulnerabilidad en los dispositivos móviles del sistema operativo *Android*.

OBJETIVOS PARTICULARES

- Analizar las amenazas más comunes que afectan al sistema operativo *Android*
- Identificar los errores más comunes que cometen los usuarios al descargar e instalar aplicaciones móviles.
- Identificar las aplicaciones que actualmente brindan más seguridad para los dispositivos móviles.
- Brindar recomendaciones de seguridad para el uso del Sistema Operativo *Android* y sus aplicaciones.

HIPÓTESIS

Si los usuarios del sistema operativo *Android* proporcionan total seguridad a los dispositivos móviles, entonces no existirá robo de información ni infección por *malware*.

MARCO TEÓRICO

1. CAPÍTULO I. DISPOSITIVOS MÓVILES Y SISTEMAS OPERATIVOS

1.1. INTRODUCCIÓN A LOS DISPOSITIVOS MÓVILES

Si pensamos en dispositivos móviles, lo primero que nos viene a la cabeza es un teléfono móvil. Pero en la actualidad son varios los dispositivos móviles disponibles en el mercado como las PC portátiles, los *Smartphone*, las *Tablets*, entre muchos más que podríamos encontrar en el mercado tecnológico.

Los dispositivos móviles tienen características únicas que les permiten entrar en una clasificación de gamas, como los son alta, media y baja respectivamente, estas características son definidas por los fabricantes, que a su vez desarrollan nuevas tecnologías que implementan en los diferentes modelos que producen.

Procesar la información, es la función de un dispositivo móvil teniendo como característica principal la movilidad del usuario, además puede ayudar a realizar llamadas telefónicas, servir de asistente personal, funcionar como *Tablet*a, reloj, televisor por mencionar algunas.

1.2. CONCEPTO DE DISPOSITIVO MÓVIL

Un dispositivo móvil (DM) se puede definir como aquel que disfruta de autonomía de movimiento y está libre de cableado.

La principal cualidad de un dispositivo móvil es su gran capacidad de comunicación, la cual permite tener acceso a información y servicios independientemente del lugar y el momento en el que se encuentre. Es decir, es una fuente de información fácil de transportar.

La movilidad de un DM está condicionada por la necesidad de utilizar una batería. Esto representa un inconveniente debido a que la batería necesita recargas periódicas, lo que dificulta en muchos casos la portabilidad del DM.

Un dispositivo móvil se caracteriza, en general, por su reducido tamaño, el cual aporta una ventaja notable: favorece la movilidad de los DM. A su vez, comporte una serie de inconvenientes, como son; que han de utilizar un procesador más simple y una memoria pequeña. Además, las interfaces con el usuario también son reducidas, ya que la mayor parte de los DM tienen una pantalla reducida, un teclado muy pequeño, o carecen de ello, reconocimiento de voz limitado, entre otros.

Un DM ofrece recursos tanto a nivel personal como a nivel empresarial. Es en este último caso en el que los DM no disponen de la capacidad requerida para sus necesidades (poco espacio de almacenamiento de datos, introducción de datos poco eficaz, visualización limitada, por mencionar algunos.).

Con todo esto, tenemos que las aplicaciones de un DM, a primera vista, son más reducidas y menos potentes que las que podamos desarrollar sobre un PC.

1.3. CARACTERÍSTICAS GENERALES DE LOS DISPOSITIVOS MÓVILES

Una gran cantidad de dispositivos electrónicos se clasifican actualmente como dispositivos móviles, desde teléfonos hasta las famosas *Tablet*as. Con tanta tecnología clasificada como móvil, puede resultar complicado determinar cuáles son las características de los dispositivos móviles.

Características de los Dispositivos Móviles[1]:

- Son dispositivos pequeños.
- La mayoría de estos aparatos se pueden transportar en el bolsillo del propietario o en un pequeño bolso.
- Tienen capacidad de procesamiento.
- Tienen conexión permanente o intermitente a una red.
- Tienen memoria (RAM, tarjetas Micro SD, flash, por mencionar algunos.)
- Normalmente se asocian al uso individual de una persona, tanto en posesión como en operación, la cual puede adaptarlos a su gusto.
- Tienen una alta capacidad de interacción mediante la pantalla o el teclado

1.4. TIPOS DE DISPOSITIVOS MÓVILES

A continuación se presentan algunos tipos de Dispositivos Móviles más utilizados en la actualidad:

1.4.1. TELÉFONO MÓVIL

El teléfono móvil es un dispositivo inalámbrico electrónico que tiene acceso a la red de telefonía celular o móvil. Su nombre se define por el uso de la red de estaciones base o antenas repetidoras, en la cual cada estación base está

[1] María Soledad Ramírez Montoya, José Vladimir Burgos Aguilar (2012). Recursos educativos abiertos y móviles para la formación de investigadores, México, Crow Quarto

compuesta por celdas o células que proveen cobertura en un ángulo y rango determinado.

La principal característica de los celulares es la portabilidad y la facilidad de realizar una comunicación desde cualquier lugar en donde se tenga cobertura de la red celular, la comunicación entre los celulares y las redes celulares se realiza a través del espectro electromagnético utilizando las frecuencias o bandas del mismo.

Cuando se realiza una llamada desde un celular, este se comunica con la celda de la estación base que le está dando cobertura al celular en ese momento, la celda se comunica con otras celdas y estaciones repetidoras hasta llegar a la celda que está dando cobertura al otro celular y está a su vez envía la comunicación al celular de destino y se realiza la comunicación.

La función de los celulares es la comunicación de voz, pero los avances tecnológicos en las diferentes áreas de las comunicaciones para la transmisión de datos, las conexiones a internet y la evolución de los equipos móviles, han generado nuevas características y servicios para los usuarios.

1.4.2. *SMARTPHONE* O TELÉFONO INTELIGENTE

Un *Smartphone* o teléfono inteligente es un dispositivo electrónico que tiene el funcionamiento de un celular o teléfono móvil pero con características de un computador personal.

Los teléfonos inteligentes tienen diferentes características especiales en tanto al *Hardware* y al S*oftware*, debido a que sus componentes son desarrollados para realizar tareas que exigen mayor capacidad de procesamiento y memoria.

Las características de *Hardware* y *Software* de los teléfonos inteligentes se encuentran definidas en el uso de un sistema operativo que administra los recursos del equipo, provee seguridad y optimiza las funcionalidades, la conectividad de los equipos a Internet y a diferentes redes utilizando las diferentes

tecnologías y estándares de comunicación inalámbricas como Infrarrojo, *Bluetooth*, WAP, GPRS, Wi-Fi, posicionamiento global GPS, entre otros, utilizan pantallas táctiles, o teclados QWRTY, en general son herramientas con bastante poder computacional e informático.

1.4.2.1. *SMARTPHONE* DE GAMA ALTA

En este nivel se agrupan los *Smartphone* que reúnen los mejores elementos y características más avanzadas en la actualidad, tienen particularidades más notables como: componentes físicos, innovaciones que proporciona la tecnología móvil para el momento de su lanzamiento, cabe mencionar que los parámetros para cada gama fluctúan cada trimestre.[2]

Ilustración 1 Smartphone de Gama Alta

[2] Servicios Track Cero, S.C., Adrián Ling, ¿Qué hace a un Smartphone de gama alta o gama baja?, Android [en línea]. 01 de septiembre de 2015, [fecha de consulta: 22 octubre 2015]. Disponible en: < https://www.unocero.com/2015/09/01/que-hace-a-un-smartphone-ser-de-gama-alta-o-gama-baja/>

1.4.2.2. *SMARTPHONE* DE GAMA MEDIA

Se caracterizan por tener pantallas de calidad, pero de menor tamaño, resolución y profundidad de pixeles; en la mayoría de los casos funcionan con una versión anterior a la más actual de su sistema operativo; los procesadores no tienen la potencia de los que encontramos en gamas superiores. En esta categoría también se sitúan cierto número de celulares que en su momento fueron considerados de alta gama, pero que se han quedado rezagados por los adelantos que se producen en la telefonía celular.[3]

Ilustración 2 Smartphone de Gama Media

1.4.2.3. *SMARTPHONE* DE GAMA BAJA

En esta categoría entran desde marcas chinas, imitaciones de gama media o alta hasta dispositivos obsoletos con funciones básicas como cámara de baja

[3] Servicios Track Cero, S.C., Adrián Ling, ¿Qué hace a un Smartphone de gama alta o gama baja?, Android [en línea]. 01 de septiembre de 2015, [fecha de consulta: 22 octubre 2015]. Disponible en: < https://www.unocero.com/2015/09/01/que-hace-a-un-smartphone-ser-de-gama-alta-o-gama-baja/>

resolución, memoria interna limitada por lo cual no es posible instalar muchas aplicaciones y no reciben actualizaciones de software los precios son económicos[4]

Ilustración 3 Smartphone de Gama Baja

1.4.3. PDA (PERSONAL DIGITAL ASSISTANT)

El PDA Asistente Personal Digital es un computador de mano, inicialmente fue diseñado como una agenda electrónica que tenía las funcionalidades de agenda, lista de contactos, bloc de notas, recordatorios, calculadora, entre otros, estas funcionalidades le permitían a los usuarios digitalizar la información personal y mantenerla de una forma organizada, otra característica importante de estos dispositivos es el sistema de reconocimiento de escritura que tenían en sus pantallas.

Un PDA Asistente Personal Digital es un dispositivo que combina el tamaño, las funcionalidades de un computador, el teléfono, las conexiones de red, el servicio de posicionamiento GPS y la conexión a internet.

[4] Servicios Track Cero, S.C., Adrián Ling, ¿Qué hace a un Smartphone de gama alta o gama baja?, Android [en línea]. 01 de septiembre de 2015, [fecha de consulta: 22 octubre 2015]. Disponible en: < https://www.unocero.com/2015/09/01/que-hace-a-un-smartphone-ser-de-gama-alta-o-gama-baja/>

1.4.4. *TABLET*

Es un equipo de computación que se encuentra ubicado en el medio de un computador portátil y *Smartphone*, también se les conoce como *Tablet*as. Entre sus características resaltan; la pantalla táctil la cual es utilizada como una interfaz de ingreso de información, en la cual se puede escribir texto e ingresarlo en el equipo y el usuario puede trabajar con el equipo sin necesidad de utilizar un teclado y un mouse, también existen *Tablet* PC que se pueden convertir y utilizar con un teclado y mouse.

Este dispositivo móvil, utiliza *Hardware* que consume pocos recursos de energía, los procesadores, las memorias, los discos duros, las pantallas entre otros, tienen la característica especial de diseño para la movilidad y para economizar recursos de energía en el funcionamiento normal del dispositivo, es decir estos dispositivos no están diseñados para el alto rendimiento o para un alto nivel de procesamiento.

El *Software* de estos dispositivos están básicamente ligado al sistema operativo del fabricante del dispositivo, debido a esto las características especiales de estos dispositivos como la escritura en las pantallas, el dibujo, la conexión a internet y otros tipos de redes se encuentran limitadas por las características y permisos que puede proveer el fabricante.

1.5. SISTEMAS OPERATIVOS MÓVILES

Los Sistemas Operativos usados para los dispositivos móviles, llámese teléfonos celulares, *Tablet*as o *Smartphone* son diversos, pero existen tres que son los principales y que ocupan casi todo el mercado de la telefonía móvil son:

1. *Android*
2. iOS
3. Windows Phone

Antes de explicar cada uno de ellos, sus características, ventajas y desventajas, expliquemos que es un Sistema Operativo Móvil.

1.5.1. CONCEPTO DE SISTEMA OPERATIVO MÓVIL

Un sistema operativo móvil o SO móvil es un sistema operativo que controla un dispositivo móvil al igual que las computadoras utilizan Windows, Linux o Mac OS, los sistemas operativos móviles son bastantes más simples que los de la PC y están orientados más a la conectividad inalámbrica, los formatos multimedia y las diferentes maneras de introducir información en ellos.

1.5.2. COMPONENTES DE LOS SISTEMAS OPERATIVOS MÓVILES

Un sistema operativo móvil también se encuentra compuesto por varias capas.

- Kernel
- Librerías o *Middle*ware
- Entorno de ejecución de aplicaciones
- Interfaz de usuario

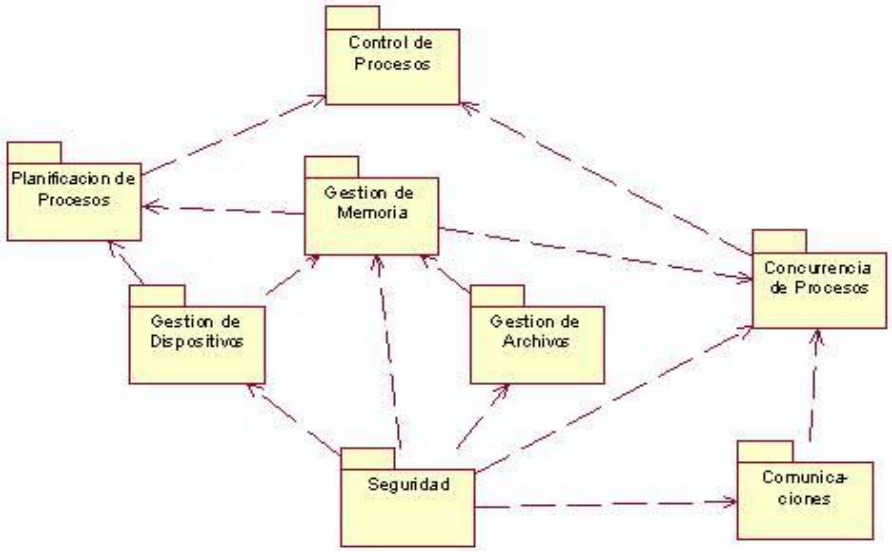


Ilustración 4. Componentes de los Dispositivos Móviles

Kernel: proporciona el acceso a los distintos elementos del *Hardware* del dispositivo. Ofrece distintos servicios a las superiores como son:

- Drivers para el *Hardware*
- Acceso y gestión de memoria
- Sistema de archivos
- Gestión de procesos

Librerías o *Middle*ware: Es el conjunto de módulos software que hacen posible la existencia de las propias aplicaciones para móviles, ofrece un conjunto de servicios que hacen posible el funcionamiento de aplicaciones distribuidas sobre plataformas heterogéneas. Está oculta ante el usuario y sirve para ejecutar las aplicaciones como:

- Motor de mensajería
- Intérpretes de páginas Web/WAP
- Motor de comunicaciones
- Códec multimedia
- Gestión del dispositivo
- Seguridad

Entorno de ejecución de Aplicaciones: Esta capa consiste de un gestor de aplicaciones y un conjunto de interfaces programables (API) abiertas y accesibles por los programadores para facilitar la creación de aplicaciones.

Una API (del inglés Application Programming Interface - Interfaz de Programación de Aplicaciones) es el conjunto de funciones y procedimientos (o métodos si se refiere a Programación Orientada a Objetos) que ofrece cierta biblioteca para ser utilizado por otro *Software* como una capa de abstracción.

La interfaz de Usuario: Esta capa es la que facilita la creación de las interfaces de usuario de las aplicaciones que facilitarán la gestión de la interacción con el usuario final y el diseño de la presentación virtual de la aplicación (*look and feel*). Los principales servicios que esta capa ofrece a las aplicaciones son: componentes gráficos: por ejemplo, pantallas, botones, listas, etc., y marco de interacción.[5]

1.6. *ANDROID*

Ilustración 5. Android

1.6.1. HISTORIA *ANDROID*

Inicialmente *Android* fue creado por *Android* Inc., una empresa de origen Californiano, implantado por sus desarrolladores Andy Rubin, Rich Miner, Nick Sears y Chris White. De hacer un Sistema Operativo para dispositivos móviles, *Android* Inc. fue el encargado del desarrollo del sistema operativo hasta que la compañía fue adquirida por Google en el 2005.

Actualmente es desarrollado por la Open Handset Alliance (una alianza comercial que cuenta con 84 compañías que se dedican a desarrollar estándares

[5] Sofía Huelches García, Dispositivos móviles y sus sistemas operativos, [en línea]. Agosto de 2014, [fecha de consulta: 31 agosto 2015]. Disponible en: < https://espaciopedagogicovirtual.wordpress.com/dispositivos-moviles-y-sus-sistemas-operativos/#_Toc395951948>

abiertos para dispositivos móviles), para la Open Handset Allience *Android* es la joya de su corona, ya que es su principal producto. El 5 de noviembre de 2007 se anunció el SO *Android*, Google liberó la mayoría del código *Android* bajo la licencia Apache (licencia de software libre). Los programas están desarrollados con lenguaje Java[6].

1.6.2. DEFINICIÓN DE *ANDROID*

"*Android* es un sistema operativo, inicialmente diseñado para teléfonos móviles. En la actualidad este sistema operativo no sólo se instala en móviles, sino también en múltiples dispositivos, como *Tablet*as, GPS, televisores, discos duros multimedia, mini ordenadores entre otros, este sistema está basado en Linux, que es un núcleo de sistema operativo libre, gratuito y multiplataforma, permite programar aplicaciones empleando una variación de Java llamada *Dalvik*, y proporciona todas las interfaces necesarias para desarrollar fácilmente aplicaciones que acceden a las funciones del teléfono (como el GPS, llamadas, agenda, etcétera) utilizando el lenguaje de programación Java" (Clodo Aldo Robledo Sacristán, 2012)

1.6.3. VERSIONES DE *ANDROID*

Cada actualización del sistema operativo *Android* es desarrollada bajo un nombre en código de un elemento relacionado con postres, los nombres en código están en orden alfabético:

[6] Danny Salas, El Android libre, La historia y los comienzos de Android, el sistema operativo de Google, [en línea]. 18 de Agosto de 2011, [fecha de consulta: 31 agosto 2015]. Disponible en: < http://www.elandroidelibre.com/2011/08/la-historia-y-los-comienzos-de-android-el-sistema-operativo-de-google.html>

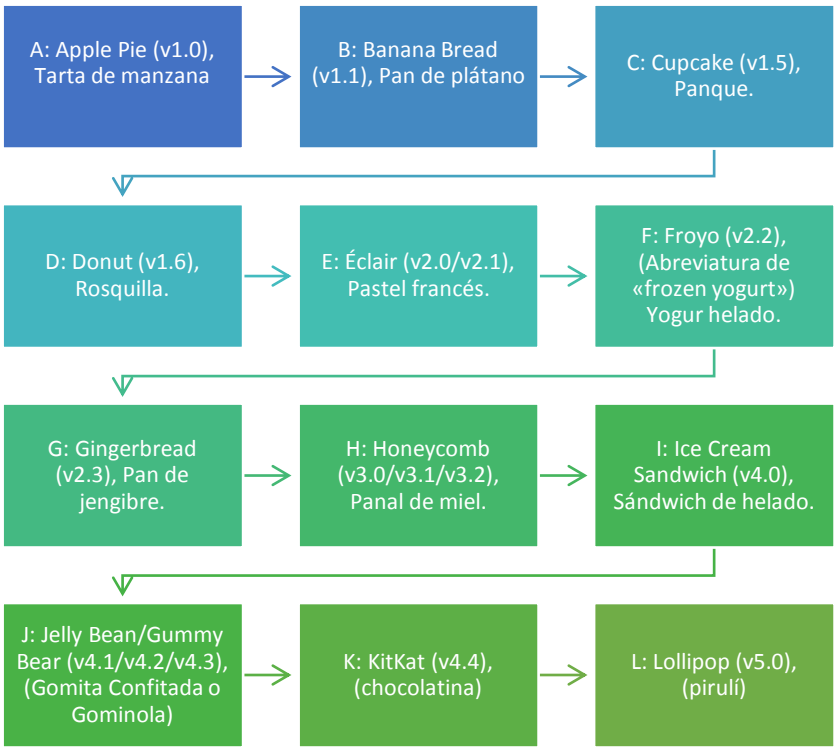
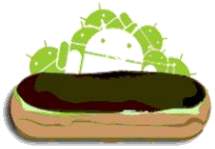


Ilustración 6. Versiones Android

Tabla 1. Características de las Versiones Android

Versión	Lanzamiento	Características
Android 1.0 APPLE PIE	23 de septiembre de 2008 	• *Android* Market • Navegador Web • Soporte Cámara • Carpo de iconos de aplicaciones • Acceso a servidores de correo electrónico por web soporte POP3, IMAP4 y SMTP • Sincronización de Gmail con la aplicación de Gmail. • Sincronización de Google Contacts y Calendar • Google Maps con Latitude y Street usando GPS. • Mensajería instantánea Google Talk, mensajes de texto y MMS. • Reproductor de medios • Notificaciones por timbre, LED o vibración. • Marcación por voz

Versión	Lanzamiento	Características
		• Fondo de escritorio • Reproductor de vídeo YouTube • Otras aplicaciones incluyen: alarma, Calculadora, marcación (teléfono), pantalla de inicio (launcher), Imágenes (Galería) y ajustes. • Soporte para Wi-Fi y *Bluetooth*.
Android 1.1 BANANA BREAD	9 de febrero de 2009 	• Detalles y reseñas disponibles cuando un usuario busca negocios en los mapas. • 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.
Android 1.5 Cupcake	30 de abril de 2009 	• Soporte para teclados virtuales de terceros • Soporte para *Widgets* • Grabación y reproducción en formatosMPEG-4y3GP. • Auto-sincronización y soporte para *Bluetooth* • Características de Copiar y pegar • Fotos de los usuarios son mostradas para favoritos en los contactos. • Marcas de fecha/hora mostradas para eventos • Pantallas de transiciones animadas. • Agregada la animación de inicio por defecto actual. • Habilidad de subir vídeos a YouTube.
Android 1.6 DONUT	5 de septiembre de 	• Mejora en la búsqueda por entrada de texto y voz. • Habilidad de los desarrolladores de incluir su contenido en los resultados de búsqueda. • Google Play. • Galería, cámara y videocámara con mejor integración. • La galería ahora permite a los usuarios

Versión	Lanzamiento	Características
	2009	seleccionar varias fotos para eliminarlas. • Actualización soporte a tecnología • Soporte para resoluciones de pantalla VGA. • Mejoras de velocidad en búsqueda y aplicaciones de cámara.
Android 2.0/2.1 ECLAIR	26 de octubre de 2009 	• Soporte intercambio de correo, con bandeja combinada • Soporte *Bluetooth* 2.1. • Habilidad para tocar una foto de un contacto y seleccionar llamar, enviar SMS o correo a la persona. • Habilidad para concentrar todos los mensajes SMS y MMS guardados, • Nuevas características para la cámara, incluyendo soporte de flash, zoom digital, modo escena, balance de blancos, efecto de colores y enfoque macro. • Renovada la interfaz de usuario. • Vista agenda del calendario mejorada. • Soporte para más tamaños de pantalla y resoluciones, con mejor contraste. • Mejorado Google Maps 3.1.2. • Adición de fondos de pantalla animados.
Android 2.2.x FROYO	20 de mayo de 2010	• Optimizaciones en velocidad, memoria y rendimiento. • Mejoras adicionales de rendimiento Just-in-time (JIT). • Integración del motor de JavaScript V8 de Chrome • Soporte para el servicio *Android* Cloud • Accesos directos de las aplicaciones teléfono y navegador web • 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. • Cambio rápido entre múltiples lenguajes de teclado. • Discado por voz e intercambio de contactos

Versión	Lanzamiento	Características
		• Soporte para docks *Bluetooth*-habilitado • Soporte para contraseñas numéricas y alfanuméricas. • Soporte para subida de archivos en la aplicación del navegador. • Soporte para instalación de aplicaciones en la memoria expandible. • Soporte para Adobe Flash. • Galería permite ver pilas de imágenes.
Android 2.3.x GINGERBREAD	6 de diciembre de 2010 	• Actualizado el diseño de la interfaz de usuario • Soporte para tamaños y resoluciones de pantalla. • Soporte nativo para SIP y telefonía por internet VoIP. • Entrada de texto del teclado virtual. • Mejoras en la funcionalidad de copiar/pegar • Soporte para Near Field Communication (NFC). • Nuevos efectos de audio. • Nuevo gestor de descargas. • Soporte para múltiples cámaras. • Mejoras en la administración de la energía. • Mejorado soporte para el desarrollo de código nativo. • Mejoras en audio, gráficos y entrada para desarrolladores de juegos. • Recolector basura concurrente. • Soporte nativo para más sensores.
Android 3.0 HONEYCOMB	22 de febrero de 2011	• Soporte optimizado para *Tablets*. • Agregada barra de sistema y barra de acción. • Multitarea simplificada. • Teclado rediseñado. • Interfaz simplificada y más intuitiva para copiar/pegar. • Las pestañas múltiples reemplazan las ventanas. • Acceso rápido a las características de la cámara. • Habilidad para ver álbumes y otras colecciones.

Versión	Lanzamiento	Características
		• Nueva interfaz de contactos y correo de dos paneles. • Soporte para video chat usando Google Talk. • Aceleración de *Hardware*. • Soporte para microprocesadores multi-núcleo. • Habilidad para encriptar todos los datos del usuario.
Android 4.0 ICE CREAM SANDWICH	19 de octubre de 2011 	• Separación de *Widgets* en una nueva pestaña • Facilidad para crear carpetas. • Funcionalidad de pinch-to-zoom en el calendario. • Captura de pantalla integrada. • Corrector ortográfico del teclado mejorado. • Habilidad de acceder a aplicaciones. • Funcionalidad copiar-pegar mejorada. • Mejor integración de voz y dictado de texto. • Desbloqueo facial. • Nuevo navegador web con pestañas. • Capacidad para cerrar aplicaciones. • Aplicación de la cámara mejorada. • Editor de fotos integrado. • Nuevo diseño de la galería. • Soporte para el formato de imagen WebP • Aceleración por *Hardware* de la interfaz de usuario. • Wi-Fi Direct. • Grabación de vídeo a1080Ppara dispositivos con *Android* de serie. • *Android* VPN Framework (AVF).

Versión	Lanzamiento	Características
Android 4.1 JELLY BEAN	27 de junio de 2012 	• Soporte para *Bluetooth* de baja energía. • OpenGL ES 3.0 • Modo de perfiles con acceso restringido. • DRM API de mayor calidad. • Mejora en la escritura. • Cambio de usuarios más rápida. • Locación de WiFi en segundo plano. • Auto-completar en el marcado. • Añadido el soporte para más de 5 idiomas. • Opciones para creadores de Apps. • Mejoras en el modo de conexión externa y de desarrollador (para actualizaciones vía cable USB). • Mejoras en la seguridad.
Android 4.4 KITKAT	31 de octubre de 2013 	• Arreglos en la conexión de datos. • Arreglos de enfoque de cámara en los modos HDR y normal. • Múltiples correcciones en el soporte *Bluetooth* • Solución de la desaparición de accesos directos de algunas App tras su actualización. • Arreglos de seguridad en la depuración USB. • Arreglos de seguridad en los accesos directos de las App. • Solución en la conexión automática WI-FI. • Ajustes en MMS, Email/Exchange. • Solución del atasco en la pantalla de activación. • Arreglo del LED en las llamadas perdidas. • Arreglo del gráfico de uso de datos.
Android 5.0 LOLLIPOP		• Soporte para CPU de 64 de bits. • Soporte para vistas previas de impresión. • Pantalla de bloqueo refrescada. • Mejoras de la vida de la batería. • Pantalla de bloqueo proporciona accesos directos. • Los inicios de sesión de usuarios y múltiples cuentas de usuario. • Entrada y salida de audio a través de dispositivos USB. • Las aplicaciones de terceros recuperan la

Versión	Lanzamiento	Características
	3 de noviembre de 2014 	capacidad. • La adición de 15 nuevos idiomas. • Se incluye una aplicación de linterna. • Capacidad para unirse a redes Wi-Fi. • Soporte para múltiples tarjetas SIM. • Protección de dispositivos. • Llamadas de voz de Alta Definición (HD). • Mejoras de estabilidad y rendimiento.

1.6.4. CARACTERÍSTICAS DE *ANDROID*

Tabla 2. Características Android[7]

Diseño de dispositivo	La plataforma es adaptable a pantallas de mayor resolución, VGA, biblioteca de gráficos 2D, biblioteca de gráficos 3D basada en las especificaciones de la OpenGL ES 2.0 y diseño de teléfonos tradicionales.
Almacenamiento	SQLite, una base de datos liviana, que es usada para propósitos de almacenamiento de datos.
Conectividad	*Android* soporta las siguientes tecnologías de conectividad: GSM/EDGE, IDEN, CDMA, EV-DO, UMTS, *Bluetooth*, Wi-Fi, LTE, HSDPA, HSPA+, NFC y WiMAX.GPRS, UMTS y HSDPA+.
Mensajería	SMS y MMS son formas de mensajería, incluyendo mensajería de texto y ahora la *Android* Cloud to Device Messaging Framework (C2DM) es parte del servicio de Push Messaging de *Android*.
Navegador web	El navegador web incluido en *Android* está basado en el motor de renderizado de código abierto WebKit, emparejado con el motor JavaScript V8 de Google Chrome. El navegador por defecto de Ice Cream Sandwich obtiene una puntuación de 100/100 en el test Acid3.
Soporte de Java	Aunque la mayoría de las aplicaciones están escritas en Java, no hay una máquina virtual Java en la plataforma. El *bytecode* Java no es ejecutado, sino que primero se compila en un ejecutable Dalvik y corre en la máquina Virtual Dalvik. Dalvik es una máquina virtual especializada, diseñada específicamente para *Android* y optimizada para dispositivos móviles que funcionan con batería y que tienen memoria y procesador limitados. El soporte para J2ME

[7] Wikipedia. (s.f.). Recuperado el 6 septiembre de 2015, de https://es.wikipedia.org/wiki/Android#Caracter.C3.ADsticas

	puede ser agregado mediante aplicaciones de terceros como el J2ME MIDP *Runner*.
Soporte multimedia	*Android* soporta los siguientes formatos multimedia: Web, H.263, H.264 (en 3GP o MP4), MPEG-4 SP, AMR, AMR-WB (en un contenedor 3GP), AAC, HE-AAC (en contenedores MP4 o 3GP), MP3, MIDI, Ogg Vorbis, WAV, JPEG, PNG, GIF y BMP.
Soporte para *Streaming*	*Streaming* RTP/RTSP (3GPP PSS, ISMA), descarga progresiva de HTML (HTML5 <video> tag). Adobe Flash *Streaming* (RTMP) es soportado mediante el Adobe Flash Player. Se planea el soporte de Microsoft Smooth *Streaming* con el Port de Silverlight a *Android*.
Soporte para *Hardware* adicional	*Android* soporta cámaras de fotos, de vídeo, pantallas táctiles, GPS, acelerómetros, giroscopios, magnetómetros, sensores de proximidad y de presión, sensores de luz, game pad, termómetro, aceleración por GPU 2D y 3D.
Entorno de desarrollo	Incluye un emulador de dispositivos, herramientas para depuración de memoria y análisis del rendimiento del software. Inicialmente el entorno de desarrollo integrado (IDE) utilizado era Eclipse con el *plugin* de Herramientas de Desarrollo de *Android* (ADT). Ahora se considera como entorno oficial *Android* Estudio, descargable desde la página oficial de desarrolladores de *Android*.
Google Play	Google Play es un catálogo de aplicaciones gratuitas o de pago en el que pueden ser descargadas e instaladas en dispositivos *Android* sin la necesidad de un PC.
Multi-táctil	*Android* tiene soporte nativo para pantallas capacitivas con soporte multi-táctil que inicialmente hicieron su aparición en dispositivos como el HTC Hero. La funcionalidad fue originalmente desactivada a nivel de kernel (posiblemente para evitar infringir patentes de otras compañías).
Bluetooth	El soporte para A2DF y AVRCP fue agregado en la versión 1.5; el envío de archivos (OPP) y la exploración del directorio telefónico fueron agregados en la versión 2.0; y el marcado por voz junto con el envío de contactos entre teléfonos lo fueron en la versión 2.2.
Videollamada	*Android* soporta Videollamada a través de Hangouts (ex-Google Talk) desde su versión HoneyComb.
Multitarea	Multitarea real de aplicaciones está disponible, es decir, las aplicaciones que no estén ejecutándose en primer plano reciben ciclos de reloj.
Características basadas en voz	La búsqueda en Google a través de voz está disponible como "Entrada de Búsqueda" desde la versión inicial del sistema.
Tethering	*Android* soporta *tethering*, que permite al teléfono ser usado como un punto de acceso alámbrico o inalámbrico (todos los teléfonos desde la versión 2.2) Para permitir a un PC usar la conexión de datos del móvil *Android* se podría requerir la instalación de software adicional.

1.6.5. ARQUITECTURA *ANDROID*

Ilustración 7. Arquitectura Android

Aplicaciones: Todas las aplicaciones creadas con la plataforma *Android*, incluirán como base un cliente de email (correo electrónico), calendario, programa de SMS, mapas, navegador, contactos, y algunos otros servicios mínimos. Todas ellas escritas en el lenguaje de programación Java.

Framework de aplicaciones: Todos los desarrolladores de aplicaciones *Android*, tienen acceso total al código fuente usado en las aplicaciones base. Esto ha sido diseñado de esta forma, para que no se generen cientos de componentes de aplicaciones distintas, que respondan a la misma acción, dando la posibilidad de que los programas sean modificados o reemplazados por cualquier usuario.

Librerías: *Android* incluye en su base de datos un set de librerías C/C++, que son expuestas a todos los desarrolladores a través del *framework* de las aplicaciones como por ejemplo: *Android* System C library, librerías de medios, librerías de gráficos, 3D, SQlite.

Runtime de *Android*: Incorpora un set de librerías que aportan la mayor parte de las funcionalidades disponibles en las librerías base del lenguaje de programación Java. La Máquina Virtual está basada en registros, y corre clases compiladas por el compilador de Java.

Núcleo Linux: 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. (III, (s.f.))

1.7. iOS

Ilustración 8. iOS

1.7.1. HISTORIA iOS

El 29 de Junio de 2007 fue presentado el primer iPhone, creando una nueva definición de teléfono móvil que marcaría el rumbo en la industria de la telefonía.

Con él nació su sistema operativo, iOS (anteriormente iPhone OS) una adaptación del OSX de Mac. iOS fue evolucionando desde su versión 1.0 hasta la versión más reciente. Fue creado inicialmente para iPhone pero posteriormente incluido en el resto de dispositivos: iPod Touch e iPad.

Su facilidad de uso y sus múltiples posibilidades permitió que Apple alcanzara un gran protagonismo en el mundo de la telefonía móvil frente a otros sistemas operativos móviles como su gran rival: *Android*. Apple, consciente de que los usuarios cada vez están más familiarizados con iOS, ha aprovechado para introducir cada vez más funcionalidades de iOS en OSX.

El sistema operativo de Mac está siendo “iOSsificado” con el objetivo de sacarle más partido y obtener un resultado más gratificante y reconocido por los usuarios. Como resultado de la mezcla entre OSX y iOS nace Mac OS X Lion, el primer sistema operativo para ordenadores que incorpora funcionalidades típicas de un dispositivo móvil.

Apple ha conseguido batir récords en ventas en sus cinco años de vida con su sistema operativo iOS. Su Apple Store cuenta con miles de aplicaciones, un recopilatorio solo comparable con el *Android* Market de Google.

1.7.2. DEFINICIÓN DE iOS

Es un sistema operativo móvil desarrollado por Apple Inc. Inicialmente fue creado para el iPhone, pero con el tiempo fue adaptado para los demás dispositivos móviles de esta compañía (iPad y el iPod touch)[8], otros dispositivos como el iPod Nano y el iWach utilizan otro sistema más básico y dirigido a una función más específica basado en iOS porque incorpora algunos de sus gestos e iconos y además se pueden sincronizar con teléfonos o *Tablets*.

Los iOS poseen una interfaz fluida, sencilla y elegante, sin mucha posibilidad de personalizar pero que ofrece al usuario una de las experiencias más cómodas del mercado.

Esto se debe a que iOS está diseñado para sacar el máximo provecho al *Hardware* que coloca en sus dispositivos el cual siempre se ha diferenciado considerablemente de los demás fabricantes.

[8] CONCEPTODEFINICION.DE. (s.f.). Recuperado el 11 septiembre de 2015, de http://conceptodefinicion.de/ios/

1.7.3. VERSIONES DE iOS

Tabla 3. Versiones iOS

Versión	Lanzamiento	Características
iOS 1.0 	2007	• Inicia con el iPhone 2G por defecto. • Aplicaciones Mail, Safari, Calendar, Photos, Camera, Mapas y YouTube. • Aparece la aplicación iTunes.
iOS 2.0 	2008	• Soporte para aplicaciones de terceros. • Primera versión App Store. • Soporte para A-GPS (Assisted GPS). • Mejora funcionamiento del navegador GPS en cuanto a la recepción de información sobre localización y posicionamiento.
iOS 3.0 	2009	• Soporte a mensajes MMS. • Función de copiar y pegar. • Teclado en modo horizontal. • Incorporación de notificaciones push, que permiten enviar mensajes al usuario sin la necesidad de ejecutar una aplicación (Ej. Recibir mensajes de correo nuevo sin necesidad de acceder a la aplicación de mail).
iOS 4.0 	2010	• Multitarea. • Posibilidad de organizar aplicaciones de la página de inicio en carpetas. • Unificar varias cuentas de correo en una sola carpeta de Mail. • Contador de caracteres para los mensajes SMS. • Soporte para Zoom en la cámara. • Apple adquiere la aplicación Siri.
iOS 5.0 	2011	• Incorpora grandes novedades solicitada por los usuarios durante años. • Agrega un buen centro de notificaciones mejorando la organización de las mismas. • Apple incorpora iCloud (la nube) para almacenar archivos del usuario. • Sincronizaciones: el equipo no se bloquea durante la sincronización con iTunes. • Se introducen mejoras en la sincronización por WiFi. • Integración con *Twitter* y *Facebook*.

Versión	Lanzamiento	Características
iOS 6.0 	2012	• Google Maps fue retirado de los dispositivos y crea su propia aplicación llamada Maps. • Se incluye *Passbook*, una aplicación busca simular la billetera y le permite al usuario el poder guardar cupones, tickets y formas de pago móviles. • Compartir fotos vía *Streaming* a través de iCloud.
iOS 7.0 	2013	• Cambio drástico del diseño del Sistema Operativo. • Apple introduce una interfaz renovada, mucho más sencilla y basada en un diseño plano y minimalista. • Centro de control: al que el usuario puede acceder a su equipo deslizando el dedo de abajo hacia arriba. • Permite al usuario activar y desactivar funciones como WiFi, *Bluetooth* o el modo avión. • Utiliza las funciones básicas del reproductor de música y acceder al temporalizador. • Incluye iTunes Radio un servicio de *Streaming*. • Actualizaciones automáticas.
iOS 8.0 	2014	• Mejor sincronización entre todos los dispositivos de Apple. • Funcionalidad Handoff: con lo que los usuarios pueden pasar su información de sus dispositivos móviles a su computador de escritorio o viceversa. • Cambio de pantalla a escala de grises. • Teclado más inteligente (sugiriendo palabras)
iOS 9.0 versión Beta 	2015	• Siri proactiva: se volverá proactiva al predecir lo que el usuario desea saber antes de preguntar. • Multitareas: pronto los usuarios podrán correr dos aplicaciones al mismo tiempo en la misma pantalla • Quicktype: además de multitarea, los usuarios podrán seleccionar texto y mover el cursor como si fuera un mouse. • Cerrar todas las aplicaciones de golpe. • Estilo colorido. • Versión Beta: abierta al público usuario de Apple

1.7.4. CARACTERÍSTICAS iOS

Tabla 4. Características iOS[9]

Pantalla	Es donde se ubican los íconos de las aplicaciones que vienen con el dispositivo o que se descargan desde la AppStore. También cuenta con una parte llamada Dock en su parte inferior y, en la superior, encontrará la barra de estado.
Creación de carpetas	iOS le brinda la posibilidad de crear carpetas en las que puede organizar o agrupar sus aplicaciones por categorías o de la forma que quiera.
Centro de Notificaciones	Los dispositivos con sistema operativo iOS cuentan con un centro notificaciones. Allí, llegan las noticias de todo lo que está sucediendo en las aplicaciones que se tienen instaladas en su dispositivo.
Multitareas	Este sistema operativo le permite ejecutar varias aplicaciones a la vez. Es decir, que no tiene que cerrar una aplicación para abrir otra. De hecho, puede pasar de una a otra pulsando dos veces seguidas el botón de inicio del dispositivo.
Simplicidad	La simplicidad de iOS es una característica muy notable, puesto que ofrece un menú mucho más reducido.
Seguridad	El control que Apple ejerce sobre todo su ecosistema de productos pone las cosas un poco más difíciles a los hackers malintencionados que quieren atacar a iOS, aun así cabe mencionar que ninguna plataforma es completamente segura, eso es evidente.

1.7.5. ARQUITECTURA iOS

La arquitectura iOS está basada en capas, donde las capas más altas contienen los servicios y tecnologías más importantes para el desarrollo de aplicaciones, y las capas más bajas controlan los servicios básicos.

[9] Wikipedia. (s.f.). Recuperado el 16 septiembre de 2015, de https://es.wikipedia.org/wiki/IOS

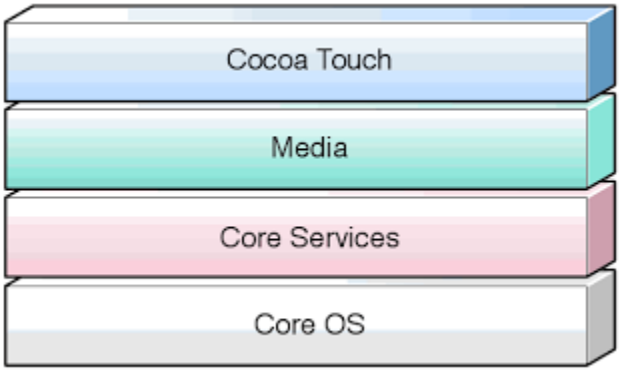


Ilustración 9. Arquitectura iOS

Cocoa Touch:

Es la capa más importante para el desarrollo de aplicaciones iOS. Posee un conjunto de Frameworks que proporciona el API de Cocoa para desarrollar aplicaciones. Esta capa es con la que el usuario interactúa con las aplicaciones (es la capa visible).

Esta capa está formada por dos *Frameworks* fundamentales:

- UIKit: contiene todas las clases que se necesitan para el desarrollo de una interfaz de usuario.
- Foundation Framework: define las clases básicas, acceso y manejo de objetos, servicios del sistema operativo.

Media: Provee los servicios de gráficos y multimedia a la capa superior.

Core Services: Contiene los servicios fundamentales del sistema que usan todas las aplicaciones como puede ser acceso a la red, base datos entre otros.

Core OS: Contiene las características de bajo nivel: ficheros del sistema, manejo de memoria, seguridad, drivers del dispositivo[10]

[10] Tecnología iOS. . (s.f.). Recuperado el 16 septiembre de 2015, de https://sites.google.com/site/tecnologiaiostm/desarrollo-de-aplicaciones/arquitectura-ios

1.8. WINDOWS PHONE

Ilustración 10. Windows Phone

1.8.1. HISTORIA WINDOWS PHONE

Windows Phone, cuyo nombre en clave durante su desarrollo era "Photon", es el sucesor de Windows Mobile, desarrollado por Microsoft y basado en el núcleo Windows Embedded CE 6.0. Microsoft mostró Windows Phone por primera vez el 15 de febrero de 2010, en el Mobile World Congress de Barcelona y reveló más detalles del sistema en el MIX 2010 el 15 de marzo. La versión final de Windows Phone 7 se lanzó el 21 de octubre de 2010 en Europa y el 8 de noviembre en Estados Unidos. Inicialmente, Windows Phone estaba destinado para ser lanzado durante el 2009, pero varios retrasos provocaron que Microsoft desarrollara Windows Mobile 6.5 como una versión de transición. La interfaz fue revisada en su totalidad y comparte características virtuales con la interfaz del dispositivo Zune HD y además utilizaba el Zune Software para gestión de contenidos, App, y actualizaciones en la séptima versión. (wikipedia, 2015)

1.8.2. DEFINICIÓN DE WINDOWS PHONE

Windows Phone (abreviado WP) es un sistema operativo móvil desarrollado por Microsoft, como sucesor de Windows Mobile. A diferencia de su predecesor está enfocado en el mercado de consumo en lugar de en el mercado empresarial. Con Windows Phone; Microsoft ofrece una nueva interfaz de usuario que integra varios de sus servicios propios como OneDrive, Skype y Xbox Live en el sistema

operativo. Compite directamente contra *Android* de Google e iOS de Apple. Su última versión disponible y definitiva es Windows Phone 8.1, lanzado el 14 de abril de 2014.

Debido a la evidente fragmentación de sus sistemas operativos, Microsoft anunció en enero de 2015 que dará de baja a Windows Phone, para enfocarse en un único sistema más versátil denominado Windows 10, disponible para todo tipo de plataformas (teléfonos inteligentes, *Tablet*as y computadoras) (wikipedia, 2015).

1.8.3. VERSIONES WINDOWS PHONE

Tabla 5. Versiones de Windows Phone

Versión	Notas	Lanzamiento	Características
Windows CE 3.0	Pocket PC	2002	• Utiliza Windows CE 3.0 • Diseñado para dispositivos Pocket PC con pantalla 240 x 320
Windows Mobile 2003	Tercera versión Windows Mobile	23 de Junio de 2003	• Llega en 3 ediciones diferentes; dos de éstas versiones son similares Windows Mobile 2003 Pocket PC Edition y Windows Mobile 2003 Pocket PC Phone Edition, la tercera edición es Windows Mobile 2003 *Smartphone* Edition
Windows Mobile 2003 Second Edition	*Smartphone* Inteligente	24 de Marzo de 2004	• Opción de cambiar orientación de la pantalla. • Soporte para resolución de pantalla VGA (640 x 480). • Soporte para WiFi.
Windows Mobile 5.0	Magneto	9 de Mayo de 2005	• Utiliza .NET Compact Framework 1.0 SP2 plataforma de desarrollo .NET para los programas basados en .NET que utiliza una nueva versión

Versión	Notas	Lanzamiento	Características
			de Office llamada "Office Mobile". • Id de llamadas con fotos • Soporte para teclados QWERTY incluido por defecto
Windows Mobile 6.0	Crossbow	12 de Febrero de 2007	• Ofrece tres versiones: Windows Mobile 6 Standard para *Smartphone*s , Windows Mobile 6 Professional para PDA con la funcionalidad del teléfono, y Windows Mobile 6 Classic para PDA sin telefonía IP • Utiliza Windows CE 5.2
Windows Mobile 6.1	Actualización	1 de Abril de 2008	• Es una actualización menor de la plataforma Windows Mobile 6. • Incluye varias mejores en el rendimiento. • Zoom a página completa.
Windows Mobile 6.5	Actualización	11 de mayo de 2009	• Cambio completo de la interfaz de usuario para adaptarlo a los nuevos dispositivos. • Windows Market Place. • Internet Explorer Mobile 6
WINDOWS PHONE 7			
7.0.0	Primera versión Windows Phone “Fotón”	11 de octubre de 2010	• Versión inicial de Windows Phone • Bastantes carencias.
7.1.0	Primera Actualización Windows Phone 7 “Nodo”	23 de marzo de 2011	• Soporte para copiar/pegar. • Menor tiempo de arranque • Mejor rendimiento. • Mejoras en la sincronización con *Facebook.*
7.5.0	Segunda Actualización Windows Phone 7 “Mango”	27 de septiembre de 2011	• Características multitarea. • Nuevo sistema de búsqueda. • Integración con *Twitter.* • Grupos de contactos. • Mejoras en GPS e Internet 9.

Versión	Notas	Lanzamiento	Características
7.5.1	Tercera Actualización Windows Phone 7 "Tango"	_	• Minimiza requisitos del sistema operativo para la adaptación a terminales de menor coste. • Anunciada en el Congreso Mundial de Teléfonos 2012 • Nuevas funciones con limitaciones para la gama baja
7.8.0	Cuarta Actualización Windows Phone 7	30 de enero de 2013	• Mejoras en la interfaz de usuario y fondos personalizados para la pantalla de bloqueo.
WINDOWS PHONE 8			
8.0.0	Segunda versión de Windows Phone "Apollo"	Finales del año 2012	• Disponible únicamente para nuevos dispositivos debido a un cambio de Kernel (Windows CE a Windows NT) • Nuevas características como: nuevas pantallas de inicio, rincón infantil (espacio controlado), Carteras (para almacenar tarjetas de crédito), NFC, Internet E. 10, Skype integrado, nuevo Núcleo Windows NT.
8.0.1	Primera Actualización Windows Phone 8	_	• Incluye la posibilidad de mantener encendido el WiFi, aun con la pantalla bloqueada.
8.0.2	Segunda Actualización Windows Phone 8	Agosto 2013	• Incluye radio FM • Mejoras del HTML5 en Internet Explorer 10. • Solución al problema de la carpeta "Otros", que llegaba a ocupar mucha memoria interna.
8.0.3	Tercera Actualización	Enero 2014	• Soporte para procesadores Quad-Core para pantallas Full HD 1080p. • Nuevas funciones de accesibilidad. • Mejoras en la función

Versión	Notas	Lanzamiento	Características
	Windows Phone 8		"compartir conexión" • Mejoras en conexiones WiFi y *Bluetooth*.
WINDOWS PHONE 8.1			
8.1.0	Tercera versión de Windows Phone	14 de Abril de 2014	• Centro de notificaciones • Asistente de voz (cortana) • Sensor de WiFi, sensor de datos y sensor de batería. • Aplicaciones natas como: salud, comida y bebida, viaje y mapas. • Mejoras en la pantalla de inicio, posibilidad de agregar fondos de pantalla
8.1.1	Primera Actualización Windows Phone 8.1	14 de Agosto de 2014	• Carpetas vivas en la pantalla de inicio. • Mejoras en Internet Explorer. • Cortana en más idiomas • Mejoras en el centro de notificaciones. • Live tile para música, tienda, sensor de batería.
8.1.2	Segunda Actualización Windows Phone 8.1	2 de Marzo de 2015	• Última versión de Windows Phone. • Configuraciones: ahora divididas por categorías. • 3 nuevos idiomas
WINDOWS PHONE 10			
Se espera que esta versión unifique todas las plataformas como PC, *Tablet*as, *Smartphone*, Xbox One y dispositivos IoT (Internet de las cosas) La vista previa técnica de Windows Phone para teléfonos fue lanzada el 12 de febrero de 2015 y cuenta con las siguientes características: • Imagen de tamaño completo para la pantalla de inicio • Más acciones rápidas en el centro de acciones • Notificaciones interactivas • Mejora significativa en la conversión de voz a texto • Aplicación de fotos mejorada			

1.8.4. CARACTERÍSTICAS DE WINDOWS PHONE

Tabla 6. Características de Windows Phone[11]

Interfaz	Windows Phone cuenta con una interfaz de usuario llamada Modern UI. La pantalla de inicio se compone de Live Tiles, mosaicos dinámicos que son enlaces a aplicaciones u objetos individuales (como contactos, páginas web o archivos multimedia). Estos mosaicos actualizan frecuentemente manteniendo informado de cualquier cambio al usuario.
Teclado	Entre sus principales características se incluyen el Word Flow (teclado Swype), revisión ortográfica, predicción de palabras y una tecla dedicada para insertar emoticonos y otros símbolos.
Motor de búsqueda	El buscador por defecto es Bing. Antes era posible cambiar el buscador predeterminado (Bing) por Google, pero después se retiró esa función.
Cortana y búsquedas	Los dispositivos Windows Phone tienen un botón dedicado a búsquedas en la parte frontal del dispositivo.
Hubs	Windows Phone no es un sistema centralizado solamente en aplicaciones sino que se organiza en un nuevo concepto denominado Hubs. Los Hubs de Windows Phone clasifican acciones y agrupan las aplicaciones que se correspondan con una actividad determinada.
Contactos	En este lugar es donde se guardan todos los contactos y se centraliza su actividad online (como cambios de estado, imágenes compartidas y comentarios) en *Facebook*, *Twitter* y LinkedIn.
Fotos	Es el lugar donde se almacenan todas las imágenes que el usuario ha guardado en el teléfono; así como las fotos que ha tomado. En este Hub se pueden integrar todas las aplicaciones que tienen funciones de edición y distribución de imágenes
Office	En el Hub de Office se puede acceder a Word, Excel, OneNote y PowerPoint. Estas App permiten ver, editar y compartir archivos de estos servicios a través de OneDrive y SharePoint. Permite realizar comentarios y correcciones sobre documentos.
Xbox	El Hub Xbox Juegos es la zona donde se integra la parte destinada al entretenimiento en Windows Phone
Podcasts	Esta aplicación permite la reproducción de podcasts en línea y descargarlos al teléfono.

[11] Wikipedia. (s.f.). Recuperado el 22 septiembre de 2015, de https://es.wikipedia.org/wiki/Windows_Phone

1.8.5. ARQUITECTURA WINDOWS PHONE

La plataforma de Windows Phone se divide en dos grandes bloques, Screen y Cloud:

Screen: Se refiere al entorno de desarrollo que está instalado en el dispositivo, la forma tradicional de desarrollo, con la que se logran desarrollar las aplicaciones.

Cloud: Es una nueva apuesta de Microsoft que permite realizar diversas tareas o directamente trabajar vía internet.

Ilustración 11. Arquitectura Windows Phone

División Screen:

- Runtimes-On"Screen": Silverlight, XNA *Framework*, .NET Compact *Framework* y sus servicios relacionados, que proveen a la plataforma de un entorno sobre el que construir aplicaciones seguras y gráficamente ricas.
- Herramientas y soporte: Virtual Estudio 2010 y Expression Blend, junto con todas sus utilidades y documentación, crea un entorno y una experiencia de desarrollo que permiten generar aplicaciones de manera rápida y sencilla.

División Cloud:

- Servicios Cloud: Servicios en la nube como Windows Azure (plataforma ofrecida como servicio y alojada en los centros de procesamiento de datos de Microsoft, orientada a empresas), XBOX Live Service y otros servicios como los de notificaciones. Acceso a servicios de terceros, como servicios de identificación, almacenamiento, redes sociales, etc.
- Portal de Servicios: El Windows Phone Marketplace contiene servicios que permiten a los desarrolladores registrar, certificar y vender sus aplicaciones.

1.9. COMPARATIVA ENTRE SISTEMAS MÓVILES

1.9.1. VENTAJAS *ANDROID*

Tabla 7. Ventajas Android

Ventajas	Descripción
Plataforma de código abierto	*Android* está basado en el kernel de Linux. Lo que trae como consecuencia que se puede manipular.
Gran número de Aplicaciones	Existen más de 100,000 aplicaciones disponibles para teléfonos *Android*, gran parte de ellas gratuitas.
Sistema Multitarea	Esto significa que un sistema *Android* es capaz de hacer funcionar varias aplicaciones a la vez.
Personalizable y Económico	Una gran ventaja de *Android* es el poder personalizar el escritorio con *Widgets*. Además de ser muy accesible para el bolsillo del usuario.
Disponible en varios equipos y marcas	Es una gran ventaja de *Android*, que se puede conseguir en equipos de gama baja hasta la gama alta y en diferentes marcas.

1.9.2. DESVENTAJAS *ANDROID*

Tabla 8. Desventajas Android

Desventajas	Descripción
Vulnerable	Debido a que es de código abierto, *Android* se ha convertido en el sistema con mayor riesgo de vulnerabilidad, aprovechando las fallas del sistema.
Sistema Multitarea	A pesar de tener la ventaja de ser multitarea, es un arma de doble filo, ya que al tener varias aplicaciones en uso, ralentiza el equipo además de que consume mucha batería.
Necesidad de descargar aplicaciones adicionales	Esto para solucionar problemas de uso normal, lo cual implica que la memoria interna del dispositivo se llene y se vuelva lento.
Actualizaciones no disponibles	El acceso a una actualización depende del fabricante, lo que hace que una respuesta pueda tardar semanas e incluso meses en adaptar la nueva versión al móvil del usuario.

1.9.3. VENTAJAS iOS

Tabla 9. Ventajas iOS

Ventajas	Descripción
Calidad en los dispositivos	iOS cuenta con un acabado excelente
Interfaz de usuario	Algo que distingue a Apple es el haber logrado construir una interfaz de usuario altamente intuitiva y elegante, que hasta el usuario menos experimentado puede aprender a utilizar en cuestión de minutos.
Tendencia más baja de *Malware*	En iOS existe un proceso de aprobación en el App Store, en el cual las aplicaciones son revisadas antes de que se publiquen. Así que podrá bajar contenido de manera segura sin límites.
Sincronización entre equipos	Sincronización entre equipos sin necesidad de hacer nada, capacidad de contestar mensajes desde cualquier equipo sin causar duplicados y quizás la mejor manera de administrar y disfrutar de la música.
iTunes	La tienda más grande de música, al adquirir un equipo iOS tendrá acceso a la más grande tienda de música en línea.

1.9.4. DESVENTAJAS iOS

Tabla 10. Desventajas iOS

Desventajas	Descripción
Restricciones	iOS es un sistema operativo cerrado. Por lo cual no podrá hacer uso de aplicaciones elaboradas por terceros si éstas no fueron aprobadas por Apple para que fueran publicadas en su App Store
No compatible	No es compatible en cualquier dispositivo móvil, sólo se puede utilizar en equipos Apple.
Precio	Uno de los principales problemas del iOS es el precio, debido a su diseño único, el precio para obtener un equipo es muy elevado.

1.9.5. VENTAJAS WINDOWS PHONE

Tabla 11. Ventajas Windows Phone

Ventajas	Descripción
Aplicaciones de escritorio	Una gran ventaja de tener este sistema operativo móvil es que se pueden instalar las mismas aplicaciones que se usan en un ordenador.
Interfaz	La interfaz es altamente intuitiva y sencilla de usar, que cualquier usuario se adapta y reconoce las aplicaciones natas de este sistema móvil.
Integración	La integración que ha hecho Microsoft con todo su ecosistema de aplicativos es significativa, ya que es muy fácil sincronizar una PC con un *Smartphone* con Windows Phone.
Estabilidad	Sin duda alguna Windows Phone dispone de una estabilidad idónea para cualquier usuario ya que sorprende la fluidez con la que funciona con toda clase de aplicaciones.
Competitivo	Windows Phone se mantiene como uno de los sistemas operativos ya muy solicitados a pesar de su lenta incorporación en el mercado móvil.

1.9.6. DESVENTAJAS WINDOWS PHONE

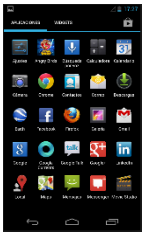
Tabla 12. Desventajas Windows Phone

Desventajas	Descripción
Ausencia de aplicaciones	Por el hecho de ser aun un sistema operativo móvil joven, tiene la gran desventaja de carecer de aplicaciones que el usuario exige, ya que no es posible encontrarlas en la tienda del dispositivo.
Sincronización multimedia	La aplicación Zune resulta muy fácil de usar, pero al momento de copiar o respaldar archivos de música, videos o fotos, se pueden encontrar diversos inconvenientes.
Navegador de internet	Lamentablemente sólo cuenta con Internet Explorer, lo cual resulta en algunas ocasiones molesto y torpe.
Actualizaciones escazas	En cuanto a las actualizaciones de las aplicaciones resulta a veces desagrado, ya que no se actualizan constantemente como lo son *Facebook* y *WhatsApp*.

1.9.7. CUADRO COMPARATIVO GENERAL

En el siguiente cuadro se muestra una tabla comparativa de los Sistemas Operativos Móviles.

Tabla 13. Comparativa general entre Sistemas Operativos Móviles

Sistema Operativo	**ANDROID**	**iOS**	**Windows PHONE**
Interfaz			
Kernel	Linux	OS X	Windows NT
Tipo de SO	Abierto	Cerrado	Cerrado
Lenguaje de programación	Java	Objective-C	C#
Seguridad	Susceptible al *Malware*	Muy buena	Buena
Costo de desarrollo	25 USD solo una vez	99 USD anuales	99 USD anuales
Adaptabilidad	Excelente	Excelente	Excelente
Plataforma	Madura	Madura	Joven
Redes soportadas	GSM, CDMA	GSM, CDMA	GSM, CDMA
Hardware soportado	Amplia gama de dispositivos	iPhone, iPad, iPod, iWatch.	Limitada gama de dispositivos
Actualización	Si	Si	Si
Tienda de aplicaciones	Play Store	iTunes	Zune, Opera
Navegador Web	Google Chrome	Safari	Opera Mini
Soporte Flash	Si	No	No
Copiar y pegar	Si	Si	Si
Duración Batería	Baja	Alta	Media

Como podemos observar, los Sistemas Operativos Móviles tienen sus pros y contras, lo cual dependerá de las necesidades del usuario y de su economía el poder obtener un dispositivo móvil con alguno de los Sistemas Móviles ya mencionados.

Basándonos en el cuadro comparativo general y por lo que se ha investigado a cerca de los Sistemas Operativos, sugerimos que el mejor Sistema Operativo para los dispositivos móviles es *Android*, ya que cuenta con una distribución libre y de código abierto, es flexible en cuanto a costo se refiere, tiene miles de aplicaciones gratuitas y brinda al usuario una personalización profunda de su dispositivo puesto que se puede realizar una serie de modificaciones ajustando la plataforma a sus necesidades y a los recursos del dispositivo. Además cuenta con actualizaciones frecuentes con características mejoradas.

1.10. MERCADO DE SISTEMAS OPERATIVOS MÓVILES

En México y en América Latina, *Android* domina el mercado de los Dispositivos Móviles con amplia mayoría sobre su principal rival, Apple, señala un estudio de ComScore.

La firma de análisis de mercado, detalla que en México el sistema operativo *Android* de Google abarca el 74.8% a un nivel muy lejano del 12% que ostenta el iOS de Apple. El sistema de Microsoft, Windows Phone, mantiene el 5.6% del mercado de *Gadgets* móviles que engloba teléfonos inteligentes y *Tablet*as.

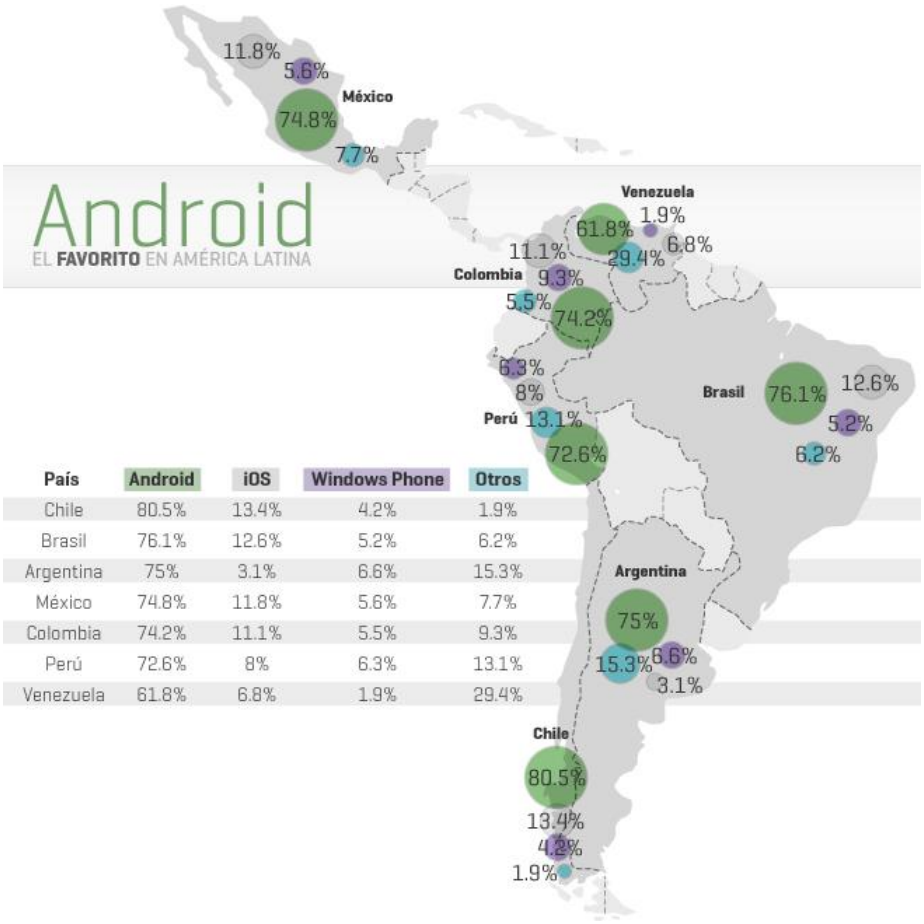
El estudio realizado en agosto pasado incluye la categoría de “otros sistemas” con un 7.7% de presencia en el país.

“Poco más de tres cuartos del tráfico de móviles en Brasil, Argentina y México también viene del sistema *Android*”, detalla ComScore en un reporte publicado.

Chile es uno de los países donde predomina el sistema de Google con el 80.5% del mercado, seguido de Brasil con el 76.1% y en la tercera posición de la tabla se ubica Argentina con el 75%.

En otros países latinoamericanos como Venezuela, Perú y Colombia, la ocupación de *Android* fue mayor al 60%, mientras que la de iOS se mantuvo por debajo del 20% y Windows Phone del 10%.

Según ComScore, ésta es la manera en que se dividen los sistemas móviles en América Latina (EXPANSIÓN, S.A. DE C.V., 2014).



País	Android	iOS	Windows Phone	Otros
Chile	80.5%	13.4%	4.2%	1.9%
Brasil	76.1%	12.6%	5.2%	6.2%
Argentina	75%	3.1%	6.6%	15.3%
México	74.8%	11.8%	5.6%	7.7%
Colombia	74.2%	11.1%	5.5%	9.3%
Perú	72.6%	8%	6.3%	13.1%
Venezuela	61.8%	6.8%	1.9%	29.4%

Ilustración 12. Sistemas Móviles en América Latina

1.11. TENDENCIA DE LOS S. O. MÓVILES EN EL MUNDO

Asia: En términos generales, el continente con una mayor penetración de *Smartphone*s en relación al uso de dispositivos móviles. Llama la atención el bajo porcentaje de uso de *Tablets*, que representa un 17% del total, frente al 77% de teléfonos inteligentes. Los dispositivos *Android* se sitúan a la cabeza con una cuota de mercado del 77%, los de iOS se encuentran justo por detrás, aunque solo representan un 14%.

Norteamérica: Si en oriente dominan los fabricantes asiáticos como Samsung, en los Estados Unidos la situación es bastante diferente. Los iPhone de Apple son los dispositivos más populares entre la población norteamericana, convirtiéndose así en uno de los lugares donde iOS obtiene una mayor cuota de mercado.

A pesar de que los teléfonos de Apple tienen una gran repercusión en los Estados Unidos, lo cierto es que en los últimos tiempos los dispositivos *Android* les han ido comiendo parte del terreno.

Sudamérica: Es un mercado dominado por *Android* (86%), la presencia de iOS es muy minoritaria (7%) y se encuentra al mismo nivel de otros sistemas operativos menos extendidos como Windows Phone (7%).

Europa: En el viejo continente la diversidad de su población se hace visible incluso en las decisiones de compra a la hora de adquirir teléfonos móviles. La gran riqueza cultural y la mezcla de mercados tan diferentes hacen que en Europa los resultados sean de lo más variado. *Android*, se posiciona con un 62% del mercado, supera claramente el 28% de iOS. Cabe destacar que Europa es uno de los pocos lugares donde RIM OS, el sistema operativo utilizado por Blackberry, sigue teniendo una pequeña representación (2%).

Los resultados son muy variables, ya que agrupan países con tendencias muy distintas. Un ejemplo de ello es la situación en el Reino Unido (48% Apple y 39% *Android*) frente a lo que ocurre en España (12% Apple y 82% *Android*). Los porcentajes referentes al tamaño de pantalla son bastante similares a los de

Norteamérica, siendo los dispositivos de entre cuatro y cinco pulgadas los más populares entre la población.

África: Con una población que en líneas generales dispone de menos recursos que la del resto de continentes, destaca por el gran uso de dispositivos móviles de gama baja. En este continente, iOS marca el mínimo de cuota con un 4%, siendo superado por Windows Phone (11%) e incluso RIM OS (5%). Por lo cual *Android* es el Sistema Operativo Móvil que domina en este continente Africano. Una de las peculiaridades de África es que presenta la mayor cuota de mercado de feature phones (teléfonos de primera generación, sin acceso a Internet de alta velocidad) con un 20% del total.

Oceanía: Por último pasamos a Oceanía, donde la situación es similar a la de Norteamérica, pero con una ventaja todavía más clara para Apple. Los dispositivos iOS representan el 56% del total.

El 78% de los teléfonos usados en Oceanía tienen una diagonal de pantalla inferior a las cinco pulgadas, algo que deriva de la alta popularidad de los dispositivos de Apple antes de la llegada de sus últimos modelos, con los que se produjo un aumento de tamaño. El hecho de que los teléfonos utilizados sean de un tamaño reducido, también se ve reflejado en la necesidad de tener un segundo dispositivo con una pantalla más grande. De este modo, mientras que el 58% del total de dispositivos son *Smartphone*s, el 42% son *Tablets* (ESTUDIOS ECONÓMICOS S.A., Miguel Yuste, 2015).

PARTICIPACIÓN DE MERCADO

OS	2013	2017
	75.3%	68.3%
iOS	16.9%	17.9%
	3.9%	10.2%
	2.7%	1.7%
Otros	1.2%	1.9%
TOTAL	100%	100%

Ilustración 13. Participación de mercado[12]

1.12. PRESENTE

Entre *Android* e iOS acabó igualándose en el terreno técnico: cada plataforma tiene su filosofía y *Android* ha contado con un apoyo crítico: la base Open Source ha permitido que operadoras y sobre todo fabricantes puedan basar sus dispositivos en una solución que se ha adaptado a todas las necesidades.

Por otra parte, Apple sigue sin licenciar su plataforma a terceros, como ocurría con Mac OS X en los ordenadores, mientras que Google simplemente quiere que *Android* lo use tanta gente como sea posible como hizo Microsoft con un Windows que funcionaba en todo tipo de PC.

Esa versatilidad y adaptabilidad de *Android* ha hecho que hoy en día esta plataforma domine el mercado de forma indiscutible.

[12] Fuente: IDS Worlwide Mobile Phone Tracker. 4 de septiembre de 2013

El sistema operativo para móviles *Android* batió el récord en el segundo trimestre del 2014, llegando a dominar 85% del mercado de *Smartphone*s, pasando de 186.8 millones de dispositivos *Android* vendidos a 249.6 millones respecto al año anterior.

El segundo mejor posicionado queda Apple, aunque en su caso también se ha visto un retroceso de un punto en la cuota de mercado debido a la poca presencia en el sector de *Smartphone*s de bajo coste, algo que *Android* tiene muy cubierto.

1.13. FUTURO

El avance de los terminales *Android* es imparable, cada vez más y más fabricantes basan sus dispositivos en una plataforma competitiva y con una comunidad de desarrolladores sobresaliente. Y por ello, no solo los antiguos dominantes del mercado han intentado reaccionar, sino que nuevos jugadores quieren entrar en el juego y luchar por un pedazo de ese pastel que hoy en día *Android* e iOS se reparten con demasiada solvencia.

Los porcentajes de ventas varían dependiendo el país y el tipo de economía de cada región. La mayoría de los países desarrollados prefieren comprar iOS, y el país con mayor predilección por el sistema de la manzana es Liechtenstein con 67% de participación. Le sigue Dinamarca con el 66% y en tercer sitio se encuentra Mónaco con 65%. Este comportamiento se replica en países con un alto nivel económico como Suiza, Australia, Canadá y Suecia.

Por otra parte, *Android* domina el mercado de los países con economías emergentes, lo cual se refleja, por ejemplo, en Papúa Nueva Guinea y Paraguay, dónde también incluye a México, con un 95% de ventas de *Android*. China e India concentran (entre los dos) más de la tercera parte de la población total del mundo; y en estos países, la participación de *Android* es del 93% del mercado, una vez

más se demuestra que los dispositivos de gama baja son un gran motor para el uso de *Android*.

Se podría decir que estamos entrando en un mundo en el que solo los '*Gadgets*' baratos y de calidad tienen salida.[13]

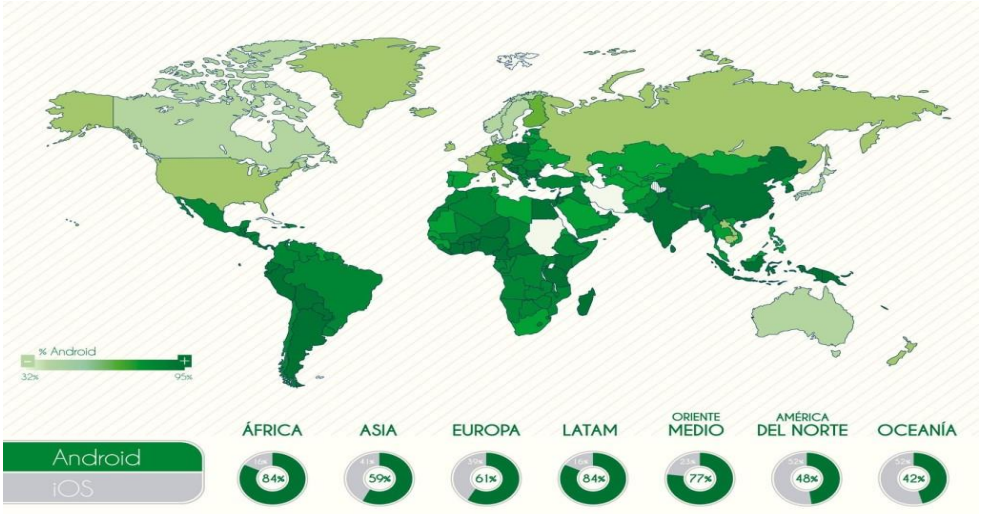


Ilustración 14. Tendencias Móviles

2. CAPÍTULO II. VULNERABILIDAD EN LOS DISPOSITIVOS MÓVILES

2.1. INTRODUCCIÓN

Los equipos móviles están expuestos a ser blanco fácil para los creadores de programas maliciosos, ya que los usuarios ingresan datos corporativos con alto grado de confidencialidad e información personal, pasando por multitud de aplicaciones de uso habitual, como el acceso a las redes sociales y la navegación por Internet. Desafortunadamente estos sistemas son vulnerables a riesgos derivados por fallas en la seguridad, ataques de *Malware* o por virus los cuales son adquiridos a través de diferentes medios, como las comunicaciones inalámbricas

[13] Alfonso López, Tendencias O.S. Móviles para el 2015, [en línea]. 15 de enero de 2015, [fecha de consulta: 11 Diciembre 2015]. Disponible en: < http://www.zonademarrones.com/tendencias-o-s-moviles-para-el-2015/>

2.2. SEGURIDAD EN LOS DISPOSITIVOS MÓVILES

Actualmente los teléfonos móviles están expuestos a ser blanco fácil para los creadores de programas maliciosos, ya que todos los usuarios acceden a internet para revisar su correo electrónico, redes sociales, etcétera, por lo que el sistema del móvil se vuelve vulnerable a riesgos derivados por fallas en la seguridad del mismo, así como a ataques de *malware* o por virus.

Las principales amenazas a los que se ven expuestos son:

- Pérdida o robo del dispositivo.
- Infecciones por virus o *Malware* vía email, *Botnets*, *Hoaxes*, *Spam*, *Rootkits*.
- Robo de información vía *Bluetooth*.
- Suplantación de identidad o *Spoofing*.
- Acceso a datos confidenciales de conversaciones, imágenes o vídeos.
- Infección al acceder a falsos códigos QR publicitarios.

De acuerdo con el documento "Tendencias 2014: el desafío de la privacidad en Internet" de ESET Latinoamérica, se estudiaron los registros de detección de *software* malicioso en dichos dispositivos, el resultado que se obtuvo se muestra en la siguiente gráfica:[14]

[14] ESET Latinoamérica, Tendencias 2014: El desafío de la privacidad en Internet (s.f.). Recuperado el 7 octubre de 2015, de http://www.eset-la.com/pdf/tendencias_2014_el_desafio_de_la_privacidad_en_internet.pdf

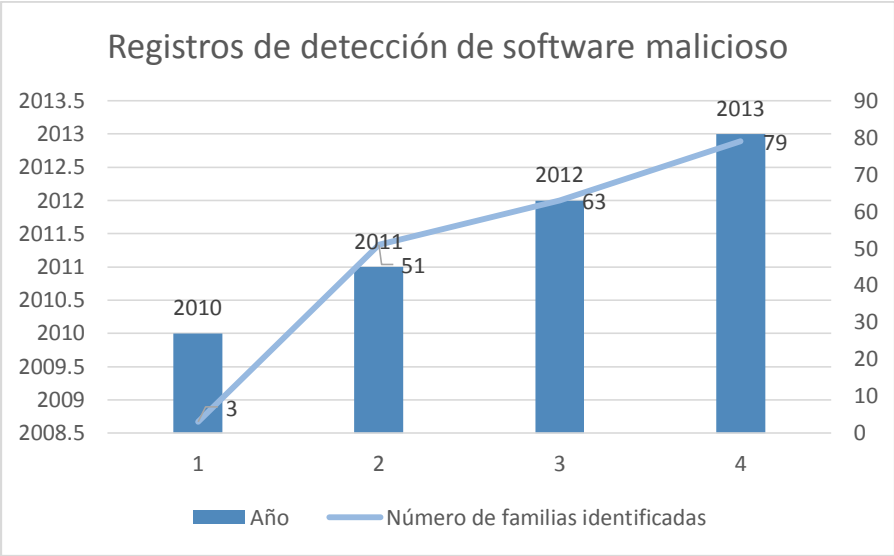


Ilustración 15. Seguridad en los dispositivos móviles

Otro problema importante del Sistema Operativo *Android* es la fragmentación, esta se refiere al hecho de que no todos los dispositivos que funcionan con *Android* utilizan la misma versión, o al menos no la más reciente.

En ocasiones, las actualizaciones del sistema son retenidas por los fabricantes de los dispositivos para evitar problemas de compatibilidad, lo que evita que las correcciones de seguridad lleguen a los usuarios.

En otros casos se lanzan al mercado nuevos modelos de *Smartphone* (teléfonos inteligentes) con versiones anteriores de la plataforma, debido principalmente a que se trata de desarrollos específicos para un tipo de dispositivo móvil.

Se han puesto en marcha distintas iniciativas que tienen como objetivo consolidar las versiones de *Android* de manera que la mayoría de los usuarios puedan hacer uso de la última versión, sin embargo, esto todavía no se logra, esto trae como consecuencia; utilizar versiones desactualizadas y esto se traduce en un importante riesgo de seguridad para los usuarios.

El código abierto para el desarrollo de aplicaciones de *Android* que proporciona Google para cualquiera de las versiones de *Android*, pone en riesgo la seguridad de la información de los usuarios ya que son más propensos a algún tipo de amenaza cibernética.

2.3. ATAQUES EN LOS DISPOSITIVOS MÓVILES

Con el avance de la tecnología y la aparición de los *Smartphone* (teléfonos inteligentes) y demás dispositivos móviles, los atacantes han comenzado a dirigirse a este mercado para el robo de información.

Cisco destaca que la International Telecommunications Union (ITU) estima que el 2010 cerró con más de 5,000 millones de usuarios de telefonía móvil alrededor del mundo y cerca de 1,000 millones de éstos son usuarios de teléfonos inteligentes.[15]

Los cuales utilizan diferentes tipos de Sistemas Operativos como; *Android*, iOS y/o Windows Phone. Entre los ataques destacados a estos dispositivos se encuentran las aplicaciones basadas en el requerimiento de permisos por parte de los usuarios, con los que logran controlar los mismos y generan cargos a las cuentas de las víctimas, ya que una vez que la aplicación se encuentra cargada en el dispositivo, se comienzan a enviar mensajes multimedia sin que el usuario se dé cuenta, sino que se percata de los cobros excesivos después de que el daño ya ha sido causado.

Los ataques a los dispositivos móviles están asociados a diferentes riesgos y vulnerabilidades que se pueden presentar con el uso de los dispositivos, en este sentido los tipos de ataques se pueden agrupar de diferentes formas y dependiendo del enfoque que se le desee dar a los ataques de los dispositivos móviles.

[15] Red y seguridad. (s.f.). Recuperado el 7 octubre de 2015, de http://redyseguridad.fip.unam.mx/proyectos/buenaspracticas/ataquesadispositivosmoviles.htmlInteligentes

2.3.1. TIPOS DE ATAQUES

Existen diferentes compañías y organizaciones que trabajan en el análisis de la seguridad, buscando los riesgos y vulnerabilidades que pueden encontrarse en los sistemas operativos móviles, los puntos de ataque para los dispositivos móviles más frecuentes a nivel nacional son:

- Las credenciales para tomar el control del dispositivo y los servicios externos del dispositivo como el correo electrónico, las cuentas de bancos.
- Los datos personales de los usuarios el nombre completo, la identificación, las claves, los datos del teléfono como los contactos, la localización, las preferencias de los usuarios.
- Los datos de los dispositivos como los números de cuenta, números de las tarjetas, las fechas de expiración.
- Acceso al dispositivo para revisar la SIM CARD del dispositivo, revisión de las conexiones telefónicas y de internet, uso del dispositivo para enviar virus, *malware* y procesamiento de actividades, robo de datos secretos y datos sensibles del dispositivo.
- Almacenamiento de datos robo, revisión y modificación de claves, información de las bases de datos, archivos de configuración, archivos de las aplicaciones, las cachés de los sistemas.
- Archivos binarios, realización de ingeniería inversa para entender el binario, búsqueda de las vulnerabilidades que pueden ser explotadas, incrustar credenciales y generación automática de claves.
- Plataformas móviles enganche de las plataformas, instalación de *malware*, aplicaciones móviles de ejecuciones automáticas no autorizadas, las decisiones de la arquitectura de aplicaciones basadas en la plataforma.
- El almacenamiento de datos, los archivos binarios y la plataforma no son independientes y se encuentran relacionados entre sí, esta es una debilidad en que puede llevar a la explotación de unos a otros, por que se conoce que es lo que está en funcionamiento.

- Modelo de amenaza si un atacante obtiene acceso físico a un dispositivo, aunque sea temporalmente, puede realizar un *Jailbreak* o liberación del dispositivo móvil, instalación aplicaciones, inserción de código malicioso, realización de copias de la información, modificaciones del sistemas, entre otras.

Los ataques que se pueden realizar a los dispositivos móviles y los sistemas operativos a través de programas dañinos o peligrosos como lo son:

- Troyanos: Aplicaciones y SMS.
- Gusanos.
- Programas Espías.
- Bombas de Tiempo.

Dichos ataques a los dispositivos móviles han provocado que se comiencen a ver como un mercado de oportunidad para el robo de información. Esto se debe a que ya comienzan a dejarse atrás las computadoras de la preferencia del consumidor.

2.3.2. RIESGOS EN LOS DISPOSITIVOS MÓVILES

En la actualidad en México existen 104 millones de líneas móviles y se estima que para este año un 50% de este total serán *Smartphone*, lo que significa que el otro 50% de las plataformas móviles podrían estar expuestas a muchos riesgos por *malware* ya que estos buscan el acceso a información personal del usuario, sin que él mismo sea consciente de ello (Campos, 2014).

2.3.3. TIPOS DE RIESGOS

Existen diferentes tipos de riesgos, esto depende del sistema operativo que utilicen los dispositivos móviles ya que cada uno presenta diferentes tipos de amenazas dentro de su sistema.

Como es sabido, hoy en día, *Android* es una de las plataformas para la cual más códigos maliciosos están apareciendo, explotando ciertas características presentes en la arquitectura del sistema y sus repositorios de aplicaciones.

Para la ejecución de las aplicaciones se necesita un conjunto de permisos, que se declaran en el *Android* Manifest.xml, *Android* asigna un User ID y un Group ID distinto a cada una de ellas. De esta manera, cada proceso se ejecuta de manera aislada ofreciendo un modelo de seguridad compacto y eficiente. Por lo cual el método de propagación de amenazas para esta plataforma suele ser a través de cuentas de desarrolladores falsas que publican aplicaciones maliciosas en Play Store o a través de repositorios de aplicaciones no oficiales por lo que se generan códigos maliciosos innovadores y avanzados que utilizan las funcionalidades del sistema operativo de Google para beneficio de los desarrolladores de códigos maliciosos. El Laboratorio de Análisis e Investigación de ESET Latinoamérica analizó 41 familias de códigos maliciosos de las cuales se detectaron[16]:

- Falsas soluciones de seguridad, que engañaban al usuario bajo la promesa de proteger el *Smartphone* cuando en realidad robaban información personal
- El 30% de las amenazas estuvieron disponibles para su descarga en Play Store.
- El 37% son troyanos SMS y el 60% de los códigos maliciosos tienen cierta característica de *botnets*, es decir, algún tipo de control remoto sobre el dispositivo.

2.4. VULNERABILIDAD EN DISPOSITIVOS MÓVILES

Como ya se ha mencionado, un *Smartphone* cuenta con capacidades similares al de una computadora, motivo por el cual es recomendable proteger la

[16] ESET Latinoamérica, Tendencias 2014: El desafío de la privacidad en Internet (s.f.). Recuperado el 7 octubre de 2015, de http://www.eset-la.com/pdf/tendencias_2014_el_desafio_de_la_privacidad_en_internet.pdf

información contenida en él de manera similar a los equipos de escritorios o notebooks.

En la seguridad de los dispositivos móviles existen una serie de consejos y buenas prácticas que los usuarios suelen tener en cuenta, sin embargo no son aplicados en el día a día, esto ante una posible vulnerabilidad, deja a muchos de ellos sin una clara respuesta sobre la seguridad en los *Smartphone*.

Una de las principales causas de falta de seguridad por parte de los usuarios es que no diferencian entre un teléfono móvil y un *Smartphone*, este último, es capaz de estar conectado las 24 horas del día, acceder a los correos electrónicos, las redes sociales o proveer al usuario las coordenadas en dónde está ubicado.

Los *Smartphone* suelen considerarse como productos de consumo, y por ello, la seguridad no está contemplada por muchos de los usuarios. Por lo cual al descargar aplicaciones para distintos fines se puede exponer la información contenida en el dispositivo.

2.4.1. TIPOS DE VULNERABILIDAD

Algunas vulnerabilidades de los *Smartphone* son las siguientes:

- El *Jailbreak*: es un proceso mediante el cual se desbloquean ciertas características de su dispositivo iOS para instalar extensiones al sistema operativo que añadan o mejoren ciertas funcionalidades.
- Liberar el dispositivo: es un proceso mediante el cual entra al sistema como súperusuario administrador o ROOT con esto se puede desbloquear su móvil para usarlo con cualquier compañía, sin problemas
- Instalar aplicaciones de fuentes no oficiales: La probabilidad del usuario de infectar su *Smartphone* con un código malicioso aumenta, además de que la mayoría de este tipo de aplicaciones suelen sustraer información del dispositivo que lo permite identificar de manera unívoca.

- Perder un *Smartphone*: El usuario tarda en darse cuenta que si no protegía su dispositivo, quien lo haya robado, o encontrado, cuenta con acceso a toda su información.
- No verificar aplicaciones instaladas: Siempre se debe verificar la calificación, comentarios e información sobre la aplicación antes de instalarla, ya que a veces las vulnerabilidades en el software instalado pueden llevar a la explotación de las mismas y qué se realice el robo de información de manera remota.
- Redes inalámbricas no seguras: El riesgo de conectarse a una red sin seguridad, y acceder a sitios como las redes sociales, el *Home Banking* o correos electrónicos se ve reflejado en que un atacante podría estar analizando el tráfico de la red y realizar el robo de las cookies de sesión, pudiendo acceder a las credenciales del usuario
- Envió de mensaje texto: Al usuario *Stagefright* por ejemplo, un video malicioso puede ser utilizado para enviar un programa que se pondrá en marcha al ser procesado por el teléfono. Una vez infiltrado en *Stagefright*, el código malicioso podría acceder a los datos y las aplicaciones guardados en su dispositivo.

2.5. *MALWARE* EN LOS DISPOSITIVOS MÓVILES

La tecnología se vuelve cada día más esencial en nuestras vidas, por lo que la mayoría de los dispositivos electrónicos que utilizamos requieren de una computadora para funcionar. Dependemos de dispositivos como portátil, celulares, *Tablet*, entre otros, para comunicarnos, trabajar y almacenar información que no podemos perder. Sin embargo, el aumento en el uso de estos dispositivos también significa que la cantidad de datos son vulnerables en la red, tanto de usuarios como de empresas, van creciendo significativamente.

Recientemente han aparecido otros *Gadgets* tecnológicos que ofrecen las mismas posibilidades que los últimos teléfonos móviles, pero sin la posibilidad de

realizar llamadas, se sitúan entre el teléfono móvil y las *Netbooks* y se les ha llamado *Tablets* o *Tablet*as electrónicas.

Los *Smartphone* y las *Tablets* han incorporado la complejidad del ordenador de uso personal, con las ventajas que esto conlleva. Sin embargo, este avance ha tenido como consecuencia efectos colaterales menos deseables, como son los problemas de seguridad y la creación de *malware* específico. La aparición de este tipo de código malicioso, entre otros factores, ha sido propiciada por la gran cantidad de datos personales y de valor que se almacenan en los teléfonos y *Tablet*as, constituyendo un valioso botín para los atacantes.

El *malware* para dispositivos móviles: está creciendo exponencialmente, ahora se tiene más de 1 millón de muestras maliciosas en las bases de datos, la mayoría del *malware* móvil tiene una estructura muy simple, sin embargo, está diseñado para robar efectivamente el dinero de la gente, no obstante, se está adaptando y evolucionando, incluyendo lentamente tácticas más engañosas y complejas para los usuarios objetivo.

Los *malware* siguen siendo un grave problema a pesar de los muchos intentos para detectarlos y evitarlos. Los creadores de *malware* Siguen desarrollando continuamente nuevos métodos para evadir las detecciones por medio de firmas, como el uso de la encriptación, empaquetamiento y la ofuscación. Se informan de un gran número de nuevos casos de *malware* cada día.

El problema más difícil es la forma de detectar de manera eficiente y eficaz los nuevos *malware*. De acuerdo con la compañía de antivirus, la mayor amenaza a la seguridad de esos datos confidenciales son los *malware*, debido a que son desarrollados con el objetivo de obtener dinero de forma ilegal, tales como fraudes, extorsiones, robo de identidad.

2.5.1. TIPOS DE *MALWARE*

Existen diferentes tipos de *malware*, los cuales son:

Primer tipo: Troyanos tradicionales.

Como su nombre indica, aquí se podría trasladar a *Android* el concepto de *malware* que se tiene en los sistemas operativos de escritorio. Dicho de otra forma, se traslada el concepto de lucro despiadado a través del robo de datos, suplantación de Apps bancaria. Resumiendo, que con una infección podemos perder toda nuestra información personal en manos de terceros que podrían sacar toda clase de provecho de ella: desde vaciar la cuenta bancaria hasta vender su información con fines de lucro.

Segundo tipo: Aplicaciones espía.

Están pensadas fundamentalmente para monitorizar las actividades de los usuarios, tanto la que va ligada a los terminales como la que no, ya que permiten el rastreo del dispositivo y de la persona que lo utiliza por geo-localización. Están diseñadas para aquellos que deseen espiar o infectar a alguien con un troyano, y entre las miles de aplicaciones prácticas que se les intentó buscar estuvo el control de menores. Normalmente Google las retira.

Tercer tipo: Réplicas falsas de aplicaciones legítimas.

Este tipo de *malware* intenta confundir al usuario. Lo que busca es o bien conseguir descargas y lucrarse con publicidad, o bien 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 mencionar unos ejemplos. Mientras que las guías legítimas o las aplicaciones de personalización suelen dejar bien claro lo que son en la imagen y descripción de la Apps, otros no se molestan en hacer una distinción, sino que se aprovechan de la confusión del usuario para infectarlo.

Cuarto tipo: Réplicas de aplicaciones funcionales y con *Adware*.

No sólo se trata de confundir al usuario, sino que reempaquetan la aplicación original con algunas variaciones en su código. Según dicen en ElevenPaths, después del último control de Google para eliminar el *malware* de la Play Store esto ocurre menos. Lo que hacen este tipo de réplicas es infectar mediante *Adware*, o lo que es lo mismo, cualquier programa que automáticamente muestra publicidad Web al usuario durante su instalación o durante su uso para generar lucro a sus autores.

Quinto tipo: Aplicaciones estafa.

Este tipo de *Fakeapp* se anda con menos sutilezas, ya que directamente busca estafar al usuario invitándole a pagar por servicios por los que no pagaría normalmente. Esto incluye suscripciones poco claras a servicios de mensajes Premium, incluso si necesitan confirmación. Esto significa que elude la confirmación por PIN de Google Play "respondiendo" automáticamente por el usuario, de forma que éste queda suscrito al servicio de mensajes de forma totalmente transparente para Google, aunque él no sabrá nada hasta que no empiecen a llegarle facturas muy abultadas.

Sexto tipo: Réplicas prácticamente exactas de aplicaciones legítimas.

Estas réplicas son simplemente *Adware*, no contienen la funcionalidad del software original que intenta suplantar. Son las *Fakeapp*s por excelencia. En todas ellas, el fabricante es inventado o el título remite a algo importante de la aplicación. Suelen tener pesos ridículos frente a los de las aplicaciones legítimas y sólo sirven para liberar el *Adware* en el terminal.

Por desgracia, este tipo de *malware* a veces no son detectadas por los programas de antivirus ya que requieren menos permisos que las aplicaciones originales de la Play Store, además que los usuarios no se percatan de un mensaje de texto puede contener un sistema profesionalización del *malware*.

2.6. AMENAZAS MÁS COMUNES EN *ANDROID*

Después de analizar las diferentes estadísticas mencionadas y los sitios que evalúan las amenazas en los dispositivos móviles, que se tratan lo largo de esta investigación, se pueden agrupar en varias categorías como troyanos (siendo los más destacados), módulos de publicidad y *Exploits* para obtener acceso de usuario administrador.

Entre las variantes de troyanos de *Android*, ESET Latinoamérica reporta la aparición de troyanos *Downloader*, los cuales buscan descargar otras amenazas desde Internet para posteriormente instalarla en el dispositivo; los troyanos *Dropper*, los cuales descargan otras amenazas que el propio troyano incluye dentro de su código; los troyanos *Clicker*, desarrollados para generar tráfico en un sitio o en un anuncio publicitario con el fin de aumentar el número de clics; y, por último, los troyanos bancarios, diseñados para buscar datos financieros específicos.

A continuación, se mencionan las amenazas más comunes que el usuario del Sistema Operativo *Android* se expone al hacer uso de Internet.

2.6.1. *ANDROID* LOCKER

Es un nuevo *Ransomware*, más peligroso que otros similares para esta plataforma como *Simplocker*, busca afectar a los usuarios bajo la apariencia de un falso antivirus. Este *malware* suele llegar a través de anuncios que aparecen a los usuarios en los que se indica que el dispositivo está infectado y que hay que descargar e instalar un fichero para poder desinfectarlo. También se han detectado casos en los que el *malware* suplanta la identidad de Flash Player, necesario para reproducir algún tipo de contenido en la red.

Entre las características de AndoridLocker se encuentran:

- Suplantación de conocidas soluciones de seguridad para ganarse la confianza del usuario y hacer que instale la aplicación maliciosa
- "Resistente" a los intentos de desinstalación del usuario.
- Cifrado de archivos en la memoria externa del dispositivo.
- Bloqueo de la ejecución de aplicaciones.
- Permanece activo tras un reinicio.

2.6.2. SUPLANTANDO APLICACIONES

Los ciberdelincuentes pretenden engañar al usuario *Android*, haciendo pasar la aplicación maliciosa por la de un instalador de Flash Player. No obstante, en las últimas variantes los creadores de esta amenaza han empezado a utilizar el nombre del antivirus Norton Internet Security para *Android*, algo que enlaza perfectamente con los falsos mensajes de alerta de virus que se muestran previamente a la descarga de esta falsa aplicación. *Android*Locker solicita permiso para convertirse en administrador del dispositivo y tomar así el control del sistema dificultando la desinstalación. Se puede pensar que, al llegar a este punto, se deben encender todas las alarmas puesto que este permiso solo lo solicitan aplicaciones muy específicas. Sin embargo, el hecho de suplantar una aplicación de seguridad que cuenta con buena reputación hace que no pocos usuarios confíen plenamente en ella y les den todos los permisos con tal de eliminar las falsas infecciones que tienen en sus dispositivos.

2.6.3. *ANDROID*/SPY.KRYSANEC

Troyano de acceso remoto, se hace pasar por varias aplicaciones legítimas para *Android*, entre ellas la aplicación de *MobileBank* (una aplicación móvil para realizar operaciones bancarias del banco ruso *Sberbank*), 3G *TrafficGuard* (una aplicación móvil para monitorear el uso de datos) y algunas otras, incluyendo la propia aplicación de seguridad ESET *Mobile Security*. Paradójicamente este troyano fue detectado por ESET. Una de las formas de infección más comunes del

malware para *Android* es porque se hace pasar por una aplicación móvil legítima que sea popular.

Los módulos le otorgan al *Backdoor* el acceso necesario al dispositivo para:

- Tomar fotografías.
- Grabar audio a través del micrófono.
- Obtener la ubicación actual por GPS.
- Obtener una lista de las aplicaciones instaladas.
- Obtener una lista de las páginas Web abiertas.
- Obtener una lista de las llamadas realizadas.
- Leer los SMS (comunes o de *WhatsApp*).

2.6.4. *SIMPLOCKER*

ESET ha analizado un troyano denominado *Android*/*Simplocker* que escanea la tarjeta SD de un dispositivo con *Android* en busca de ciertos tipos de archivos (.jpeg, .jpg, .png, .bmp, .gif, .pdf, .doc, .docx, .txt, .avi, .mkv, .3gp, .mp4), encripta estos archivos utilizando AES y exige el pago de un rescate para descifrarlos. Constituye el primer *malware* de la familia *Filecoder* destinado al sistema operativo de Google, y está activado en Tor. El resultado determina que hasta que el rescate sea pagado, los usuarios no podrán acceder a sus archivos personales (fotografías, descargas, canciones, etc.). Sin embargo, ESET *Mobile Security* para *Android*, ha desarrollado la aplicación ESET *Simplocker decrypter* que permite detectar y bloquear la aplicación maliciosa a la vez que permite recuperar los archivos.

2.6.5. EL VIRUS DE LA POLICÍA

El troyano conocido como “Virus de la Policía” afectó a cientos de usuarios en España, Europa y Latinoamérica, cuyas computadoras se bloqueaban al inicio

mostrando un supuesto mensaje del Cuerpo Nacional de Policía; con la excusa de haber detectado accesos a páginas de pornografía infantil, solicitaba cierta cantidad de dinero para desbloquear el equipo. Ahora, tras casos como *Filecoder* o *Multi Locker*, se han detectado nuevas variantes de *Ransomware* que tienen a dispositivos *Android* como objetivo.

En una de las últimas variantes, se puede observar cómo el acceso a una de las webs maliciosas con un dispositivo *Android* es redirigido a una web con contenido pornográfico que intentará descargar un fichero .apk (aplicación de *Android*) en el sistema. Al contrario de lo que sucede con las versiones de este *Ransomware* para sistemas Windows, aquí es necesario que el usuario acepte la instalación de la aplicación (y los permisos) para que este *malware* pueda activarse en el dispositivo. Esto quiere decir, que si el usuario detecta una actividad sospechosa al momento de que se solicite la instalación, la puede rechazar y evitar ser infectado.

2.6.6. ADULT PLAYER

Adult Player consiste en un reproductor de video con material pornográfico que trata de estafar al dueño del dispositivo móvil mediante un bloqueo. El *malware* se disfraza de una App conocida (*Facebook*, *Twitter*, *WhatsApp*), se instala y luego se apodera del sistema operativo, obteniendo acceso de súper usuario (root), la aplicación solicita instalar un módulo extra donde se encuentra el *malware*[17].

Una vez instalado el módulo adicional, permite que la App maneje la cámara frontal de su dispositivo para tomar una selfie. Momentos después de la fotografía le llegará un supuesto mensaje del FBI en el que se indica que el dispositivo ha sido bloqueado por seguridad y solicita un pago de 500 dólares; sin embargo, lo

[17] Informador. (08/SEP/2015). Recuperado el 22 septiembre de 2015, de http://www.informador.com.mx/tecnologia/2015/613400/6/nuevo-virus-ataca-a-Android.htm

único que se debe hacer es reiniciar el dispositivo en modo a prueba de fallos y desde ahí se podrán retirar los permisos de Adult Player.

El virus fue encontrado en más de 20 mil aplicaciones de tiendas de terceros (no en Play Store) y afecta a países como México, Estados Unidos, Brasil, Jamaica, Rusia, Alemania, Irán, Sudán e Indonesia. Los investigadores catalogaron al virus en tres familias, dado al parecido en el código que poseen entre sí: Shuanet, Kemoge y Shedun.

La única solución a este nuevo *malware* es flashear el celular de nuevo (instalar una ROM nueva). Algo que sólo lo podría hacer un experto o el fabricante del equipo. Los usuarios comunes sólo tienen una opción: cambiar de equipo.

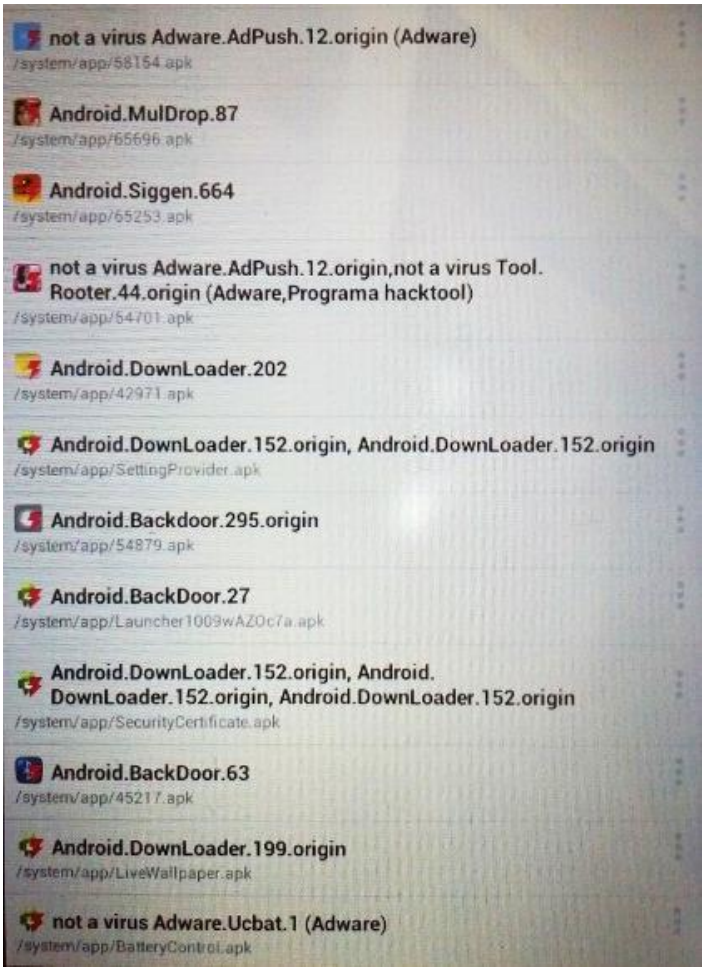


Ilustración 16. Muestra del Virus Adult Player en un DM

3. UNIDAD III. INTERFÁZ DE COMUNICACIÓN

3.1. INTRODUCCIÓN A LA INTERFÁZ DE COMUNICACIÓN

Es tal la importancia que han adquirido los Dispositivos Móviles que parece que fuera imposible el desarrollo de cualquier actividad sin la utilización de los mismos. Se han hecho imprescindibles tanto en el ámbito de las comunicaciones personales como en el entorno empresarial; así lo demuestra el dato, bastante significativo, que en el primer semestre de 2015, existen en el mundo más de 7300 millones de líneas móviles activas (Rivero, 2015), superando considerablemente a la población (la población mundial es de 7250 millones de personas).

Las comunicaciones inalámbricas constituyen la base de la conexión de los dispositivos móviles que, soportadas por distintas tecnologías, utilizan como medio de comunicación el aire y quedan expuestas a vulnerabilidades y riesgos de seguridad. En estos momentos las tecnologías inalámbricas disponibles son WiFi (Wireless Fidelity) que permite el acceso a Internet sin consumir ancho de banda, GSM (Global System for Mobile communications), *Bluetooth* para conexiones entre dispositivos móviles o con otros dispositivos fijos. NFC (Near Field Comunication), utilizada para comunicaciones de corta distancia y con aplicaciones para pagos a través del móvil., GPRS (General Packet Radio Services), de segunda generación (2G), EDGE (Enhanced Data Rate for GSM Evolution) puente entre 2G y 3G, UMTS (Universal Mobile Telecommunications System) 3G y LTE (Long Term Evolution) de 4G para acceso a Internet, llamadas telefónicas y tráfico de mensajes SMS.

Actualmente, la gran mayoría de los dispositivos móviles inteligentes poseen la capacidad de conectarse a Internet. Esto suele hacerse mediante una conexión directa de datos (GPRS o 3G) a través de las redes de un operador móvil o mediante la conexión a una red de área local que proporciona acceso a Internet (WiFi).

3.2. WLAN WiFi

Ilustración 17. WLAN WiFi

WiFi es una de las tecnologías de comunicación inalámbrica mediante ondas más utilizada hoy en día, también llamada WLAN (Wireless Lan, red inalámbrica) o estándar IEEE 802.11. WiFi no es una abreviatura de Wireless Fidelity, simplemente es un nombre comercial. WLAN es una de las áreas de más rápido crecimiento de las tecnologías inalámbricas debido a su flexibilidad y a la velocidad en transferencia de datos.

Muchas WLAN están basadas sobre las tecnologías de espectro ensanchado y la conectividad a redes cableadas es suministrada a través de un Punto de Acceso que puede ser conectado a una LAN cableada o a cualquier tipo de red para acceder a Internet o a bases de datos corporativas.

Los dispositivos móviles se conectan al AP cuando ellos están dentro del rango (una celda que puede expandirse de 10 a 100 metros). Una vez conectado al AP, el dispositivo móvil puede comunicarse con otros dispositivos en la celda u otros recursos a través del AP.

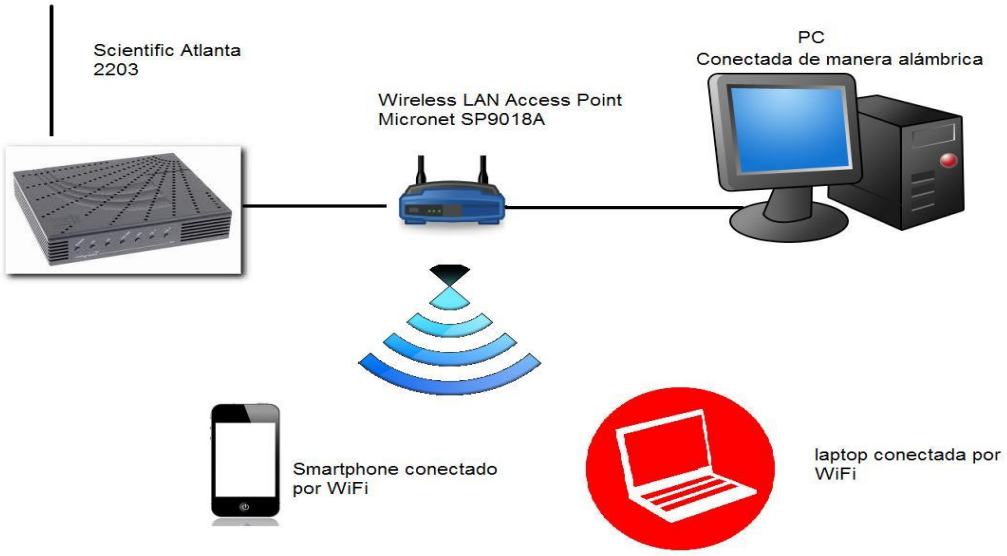


Ilustración 18 Configuración WLAN

Muestra una simple configuración WLAN. Cada dispositivo móvil en la WLAN tiene un adaptador WLAN que opera en ciertos rangos de frecuencia. La conectividad a redes cableadas es suministrada a través de un AP.

El estándar 802.11b es muy popular, aunque 802.11g está ganando terreno. 802.11b conocido como WiFi soporta velocidades de hasta 11 Mbps. Las LAN IEEE 802.11b operan muy similar a las redes cableadas

3.2.1. PRINCIPALES AMENAZAS WiFi

Son muchas las amenazas a las que el usuario del dispositivo móvil está expuesto al adherirse a una red WiFi, por lo cual mencionaremos algunas de ellas, para evitar caer en ellas.

Tabla 14. Principales Amenazas

Puntos de acceso piratas	Dispositivos que se hacen pasar por puntos "legales". En general se implementan con un simple ordenador con una tarjeta WiFi en modo "master" capaz de actuar como un punto de acceso a todos los niveles. A partir de aquí, todo el tráfico de los equipos que se conecten pasará por él, pudiendo tanto realizar ataques "*man in the Middle*" como accesos no autorizados al equipo conectado.
Intercepción de datos	Es la práctica que consiste en escuchar las transmisiones de varios usuarios de una red inalámbrica.
Redes públicas o abiertas	En éstas se puede estar navegando en la misma red que un usuario malicioso. El atacante puede analizar, con mucha facilidad, los paquetes que viajan en la red y así obtener contraseñas o instalar software malicioso en el ordenador de un usuario conectado.

3.2.2. MEDIDAS DE PROTECCIÓN WiFi

Usar conexiones cifradas: Algo que Google ofrece por defecto cuando estamos identificados en sus servicios y hacen que Gmail, Google+ o Google Calendar se sirvan bajo https. *Twitter* también aprendió la lección y ahora ofrece el servicio bajo SSL también y, en el caso de *Facebook*, es algo que se tiene que activar por el usuario a través de las opciones de configuración de una cuenta.

Métodos de control de acceso: Las características de medio compartido y accesibilidad de las redes WiFi hacen del sistema de control de acceso una pieza fundamental de los sistemas WLAN, aunque muchas veces por facilidad de instalación, por evitar problemas de gestión o bien por evitar tener que dar un soporte extra a los usuarios, se instalan puntos de acceso WiFi sin ningún método de autenticación.

Los objetivos principales de estos métodos son:

- Máxima efectividad en el control de acceso a la WiFi,
- Seguridad de cara a la transmisión de credenciales de los usuarios, y
- Por último sencillez y facilidad de uso.

Filtrado por MAC: Este método de control de acceso está muy extendido por su facilidad de configuración. Se basa en realizar dicho control mediante la comprobación de la dirección MAC de nivel 2. Su implantación es muy sencilla, ya que sólo se necesita declarar bien en el punto de acceso, bien en un servidor aparte, las direcciones MAC que están autorizadas para conectarse a la WLAN. Esta dirección MAC debe ser única par a cada uno de los dispositivos conectados a la LAN y viene predefinida de fábrica para todos ellos.

Clave WEP compartida: Es otro de los métodos más común utilizado hoy en día y consiste en utilizar una clave WEP en la red WiFi que sólo conocen los clientes autorizados. Efectivamente, es un método que reduce la carga de gestión respecto al método anterior, no hay que tocar la configuración cada vez que hay un cliente nuevo, sino que basta con darle la clave a utilizar. Esta facilidad introduce una clara debilidad y es que muchos clientes llegan a conocer la clave WEP, incluso clientes itinerantes que alguna vez necesitaron conexión y se les proporcionó la clave WEP y nunca más se cambió, ya que cada vez que ésta se actualiza hay que avisar a todos los clientes de que hay una clave nueva y que tienen que cambiarla.

802.1X: Es un estándar de control de acceso a nivel de acceso al medio (nivel 2), con lo que a diferencia de otros sistemas, en este caso el cliente no tiene una conexión efectiva con acceso al medio hasta que no se haya autenticado satisfactoriamente.

3.3. SMS

El servicio de mensajes cortos o servicio de mensajes simples, más conocido como SMS (por las siglas del inglés Short Message Service), es un servicio

disponible en los dispositivos móviles que permiten el envío de mensajes cortos, conocidos como mensajes de texto.

El SMS se diseñó originalmente como parte del estándar GSM de telefonía móvil digital, y actualmente está disponible en una amplia variedad de redes, incluidas las redes 4G. El SMS sirve para teléfonos fijos y otros dispositivos de mano.

Un mensaje SMS es una cadena alfanumérica de hasta 140 caracteres o de 160 caracteres de 7 bits, y cuyo encapsulado incluye una serie de parámetros. En principio, se emplean para enviar y recibir mensajes de texto normal, pero existen extensiones del protocolo básico que permiten incluir otros tipos de contenido, dar formato a los mensajes o encadenar varios mensajes de texto para permitir mayor longitud (formatos de SMS con imagen de Nokia, tonos IMY de Ericsson, estándar EMS para dar formato al texto e incluir imágenes y sonidos de pequeño tamaño).

En GSM existen varios tipos de mensajes de texto: mensajes de texto "puros", mensajes de configuración (que contienen los parámetros de conexión para otros servicios, como WAP o MMS), mensajes WAP Push, notificaciones de mensajes MMS.

3.3.1. PRINCIPALES AMENAZAS SMS

El *Spam* de mensajes de texto es una amenaza triple.

- Suele usar la promesa de regalos gratis, como computadoras o tarjetas de regalo, u ofrecimientos de productos tales como hipotecas baratas, tarjetas de crédito o servicios de alivio de deuda para lograr que usted revele información personal. Si usted quiere reclamar su regalo o aceptar un ofrecimiento, puede que tenga que compartir información personal, por ejemplo, cuánto gana, cuánto debe, o los datos de su cuenta bancaria, número de tarjeta de crédito o de su Seguro Social. Hacer clic sobre el enlace del mensaje puede instalar un programa malicioso que recolecta información de su dispositivo. Una vez que el "*Spam*mer" consigue su

información, se la vende a comerciantes, o lo que es peor, a ladrones de identidad.

- Puede originar cargos no deseados en la factura de su dispositivo. Su proveedor de servicio de telefonía celular puede cobrarle simplemente por la recepción de un mensaje de texto, sin importar si usted lo solicitó.
- Puede reducir la velocidad de su dispositivo ocupando espacio en la memoria del mismo.

***El Dorkbot* y el troyano *SMS Boxer*.**

El ataque comienza con un e-mail supuestamente proveniente de una compañía de telefonía móvil, en el que se le informa al destinatario que ha resultado ganador de un iPhone 4. El mensaje incluye un saludo personalizado y solicita el ingreso a un sitio para reclamar la recompensa. Sin embargo, al acceder a dicho sitio el usuario ingresa a una página en la que se le indica que para obtener el premio debe descargar un “software de comprobación”, que en realidad es un archivo ejecutable que contiene la amenaza.

3.3.2. MEDIDAS DE PROTECCIÓN SMS

- Elimine todos los mensajes de texto que le pidan que confirme o dé información personal. las compañías legítimas no piden números de cuenta, contraseñas ni otra información por email ni por mensaje de texto.
- No responda ni haga clic en los enlaces de los mensajes: los enlaces pueden instalar programas maliciosos en su computadora y pueden dirigirlo a sitios de imitación que parecen verdaderos pero cuyo propósito es robarle su información.
- Trate su información personal como si fuera dinero en efectivo: su número de Seguro Social, número de tarjeta de crédito y los números de cuentas bancarias y servicios públicos se pueden usar para robarle dinero o para abrir

nuevas cuentas a su nombre. No de ninguno de esos datos en respuesta a un mensaje de texto.

- Inscriba el número de su teléfono en el Registro Nacional No Llame.
- Revise la factura de su dispositivo para controlar si hay cargos no autorizados y si encuentra alguno, repórtelo a su proveedor.

3.4. BLUETOOTH

Se trata de un protocolo, orientado principalmente al intercambio de datos entre dos dispositivos, muy popular antes de que se extendiera el uso de WiFi e Internet en los terminales móviles.

Bluetooth es una tecnología de conectividad inalámbrica de corto alcance que, por sus características de transmisión, se convierte en una buena opción para interconectar pequeños dispositivos. Su facilidad de uso, capacidad de transmisión y costo han provocado que su despliegue resulte espectacularmente rápido y extenso, ampliando las posibilidades de conectividad personal en cualquier lugar. En la actualidad, es raro encontrar una nueva computadora portátil, agenda de mano o teléfono móvil que no disponga de este tipo de conexión, y su uso se ha extendido a otros elementos como altavoces, manos libres, conexión a redes, dispositivos de almacenamiento y otros. Tanto es así, que la evolución de esta tecnología se plantea para sustituir a las sufridas conexiones USB.

Sin embargo, como siempre ocurre con las tecnologías emergentes, se ha puesto todo el énfasis en la sencillez de uso y posibilidades de conexión dejando de lado otros aspectos no menos importantes de las transmisiones actuales y que preocupan a los usuarios, como es la seguridad. Algunos ataques sobre estas conexiones, la publicación de algunas vulnerabilidades y la difusión de procedimientos para atacar dispositivos móviles han sembrado la duda sobre los beneficios de esta tecnología.

3.4.1. PRINCIPALES AMENAZAS *BLUETOOTH*

Todos conocemos y hacemos uso de las bondades que aporta la conexión *Bluetooth* a nuestros dispositivos, como facilitar las comunicaciones entre equipos móviles y fijos; eliminar los cables y conectores entre éstos; y ofrecer la posibilidad de crear pequeñas redes inalámbricas y facilitar la sincronización de datos entre equipos personales.

El *Bluetooth* ha sido vulnerable ante posibles amenazas desde que hizo su aparición. El primer *malware* que atacó este sistema fue el gusano Cabir, el primer gusano inalámbrico de la historia. Se transmitía a teléfonos móviles usando la plataforma Symbian, cuando estos se encendían y activaban el modo visible. Sin embargo, los efectos no eran realmente dañinos; enviaba un mensaje con un archivo caribe.ss adjunto y una vez se descargaba el archivo se mostraba la palabra “Caribe” en la pantalla.

Tabla 15. Amenazas por Bluetooth

Bluejacking es *Spam*.	A través de esta técnica se envían mensajes (por ejemplo, una tarjeta de visita virtual) a usuarios en un radio de 10 metros; al descargarse dicha tarjeta, ésta añade el contacto en la agenda ya infectada. Este contacto, además, puede enviar mensajes al dispositivo atacado.
Car *Whisperer*	Es un software que permite a los atacantes capturar el audio de los coches que dispongan de un dispositivo manos libres. Este método permite al ciberdelincuente escuchar las conversaciones y llamadas que quiera.
Bluebugging	Es más peligroso que los dos anteriores. Este ataque permite tener acceso remoto al teléfono del usuario y utilizar sus funciones: escucha de llamadas, envío de mensajes. Además, todo esto sucede sin que el dueño del teléfono se percate. Esto puede suponer una factura mayor de lo habitual, sobre todo si se ha utilizado el *bluebugging* para realizar llamadas internacionales

3.4.2. MEDIDAS DE PROTECCIÓN *BLUETOOTH*

Cuando se establece la conexión *Bluetooth*, el dispositivo que actúa como maestro establece un patrón de saltos, de forma Pseudo aleatoria, que se utilizará durante la comunicación y que seguirán aquellos dispositivos que actúan como esclavos, una vez que hayan recibido dicha secuencia, mediante un paquete específico denominado FHS (Sincronización de Salto de Frecuencia).

El intercambio de paquetes entre dispositivos se produce de acuerdo a esta secuencia preestablecida, de forma que en cada instante de tiempo, cada dispositivo envía o recibe paquetes en un determinado canal.

Seguridad para *Bluetooth*:

1. Activar *Bluetooth* sólo cuando se vaya a utilizar.
2. Asignar un nombre al dispositivo que no refleje marca ni modelo.
3. Configurar el dispositivo para que no resulte visible para otros dispositivos.
4. Revisar periódicamente la lista de dispositivos de confianza registrados.
5. Utilizar claves de emparejamiento con al menos 5 caracteres.
6. Requerir autentificación en cualquier intento de acceso.
7. No aceptar conexiones ni transferencias no solicitadas.
8. Utilizar cuando sea posible cifrado en las transmisiones.
9. Mantener actualizado el software del dispositivo de mano.
10. Utilizar siempre que sea posible el bloqueo del dispositivo por clave.
11. Evitar guardar en los dispositivos de mano archivos “delicados”.

3.5. RED 2G/3G

La telefonía celular simplemente nace y se desarrolla de la necesidad que tiene el ser humano de comunicarse, por lo cual ha tenido una gran evolución en la telefonía.

Primera generación (1G)

En 1981, las compañías de telefonía móvil necesitaban algún estándar para que los teléfonos móviles pudiesen comunicarse entre ellos y de ahí surgieron la tecnología 1G, la cual solo soportaba llamadas de voz pero nada de tráfico de datos. Hoy en día, está en desuso.

Segunda generación (2G)

Se presentó en el año 1992 y supuso un salto de la telefonía móvil analógica a una totalmente digital. Es una tecnología que aún se utiliza a día de hoy y es conocida comúnmente como GSM. Con el 2G se pudieron empezar a transmitir datos y mandar los primeros mensajes de texto o SMS.

También se creó el GPRS que puede ofrecer unas velocidades de hasta 250Kbps, en zonas con mejores condiciones. En zonas rurales, donde las torres de telefonía están muy alejadas la velocidad puede bajar hasta los 20Kbps. Para mejorar este rendimiento podríamos necesitar un amplificador GSM. Este estándar es adecuado para utilizar datos móviles con aplicaciones de mensajería, como *WhatsApp*, o leer e-mails.

Tercera generación (3G)

En el año 2000 supuso un nuevo salto cualitativo en las comunicaciones móviles. La demanda de tasas de transmisión de datos crecía de forma constante y esto obligó a las compañías a seguir mejorar el servicio. Con el 3G se pudo empezar a navegar por Internet de forma fluida e incluso ver vídeos online (YouTube, Vimeo, entre otras). Actualmente, la velocidad máxima que se puede conseguir es de hasta 20Mbps.

La frecuencia más usada para 3G es 2100MHz. El problema de esta banda es que no se propaga tan bien a través del aire y las paredes como las banda utilizadas para el 2G. Esto significa que las operadoras tenían que instalar un número mayor de estaciones base de telefonía 3G para poder dar servicio a la misma cantidad de población.

Cuarta generación (LTE)

2013 fue el año del lanzamiento definitivo de la tecnología LTE, comúnmente conocida como 4G. Actualmente está en una fase de despliegue en Europa y aunque la cobertura disponible no se acerca a la de 3G, sí que la inmensa mayoría de capitales ya tienen 4G. A día de hoy, la velocidad de transmisión real de estos servicios no mejora de forma ostensible el rendimiento de la cobertura 3G pero se espera que en los próximos años esté por encima de los 50Mbps.

Las llamadas de teléfono se gestionan mediante una variante del 4G, denominada VoLTE. Esta extensión permite manejar las llamadas de manera mucho más eficaz y con una calidad de sonido mayor. Es importante recordar que solo con *Smartphone* 4G se puede tener acceso a la red 4G.[18]

3.5.1. PRINCIPALES AMENAZAS RED 2G/3G

La funcionalidad de SMS (Servicio de mensajes cortos) de los dispositivos móviles permite el envío de mensajes cortos empleando la infraestructura GSM (Sistema Global para Comunicaciones Móviles, o 2G) empleada para las comunicaciones de voz de la telefonía móvil (mediante conmutación de circuitos).

El módulo SMS también puede gestionar datos binarios, como tonos de llamada, y ficheros multimedia (audio, vídeo e imágenes), sobre todo en sus variantes avanzadas: EMS (Servicio de mensajería mejorado) y MMS (Servicio de mensajes multimedia).

En el caso de dispositivos basados en *Android*, iPhone y Windows Mobile, durante el año 2009 se publicaron vulnerabilidades de denegación de servicio, y en algunos casos, de transferencia de ficheros y ejecución de código sin la intervención del usuario. Como los son:

- Enviar un mensaje SMS malicioso y provocar una denegación de servicio en el dispositivo víctima, o incluso tomar control del mismo mediante la ejecución remota de código.

[18]La cueva GSM (s.f.). Recuperado el 11 octubre de 2015, de http://www.lacuevagsm.com/cobertura-movil-2/diferencia-entre-2g-3g-y-4g/

- Ausencia de medidas de seguridad en los mensajes administrativos intercambiados entre la infraestructura del operador de telefonía móvil y los dispositivos de los usuarios, como por ejemplo las notificaciones de mensajes en el buzón de voz, permitiendo a un atacante generar mensajes falsos de este tipo.
- El troyano Ambler, combinaba el uso de SMS, con el acceso a Internet de los DM y la ingeniería social, instando al usuario a visitar una página web a través de la cual se pretendía infectar a la víctima.
- Ataques activos basados en la suplantación de la propia red de telefonía móvil, se basa en suplantar una celda GSM empleando tecnologías 2G, ya que en éstas la autentificación se realiza en un solo sentido, es decir, desde la tarjeta SIM del terminal hacia la red. GSM (o 2G), las terminales se conectan automáticamente, sin ninguna intervención por parte del usuario, a la celda que ofrece mayor intensidad de señal, lo que permite a un atacante posicionarse como la celda preferente para los DM cercanos.
- Las tecnologías de UMTS (Sistema universal de telecomunicaciones móviles, o 3G) permiten a los dispositivos móviles disponer de conexiones de datos de banda ancha casi permanentes las 24 horas del día.
- La 2G permite el establecimiento de comunicaciones de datos casi permanentes las 24 horas del día mediante los estándares GPRS (paquete general de Radio servicio, conocido como 2.5G) y EDGE (Velocidades de datos mejoradas para GSM Evolución, conocido como 2.75G), empleados por estaciones base sin capacidades UMTS (3G) Las comunicaciones de datos a través de GPRS y EDGE emplean los estándares TCP/IP, por lo que los dispositivos móviles están expuestos a todas las amenazas de seguridad existentes en estos entornos y redes.[19]

El impacto de este tipo de vulnerabilidades en tecnologías de comunicación tan extendidas como SMS es enorme, ya que la funcionalidad SMS está siempre activa en los DM.

[19] mayo de 2013, Raúl Siles, fundador y analista de seguridad de Taddong S.L.

Potencialmente es posible atacar cualquier dispositivo móvil vulnerable a nivel mundial con sólo conocer su número de teléfono, y existen notables carencias en los mecanismos de protección y software de seguridad específico para tráfico SMS.

Los dispositivos móviles se conectan a través de la red 2G cuando la red 3G no está disponible (por falta de cobertura o por un ataque de denegación de servicio que sature la señal en el rango de frecuencias empleado), viéndose expuestos a los ataques de suplantación de la red y captura de tráfico mencionados se debe tener en cuenta que muchos operadores y proveedores de telefonía móvil emplean la misma clave pre-compartida entre el DM del usuario y la red tanto para las comunicaciones 2G como 3G. Por tanto, si el dispositivo hace uso de ambas redes, y un atacante obtiene la clave mediante los ataques descritos sobre 2G, también podrá descifrar el tráfico de 3G.

En 3G, no se conocen vulnerabilidades asociadas a este tipo de tecnología, aunque debe tenerse en cuenta que cualquier intercambio de información se basa en la confianza que el usuario tiene en el proveedor de telefonía móvil, encargado de cursar todo el tráfico desde y hacia el dispositivo a través de su infraestructura de red.

3.5.2. MEDIDAS DE PROTECCIÓN RED 2G/3G

Se aconseja que se tenga ciertas medidas de seguridad para evitar algún tipo de ataque en la comunicación de telefonía móvil. Algunas de ellas son:

- La funcionalidad de conexión a redes de datos de telefonía móvil (GPRS, EDGE, o UMTS) debe ser deshabilitada cuando no se requiere establecer una conexión mediante estas tecnologías.
- Para proteger la confidencialidad de las comunicaciones y llamadas de voz sobre redes no fiables existe software de cifrado extremo a extremo, como el proporcionado por *Cellcrypt* (para Symbian y BlackBerry), *Sigillu*

(multiplataforma). Las comunicaciones de voz cifradas pueden ser cursadas sobre cualquier red de datos: 2.5G, 3G, 3.5G y WiFi.

- La mayoría de los ataques es por mensaje de texto SMS por lo que se recomienda no abrir ningún mensaje de texto no esperado o solicitado, práctica similar a la empleada para la gestión de correos electrónicos en equipos portátiles y de sobremesa, o dispositivos móviles.
- Debido a las numerosas vulnerabilidades existentes en los protocolos y estándares de comunicaciones móviles englobados bajo las tecnologías 2G, se recomienda utilizar únicamente las tecnologías de comunicación móviles 3G

3.6. NFC (NEAR FIELD COMMUNICATION)

NFC es una tecnología inalámbrica de corto alcance que permite una interconexión entre dispositivos electrónicos de una manera intuitiva, sencilla y simple, NFC opera en la frecuencia de 13.56 MHz, banda que no necesita de ninguna licencia administrativa para transmitir, y que permite la operación a una distancia inferior a 10 centímetros con velocidades de transmisión de 106 Kbit/s, 212 Kbit/s y 424 Kbit/s.

La comunicación se produce cuando dos dispositivos NFC están próximos entre sí, por lo que la comunicación es inherentemente segura debido al corto alcance de la transmisión, lo que dificulta cualquier captura de la señal por otro dispositivo ajeno a la comunicación[20]. La tecnología NFC es una extensión del estándar ISO/IEC-14443 para tarjetas de proximidad sin contactos que combina la interface de una tarjeta inteligente y un lector en un único dispositivo, lo que lo hace compatible con toda la infraestructura de pago sin contactos y de transporte existente actualmente.

[20]Taringa, (s.f.). Recuperado el 20 octubre de 2015, de http://www.taringa.net/post/info/4612231/Tecnologia-NFC

Se puede utilizar para diferentes actividades como:

- Transferir fotos, vídeo o música
- Identificación y control del coche
- Cajeros automáticos 2.0
- Compras más allá de los códigos QR
- Identificación en eventos
- Pagos móviles

Ilustración 19. NFC (Near Field Communication)

3.6.1. PRINCIPALES AMENAZAS NFC

Nuevas tecnologías inalámbricas, como NFC (Near Field Communication) aparecieron desde el año 2010 en el mundo de los dispositivos móviles para convertirlos en medios de pago habituales.

Esto conlleva a diversas amenazas como lo son:

- La tecnología NFC emplea un rango de radio frecuencia no licenciado, concretamente, 13,56 MHz. NFC establece comunicaciones de corto alcance (unos pocos centímetros) con un ancho de banda de hasta 424 Kbps.

- NFC permite almacenar los datos de una tarjeta de crédito en la tarjeta SIM del terminal móvil, habilitando la realización de pagos en tiendas sin disponer de tarjeta de débito o crédito, o dinero en efectivo, tras introducir el comerciante el importe de la transacción en el DM punto de venta compatible NFC, el pago se realiza cuando el usuario aproxima su dispositivo móvil a dicho terminal.
- La aplicación llamada “Punto BIP”, permitía cargar crédito con simplemente un par de clics, esta aplicación daba la posibilidad de cargar una suma importante de dinero a la cuenta ligada a la tarjeta de transporte e inclusive cambiar su número para aprovechar el saldo de otra persona o evitar que esta sea bloqueada.
- El robo de información podría ocurrir en el momento en que el usuario realiza el pago, como también en el mismo dispositivo que implementa dicha tecnología.

3.6.2. MEDIDAS DE PROTECCIÓN NFC

Se aconseja que se tenga ciertas medidas de seguridad para evitar algún tipo de ataque:

- Al realizar pagos por medio de NFC la tarjeta guarda información en la SIM, por lo que si se extravía o roban el teléfono móvil pueden tener acceso a este tipo de información, se recomienda hacer limpieza constantemente de la información almacenada para evitar el almacenamiento de información en el dispositivo.
- Es fundamental que tanto los datos de pagos almacenados en el equipo como la transmisión de información que ocurre al momento de pagar, cuenten con un mecanismo de cifrado robusto.

4. CAPÍTULO IV. PRÁCTICAS DE SEGURIDAD CASO DE ESTUDIO

4.1. CASO DE ESTUDIO CON BASE A ENCUESTAS

Aplicamos una Encuesta formulada con 22 preguntas, se llevó acabo en el Centro Universitario, UAEM Texcoco; con el grupo: LCN055C, de la Licenciatura en Contabilidad, turno Vespertino en la asignatura de Mercados Financieros impartida por el M. en C. Juan Manuel Muñoz Araujo, integrado por 38 alumnos de edades entre 18 a 40 años respectivamente, de los cuáles 30 alumnos fueron seleccionados para dicha encuesta, para así obtener una mejor información acerca del proyecto de Tesis, titulado: “Análisis de la vulnerabilidad en las aplicaciones *Android* de los dispositivos móviles”, de los cuales obtuvimos los siguientes resultados, no sin antes mostrar la encuesta aplicada.

PROYECTO DE TESIS "ANÁLISIS DE LA VULNERABILIDAD EN LAS APLICACIONES ANDROID DE LOS DISPOSITIVOS MÓVILES"

LICENCIATURA EN INFORMÁTICA ADMINISTRATIVA

Encuesta

1. ¿CUENTAS CON ALGÚN DISPOSITIVO MÓVIL?
   A) SI B) NO
2. ¿QUÉ TIPO DE DISPOSITIVO MÓVIL TIENES?
   A) TELÉFONO MÓVIL B) SMARTPHONE C) TABLET D) OTRO
3. ¿CON QUÉ SISTEMA OPERATIVO MÓVIL CUENTA TU DISPOSITIVO MÓVIL?
   A) ANDROID B) iOS C) WINDOWS PHONE D) OTRO
4. ¿DISPONES DE ALGUNA CONEXIÓN A INTERNET EN TU DISPOSITIVO MÓVIL?
   A) SI B) NO
5. RESPECTO A LA CONEXIÓN A INTERNET, ¿A TRAVÉS DE QUÉ FORMA LO HACES?
   A) CONEXIÓN WIFI B) CONEXIÓN DE DATOS
6. ¿CON QUE FRECUENCIA CONECTAS TU DIPOSITIVO MÓVIL A UNA RED?
   A) SIEMPRE B) ALGUNAS VECES C) CASI NUNCA D) NUNCA
7. RESPECTO A LA CONEXIÓN WiFi ¿TE HAS CONECTADO A ALGUNA RED PÚBLICA O ABIERTA?
   A) SI B) NO
8. ¿ESTÁS CONSCIENTE QUE AL CONECTAR TU DISPOSITIVO MÓVIL A UNA RED PÚBLICA O ABIERTA PUEDE SER MÁS SUSCEPTIBLE A ALGÚN ATAQUE DE MALWARE O VIRUS?
   A) SI B) NO C) NO TENGO IDEA
9. ¿TU DISPOSITIVO MÓVIL DISPONE DE CONEXIÓN BLUETOOHT?
   A) SI B) NO
10. ¿TIENES SIEMPRE ACTIVADA TU CONEXIÓN BLUETOOH?
    A) SIEMPRE B) ALGUNAS VECES C) CASI NUNCA D) NUNCA
11. ¿ACTIVAS TU CONEXIÓN BLUETOOHT PARA RECIBIR ARCHIVOS?
    A) SI B) NO
12. RESPECTO A LA CONEXIÓN SMS ¿HAS RECIBIDO MENSAJES DE NÚMEROS DESCONOCIDOS O PUBLICITARIOS CON LINKS DE DESCARGA?
    A) SI B) NO
13. ¿HAS LEÍDO EL CONTENIDO DE ÉSTOS MENSAJES PUBLICITARIOS?
    A) SI B) NO
14. ¿DESCARGAS APLICACIONES DIRECTAMENTE DE LA TIENDA DE TU DISPOSITIVO MÓVIL? (Play Store, App Store, Windows S.)
    A) SI B) NO
15. ¿POR LO REGULAR, CON QUÉ FRECUENCIA DESCARGAS APLICACIONES GRATUITAS O DE PAGO?
    A) SIEMPRE B) ALGUNAS VECES C) CASI NUNCA D) NUNCA
16. POR LO GENERAL, ¿QUÉ TIPO DE APLICACIONES DESCARGAS?
    A) ENTRETENIMIENTO B) SOCIALES C) PRODUCTIVIDAD D) NOTICIAS
17. ¿HAS INSTALADO APLICACIONES DE ORÍGENES DESCONOCIDOS EN TU DISPOSITIVO MÓVIL?
    A) SI B) NO
18. ¿CREES HABER INFECTADO TU SMARTPHONE POR VIRUS CON ALGUNA APLICACIÓN DESCARGADA?
    A) SI B) NO
19. ¿QUÉ ACCIONES HAS TOMADO ANTE ÉSTAS AMENAZAS DE MALWARE?
    _____
20. ¿PRESTAS ATENCIÓN A LA SEGURIDAD DE LA INFORMACIÓN QUE TIENES ALMACENADA EN TUS DISPOSITIVO MÓVIL?
    A) SI B) NO
21. ¿HACES USO DE ALGÚN ANTIVIRUS PARA TU DISPOSITIVO MÓVIL? (En caso de que la respuesta sea NO saltar la preg. 18)
    A) SI B) NO
22. ¿QUÉ APLICACIÓN DE ANTIVIRUS TIENES INSTALADO EN TUS DISPOSITIVO MÓVIL?

Ilustración 20. Muestra de la Encuesta Aplicada

A continuación se desglosa cada pregunta de la Encuesta con los resultados obtenidos mediante gráficos para su mejor comprensión.

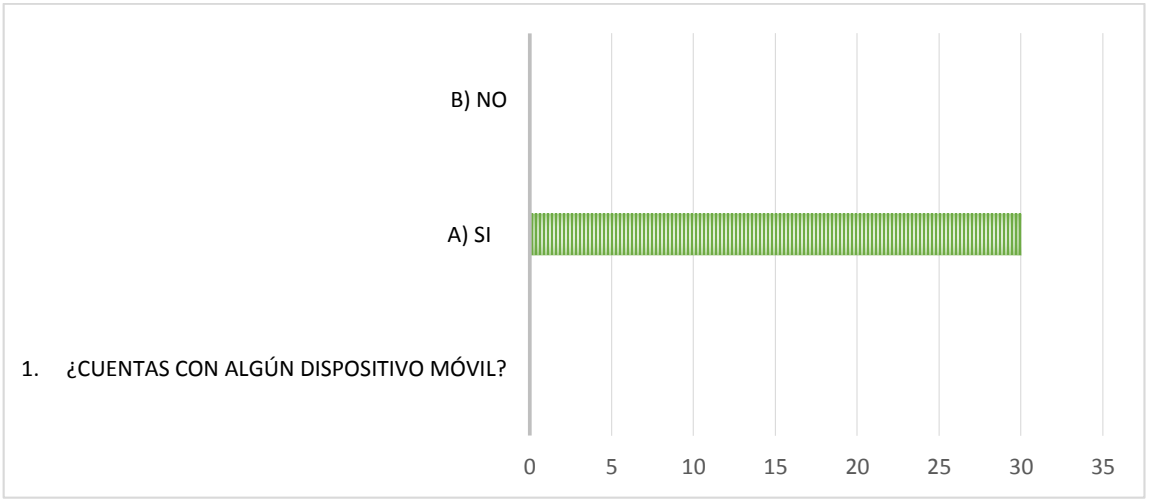


Ilustración 21. Pregunta 1

El cien por ciento de los encuestados dijeron que cuentan con un dispositivo móvil.

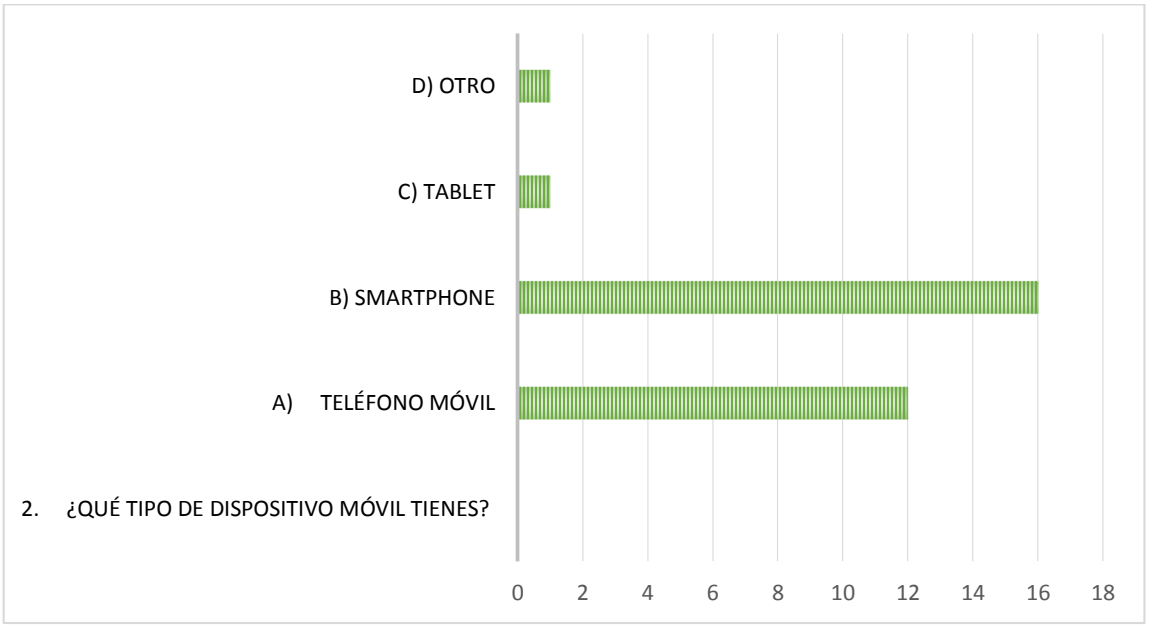


Ilustración 22. Pregunta 2

La mayoría de los encuestados cuentan con un *Smartphone*, seguido de un teléfono móvil y una minoría cuenta con *Tablets* u otro dispositivo.

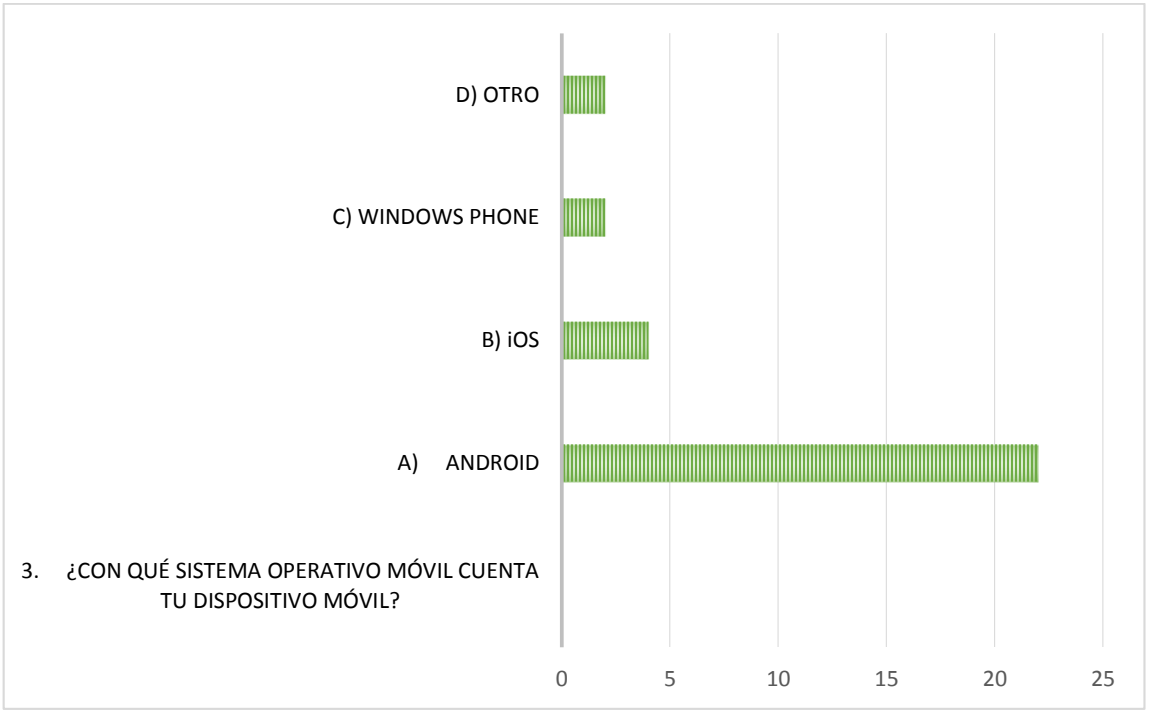


Ilustración 23. Pregunta 3

Como podemos observar más del 80% de los encuestados cuentan con el Sistema Operativo *Android* en su Dispositivo Móvil.

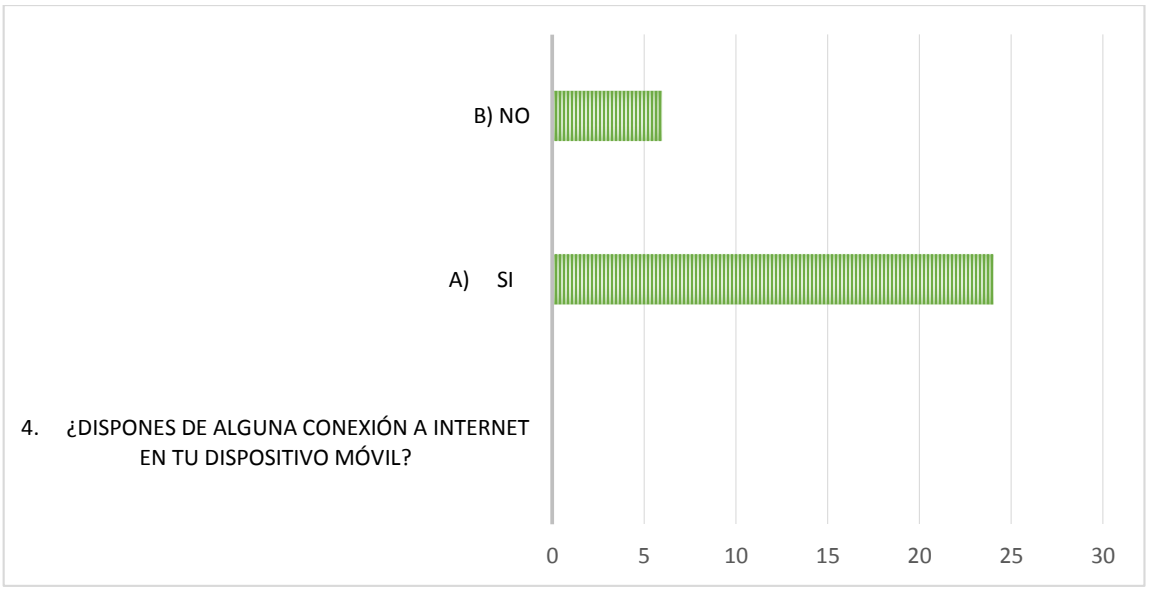


Ilustración 24. Pregunta 4

La mayoría de los encuestados disponen de una conexión a internet móvil.

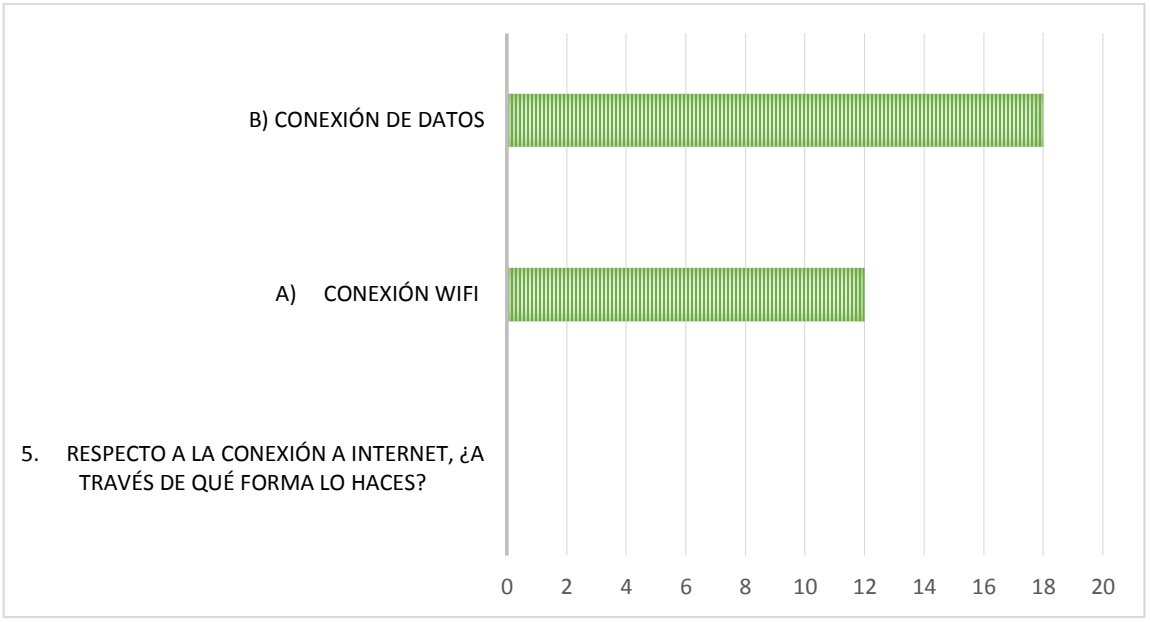


Ilustración 25. Pregunta 5

Más de la mitad de los encuestados se conecta a internet a través de los datos móviles de su compañía telefónica.

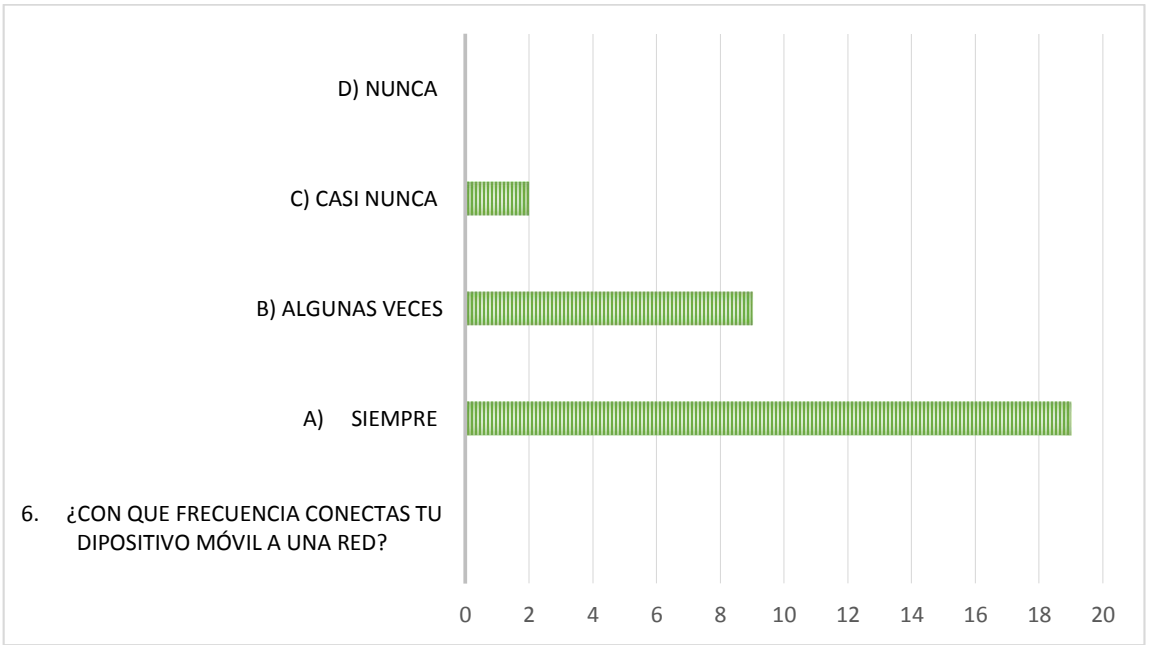


Ilustración 26. Pregunta 6

Una gran mayoría de los encuestados están siempre conectados a internet.

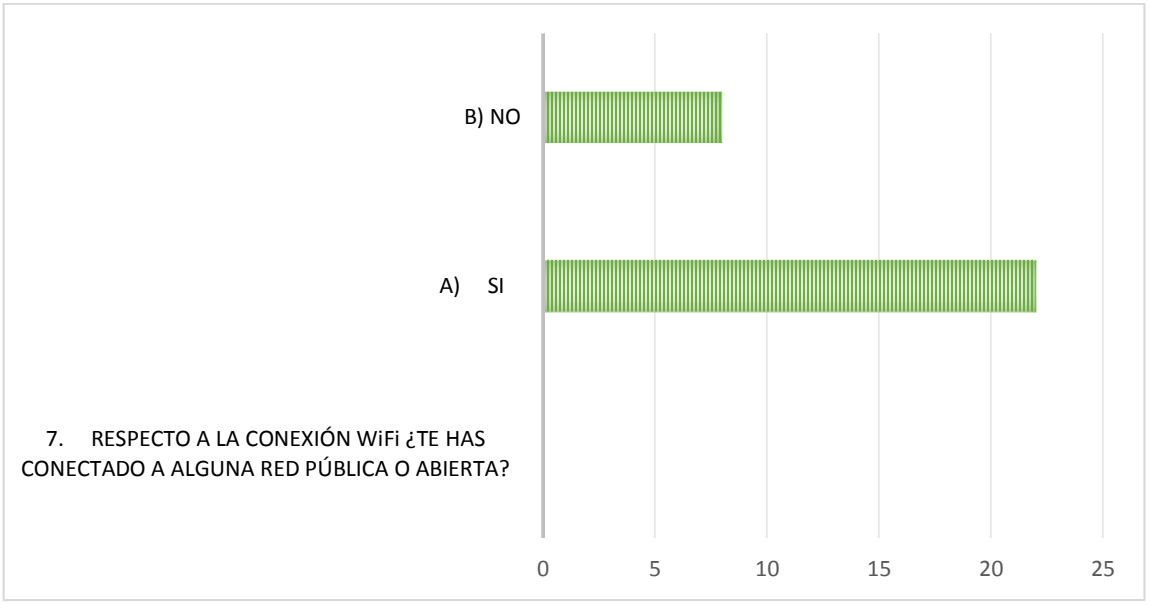


Ilustración 27. Pregunta 7

La mayoría de los encuestados se ha conectado a una red abierta.

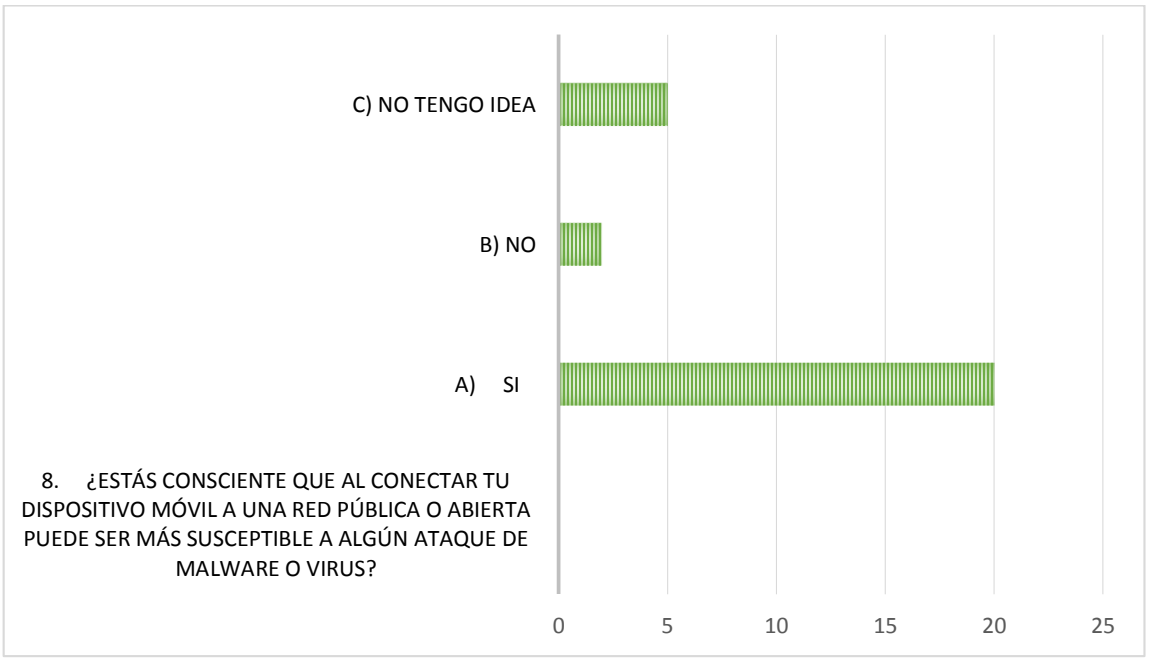


Ilustración 28. Pregunta 8

La mayoría de los encuestados están conscientes que al conectarse a una red abierta exponen su Dispositivo Móvil a algún tipo de ataque.

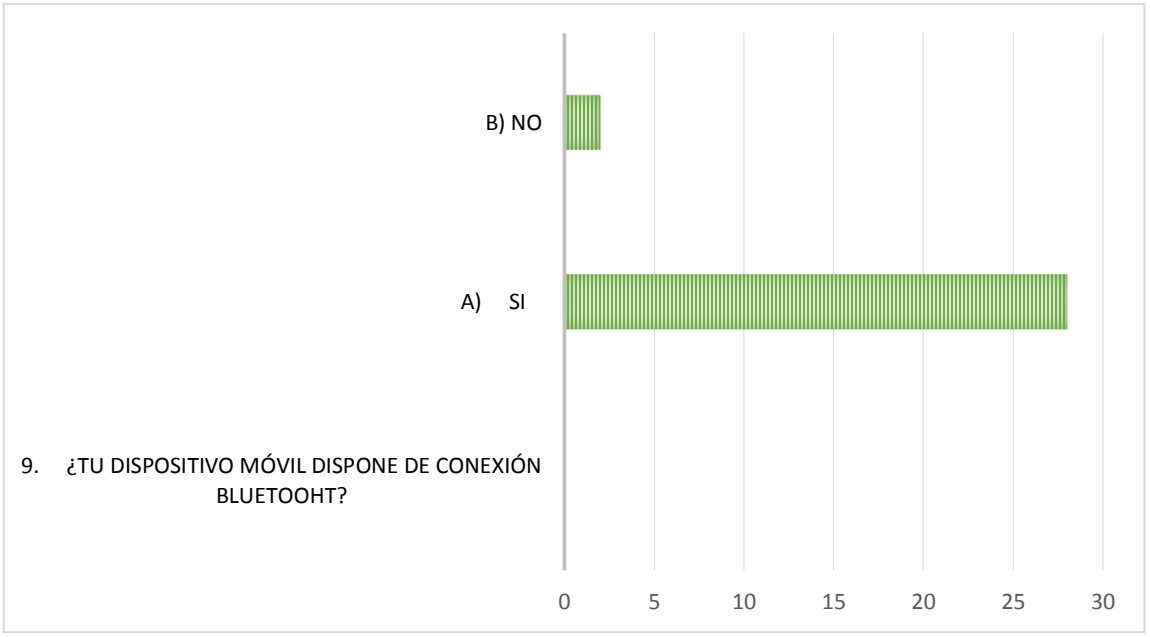


Ilustración 29. Pregunta 9

Más del 90% de los encuestados disponen de una conexión *Bluetooth*.

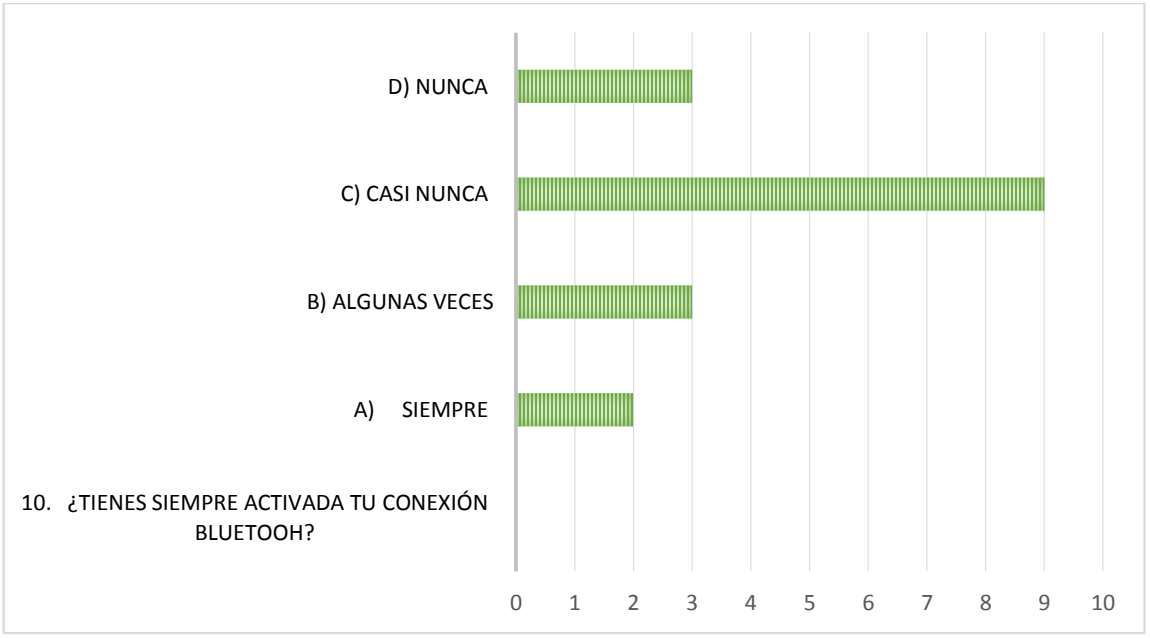


Ilustración 30. Pregunta 10

De los encuestados la mayoría contestó que casi nunca hacen uso de la conexión *Bluetooth*.

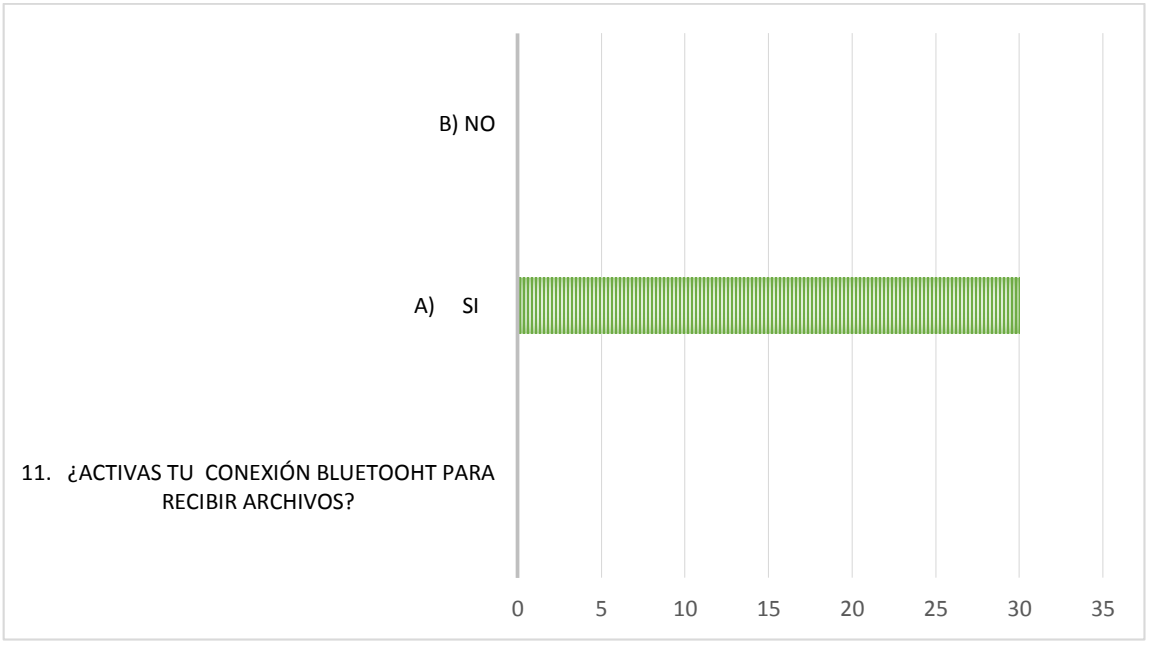


Ilustración 31. Pregunta 11

Todos los encuestados reciben archivos por medio de conexión *Bluetooth* cuando tienen activada esta opción.

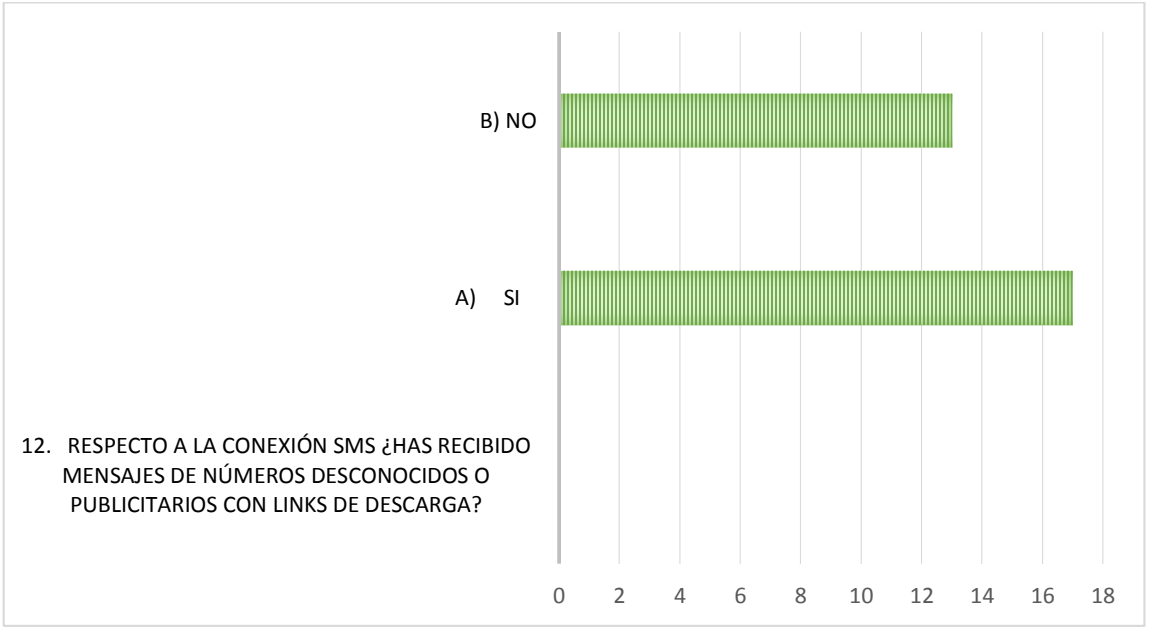


Ilustración 32. Pregunta 12

Más de la mitad de los encuestados han recibido mensajes publicitarios.

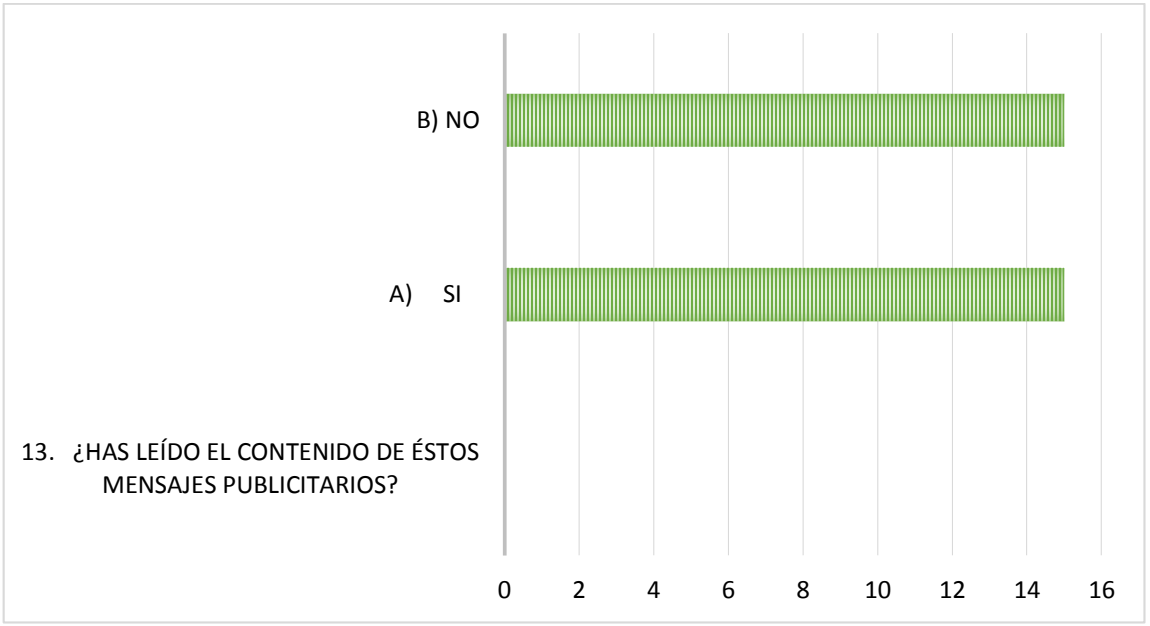


Ilustración 33. Pregunta 13

El 50% de los encuestados han leído mensajes con contenido publicitario, la otra mitad ha hecho caso omiso a estos mensajes.

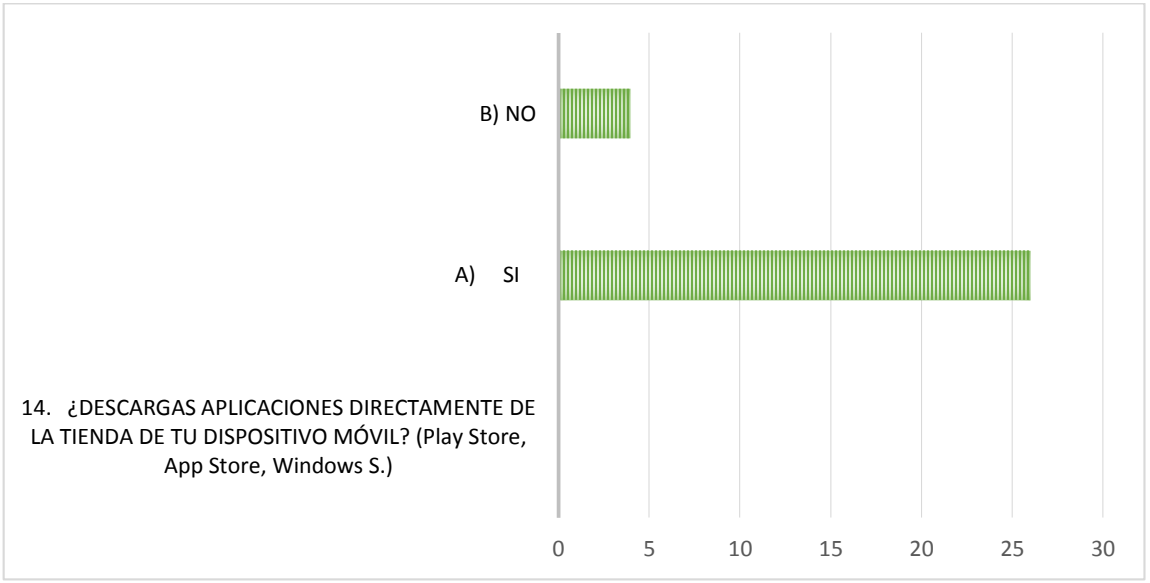


Ilustración 34. Pregunta 14

Más del 90% de los encuestados descarga aplicaciones directamente desde la tienda oficial.

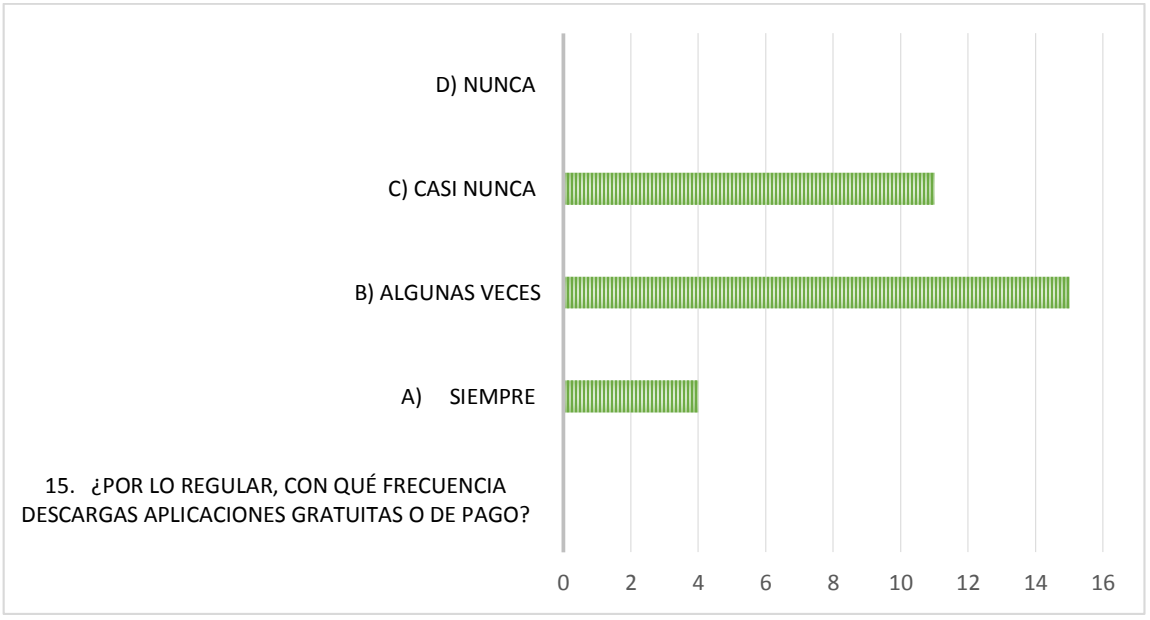


Ilustración 35. Pregunta 15

La mitad de los encuestados han descargado alguna vez aplicaciones.

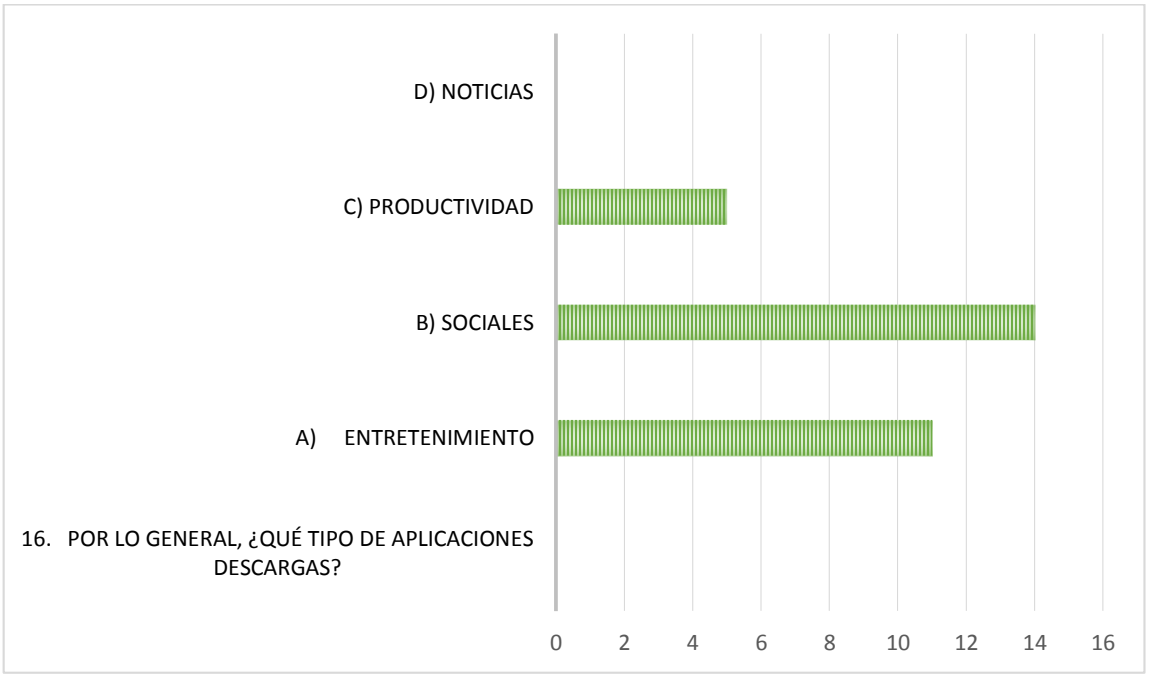


Ilustración 36. Pregunta 16

El 45% de los encuestados descargan aplicaciones de interés social, otra parte para entretenimiento y otros para productividad.

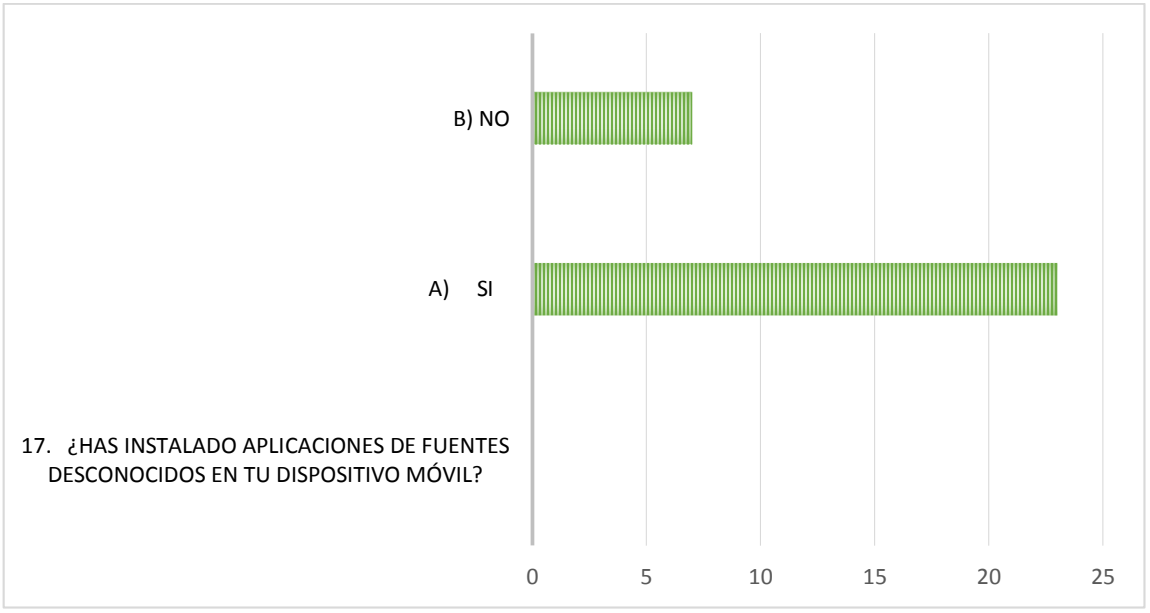


Ilustración 37. Pregunta 17

La mayoría de los encuestados ha instalado aplicaciones de otras fuentes diferentes a la tienda oficial de su S.O.

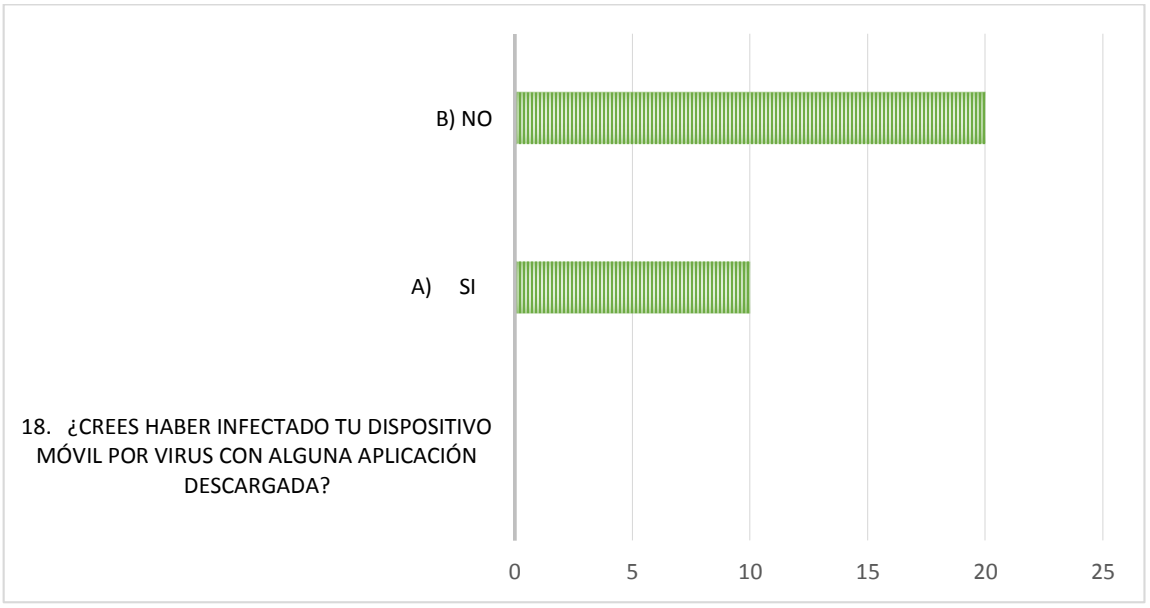


Ilustración 38. Pregunta 18

Una tercera parte de los encuestados dijeron haber infectado su Dispositivo Móvil con algún tipo de virus.

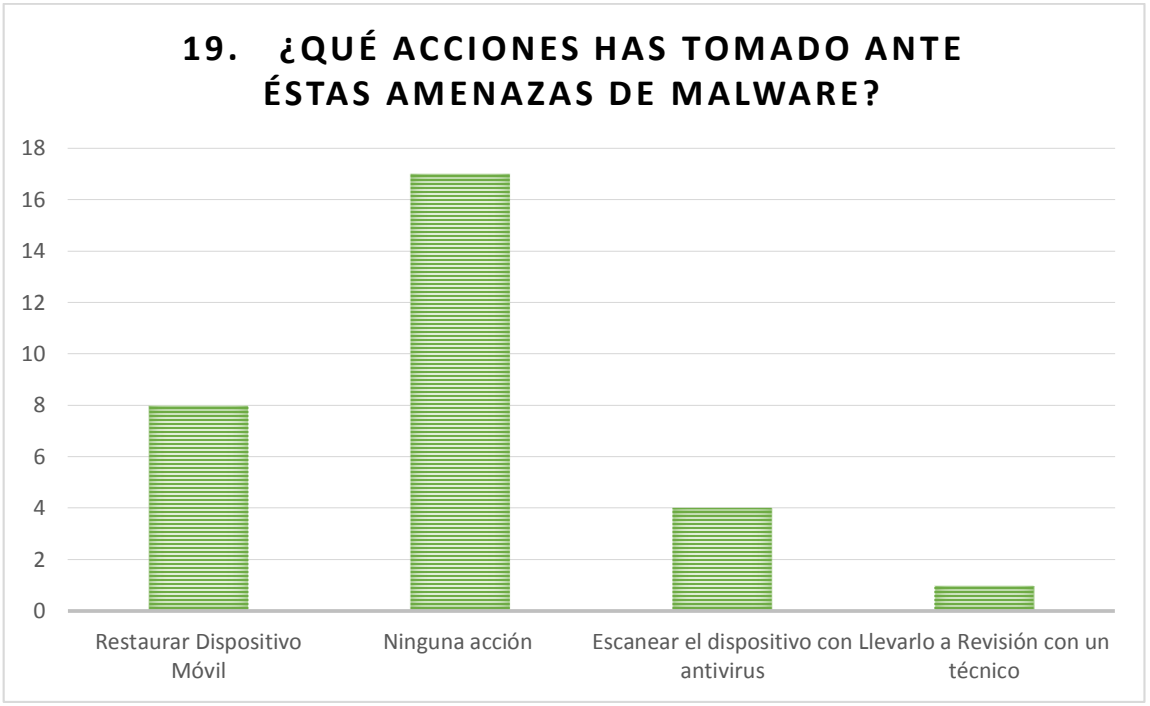


Ilustración 39. Pregunta 19

Más del 50% de los encuestados ha optado por no tomar ninguna acción ante alguna amenaza de *malware*.

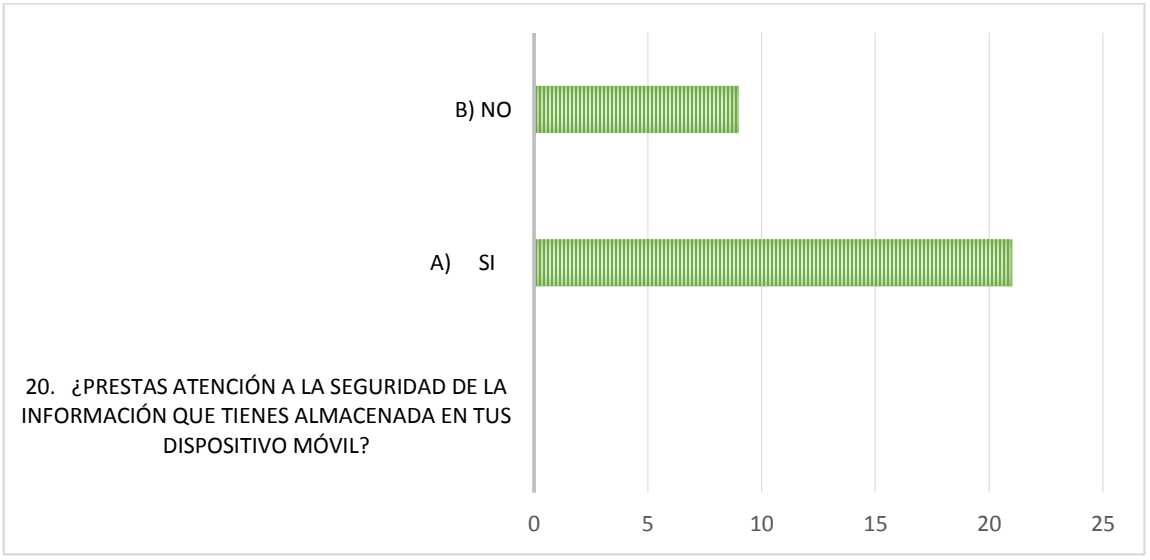


Ilustración 40. Pregunta 20

La mayoría de los encuestados muestra interés por la seguridad de su información almacenada en su Dispositivo Móvil.

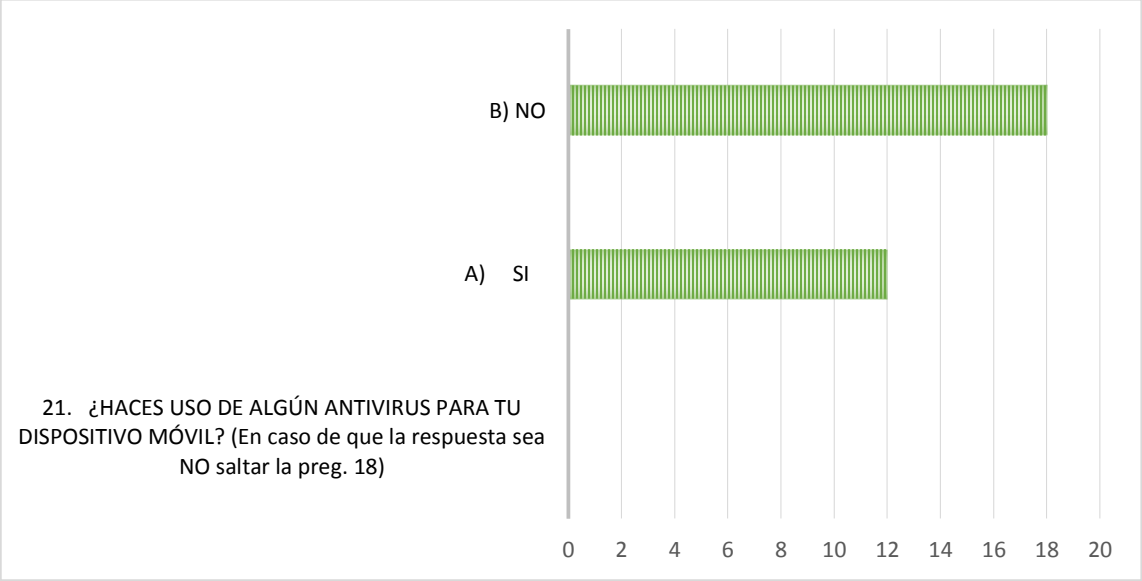


Ilustración 41. Pregunta 21

De los encuestados, una gran mayoría no hace uso de algún tipo de antivirus.

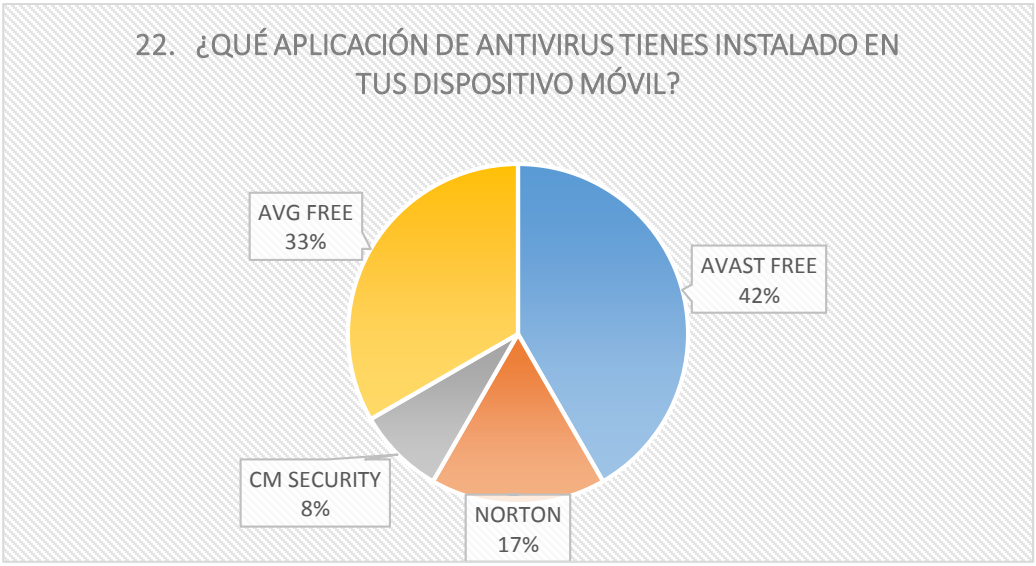


Ilustración 42. Pregunta 22

El 42% de los encuestados que sí utilizan antivirus, respondieron que utilizan AVAST FREE para resguardar la seguridad de su Dispositivo Móvil.

4.2. RECOMENDACIONES DE SEGURIDAD

Con base en las encuestas aplicadas se pudo apreciar que los usuarios de los Dispositivos Móviles prestan poco interés en la seguridad de la información almacenada en su DM. Por lo cual, en este apartado se proporciona una serie de recomendaciones que a nuestro criterio son funcionales para la seguridad de su información de los usuarios, ya que fueron probadas en un DM. Se recomiendan algunas aplicaciones de seguridad por defecto del S.O. *Android,* Antivirus, aplicaciones para mejorar la privacidad, aplicaciones de localización de DM por mencionar algunas.

Esto para que el usuario pueda proteger su información de cualquier tipo de ataque cibernético.

Dichas recomendaciones se llevaron a cabo en un dispositivo móvil de gama media con el sistema operativo *Android*, con las siguientes especificaciones: *Smartphone* LG, modelo L65, *Android* 4.4.2 Kit Kat, procesador de 1.2 GHz Dual Core y pantalla 4.3".

Ilustración 43 Smartphone LG, modelo L65

4.2.1. SEGURIDAD POR DEFECTO DEL S. O. *ANDROID*

Estos servicios están disponibles para la mayor parte de dispositivos que ostentan el Sistema Operativo Android, sin la necesidad de instalar algún tipo de software o aplicaciones. El usuario es el rival más débil de la cadena de seguridad. Incluso la adición de estos ajustes básicos puede hacer más seguros a una gran cantidad de usuarios. Google desde sus inicios, ha dejado la responsabilidad de protección de los dispositivos a terceros. No obstante, la compañía ha introducido y reforzado la protección por ellos mismos.[21]

4.2.1.1. ADMINISTRADOR DE DISPOSITIVOS *ANDROID*

El administrador de dispositivos Android que permite al usuario de forma remota: localizar, bloquear, eliminar el contenido o hacer que alarme el dispositivo. No es un sistema de seguridad perfecto, pero es lo mínimo que todo usuario debería tener.

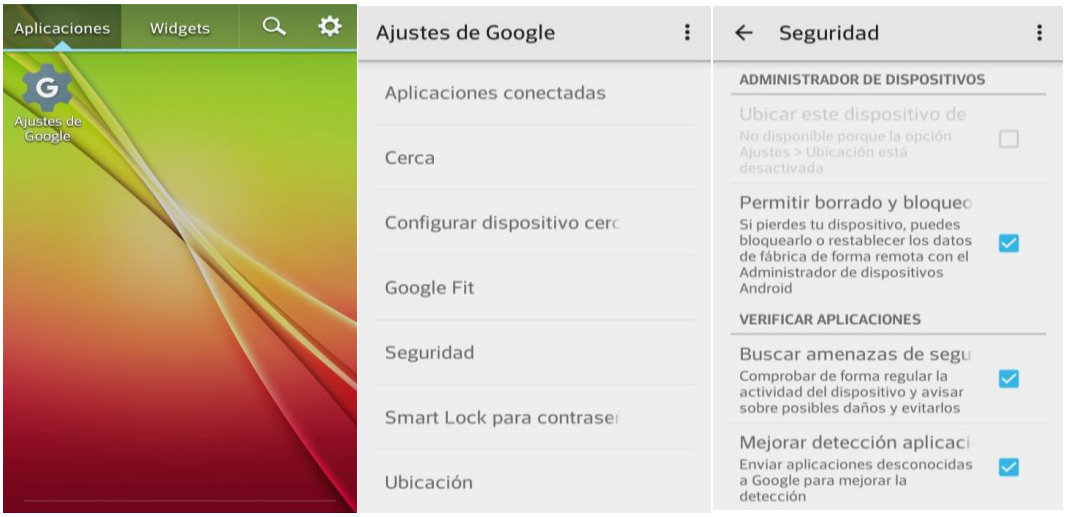


Ilustración 44. Administrador de dispositivos Android

[21] Hipertextual, (s.f.). Recuperado el 02 noviembre de 2015, de. http://hipertextual.com/archivo/2013/12/seguridad-dispositivos-moviles-consejos/

4.2.1.2. GOOGLE AUTHENTICATOR

Activación de la autenticación de dos pasos, la verificación de dos factores no es sólo una protección para su teléfono, sino que protege todas las cuentas de Google. Si no está utilizando la autenticación de dos pasos, es recomendable hacerlo. En Android, puede instalar la aplicación Google Authenticator (o una alternativa) para acceder fácilmente a los códigos, o recibir códigos a través de SMS.

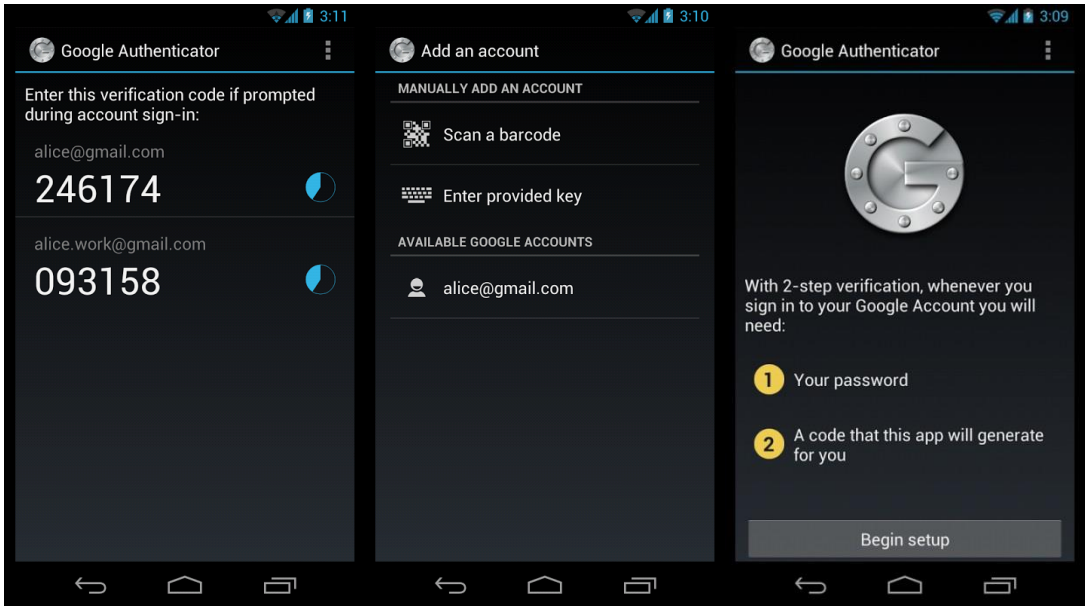


Ilustración 45. Google Authenticator

Google ofrece esta funcionalidad tal y como su nombre indica, cuando es necesario acceder a cualquier servicio de Google no solo sea necesario introducir la contraseña, sino que también será necesario proporcionar un código único que será enviado por Google al propietario de la cuenta. También se debe activar esta funcionalidad de verificación de dos pasos en todos y cada uno de los servicios que sean compatibles.

4.2.1.3. CIFRAR EL TELÉFONO

Cifrar el teléfono es algo que, por lo menos, cualquier usuario debe hacer si toma la decisión de vender su dispositivo Android. Pero no es solo el único caso en el que se debe utilizar, ya que la encriptación de su dispositivo es un buen hábito, incluso durante el uso diario. El único inconveniente es que, en algunos dispositivos más antiguos o más lentos, el cifrado puede significar un poco de reducción en cuanto a rendimiento se refiere. Sin embargo, la mayoría de los dispositivos modernos de grandes capacidades y potencia, apenas se experimentará una reducción de velocidad.

Ilustración 46. Encriptación de datos

Si desea cifrar su dispositivo Android, deberá dirigirse a los ajustes del dispositivo móvil, opción de Seguridad y marcar la configuración Encriptar Teléfono.

El proceso inicial llevará algún tiempo (una hora aproximadamente), y después se debe introducir un PIN o una contraseña, la primera vez que arranque el dispositivo. Es recomendable tener el dispositivo totalmente cargado y

conectado al comenzar el proceso o bien, realizar el proceso conectado al cargador. El sistema ni siquiera le permitirá comenzar el proceso de cifrado, si el dispositivo no está cargado completamente. Este proceso es bastante delicado ya que si se interrumpiera podría perder los datos para siempre.

4.2.1.4. BLOQUEAR LA PANTALLA

Hay varias formas de bloquear su dispositivo móvil en Android, incluyendo un PIN, el patrón de movimiento, una contraseña, o incluso desbloqueo mediante rasgos faciales. Utilice uno de ellos.

Anteriormente los usuarios no tomaban ningún tipo de medida de seguridad en su teléfono. Si bien esto no está limitado únicamente al bloqueo del uso de la pantalla, también indica que incluso la más básica medida de seguridad como la del bloqueo de pantalla no siempre se sigue.

Para configurar esta función debe ir a los ajustes de su dispositivo, diríjase a pantalla y desde allí acceda a las opciones de bloqueo de pantalla. (Este proceso puede variar en algunos dispositivos).

Ilustración 47. Bloqueo de la pantalla

4.2.1.5. AÑADIR INFORMACIÓN DEL PROPIETARIO A LA PANTALLA DE BLOQUEO

No todo el que se hace con su DM tiene por qué tener malas intenciones. De hecho al perder su teléfono, puede ser encontrado por alguien que trate de devolvértelo. Ayuda a esta acción mediante la adición de información acerca del propietario en la pantalla de bloqueo.

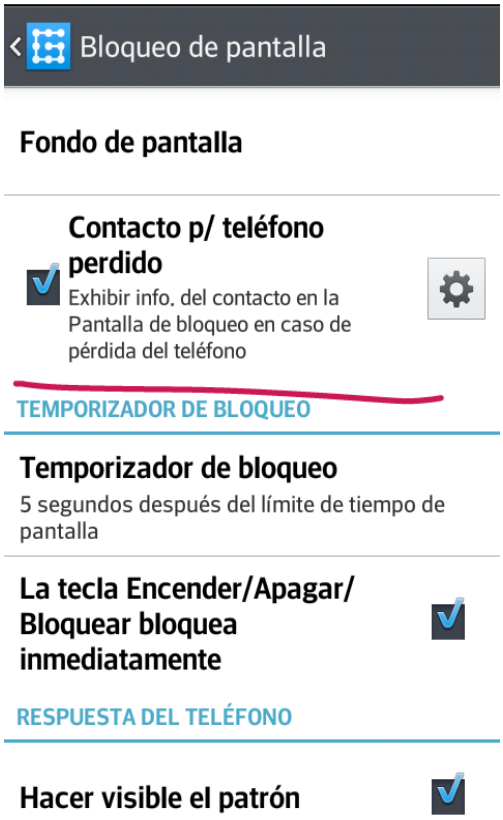


Ilustración 48. Información del propietario

Para configurar esta función deberá ir a los ajustes de su dispositivo, seleccionar la opción Pantalla y de la lista seleccionar Contacto p/teléfono perdido. Es aquí donde aparecerá un campo donde podrá introducir el texto que considere oportuno.

4.2.2. APLICACIONES PARA MEJORAR LA SEGURIDAD

4.2.2.1. ANTIVIRUS RECOMENDADOS

Anti-virus Dr. Web Light

Ilustración 49. Antivirus Dr. Web Ligth

Este antivirus resultó interesante, ya que detectó aplicaciones maliciosas que otros no, como es el caso de la Aplicación Adult Player, considerada una de las peores amenazas para Android, ya que este malware se instala en la raíz del dispositivo para que no pueda ser removido por el usuario común, más que por un técnico especializado.

Funciones y ventajas

- Escaneo rápido o completo del sistema de archivos, escaneo selectivo de archivos y carpetas por solicitud del usuario.
- Escaneo del sistema de archivos en tiempo real.

- Detección de programas maliciosos nuevos y desconocidos con ayuda de la tecnología única Origins
- Protección de la tarjeta SD contra la infección de archivos autoejecutables que constituyen una amenaza para los dispositivos.
- Las amenazas detectadas son movidas a la Cuarentena con la posibilidad de restaurar posteriormente los archivos.
- Estadística detallada del funcionamiento del antivirus.
- *Widgets* cómodos e informativos en el escritorio para acceder a la aplicación. (Play, 2015)

AMC Security

Ilustración 50. AMC Security

Este antivirus ayuda a detectar amenazas en su dispositivo, acelerar y optimizar las aplicaciones instaladas, a su vez aumentar al máximo el rendimiento de su DM.

Funciones:

- Puede reemplazar aplicaciones similares de una sola vez.
- Escanear, Refuerzo, Seguridad vienen con varias herramientas imprescindibles que le aseguran protección integral a su equipo.

- Escaneo rápido: permite limpiar todas las aplicaciones en ejecución, basura caché, registros de privacidad y archivos APK.
- Escaneo profundo: le permitirá limpiar archivos basura, archivos grandes y archivos residuales.
- Antivirus: AMC Security protege su dispositivo contra virus, troyanos, vulnerabilidades, malware y spyware.
- Refuerzo: le ayuda a eliminar las aplicaciones que se estén ejecutando en segundo plano y a limpiar la memoria RAM para optimizar su dispositivo de una sola vez.
- Acelerador de Juego: mejora su experiencia de juego y su velocidad para que ésta sea fluida y sin demoras.
- Antirrobo: en caso de pérdida o extravío de su equipo, le permite bloquearlo dando un aviso de alarma mediante el envío un mensaje. (Play, 2015)

Avast Free Antivirus

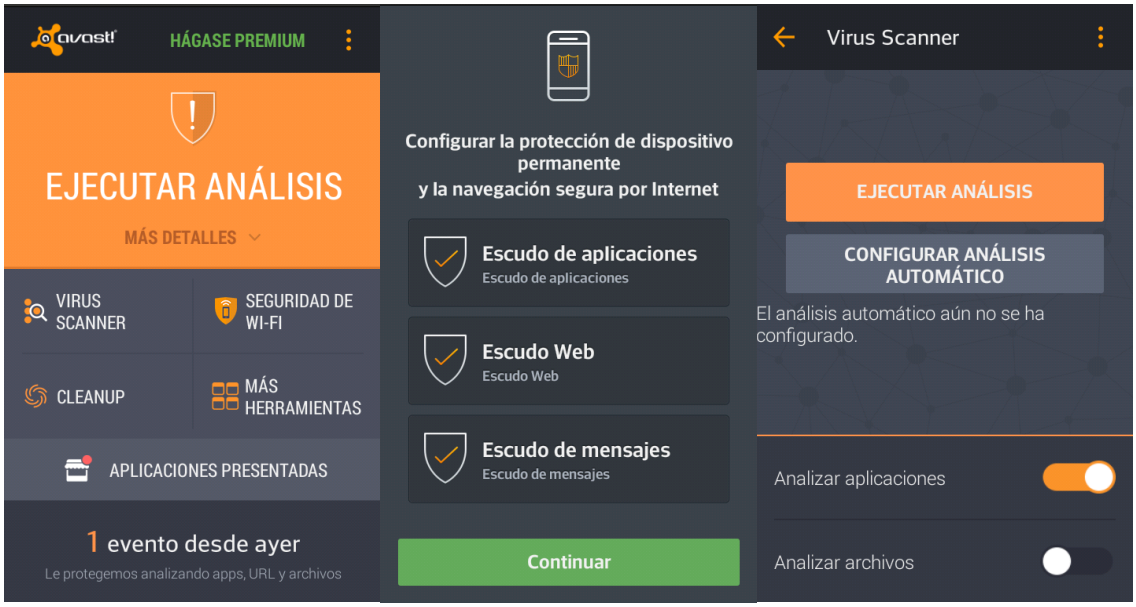


Ilustración 51. Avast Free Antivirus

Avast Mobile Security es un Antivirus para Android que ayuda a mantener a su dispositivo móvil libre de virus, malware y spyware.

Funciones y características:

- Analiza automáticamente sus aplicaciones instaladas y el contenido de la tarjeta de memoria SD.
- Ayuda a mantener su privacidad bloqueando números que se pongan en contacto con usted que no desee.
- Bloquea los enlaces infectados por malware para una navegación Web segura.
- Bloquea el acceso de hackers, sólo en dispositivos rooteados.
- Bloquea un gran número de aplicaciones que el usuario determine
- Activa una alarma y borra datos de la memoria para mantener seguro sus datos en caso de robo. (Play, 2015)

K**aspersky Internet Security**

Ilustración 52. Kaspersky Internet Security

Este antivirus ofrece las últimas tecnologías móviles, incluida una protección superior de antirrobo, y es absolutamente gratis, con más funciones de seguridad como lo son:

- Las tecnologías más recientes contra virus, *Spyware*, Troyanos y más
- Ejecuta un escáner contra malware en su dispositivo cuando lo desee.

- Tiene la función de bloqueo, localización y eliminación completa de los datos almacenados en su dispositivo.
- Cuenta con una alarma en la que puede activar de forma remota, lo que lo ayuda a encontrar su dispositivo si éste se encuentra en algún lugar cercano.
- Lo protege de llamadas y mensajes de texto no deseados. (Play, 2015)

Avira Antivirus Security

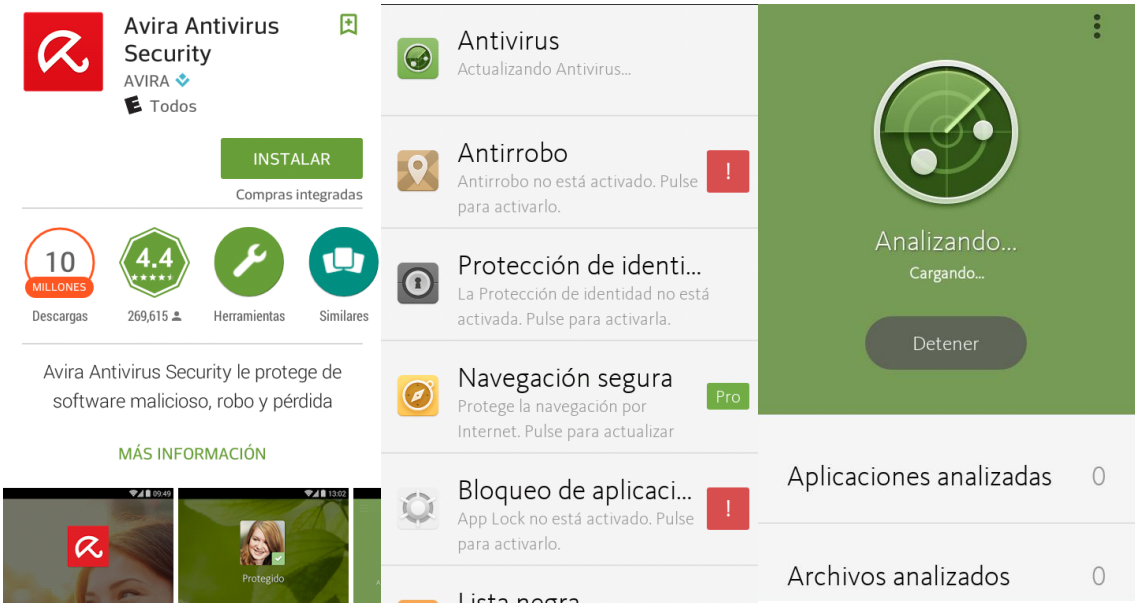


Ilustración 53. Avira Antivirus Security

Esta aplicación protege su dispositivo de software malicioso y le brinda las siguientes características:

- Bloquea virus de forma eficaz así como otros tipos de software malicioso.
- Encuentra su Dispositivo Móvil en caso de extravío o robo.
- Protege sus datos privados (fotografías, videos o SMS) frente a robo.
- Evita el acceso no autorizado a otras aplicaciones instaladas en su dispositivo.

- Pone de relieve recursos de sistema para ayudar a ahorrar energía de la batería.
- Analiza automáticamente las Aplicaciones e incluso las actualiza.
- Analiza unidades de almacenamiento como la memoria externa. (Play, 2015)

.

Panda *Mobile Security*

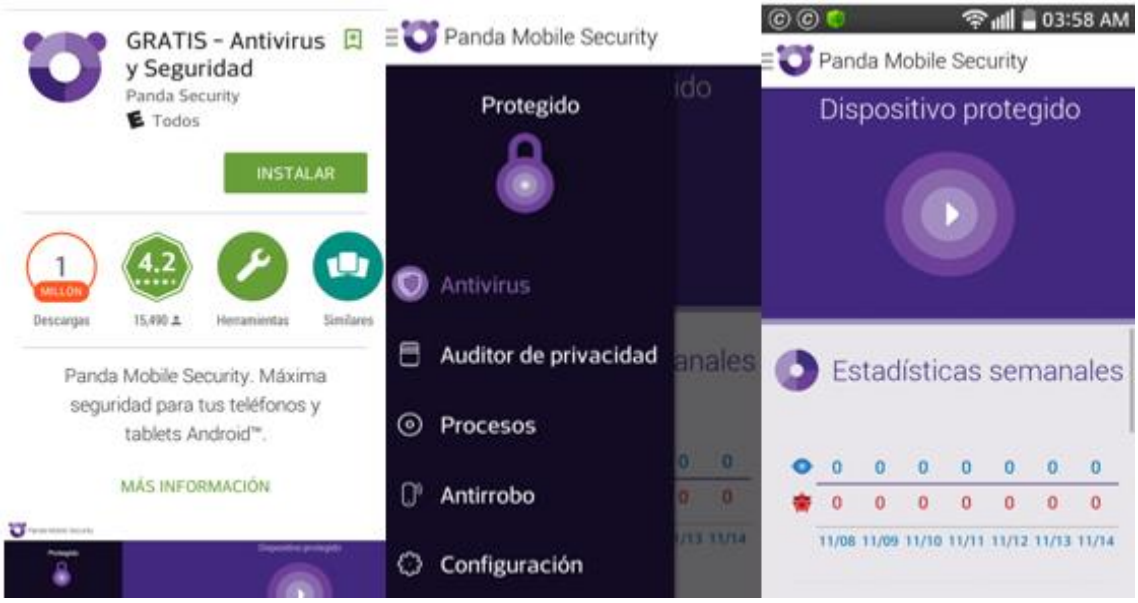


Ilustración 54. Panda Security Antivirus y Seguridad

Este Antivirus protege su dispositivo móvil contra virus, *malware* o *spyware*. También bloquea aplicaciones que acceden sin permiso a sus datos confidenciales para proteger su privacidad.

Características de la aplicación:

- Es un Antivirus en tiempo real, ya que analiza automáticamente cada aplicación que descargue antes de su primer uso.

- Analiza la tarjeta SD que introduzca en su dispositivo.
- Tiene la capacidad de aumentar la velocidad de su dispositivo.
- Localiza su dispositivo móvil en caso de robo o extravío. (Play, 2015)

Norton Antivirus & Seguridad.

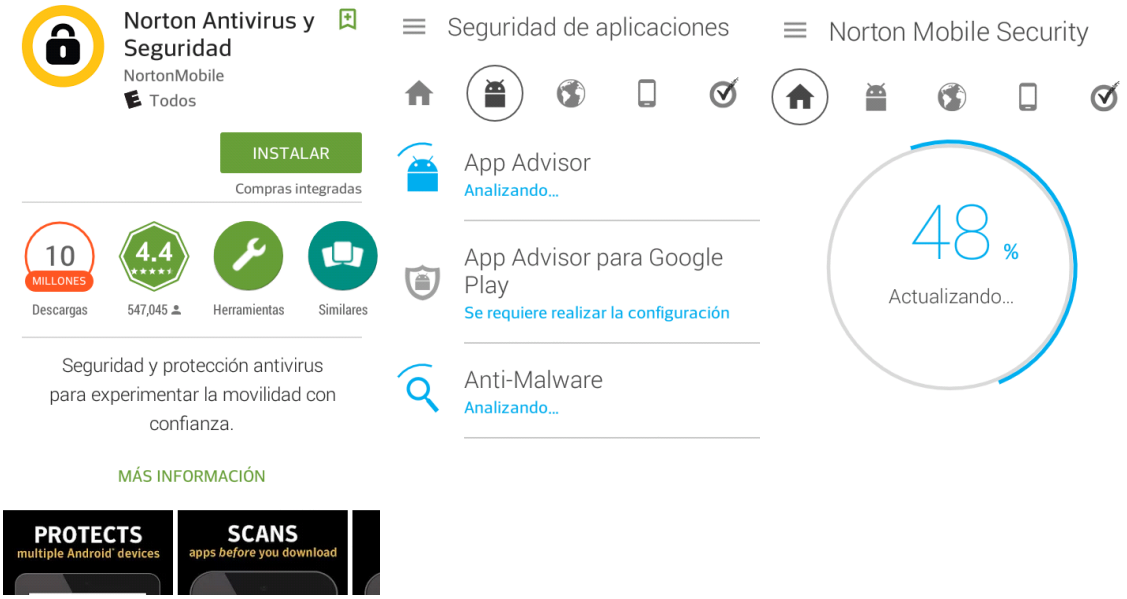


Ilustración 55. Norton Antivirus & Seguridad

Norton, un antivirus para Android que combate contra amenazas como aplicaciones maliciosas, robo o pérdida. Esta aplicación le proporciona protección avanzada y preventiva contra aplicaciones potencialmente peligrosas que pueden generar la fuga de contenido o información personal, un uso excesivo de los datos o la batería y comportamiento intrusivo.

Funciones:

- Protege su DM contra amenazas por virus o *malware*
- Con la utilización de SMS puede bloquear de manera remota su teléfono perdido o robado.

- Puede analizar y eliminar las aplicaciones que contengan programas maliciosos o virus que pueden dañar su dispositivo móvil. (Play, 2015)

AVG Mobile Antivirus

Ilustración 56. AVG Mobile Antivirus

Es un Antivirus en tiempo real, catalogado como de los más valorados, además es gratuito. Protege su dispositivo por infecciones de virus, malware, spyware y mensajes de texto nocivos y ayuda a mantener sus datos personales a salvo.

Funciones:

- Analiza las aplicaciones, configuraciones y archivos en tiempo real para detectar aplicaciones maliciosas.
- Tiene la opción de búsqueda o localización de su teléfono perdido o robado mediante Google Maps.
- Bloquea o borra la información de su dispositivo para proteger su privacidad.
- Puede navegar en la Web de forma segura y lo mantiene a salvo de ataques de *phishing*.

- Controla la batería, el almacenamiento y el uso del paquete de datos.
- Identifica las configuraciones no seguras de su dispositivo. (Play, 2015)

ESET *Mobile Security* & Antivirus

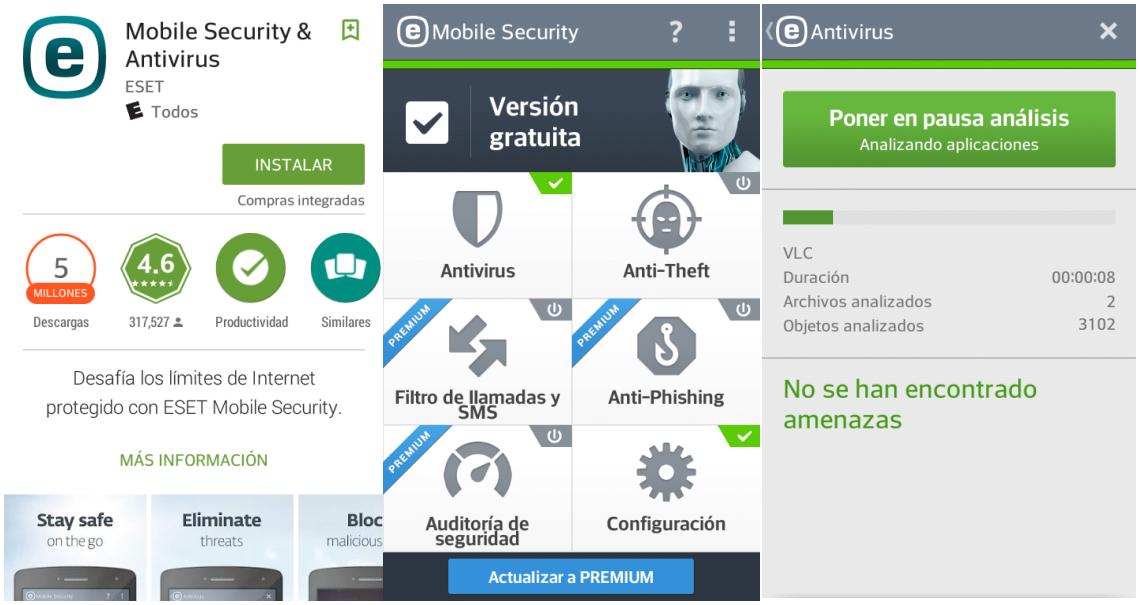


Ilustración 57. ESET Mobile Security & Antivirus

ESET Mobile Security es un antivirus que protege su dispositivo móvil para una navegación Web segura, además analiza sus aplicaciones para detectar programas maliciosos como virus o malware.

Funciones:

- Analiza y explora el acceso de las aplicaciones y los archivos que descargue.
- Tiene la opción de cuarentena.
- Bloquea su dispositivo de forma remota, localiza por GPS y borra su información por medio de un SMS.
- En la versión Premium puede bloquear SMS, MMS y llamadas. (Play, 2015)

McAfee Security & Power

Ilustración 58. McAfee Security & Power

Esta aplicación de antivirus protege y mejora el rendimiento de su dispositivo móvil Android con las funciones Anti-Theft, localiza su dispositivo en caso de pérdida o robo, brinda protección de privacidad en aplicaciones, y optimiza su rendimiento.

Funciones:

- Bloquea y activa una alarma de forma remota, alerta antes posibles ataques WiFi.
- Tiene la opción de realizar copias de seguridad y restauración de datos.
- Brinda protección contra desinstalación de aplicaciones.
- Bloquea llamadas no deseadas y cuenta con un filtro SMS.
- Mantiene al día sobre su estado de seguridad y soluciona los problemas con un solo toque,
- Libera memoria (RAM), aumenta el rendimiento de su Smartphone y ahorra energía.
- Antivirus y protección Web antivirus. siempre activo para eliminar virus en archivos, SMS, tarjetas SD, aplicaciones y sus descargas. (Play, 2015)

4.2.3. APLICACIONES PARA MEJORAR LA PRIVACIDAD

AppLock

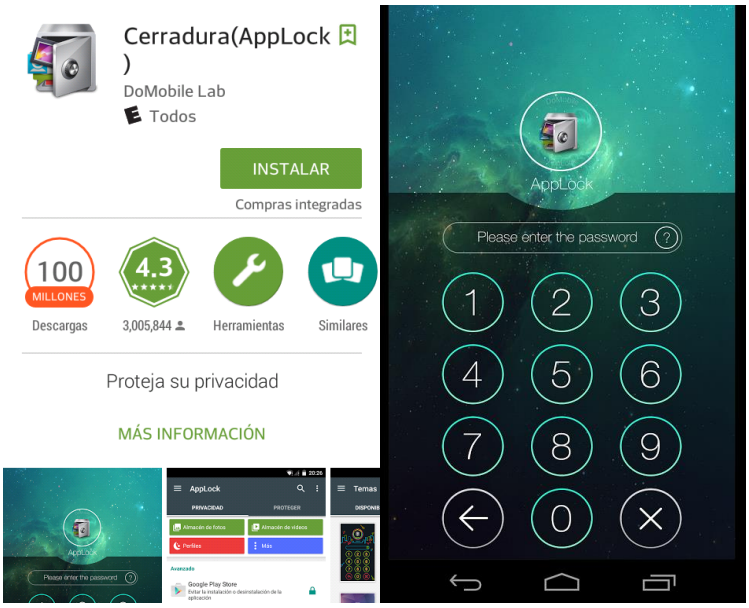


Ilustración 59. AppLock

La aplicación AppLock bloquea mensajes SMS, contactos, Facebook, galería, configuración, llamadas y cualquier aplicación que desee, con múltiples opciones, protegiendo su privacidad.

Funciones:

- Protege cualquier aplicación utilizando una contraseña o patrón.
- Cuenta con una bóveda de fotos y de video.
- Bloquea su dispositivo en automático después de cierto tiempo.
- Posee un interruptor de bloqueo (WiFi, datos móviles).
- Puede bloquear llamadas entrantes o salientes que usted determine.
- Bloquea los servicios de Play Store.
- Previene la desinstalación de aplicaciones.

- Esta aplicación no puede ser detenida por gestores de tareas.
- Utiliza poca memoria y ahorra batería. (Play, 2015)

Threema

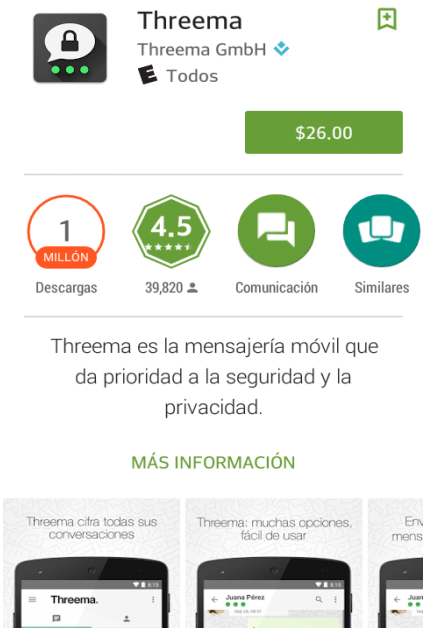


Ilustración 60. Threema

Threema es una aplicación que brinda el servicio de mensajería segura. Conserva sus datos fuera del alcance de los hackers, empresas y el gobierno, y lo puede utilizar de forma completamente anónima. Además, ofrece una extensa gama de funcionalidades.

Características:

- Cuenta con el cifrado más potente
- Garantiza su privacidad.
- No solo ofrece el servicio de mensajería privada y cifrada, sino que también ofrece multitud de posibilidades como; el envío de mensajes de texto y voz, además puede enviar archivos multimedia y hasta compartir su ubicación.
- Requiere de permisos del usuario para cualquier cambio. (Play, 2015)

LastPass

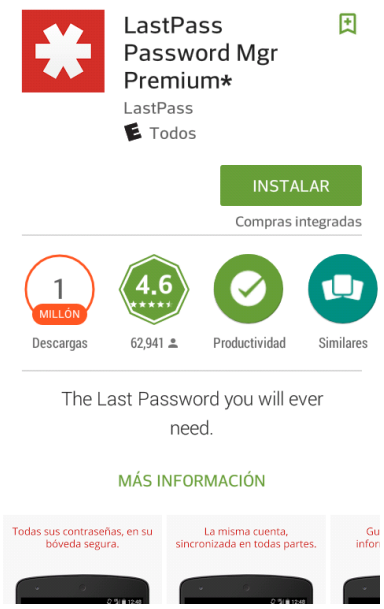


Ilustración 61. LastPass Password Mgr

Esta aplicación es un gestor de contraseñas destacado, que simplifica la vida en línea a millones de personas en todo el mundo. Este servicio es gratuito durante los primeros días, después tendrá que actualizar a la versión Premium para una mayor seguridad.

Funciones:

- Guarda los nombres de usuarios y contraseñas de todas sus cuentas en línea.
- Tiene la opción de guardar membrecías, tarjetas de crédito y otra información importante en notas seguras.
- Puede compartir inicios de sesión con amigos y familiares.
- Además puede acceder a su información fuera de línea a través de las extensiones de los motores de búsquedas y aplicaciones móviles.
- Cuenta con la opción de sincronizar todas sus contraseñas e inicios de sesión entre todas sus computadoras y dispositivos.

- Esta aplicación no tiene acceso a su información cifrada por lo que su información permanece segura. (Play, 2015)

G. Cloud Backup

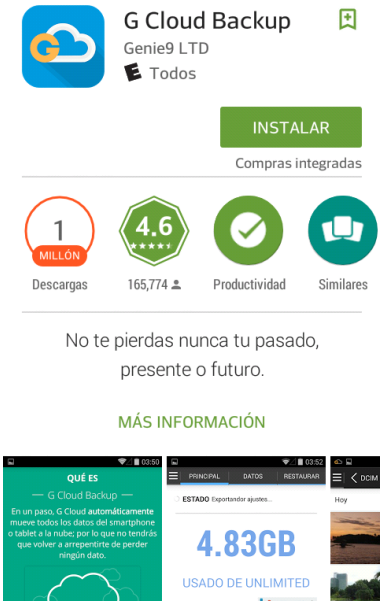


Ilustración 62. Cloud Backup

Esta aplicación es increíblemente fácil de usar, ya que su interfaz de usuario es muy sencillo.

Funciones:

- Puede volver atrás en el tiempo para ver llamadas de hace un año, vídeo y cualquier otro dato desde la barra de memorias
- Realiza copias de seguridad automáticas de mensajes (SMS), contactos, registros de llamadas, ajustes, fotos, música y videos.
- Protege la aplicación con una contraseña.
- No es necesaria ninguna configuración especial ni rootear su dispositivo.
- Restaura/migra a un nuevo dispositivo con una sola pulsación.
- Respalda todas las versiones de cada archivo.

- Opciones avanzadas para cambiar el horario programado diario, desactivar horario automático. (Play, 2015)

4.2.4. APLICACIONES DE LOCALIZACIÓN DEL DISPOSITIVO MÓVIL.

Capptura

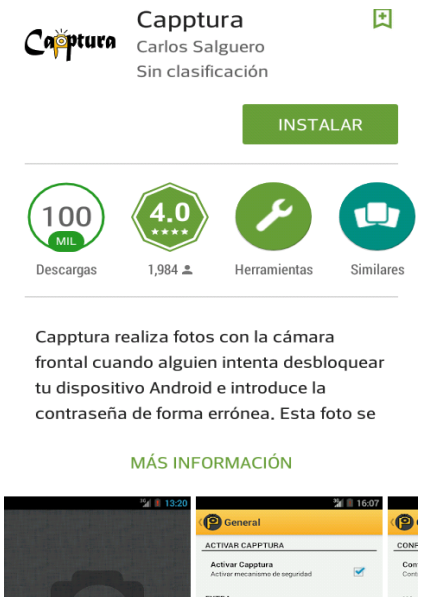


Ilustración 63. Capptura

Capptura es una aplicación que realiza fotos con la cámara frontal cuando alguien intenta desbloquear su dispositivo Android o introduce la contraseña de forma errónea, esta foto se envía, junto con la localización GPS, a la cuenta de correo que previamente elija. También cuenta con la función de grabar video. De este modo, ante un posible robo, podrá saber dónde se encuentra su dispositivo e incluso reconocer la cara del ladrón en una foto.

- La configuración es amigable.
- No necesita rootear su dispositivo.
- Localización GPS
- Si no hay conexión a Internet en el momento preciso, Capptura mandará el correo cuando vuelva la conexión.

- Opción para auto-habilitar la conexión a Internet. De este modo, Capptura habilitará la conexión de datos del dispositivo así como la WiFi para poder mandar el correo electrónico. Una vez enviado se desactivará la conexión.
- Opción para auto-desactivar modo avión. Si alguien intenta desbloquear el dispositivo y este se encuentra en modo avión, Capptura lo desactivará para enviar la foto por correo electrónico.
- Posibilidad de enviar correo electrónico en caso de que la tarjeta SIM sea cambiada. (Play, 2015)

Prey Anti-Robos

Ilustración 64. Prey Anti- Robos

Con esta aplicación puede recuperar su dispositivo móvil, que haya sido perdido o robado. Además es completamente gratis y así mismo tiene la opción de proteger hasta 3 dispositivos de diferentes sistemas operativos con una sola cuenta.

Funciones:

- Encuentra su dispositivo móvil en un mapa a través de geo-localización con GPS y triangulación de redes WiFi.

- Recibe reportes con fotos tomadas desde su dispositivo, capturas de pantalla y ubicación.
- Activa una alarma de forma remota, incluso si su dispositivo está en modo silencioso.
- Muestra un mensaje de alerta personalizado en la pantalla del dispositivo.
- Recopila la información de las redes a las que su dispositivo se conecte para una ubicación más exacta. (Play, 2015)

4.2.5. APLICACIONES PARA NAVEGADORES

Ilustración 65. Navegadores Web

Se recomiendan los siguientes Navegadores Web.

Firefox

Esta aplicación Web ofrece una búsqueda rápida e inteligente, además de que anticipa sus necesidades y provee de forma intuitiva varios resultados de búsqueda. Ofrece una navegación privada con protección contra rastreo, bloquea

partes de las páginas web que pueden rastrear su actividad. Firefox recuerda sus aplicaciones utilizadas recientemente.

Google Chrome

Con esta aplicación puede navegar de forma rápida en su dispositivo móvil Android. Sincroniza su dispositivo con otros dispositivos como una computadora de escritorio. Reduce el uso de datos móviles mientras navega en la web. Realiza búsquedas por voz para encontrar respuestas a sus preguntas mientras se desplaza sin tener que escribir su consulta. Contiene gestos intuitivos, utiliza el modo incógnito para navegar sin guardar su historial

UC Browser

Con esta aplicación puede navegar de una forma muy rápida. Ofrece una gestión intuitiva de pestañas. Soporta descargas múltiples, en segundo plano, descarga en la nube siempre con conexión automática. Puede controlar el vídeo por gestos: controles de brillo, volumen y progreso. Protege su privacidad con navegación en Incógnito. Puede seleccionar temas personalizables, como su imagen favorita para hacer su navegador único. Cuenta con la opción de modo noche para disfrutar de una lectura agradable en entornos de poca luz.

4.2.6. APLICACIONES PARA REDES SOCIALES

Las redes sociales juegan un papel muy importante en los dispositivos móviles, como pudimos apreciar el 45% de los usuarios encuestados descarga aplicaciones en relación a las redes sociales, ya que éstas cuentan con un número de descargas muy elevadas a nivel global como se muestra a continuación:

- Facebook de 1,000,000,000 a 5,000,000,000
- Instragram de 500,000,000 a 1,000,000,000
- Twitter de 100,000,000 a 500,000,000
- WhatsApp de 1,000,000,000 a 5,000,000,000 (Play, 2015)

Al hacer uso de estas aplicaciones conlleva a una serie de riesgos como: pérdida de la privacidad, robo de información personal, despojo bancario, suplantación de identidad, por mencionar algunas.

A continuación se da a conocer las amenazas más comunes a los que el usuario está expuesto al hacer uso de las redes sociales con mayor impacto en los dispositivos móviles.

Tabla 16. Redes Sociales

RED SOCIAL	RIESGOS o VULNERABILIDADES
Facebook 	• Clickjacking o Lifehacking: Los ciberdelincuentes aprovechan la curiosidad humana para distribuir videos, fotografías o enlaces que llamen el interés del usuario e inviten a entrar. • Suplantación de la identidad: los hackers crean una cuenta parecida a la del usuario para hacerse pasar por este y así obtienen información valiosa para extorsionar. • Asprox.N: llega a través de un mail con un archivo adjunto informando que la contraseña ha sido modificada, al descargar este contenido reenvía *Spam* a sus contactos con el mismo proceso.
Instagram 	• Esta aplicación presenta una vulnerabilidad muy enorme ya que para el ciberdelincuente es muy fácil hackear la cuenta en cuestión de minutos y así acceder al perfil para modificar los datos. • Las cookies de sesión no viajan cifradas, por lo que pueden ser capturadas.
Twitter 	• Phishing: aparece como un link que publicó un contacto, al hacer clic sobre este envía mensajes directos a sus seguidores con enlaces diseñados para propagar *Spam*. • Bug o fallas en la aplicación: en el nuevo acortador de URL que sólo permite 140 caracteres, un usuario descubrió la forma de poder escribir mensajes de más de 2.000 caracteres de extensión.
	• Falsa invitación de llamadas de voz: los ciberdelincuentes distribuyen *malware* descargada de forma automática

RED SOCIAL	RIESGOS o VULNERABILIDADES
WhatsApp 	• WhatsApp Web maliciosas: sitios web fraudulentos con el fin de robar datos bancarios, piden números de teléfonos de los usuarios y después lo suscriben a servicios Premium con tarifas especiales. • Doble clic (palomitas azules): con la demanda que se tuvo para desactivar el doble clic, los ciberdelincuentes anunciaron en redes sociales una aplicación para acabar con dicha información de lectura, con esto suscriben al usuario a un servicio de SMS Premium.

4.3. RECOMENDACIONES DE SEGURIDAD PARA EL USO DEL SISTEMA OPERATIVO *ANDROID* Y TUS APLICACIONES.

Como se puede analizar a través de las diferentes aplicaciones mencionadas en este proyecto de investigación, hay una gran cantidad de herramientas que nos brindan la posibilidad de proteger nuestros dispositivos Android, desde aquellas que vienen con el sistema operativo, hasta aquellas que se encuentran en el Play Store gratuitas y Premium. Por ello sugerimos un esquema de seguridad que involucre el uso combinado de estas aplicaciones obteniendo una mejor protección para evitar que los dispositivos móviles sean afectados por diferentes amenazas, e incluso, en caso de pérdida o robo, minimizando las consecuencias en cuanto al manejo de la información personal si el dispositivo no pudiera ser recuperado.

1. ACTIVAR LA SEGURIDAD INCLUIDA EN ANDROID

Teniendo en cuenta que Android tiene varias opciones por defecto para mejorar la seguridad del dispositivo, se mencionan a continuación aquellas que brindan al usuario mayor eficiencia y practicidad al momento de implementarlas.

Es recomendable activar el administrador de dispositivos de Android, esta opción permitirá ubicar el teléfono (incluso hacerlo sonar), bloquear o eliminar los

datos remotamente, sin embargo, si su dispositivo no tiene plan de datos o no se encuentra conectado a Internet, no se podrá hacer uso de estas funciones.

2. IMPLEMENTAR UN ANTIVIRUS

Al momento de elegir e instalar un antivirus se encuentran varias opciones, si el dispositivo se conecta a una red segura posiblemente implementar una aplicación como Anti-virus Dr. Web Light que brinda beneficios para una administración centralizada, al igual, AMC Security que es una buena alternativa puesto se destaca entre muchas otras.

3. IMPLEMENTAR APLICACIÓN ANTIRROBO

En la actualidad es muy común que los usuarios pierdan o sean víctimas por robo de su dispositivo móvil, por lo cual se recomienda implementar una aplicación que le permita al usuario ubicar o por lo menos intente encontrar a quien tenga el dispositivo para recuperarlo. Se debe tener en cuenta que para este tipo de aplicaciones se recomienda siempre apoyarse en la fuerza pública en caso de ubicarlo y no tratar de recuperarlo sólo. Como fue posible observar, entre las aplicaciones investigadas tenemos a Capptura, que está entre las más completas, porque incluso podemos obtener fotos con la cámara frontal cuando alguien intenta desbloquear el dispositivo, dicha foto se enviará junto con la localización GPS, incluso si no hay conexión a Internet en el preciso momento del robo, Capptura mandará el correo cuando obtenga una conexión. También podríamos optar por instalar Prey Anti Robos que también es una aplicación muy completa y con muchos beneficios.

4. REALIZAR COPIAS DE SEGURIDAD

Si la información utilizada en el dispositivo es importante, y su pérdida ocasionara graves consecuencias, entonces sería conveniente utilizar alguna solución de copias de seguridad.

Google dispone de un servicio de copias de respaldo de los archivos de datos o multimedia del dispositivo, al igual que copiar los ajustes del dispositivo

(contraseñas de las redes WiFi, favoritos, datos de aplicaciones, opciones de configuración) en los servidores de Google.

Hay programas que sincronizan los datos almacenados con el ordenador de escritorio como G Cloud Backup, o en alguna aplicación ofrecida por el fabricante como LG, Samsung o Sony por mencionar algunos, de forma que los datos están siempre disponibles y actualizados. En caso de pérdida de su dispositivo móvil, la información seguiría estando disponible y a salvo.

4.4. RECOMENDACIONES GENERALES PARA UN USO SEGURO DEL DISPOSITIVO MÓVIL

El uso de aplicaciones para implementar seguridad está habilitando las opciones que trae por defecto el sistema operativo Android o instalando aplicaciones de terceros, con ello se disminuye en gran medida la posibilidad de éxito de una amenaza, sin embargo, ninguna aplicación es meramente confiable y mucho menos si el usuario no realiza buenas prácticas de seguridad al momento de utilizar su dispositivo móvil, en concreto, para completar el esquema de seguridad, se deben seguir recomendaciones que a continuación se mencionan:

1. DESCARGAR APLICACIONES EXCLUSIVAMENTE DE GOOGLE PLAY STORE

Como es sabido, existen tiendas de aplicaciones semejantes a Play Store, de las cuales los usuarios pueden descargar aplicaciones. Algunas de ellas se consideran ilegales por ofrecer aplicaciones prohibidas por Google, por ejemplo ofrecer gratis aplicaciones que tienen costo, publicar aplicaciones propietarias de cualquier usuario sin ser validadas previamente por el equipo de Google, aplicaciones que violan los derechos de autor, aplicaciones que permiten tomar el

control administrativo y modificar el sistema operativo de Android (Rootear), por mencionar algunas de tantas que existen.

2. NO CONECTARSE A REDES WIFI PÚBLICAS Y ABIERTAS.

Esta recomendación va más enfocada a la seguridad de los datos personales y no únicamente a la del dispositivo. Las redes inalámbricas WiFi públicas son más vulnerables a los ataques del tipo man in the middle (hombre en el medio). Esto quiere decir que cuando el dispositivo móvil envía peticiones al proveedor de servicios de Internet es posible que una tercera persona las intercepte, consiguiendo acceder a los datos personales como por ejemplo contraseñas y saltarse las medidas de privacidad que tenga la versión de Android. Si se encuentra fuera de casa, se recomienda usar siempre los datos móviles de su compañía.

3. DESACTIVAR COMUNICACIONES INALÁMBRICAS.

Es de gran importancia tener en cuenta que si no se van a utilizar las redes inalámbricas en un tiempo determinado, se desactiven. Las redes más usuales suelen ser WiFi, Bluetooth, y los datos móviles.

Es común que los ciberdelincuentes realicen ataques contra redes inalámbricas, utilizando puntos de acceso falsos, y engañando al dispositivo para que se conecte automáticamente a una red de supuesta confianza. El usuario navegaría entonces sin tener la seguridad de que el tráfico está siendo monitorizado por el atacante.

4. NO ALMACENAR INFORMACIÓN VALIOSA.

La información más sensible del usuario no debe ser almacenada en los dispositivos móviles aunque estén cifrados, puesto que estos dispositivos siempre

están expuestos a riesgos mayores. Ya que los criminales podrían utilizar dicha información para realizar estafas.

5. TENER INSTALADAS SÓLO APLICACIONES NECESARIAS, NO CAER EN EL EXCESO.

Caer en el exceso de instalar aplicaciones innecesarias en el dispositivo móvil, no solo hace que el aparato sea lento en su funcionamiento, sino que aumenta el riesgo de que una de estas aplicaciones tenga una vulnerabilidad que pueda ser aprovechada por un atacante y así conseguir el control del mismo.

Por ello se recomienda desinstalar toda aplicación que no sea precisamente necesaria para el desempeño del dispositivo, y así minimizar el riesgo de exponer al dispositivo móvil a una aplicación vulnerable.

Es conveniente leer los términos y condiciones que se deben aceptar antes de instalar una aplicación y de la misma forma comprobar la reputación de la misma. Los sistemas operativos de los dispositivos incluyen un sistema de actualización de aplicaciones, mediante una notificación, informan que existe una nueva versión de una aplicación instalada. Estas actualizaciones, además de añadir funcionalidades, corrigen fallos en la seguridad de su dispositivo. Cuando el sistema muestre una actualización disponible de alguna aplicación, se debe aceptar y aplicar la nueva versión. Manteniendo el sistema actualizado se evitan posibles infecciones por aplicaciones vulnerables.

CONCLUSIONES

Al inicio de esta investigación se plantearon objetivos claros, como el de brindar recomendaciones de seguridad a los usuarios de los dispositivos móviles *Android* que no tienen la más remota idea de los riesgos a los que están expuestos al hacer uso de una red ya sea WiFi o de datos móviles de su compañía, además de los errores más comunes que cometen al descargar aplicaciones móviles.

Es importante conocer las medidas necesarias de seguridad de nuestro dispositivo móvil, ya que de ello depende que no hagamos vulnerable nuestro sistema operativo, por ello se recomienda seguir las recomendaciones que planteamos en este proyecto de investigación.

En la actualidad es importante señalar que los dispositivos móviles han tomado un papel de mucha trascendencia en la vida diaria de las personas, así mismo es preciso saber que los creadores de *Malware* han hecho todo posible por atacar este sector, ya que es un mercado de gran valor. De ello emerge la necesidad de tener seguridad móvil en los dispositivos que tienen como propósito el mantener la integridad de la información que pueda ser manejada de forma tangible.

Por ello es imprescindible conseguir que los usuarios estén enterados y creen conciencia sobre los peligros que existen en nuestros tiempos al utilizar éstos dispositivos móviles. Puesto que al dar un paso en falso en cuestión a la seguridad exponen su información confidencial al acecho de éstos criminales y pudiesen resultar muy graves las pérdidas.

Así mismo como se mencionó en el trayecto de esta investigación es de conocedores llevar a cabo las buenas prácticas de seguridad que sean necesarias para que los dispositivos móviles de los usuarios estén siempre al margen de estas recomendaciones hasta donde sea posible.

Como pudimos notar a través de la encuesta realizada a usuarios que desconocen sobre la seguridad de sus equipos móviles pudimos observar que la mayoría de éstos no implementan medidas de seguridad, mucho menos tienen el conocimiento de instalar un buen antivirus cómo los que recomendamos anteriormente, además pudimos darnos cuenta con un margen de 30 encuestados que la mayoría de usuarios desconocen por completo las vulnerabilidades que tiene este sistema operativo móvil.

GLOSARIO

.apk: Es una extensión de Android Aplication Package, es decir, se trata de un archivo de instalación pensado para el sistema operativo Android para dispositivos móviles. Un archivo .apk contiene tanto la aplicación en sí misma como el instalador que permite que se pueda guardar y ejecutar en el dispositivo.

***Adware*:** Es un software, generalmente no deseado, que facilita el envío de contenido publicitario a un equipo.

Amenaza: Una amenaza informática es toda circunstancia, evento o persona que tiene el potencial de causar daño a un sistema en forma de robo, destrucción, divulgación, modificación de datos o negación de servicio (DoS).

Anti*Spam*: Es un producto, herramienta, servicio o mejor práctica que detiene el *Spam* o correo no deseado antes de que se convierta en una molestia para los usuarios. El anti*Spam* debe ser parte de una estrategia de seguridad multinivel.

Antivirus: Es una categoría de software de seguridad que protege un equipo de virus, normalmente a través de la detección en tiempo real y también mediante análisis del sistema, que pone en cuarentena y elimina los virus. El antivirus debe ser parte de una estrategia de seguridad estándar de múltiples niveles.

Aplicaciones engañosas: Son programas que intentan engañar a los usuarios informáticos para que emprendan nuevas acciones que normalmente están encaminadas a causar la descarga de *malware* adicional o para que los usuarios divulguen información personal confidencial.

Ataques Web: Es un ataque que se comete contra una aplicación cliente y se origina desde un lugar en la Web, ya sea desde sitios legítimos atacados o sitios maliciosos que han sido creados para atacar intencionalmente a los usuarios de ésta.

Backdoor: Se trata de un programa que se introduce en el dispositivo móvil y establece una puerta trasera a través de la cual es posible controlar el sistema afectado, sin conocimiento por parte del usuario. Los más conocidos

mundialmente son el BackOrifice y el NetBus, dos de los primeros backdoors, que hasta nuestros días siguen vigentes aunque en menor cantidad dado que la mayoría de los programas antivirus los detectan.

Botnets: Es un tipo de programa malicioso que permite a un atacante tomar el control de un equipo infectado. Por lo general, los botnets, también conocidos como "robots web" son parte de una red de máquinas infectadas, conocidas como, que comúnmente está compuesta por máquinas víctimas de todo el mundo.

Ciberdelito: Es un delito que se comete usando una computadora, red o *Hardware*. La computadora o dispositivo puede ser el agente, el facilitador o el objeto del delito. El delito puede ocurrir en la computadora o en otros lugares.

Clicker: La herramienta, que permite el recuento remoto de datos de forma automática e inmediata, se empieza a integrar en las escuelas españolas.

Cracker: Es considerado un "vandálico virtual". Este utiliza sus conocimientos para invadir sistemas, descifrar claves y contraseñas de programas y algoritmos de encriptación, ya sea para poder correr juegos sin un CD-ROM, o generar una clave de registro falsa para un determinado programa, robar datos personales, o cometer otros ilícitos informáticos.

Dalvik: Es la máquina virtual de proceso dentro de Android, es el software que ejecuta las aplicaciones en los dispositivos con Android. Una máquina virtual de este tipo, se ejecuta como un proceso normal dentro de un sistema operativo y soporta un solo proceso. Su objetivo es el de proporcionar un entorno de ejecución independiente de la plataforma de hardware y del sistema operativo, que oculte los detalles de la plataforma subyacente y permita que un programa se ejecute siempre de la misma forma sobre cualquier plataforma.

Dorkbot: Es un gusano diseñado principalmente para el robo de información, una vez que se infectó un equipo con este código malicioso todas las tareas que realice el usuario son interceptadas por este malware y enviadas al atacante. Por defecto roba credenciales de Facebook, Twitter, Google+, Hotmail y otros servicios en línea para compras por Internet incluyendo el robo de credenciales bancarias.

Droppers: Son software que utilizan varios métodos para difundir e instalar virus troyanos en las computadoras. Los trojan droppers, que son ellos mismos ya sea troyanos u otra clase de virus, pueden dañar la computadora y dañar al usuario a través de los datos y el robo de identidad.

Encriptación: La encriptación es un método de cifrado o codificación de datos para evitar que los usuarios no autorizados lean o manipulen los datos. Sólo los individuos con acceso a una contraseña o clave pueden descifrar y utilizar los datos. A veces, el *malware* utiliza la encriptación para ocultarse del software de seguridad.

***Exploits* o Programas intrusos:** Los programas intrusos son técnicas que aprovechan las vulnerabilidades del software y que pueden utilizarse para evadir la seguridad o atacar un equipo en la red.

Fakeapps: Las aplicaciones falsas "puras", que simulan ser algún otro juego popular, suelen pesar poco (entre 200 y 500 kbs) y estar destinadas directamente a la publicidad invasiva. Pueden realizar varias funciones en el dispositivo de su "víctima", entre otras. La intensión de éstas falsas aplicaciones, es bombardear al usuario con ventanas emergentes, banners y todo tipo de publicidad, hasta el punto de que (si los programas se inician con el teléfono) sea complicado utilizar el dispositivo.

Filecoder/Cryptolocker: Se trata de un malware que cifra los archivos en un dispositivo móvil y en cualquier recurso de la red compartido que se encuentre accesible desde esa máquina. Este ransomware cifra los archivos basándose en su extensión (.pdf, .doc, .jpg y muchas otras) la clave clara para descifrar los archivos afectados se almacena en el servidor del atacante y no puede ser obtenida en el ordenador de la víctima.

Flashear: Cargar datos en un chip de memoria de estado sólido, en especial los que contienen el sistema operativo para dispositivos y periféricos electrónicos.

Gusanos: Los gusanos son programas maliciosos que se reproducen de un sistema a otro sin usar un archivo anfitrión, lo que contrasta con los virus, puesto que requieren la propagación de un archivo anfitrión infectado.

Hacker: Es aquella persona experta en alguna rama de la tecnología, a menudo informática, que se dedica a intervenir y/o realizar alteraciones técnicas con buenas o malas intenciones sobre un producto o dispositivo.

Hoaxes: Los hoaxes son un tipo de malware bastante simple pero no por ello menos efectivo. Se trata de e-mails que contienen información engañosa sobre los temas más diversos. Así, pueden avisar sobre virus inexistentes excepcionalmente dañinos, o acerca de “leyendas urbanas” de todo tipo.

Home banking: o Banca en Línea es el servicio por el cual se pueden ejecutar transacciones bancarias por medios electrónicos específicamente vía redes privadas o públicas como la Internet. Su nombre viene de la posibilidad de hacer transacciones desde la casa (Home) y no tener que asistir personalmente a un banco (Bank).

Jailbreak: Es el término genérico que se le ha puesto a los métodos que hay para saltarse las medidas de seguridad impuestas por Apple en su sistema iOS y poder instalar, modificar y cambiar cualquier cosa del sistema. Diferentes desarrolladores y equipos han dedicado un número incontable de horas a analizar minuciosamente el código del software de Apple para ver por donde podían colarse.

Java: Es un lenguaje de programación de propósito general, concurrente, orientado a objetos que fue diseñado específicamente para tener tan pocas dependencias de implementación como fuera posible. Su intención es permitir que los desarrolladores de aplicaciones escriban el programa una vez y lo ejecuten en cualquier dispositivo.

Kemoge: Es una mezcla de malware con troyano. Es tan invasivo que no lo elimina ni un reseteo del equipo. Así lo dio a conocer la empresa Lookout dedicada a la tecnología y a analizar aplicaciones del sistema operativo Android. El malware se disfraza de una aplicación conocida (Facebook, Twitter, Whatsapp),

se instala y luego se apodera del sistema operativo, obteniendo acceso de súper usuario (root). Una vez que logró ese objetivo, el malware puede instalar aplicaciones a gusto, llenar el dispositivo con publicidad, o dejar una "puerta abierta" para otros programas maliciosos.

LastPass: Es un programa original que sirve para gestionar las decenas y decenas de contraseñas que acumulamos a través de los años y constantemente debemos modificar por pedido de los sitios, algo que nuestra mente no puede soportar.

***Malware*:** El *malware* es la descripción general de un programa informático que tiene efectos no deseados o maliciosos. Incluye virus, gusanos, troyanos y puertas traseras. El *malware* a menudo utiliza herramientas de comunicación populares, como el correo electrónico y la mensajería instantánea, y medios magnéticos extraíbles, como dispositivos USB, para difundirse.

Middleware: Es un software de computadora que conecta componentes de software o aplicaciones para que puedan intercambiar datos entre éstas. Es utilizado a menudo para soportar aplicaciones distribuidas.

Phishing: Se refiere a uno de los métodos más utilizados por delincuentes cibernéticos para estafar y obtener información confidencial de forma fraudulenta como puede ser una contraseña o información detallada sobre tarjetas de crédito u otra información bancaria de la víctima.

Ransomware: Es un software malicioso que una vez se ejecuta en el dispositivo móvil impide el funcionamiento normal del mismo, ya que entre otras, puede bloquear el acceso a algunos de los archivos (archivos de imagen, archivos de música, por mencionar algunos).

***Root* / Superusuario:** Usuario sobre el que no se aplica ningún tipo de restricción de acceso, y que dispone de todos los privilegios de acceso, pudiendo crear o eliminar usuarios, acceder a archivos ocultos o de sistema y/o iniciar y acabar servicios.

Rootear: De la palabra root que en sistemas basados en Unix y Linux se trata del usuario raíz con derechos absolutos para modificar o cambiar atributos de cualquier archivo o carpeta, esto nos da acceso completo a las opciones de Hardware como son el Audio, el GPS, Video, WiFi, etc, además de permitirnos ejecutar cualquier programa.

***Rootkits*:** Componente de *malware* que utiliza la clandestinidad para mantener una presencia persistente e indetectable en un equipo. Las acciones realizadas por un rootkit, como la instalación y diversas formas de ejecución de códigos, se realizan sin el conocimiento o consentimiento del usuario final.

Simplocker: Es un troyano que infectando a dispositivos móviles con sistema Android, cifrando los archivos y exigiendo una recompensa como rescate de los mismos. El troyano fue descubierto por los investigadores de seguridad de ESET. Parece ser que se trata de una prueba de concepto toda vez que los ataques son limitados por el momento y dirigidos a una región geográfica específica (Ucrania). Es el primer ransomware para Android.

Shedun: Una variante que es capaz de ganar permiso para entrar al Sistema de Accesibilidad de Android y permitir la instalación automática de cualquier aplicación cuyo propósito es el de bombardear agresivamente al usuario con publicidad

Shuanet: Es un nuevo adware que intenta rootear el dispositivo móvil para que nunca se pueda eliminarlo. Shuanet no sólo muestra anuncios, sino que además intenta rootear cualquier dispositivo en el que se instale, lo que permite que el malware sobreviva incluso a un reseteo de fábrica o hard reset. Shuanet comparte mucho código con otros troyanos adware que Lookout ha detectado recientemente como Kemoge y Shedun. Lo interesante de Shuanet es que no busca causar estragos en los dispositivos infectados, este es un adware, ante todo, por lo que el objetivo es conseguir que la gente use sus dispositivos y que vean los anuncios.

***Smartphone*:** Es un tipo teléfono móvil inteligente construido sobre una plataforma informática móvil, con una mayor capacidad de almacenar datos y realizar

actividades semejantes a una minicomputadora, y con una mayor conectividad que un teléfono móvil convencional.

***Spam*:** También conocido como correo basura, el *Spam* es correo electrónico que involucra mensajes casi idénticos enviados a numerosos destinatarios. Un sinónimo común de *Spam* es correo electrónico comercial no solicitado (UCE).

Spammer: Se refiere al grupo de personas o individuos que provocan el correo basura (Spam)

Spoofing: Es el conjunto de técnicas que se utilizan para suplantar la identidad de un usuario o servidor, generalmente con intenciones maliciosas.

***Spyware*:** Paquete de software que realiza un seguimiento y envía información de identificación personal o información confidencial a otras personas. La información de identificación personal es la información que puede atribuirse a una persona específica, como un nombre completo.

Stagefright: Es el apodo que ha recibido un fallo de seguridad descubierto en el sistema operativo Android, a través del cual se puede hackear un dispositivo que utilice Android enviando contenido multimedia en forma de MMS o a través de un archivo con formato MP3 o MP4. Al hacer esto, el mecanismo libStageFright, que vive dentro del sistema operativo y sirve para procesar contenido multimedia, funciona como un puente de acceso entre el atacante y el dispositivo.

Troyanos: Son un tipo de código malicioso que parece ser algo que no es. Una distinción muy importante entre troyanos y virus reales es que los troyanos no infectan otros archivos y no se propagan automáticamente. Los caballos de Troya tienen códigos maliciosos que cuando se activan causa pérdida, incluso robo de datos.

Virus: Programa informático escrito para alterar la forma como funciona una computadora, sin permiso o conocimiento del usuario. Un virus debe cumplir con dos criterios: debe ejecutarse por sí mismo y debe reproducirse. Los virus pueden infectar computadores de escritorio y servidores de red.

BIBLIOGRAFÍA

Campos, T. (12 de Abril de 2014). Conoce los datos de las 104 millones de líneas móviles en México. (T. Campos, Ed.) México, México, México. Obtenido de http://www.xataka.com.mx/celulares-y-smartphones/conoce-los-datos-de-las-104-millones-de-lineas-moviles-en-mexico

Clodo Aldo Robledo Sacristán, D. R. (2012). *Programación en Android.* España: Aula Mentor.

ESTUDIOS ECONÓMICOS S.A., Miguel Yuste. (14 de Enero de 2015). *Los móviles más usados según la zona del planeta.* Obtenido de http://cincodias.com/cincodias/2015/01/14/mwc/1421257629_093393.html

EXPANSIÓN, S.A. DE C.V. (27 de Octubre de 2014). *Android domina el mercado de los Smartphones.* Obtenido de 7 de cada 10 Smartphones en México son Android: http://www.cnnexpansion.com/tecnologia/2014/10/27/siete-de-cada-10-mexicanos-usan-android

III, U. C. ((s.f.)). *Software de Comunicaciones.* Madrid: ( ).

Play, G. (11 de Noviembre de 2015). Google Play. México, México, México. Obtenido de https://play.google.com/store

Rivero, F. (2015). *Informe Mobile en España y en el Mundo 2015.* España: CEO ditrendia.

wikipedia. (22 de septiembre de 2015). Obtenido de https://es.wikipedia.org/wiki/Windows_Phone